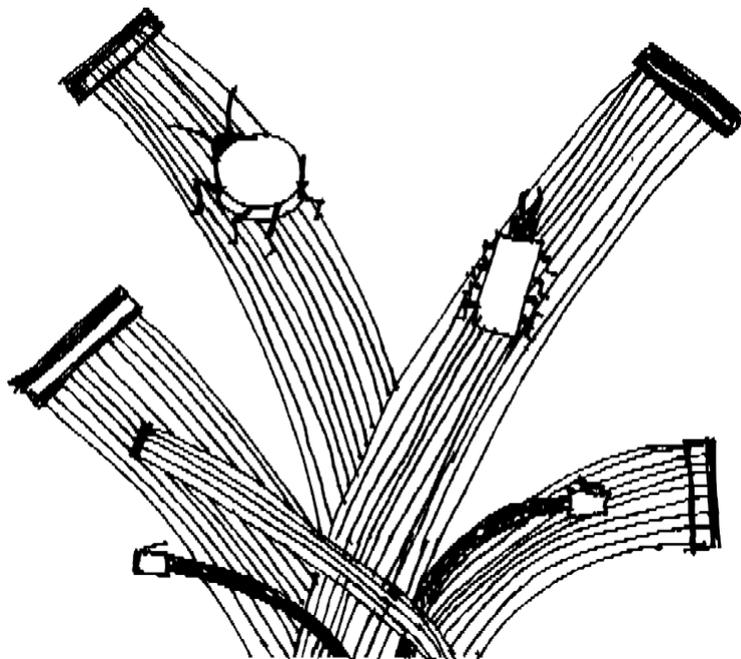


Guida all'autodifesa digitale

lavoro collettivo



sesta edizione

inverno 2023

guida all'autodifesa digitale

Lavoro collettivo
guide@boum.org

Impronta digitale
OpenPGP: D487 4FA4 F6B6
88DC 0913 C9FD 326F 9F67
250B 0939

inverno 2023

Realizzato con software libero, in particolare *bookdown*, *Pandoc* e *LaTeX* per l'impaginazione, *GIMP* e *Inkscape* per le immagini, *Scribus* per le copertine, *Git* e numerose discussioni per lavorare insieme, il tutto sotto *Debian GNU/Linux* e *Tails*.



Copyleft: quest'opera è libera, è possibile copiarla, distribuirla e modificarla in base ai termini della *Free Art License* - <http://www.artlibre.org/>

ISBN : 978-2-912631-05-3

Contenuti

Contenuti	iii
Prefazione alla presente edizione Perché questa guida?	xi
Il lato negativo della memoria digitale	1
Niente da nascondere?	1
Comprendere per poter scegliere	2
Prendetevi il tempo per capire	3
Come leggere questa guida	5
Un tomo "offline"	5
Un tomo "online"	5
Gettarsi via	5
Volume 1 - Off-line	9
<hr/>	
I Comprensione	11
<hr/>	
Introduzione	13
1 Nozioni di base sul computer	15
1.1 Macchine per l'elaborazione dei dati	15
1.2 Hardware	15
1.3 Elettricità, campi magnetici, rumore e onde radio	21
1.4 Software	22
1.5 Memorizzazione dei dati	23
2 Tracce su ogni piano	27
2.1 In RAM	27
2.2 In memoria virtuale	28
2.3 Sonno e ibernazione	28
2.4 Giornali	29
2.5 Backup automatici e altri elenchi	29
2.6 Metadati	30

3	Malware, bug e spyware	31
3.1	Contesto giuridico	31
3.2	Malware	32
3.3	Attrezzatura per spie	34
3.4	Keylogger o registratori di sequenze di tasti	35
3.5	Piattaforme di indagine digitale.....	36
3.6	Problemi di stampa?	36
4	Alcune illusioni sulla sicurezza	39
4.1	Software proprietario, open source e libero.....	39
4.2	La password di un account non protegge i suoi dati	41
4.3	Informazioni sulla "cancellazione" dei file.....	42
4.4	Software portatile: una falsa soluzione.....	44
5	Un modo per proteggere i dati: la crittografia	47
5.1	Proteggere i dati da occhi indiscreti.....	47
5.2	Garantire l'integrità dei dati	53
5.3	Simmetrico, asimmetrico?	55
II	Scegliere le risposte appropriate	57
<hr/>		
	Introduzione	59
6	Fiducia e riduzione del rischio	61
6.1	Riduzione del rischio	61
6.2	Una storia di fiducia.....	62
7	Valutazione del rischio	63
7.1	Cosa vogliamo proteggere?	63
7.2	Da chi ci stiamo proteggendo?.....	63
8	Definizione di un criterio di sicurezza	65
8.1	Una questione di compromesso	65
8.2	Cosa fare?.....	65
8.3	Alcune regole.....	66
	Casi d'uso	69
9	Caso d'uso: un nuovo inizio, per smettere di pagare il pifferaio	71
9.1	Sfondo.....	71
9.2	Valutazione dei rischi	72
9.3	Definizione di un criterio di sicurezza	72
10	Caso d'uso: lavorare su un documento sensibile	79
10.1	Contesto.....	79
10.2	Valutazione dei rischi	79
10.3	Qual è il sistema operativo migliore per lavorare sul documento?	80
10.4	Lavorare su un documento sensibile... su un sistema <i>attivo</i>	82
10.5	Lavorare su un documento sensibile... in Windows	82
10.6	Pulire i metadati del documento finito	88
10.7	Limiti comuni a queste politiche di sicurezza	88

11 Caso d'uso: archiviazione di un progetto completato	89
11.1 Contesto	89
11.2 È davvero necessario?	89
11.3 Valutazione dei rischi	89
11.4 Metodo	90
11.5 Quale passphrase?	90
11.6 Un disco rigido? Una chiave? Diverse chiavi?	91
III Strumenti	93
<hr/>	
Introduzione	95
12 Utilizzo di un terminale	97
12.1 Che cos'è un terminale?	97
12.2 Informazioni sui controlli	98
12.3 Privilegi amministrativi	99
12.4 Avvertimento	100
12.5 Un esercizio	100
12.6 Attenzione alle tracce!	101
12.7 Ulteriori informazioni	101
13 Scegliere una passphrase	103
14 Avvio da CD, DVD o chiavetta USB	107
14.1 Prova ingenuamente	107
14.2 Tentativo di selezione di un dispositivo di avvio una tantum	107
14.3 Modifica dei parametri del firmware	108
15 Utilizzo di un sistema <i>live</i>	113
15.1 Sistemi <i>vivi</i> discreti	113
15.2 Scaricare, controllare e installare Tails	114
15.3 Clonazione o aggiornamento di una chiave Tails	115
15.4 Avvio su un sistema <i>live</i>	115
15.5 Usare la persistenza di Tails	116
16 Installazione di un sistema crittografato	119
16.1 Limiti	119
16.2 Scarica il supporto per l'installazione	120
16.3 Controllare l'ingombro dell'immagine di installazione	121
16.4 Preparazione del supporto di installazione	122
16.5 L'installazione stessa	123
16.6 Impostazione del repository principale dei pacchetti Debian	128
16.7 Alcuni consigli per continuare	129
16.8 Documentazione su Debian e GNU/Linux	129
17 Scelta, verifica e installazione del software	131
17.1 Criteri di selezione	131
17.2 Trovare e installare il software	134
17.3 Trovare e installare un pacchetto Debian	135
17.4 Aggiunta di depositi	136

18 Eliminare i dati "per davvero	I	139
18.1 Un po' di teoria		139
18.2 Su altri sistemi		140
18.3 Andiamo		140
18.4 Eliminazione di file... e del loro contenuto		141
18.5 Eliminare un intero disco "per davvero"		141
18.6 Eliminazione dell'intero contenuto di un disco		142
18.7 Rendere irrecuperabili i dati precedentemente cancellati		143
19 Partizionare e criptare un disco rigido		145
19.1 Panoramica		145
19.2 Preparazione di un disco per la crittografia		146
19.3 Creare una partizione non criptata		147
19.4 Creazione di una partizione crittografata		148
19.5 Utilizzo di un disco rigido crittografato		148
20 Salvataggio dei dati		151
20.1 Caso speciale di memorizzazione persistente di Tails		151
20.2 Con file manager e archiviazione crittografata		151
20.3 Utilizzo di Déjà Dup		153
21 Condividere un segreto		157
21.1 Condividere una passphrase		157
21.2 Ricostruzione della passphrase		158
22 Utilizzo delle checksum		161
22.1 Ottenere il checksum di un file		161
22.2 Controllare l'integrità del file		162
23 Installazione e utilizzo di un sistema virtualizzato		163
23.1 Installazione di Virtual Machine Manager		163
23.2 Abilitazione della virtualizzazione hardware		164
23.3 Installazione di un Windows virtualizzato		165
23.4 Acquisizione di un'istantanea di una macchina virtuale		168
23.5 Ripristino dello stato di una macchina virtuale da un'istantanea		168
23.6 Installazione di nuovo software su un sistema virtualizzato		169
23.7 Condivisione di una chiavetta USB con un sistema virtualizzato		170
23.8 Condivisione di un CD o DVD con un sistema virtualizzato		171
23.9 Condividere una cartella con un sistema virtualizzato		171
24 Mantenere il sistema aggiornato		175
24.1 Mantenere le code aggiornate		175
24.2 Mantenere aggiornato un sistema crittografato		176
24.3 Aggiornamenti giornalieri per un sistema criptato		176
24.4 Aggiornamento a una nuova versione stabile		177
25 Pulire i metadati dei documenti		185
25.1 Installazione del software necessario		185
25.2 Pulizia di uno o più file		185

Volume 2 - Online **189****IV Comprensione** **191**

Introduzione	193
26 Nozioni di base della rete	197
26.1 Computer interconnessi	197
26.2 Protocolli di comunicazione.....	199
26.3 Reti locali.....	203
26.4 Internet: reti interconnesse	205
26.5 Clienti e server	209
27 Tracce lungo tutta la linea	213
27.1 Sul computer client.....	213
27.2 Sulla scatola: indirizzo hardware della scheda di rete.....	215
27.3 Sui router: intestazioni dei pacchetti	217
27.4 Sul server.....	217
27.5 Le tracce che lasciamo dietro di noi.....	219
28 Monitoraggio e controllo delle comunicazioni	221
28.1 Chi rivuole i dati?.....	221
28.2 Registri e conservazione dei dati	224
28.3 Ascolto di massa	229
28.4 Attacchi mirati	231
28.5 In conclusione	238
29 Web 2.0	239
29.1 Applicazioni Internet ricche".....	239
29.2 ... e navigatori volontari	240
29.3 Centralizzazione dei dati	240
29.4 Controllo del programma	241
29.5 Dalla centralizzazione al self-hosting decentralizzato.....	242
30 Identità contestuali	243
30.1 Definizioni	243
30.2 Dall'identità contestuale all'identità civile	244
30.3 Compartimentazione	246
30.4 Social media: funzioni centralizzate e un'identità unica	247
31 Nascondere il contenuto delle comunicazioni: la crittografia asimmetrica	249
31.1 Limiti della crittografia simmetrica	249
31.2 Una soluzione: la crittografia asimmetrica.....	249
31.3 Crittografia end-to-end	251
31.4 Firma digitale.....	252
31.5 Verifica dell'autenticità della chiave pubblica	253
31.6 Riservatezza persistente.....	258
31.7 Sintesi e limiti.....	258
32 Routing Tor o onion	261
32.1 Il problema: nascondere origine e destinazione	261
32.2 Una soluzione: Tor	261
32.3 servizi di cipolla.....	266
32.4 Entrare nella rete Tor	266
32.5 Alcuni limiti di Tor.....	267

V	Scegliere le risposte giuste	273
<hr/>		
	Introduzione	275
	33 Caso d'uso: siti web di consulenza	277
	33.1 Sfondo	277
	33.2 Valutazione dei rischi	277
	33.3 Definizione di un criterio di sicurezza	278
	33.4 Scegliere tra gli strumenti disponibili	279
	33.5 Navigare sui siti web con Tor Browser	281
	33.6 Navigazione nei siti web con Tails	282
	34 Caso d'uso: pubblicazione di un documento	285
	34.1 Sfondo	285
	34.2 Valutazione dei rischi	285
	34.3 Definizione di un criterio di sicurezza	285
	35 Caso d'uso: scambio di messaggi	289
	35.1 Sfondo	289
	35.2 Valutazione dei rischi	289
	35.3 Due questioni.....	290
	35.4 Webmail o client di posta?.....	290
	35.5 Webmail.....	291
	35.6 Posta del cliente.....	292
	35.7 Scambiare e-mail nascondendo la propria identità	293
	35.8 Scambio di e-mail riservate	295
	36 Caso d'uso: dialogo	299
	36.1 Sfondo	299
	36.2 Valutazione dei rischi	299
	36.3 Definizione di un criterio di sicurezza	299
	36.4 I limiti	301
	37 Caso d'uso: condivisione di documenti sensibili	303
	37.1 Sfondo	303
	37.2 Valutazione dei rischi	303
	37.3 Proteggere la fonte.....	304
	37.4 Protezione dei destinatari.....	305
	37.5 Protezione dei file riservati	305
VI	Strumenti	309
<hr/>		
	Introduzione	311
	38 Installazione e configurazione del browser Tor	313
	38.1 Installare il browser Tor	314
	38.2 Aggiornamento del browser Tor	314
	39 Navigare sul web con Tor	315
	39.1 Andare alla cartella di download di Tor Browser	315
	39.2 Limiti di geolocalizzazione	316
	40 Scelta del web hosting	319
	40.1 Alcuni criteri di selezione.....	319
	40.2 Tipo di contenuto.....	320
	40.3 In pratica.....	322

41 Verifica di un certificato elettronico	323	
41.1 Verificare un certificato o un'autorità di certificazione.....	323	
41.2 Trovare l'impronta digitale di un certificato già installato	326	
42 Utilizzare una tastiera visiva in Tails	327	
43 Configurazione e utilizzo del client di posta Thunderbird	329	
43.1 Avviare Thunderbird	329	
43.2 Configurazione del routing a cipolla per Thunderbird.....	329	
43.3 Impostare una password principale in Thunderbird.....	330	
43.4 Impostazione di un account di posta elettronica	330	
43.5 Configurazione avanzata di Thunderbird	331	
44 Utilizzare la crittografia OpenPGP in Thunderbird	333	
44.1 Creare una coppia di chiavi	333	
44.2 Esportare e condividere la nostra chiave pubblica	336	
44.3 Importazione, verifica ed esportazione di chiavi pubbliche.....	337	
44.4 Gestione della coppia di chiavi: estendere, modificare, revocare la coppia di chiavi	340	
44.5 Crittografare e/o firmare le e-mail in Thunderbird.....	342	
45 Utilizzo della crittografia OpenPGP in ufficio	343	
45.1 Importare una chiave nel portachiavi di Office.....	343	
45.2 Firmare una chiave	344	
45.3 Verifica di una firma digitale	345	
45.4 Dati di firma	346	
45.5 Crittografia dei dati.....	347	
45.6 Decrittazione dei file	348	
46 Utilizzo della messaggistica istantanea con OTR	351	
46.1 Installare il client di messaggistica istantanea Pidgin.....	351	
46.2 Avviare Pidgin.....	351	
46.3 Impostazione di un account di posta elettronica	352	
46.4 Creare un account di messaggistica istantanea XMPP.....	352	
46.5 Crittografia della connessione al server.....	352	
46.6 Attivazione del plugin OTR (<i>Off-the-Record</i>).....	352	
46.7 Impostazione di una conversazione privata	353	
47 Gestione delle password	355	
47.1 Scegliere una buona passphrase	355	
47.2 Utilizzo di un gestore di password	355	
48 Utilizzo di OnionShare	359	
48.1 Usare OnionShare in Tails.....	359	
48.2 Usare OnionShare in Debian.....	359	
Chi parla?	361	
Indice	363	
Crediti	367	

Prefazione alla presente edizione

Dalla pubblicazione della seconda edizione cartacea *della guida* nel 2017, sono emerse nuove informazioni sulle tecnologie di spionaggio digitale, sugli strumenti che raccomandiamo o sulle leggi che subiamo.

*
* *

Iniziamo con un viaggio nel lato oscuro delle novità digitali.

"I dati determinano tutto ciò che facciamo" ¹ Il cinico slogan di Cambridge Analytica. Questa società è stata al centro di uno scandalo che ha messo in luce il potere dei grandi gruppi di Internet sulla società: ha sottratto i dati personali di decine di milioni di account Facebook con il consenso della piattaforma per un cosiddetto "studio scientifico". Ha poi venduto i suoi servizi di manipolazione psicologica mirata, che sono stati utilizzati per influenzare la campagna presidenziale del 2015 in Nigeria ² le elezioni presidenziali statunitensi del 2016 e il voto della Brexit. ³ Lo scandalo è stato svelato dai media nel 2018 grazie alle rivelazioni di un ex dipendente.

Con il COVID-19 sono stati raggiunti nuovi traguardi nell'abuso della tecnologia digitale. "Nell'era del COVID-19, la connettività non è una merce, ma una necessità. Praticamente tutte le attività umane - commercio, istruzione, salute, politica, socializzazione - sembrano essersi spostate online. [...] Gli Stati e gli attori non statali in ogni Paese stanno ora sfruttando le opportunità create dalla pandemia per plasmare nuove narrazioni online, censurare il discorso critico e costruire nuovi sistemi tecnologici di controllo sociale." ⁴ Queste sono le conclusioni dell'organizzazione per la libertà digitale Freedom House.

La tessera sanitaria francese, ad esempio, è un codice a barre bidimensionale firmato digitalmente che contiene il nome e lo stato di salute della persona, oltre a informazioni sulle vaccinazioni ricevute e sulle date delle ultime iniezioni. Queste informazioni non solo sono leggibili in chiaro, ma permettono anche di "dedurre informazioni sanitarie ancora più private su alcuni cittadini". ⁵ Al di là di queste critiche a

1. "Data drives all we do" in inglese, citato da Le Monde (*Le Monde*, 2018, *Ce qu'il faut savoir sur Cambridge Analytica, la société au-c-ur-du-scandale Facebook* [https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html]).

2. Wikipedia, 2022, *Christopher Wylie* [https://fr.wikipedia.org/wiki/Christopher_Wylie].

3. Wikipedia, 2021, *Facebook-Cambridge Analytica scandalo* [https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica].

4. Adrian Shahbaz e Allie Funk, 2020, *The Pandemic's Digital Shadow*, in Freedom House, 2020, *Freedom of the Net 2020* [https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf].

5. Florian Maury, Piotr Chmielnicki, 2021, *Health Pass e privacy: quali rischi?* [<https://www.broken-by-design.fr/posts/pass-sanitaire/>].

il modo in cui funziona il passaggio sanitario, la sua adozione di massa abitua la popolazione a sottoporsi a un controllo capillare attraverso strumenti digitali ⁶.

Célia Izoard denuncia "sotto la maschera di Covid, la completa digitalizzazione della società". ⁷ che "continua, brutalizzando quotidianamente le persone obsolete e refrattarie". ⁸. Per lei, la domanda a cui troppo spesso rispondono le politiche sanitarie è "come può la Francia utilizzare la pandemia per consolidare la sua leadership tecnologica ed economica sulla scena internazionale?". In un rapporto del Senato francese si legge: "Le prospettive aperte dall'uso delle tecnologie digitali sono immense e la crisi di Covid-19 ha dato solo un assaggio dei molti usi possibili. [Sarebbe irresponsabile non cogliere queste opportunità".⁹

Le frontiere dell'Unione europea offrono un assaggio di quelle che potrebbero essere queste "opportunità". Con il programma E-Borders, "gli spazi digitali per la raccolta di dati sui migranti sono al centro della strategia dei partner europei". ¹⁰. Frontex, l'agenzia europea per la guardia di frontiera e costiera, è orgogliosa di fare un uso sempre maggiore di tecnologie "in costante evoluzione". ¹¹ automazione, robotizzazione e intelligenza artificiale. ¹².

L'uso di queste frontiere come laboratori fa eco al crescente utilizzo nelle indagini giudiziarie di metodi di sorveglianza digitale, fino a poco tempo fa riservati all'antiterrorismo: l'uso di keylogger, la decrittazione di hard disk e così via. Ad esempio, in un'indagine che ha preso di mira il movimento antinucleare intorno a Bure, sono stati analizzati decine di computer e telefoni. ¹³. Secondo un magistrato, "l'eccezionalità delle misure investigative, con tecnologie altamente avanzate e intercettazioni, deriva da tutti gli impedimenti dell'associazione a delinquere". ¹⁴

Seguendo la stessa logica, sembra che gli Stati stiano organizzando attacchi utilizzando falle di sicurezza ancora sconosciute (le cosiddette "vulnerabilità zero-day") in modo sempre più massiccio. Queste sono state utilizzate dalla Cina contro gli uiguri nel 2018, spingendo un'organizzazione statunitense per le libertà digitali ad affermare che "è altamente probabile che questa non sarà l'ultima volta che vedremo un attore statale prendere di mira un gruppo etnico o attivista".
in massa grazie alle vulnerabilità...".

[pagi
na
33

6. La Quadrature du Net, 2021, *Passé sanitaire: quelle surveillances redouter?*

[<https://www.laquadrature.net/2021/08/19/passe-sanitaire-quelle-surveillance-redouter/>].

7. Célia Izoard, 2021, *Sous le masque du Covid, la numérisation intégrale de la société*, Reporterre [<https://reporterre.net/Sous-le-masque-du-Covid-la-numerisation-integrale-de-la-societe>].

8. Célia Izoard, 2021, *La numérisation du quotidien, une violence inouïe et ordinaire*, Reporterre [<https://reporterre.net/La-numerisation-du-quotidien-une-violence-inouie-et-ordinaire>].

9. Véronique Guillotin, Christine Lavarde, René-Paul Savary, 2021, *Rapporto d'informazione fatto au nom de la délégation sénatoriale à la prospective sur les crises sanitaires et outils numériques: répondre avec efficacité pour retrouver nos libertés*, Senato francese [<https://www.senat.fr/rap/r20-673/r20-6731.pdf>], p. 51.

10. Catherine Puzzo, 2018, *Multiple borders and new agents of migration control in the UK*, Sciences & Actions Sociales n° 9, p 20 [<https://www.cairn.info/revue-sciences-et-actions-sociales-2018-1-page-18.htm#pa20>].

11. Frontex, 2017, *Research and Development in border management* [<https://frontex.europa.eu/media-centre/multimedia/videos/research-and-development-in-border-management-GIoAn>] (in English).

12. Piotr Szostak, 2021, *Con droni e algoritmi, l'Europa costruisce un muro virtuale contro i migranti*, Gazeta Wyborcza tradotto da Courrier International [<https://www.courrierinternational.com/article/interview-with-drones-and-algorithms-europe-builds-a-virtual-wall-against-them>].

13. Marie Barbier, Jade Lindgaard, 2020, *L'État a dépensé un million d'euros contre les antinucléaires de Bure*, Reporterre [<https://reporterre.net/2-3-L-Etat-a-depense-un-million-d-euros-contra-les-antinucleaires-de-Bure>].

14. Laurence Blisson, magistrato ed ex segretario generale del Syndicat de la magistrature, citato da Marie Barbier e Jade Lindgaard (*op. cit.*).

zero-day ¹⁵. Aziende come NSO Group ¹⁶ o Cellebrite ¹⁷ vendono spyware che includono tali strumenti.

A seguito di tutte queste rivelazioni mediatiche, la protezione della privacy digitale è più attuale che mai. A tal punto che le aziende stanno sfruttando la questione per offrire servizi "sicuri", con i loro ben noti limiti: il desiderio di fare profitto porta a pretendere di fornire garanzie che non sono in grado di mantenere. Nel 2021, il provider di posta elettronica criptata Protonmail ha fornito alle autorità francesi informazioni sugli attivisti di Gioventù per il Clima che affermava di non registrare. ¹⁸ In seguito Protonmail ha affermato di non poter rifiutare una simile richiesta legale e ha modificato il suo sito, che affermava il contrario. ¹⁹.

Nel 2021, Proton ha risposto a 4.920 richieste legali (su 6.243 richieste) ricevuto) ²⁰.

*
* *

Sul fronte giuridico a livello europeo, nel maggio 2018 sono entrati in vigore diversi testi di legge che riguardano i dati personali: un regolamento che stabilisce il quadro generale per la protezione dei dati (RGPD) ²¹ nonché una direttiva applicabile esclusivamente ai fascicoli in ambito penale (direttiva polizia-justizia) ²². Si suppone che questi regolamenti proteggano i dati personali regolando il modo in cui possono essere trattati ²³ dalle amministrazioni e dalle organizzazioni pubbliche. Il RGPD richiede inoltre che i dati personali siano conservati e trattati in modo sicuro. In pratica, il regolamento è scarsamente attuato dalle organizzazioni, in quanto le violazioni vengono monitorate molto poco. ²⁴. La direttiva che si applica ai trattamenti giudiziari e di polizia, invece, facilita i trasferimenti di dati tra le forze dell'ordine a livello europeo e non solo. ²⁵.

La battaglia legale sulla conservazione dei dati a livello europeo illustra chiaramente i limiti di queste normative. La Corte di giustizia dell'Unione europea (CGUE) ha invalidato due volte la direttiva europea sulla protezione dei dati. ^{26 27} due volte, prima di arrivare, infine, a de-

15. Cooper Quintin e Mona Wang, 2019, *Watering Holes and Million Dollar Dissidents: the Changing Economics of Digital Surveillance*, Electronic Frontier Foundation [<https://www.eff.org/deeplinks/2019/09/watering-holes-and-million-dollar-dissidents-changing-economics-digital>], .

16. Le Monde, 2021, *Apple corregge la falla del computer legata al software di spionaggio Pegasus* [https://www.lemonde.fr/pixels/article/2021/09/14/apple-repare-une-faille-informatique-liee-au-logiciel-d-espionnage-pegasus_6094541_4408996.html].

17. Privacy International, 2012, *La società di sorveglianza Cellebrite trova un nuovo exploit: Spiare i richiedenti asilo* [<https://privacyinternational.org/fr/node/2776>].

18. Gaspard d'Allens, 2021, *Grazie alla sua reputazione di sicurezza, Protonmail ha fornito alla polizia informazioni su attivisti per il clima*, Reporterre [<https://reporterre.net/Repute-sur-Protonmail-a-livre-a-la-police-des-Informazioni-sui-militanti-del-clima>].

19. Emma Confrere, 2021, *Émoi après que la messagerie sécurisée ProtonMail a collaboré a un'inchiesta giudiziaria*, Le Figaro [<https://web.archive.org/web/20210916174658/https://www.lefigaro.it/sector/high-tech/mefter-secure-messaging-protonmail-a-collabore-a-enquet>].

e-j udiciary-20210907].

20. Proton, 2022, *Rapporto sulla trasparenza* [<https://proton.me/legal/transparency>].

21. Gazzetta ufficiale dell'Unione Europea, 2016, *Regolamento (UE) n. 2016/679 del 27 aprile 2016, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE* [<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679>].

22. Journal officiel de l'Union Européenne, 2016, *Direttiva n. 2016/680 del 27 aprile 2016* [<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680>], nota come "Direttiva Police-Justice".

23. Per "trattamento" si intende qualsiasi cosa relativa alla raccolta, all'aggregazione, all'utilizzo o alla condivisione dei dati.

24. La Quadrature du Net, 2021, *Les GAFAM échappent au RGPD, la CNIL complice* [<https://www.laquadrature.net/2021/05/25/les-gafam-echappent-au-rgpd-avec-la-complicite-de-la-cnil/>].

25. La Quadrature du Net, 2016, *Sintesi della direttiva sui dati personali* [https://wiki.laquadrature.net/Synth%C3%A8se_de_la_directive_sur_les_donn%C3%A9es_personnelles_et_ses_transferts_et_ses_changes_de_donn%C3%A9es_personnelles].

26. Corte di Giustizia dell'Unione Europea, 2014, *La Corte di Giustizia dichiara la direttiva sulla conservazione dei dati non validi*, Comunicato stampa n. 54/14 []. 54/14 [<https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>] sulla sentenza "Digital Rights".

27. Corte di giustizia dell'Unione europea, 2016, *gli Stati membri non possono imporre un obbligo generale di obbligo di conservazione dei dati per i fornitori di servizi di comunicazione*

[pigi
na
29] Richiesta della Francia ,²⁸ per una parziale inversione di posizione²⁹. La Francia ha colto l'occasione per mantenere la conservazione sistematica dei log delle connessioni a fini di sicurezza nazionale o per rintracciare gli autori di reati.³⁰ Il Belgio, invece, ha confermato di voler sostanzialmente abbandonare la conservazione generalizzata e indifferenziata dei dati di connessione.

³¹.
Le altre nuove normative applicabili in Francia sono troppo numerose per essere elencate in questa sede.³² Poiché non è lo scopo principale di questo libro, ci limiteremo a citare due esempi. Il potere di censura delle autorità è stato esteso, con la possibilità di rimuovere i contenuti web per "contenuto terroristico" in meno di un'ora.³³ O l'ennesimo gioco di prestigio usato per annunciare la fine dello stato di emergenza, normalizzando al contempo alcune delle sue esorbitanti disposizioni di diritto comune.³⁴ Una proroga indefinita dello stato di emergenza".³⁵

Ancora una volta, nonostante il diffondersi di un sentimento di impotenza, queste varie rivelazioni sullo stato della sorveglianza digitale rendono ancora più necessario dotarsi dei mezzi per comprenderla e adattare le nostre pratiche di conseguenza.

*
* *

Dall'ultima edizione della *guida*, l'evoluzione tecnica ha portato anche all'aggiornamento di alcuni passaggi: la diffusione dei dischi SSD impone di ripensare la cancellazione dei dati; le tecnologie dei processori si sono evolute.³⁶ Per quanto riguarda le animazioni web, la tecnologia *Flash*, che poneva numerosi problemi di privacy, è stata abbandonata a favore di HTML5 e delle varie tecnologie associate... che pongono nuovi problemi.

Per quanto riguarda gli attacchi, gli aggiornamenti riguardano il firmware (ad esempio il Management Engine di Intel) e l'esfiltrazione dei dati tramite falle nei servizi Web.

électroniques, Comunicato stampa no. 145/16 [https://curia.europa.eu/jcms/jcms/p1_268807/fr/] sulla vicenda "Tele2".

28. Consiglio di Stato francese, 2018, *lettura del 26 luglio 2018* [<https://www.conseil-etat.fr/fr/ari-aneweb/CE/decisione/2018-07-26/394922>].

29. Corte di Giustizia dell'Unione Europea, 2020, *La Corte di Giustizia conferma che il diritto di l'Unione osta a una normativa nazionale che impone a un fornitore di servizi di comunicazione elettronica, ai fini della lotta contro la criminalità in generale o della salvaguardia della sicurezza nazionale, di trasmettere o memorizzare dati su base generale e indifferenziata in materia di traffico e localizzazione*, Comunicato stampa no. 123/20 [<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf>] sui casi Privacy International, La Quadrature du Net, French Data Network e Ordre des barreaux francophones et germanophone.

30. Consiglio di Stato francese, 2021, *decisione del 21 aprile 2021* [<https://www.conseil-etat.fr/conten-t/download/159464/file/393099.pdf>].

31. Corte costituzionale belga, 2021, *Sentenza no. 57/2021 del 22 aprile 2021* [<https://www.const-court.be/public/f/2021/2021-057e.pdf>].

32. Elenco non esaustivo: Legge n. 2019-222 del 23 marzo 2019 sulla programmazione 2018-2022 e riforma della giustizia, la legge n. 2019-1479 del 28 dicembre 2019 sulle finanze per il 2020, la legge n. 2020-766 del 24 giugno 2020 volta a combattere i contenuti di odio su Internet, l'ordinanza n. 2020-1733 del 16 dicembre 2020 sulla parte legislativa del codice sull'ingresso e il soggiorno degli stranieri e il diritto di asilo, la legge n. 2021-646 del 25 maggio 2021 per la sicurezza globale che preserva le libertà, la legge n. 2021-1109 del 24 agosto 2021 che rafforza il rispetto dei principi della Repubblica, la legge n. 2021-996 del 24 agosto 2021 che rafforza il rispetto dei principi della Repubblica, la legge n. 2021-996 del 24 agosto 2021 che rafforza il rispetto dei principi della Repubblica. 2021-646 del 25 maggio 2021 per la sicurezza globale che preserva le libertà, legge n. 2021-1109 del 24 agosto 2021 che rafforza il rispetto dei principi della Repubblica, legge n. 2021-998 del 30 luglio 2021 sulla prevenzione degli atti di terrorismo e di intelligence...

33. Il governo ha lottato con le unghie e con i denti per ottenerlo. *La Quadrature du Net, 7 mai 2021, Règlement de censure terroriste adopté : résumons* [<https://www.laquadrature.net/2021/05/07/element-de-censure-terroriste-adopté-resumons/>].

34. *Developpez.com*, 2017, *Francia: i deputati approvano il sequestro di hardware informatico e la copia dei dati di un sospetto* [<https://www.developpez.com/actu/162736/France-les-deputés-approuvent-la-saisie-de-matériel-informatique-et-la-copie-de-données-d'un-suspect-dans-le-cadre-de-la-lutte-contre-le-terrorisme/>].

35. *Commission nationale consultative des droits de l'Homme*, 6 luglio 2017, *parere sul disegno di legge che rafforza la sicurezza interna e la lotta contro il terrorismo* [<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036039262>].

36. In particolare con la scomparsa dei processori a 32 bit.

Le spiegazioni su Tor sono state ampiamente riviste, in quanto Tor non sostiene più di fornire l'anonimato, ma piuttosto la riservatezza. Anche le raccomandazioni per la scelta delle passphrase e l'uso delle password sono state riviste per tenere conto delle nuove ricerche sull'argomento.

Per quanto riguarda gli strumenti, sono state rilasciate due nuove versioni del sistema operativo Debian GNU/- Linux e nuove versioni del sistema *live* Tails. Questo aggiornamento della *guida* si basa su Debian 11 "Bullseye", che ha portato molti cambiamenti sia alla grafica che al software offerto. Gli strumenti sono stati quindi rivisti per garantire che le ricette funzionino su questi nuovi sistemi. Ciò ha comportato anche una serie di modifiche, tra cui una revisione dell'uso del chif- frement OpenPGP in Thunderbird e nuove istruzioni per l'uso del Tor Browser.

Gli smartphone vengono sempre più spesso presi di mira nelle indagini di polizia come quella di Bure³⁷ e molti dei dispositivi che sfruttano le vulnerabilità *zero-day* prendono di mira proprio *gli smartphone*. Tuttavia, questa guida non si occupa della riduzione del rischio nell'uso degli smartphone. Sarebbe necessario un lavoro completo, per il quale le persone che aggiornano questa *guida* non hanno né il tempo né le competenze. Il funzionamento stesso della telefonia mobile solleva difficili questioni di privacy.³⁸

Dobbiamo tenere conto di questi nuovi sviluppi nel nostro approccio al mondo digitale e nelle nostre politiche di sicurezza.

*
* *

Al di là delle evoluzioni tecniche, una nuova dinamica di scrittura intorno alla *guida* ha portato a sviluppi più generali.

È stata effettuata una rilettura completa che ha portato a numerose riformulazioni ed esempi aggiornati. Una nuova sezione sulla riduzione del rischio applicata agli strumenti digitali è stata aggiunta alla scelta di risposte adatte a ogni situazione. Il caso d'uso *Lavorare su un documento sensibile* è stato rielaborato e il caso d'uso *Pubblicare un documento* include ora la protezione delle persone che lo consulteranno.

La questione del genere nelle formulazioni della *guida* è presente fin dalla sua nascita. Per questa edizione si è cercato di utilizzare il più possibile la scrittura epicena. Ma la lingua francese è così discriminante che non sempre è possibile trovare formulazioni non di genere. In questi casi, abbiamo deciso di usare il femminile, andando contro le regole abituali che prevedono l'uso del maschile. Tuttavia, mentre scriviamo questa prefazione e giustifichiamo le nostre scelte, ci rendiamo conto che ciò non permette alle persone transgender o non binarie di sentirsi incluse, anche all'interno del team *della guida*. A pochi mesi dall'uscita del libro, purtroppo non possiamo pensare di rifare questo lavoro. Aspetteremo la prossima edizione, se arriverà, per trovare una soluzione inclusiva.

*
* *

Grazie a questa revisione, ci auguriamo che le pagine che seguono continuino a essere un saggio compagno di viaggio nella giungla digitale... almeno fino alla prossima.

37. Marie Barbier, Jade Lindgaard, 2020, *La justice a massivement surveille les militants antinucléaires de Bure*, Reporterre [<https://reporterre.net/1-3-La-justice-a-massivement-surveille-les-militants-antinucleaires-de-Bure>].

38. Surveillance Self-Defense, 2018, *The Problem with Mobile Phones* [<https://ssd.eff.org/en/module/le-probl%C3%A8me-with-the-t%C3%A9l%C3%A9phones-portables>].

7 7 7 7 7
BUG312378
XP0124718

Perché questa guida?

Il lato negativo della memoria digitale

Al giorno d'oggi, computer, Internet e telefoni cellulari tendono a occupare sempre più spazio nella nostra vita. La tecnologia digitale sembra spesso molto pratica: è veloce, si può parlare con molte persone lontane, si può avere tutta la propria storia in foto, si possono scrivere facilmente testi ben formattati... ma non ha solo vantaggi; o almeno, non li ha solo per noi, ma anche per altre persone che non vogliamo necessariamente aiutare.

È molto più facile origliare le conversazioni al cellulare che in una strada rumorosa, o trovare le informazioni di cui si ha bisogno su un disco rigido piuttosto che su uno scaffale stracolmo di fogli.

Inoltre, molte delle nostre informazioni personali finiscono per essere pubblicate da qualche parte, da noi stessi o da altri, sia perché siamo incoraggiati a farlo - è questo il senso del *Web 2.0* - sia perché le tecnologie lasciano tracce, o semplicemente perché non stiamo attenti.

Niente da nascondere?

"Ma non siate paranoici: non ho nulla da nascondere!", potremmo rispondere all'affermazione precedente...

Tuttavia, due semplici esempi tendono a dimostrare il contrario: nessuno vuole che i codici segreti della propria carta di credito o del proprio account *eBay* finiscano nelle mani sbagliate. Né si vorrebbe essere derubati perché il proprio indirizzo è stato pubblicato su Internet e la propria assenza è stata confermata sui social media.

Ma al di là di queste sciocche questioni di difesa della proprietà privata, la riservatezza dei dati dovrebbe essere un problema *in sé*.

Innanzitutto perché non siamo noi a giudicare cosa è o non è consentito fare con un computer. Le persone vengono arrestate sulla base delle tracce lasciate dall'uso di strumenti digitali per attività non gradite a un governo, non necessariamente il proprio, e non solo in Cina o in Iran.

Molti soggetti, siano essi governi, datori di lavoro, pubblicitari o poliziotti³⁹ hanno un interesse personale ad accedere ai nostri dati. La crescente importanza di

39. Il termine "poliziotto" è qui utilizzato come definito nell'introduzione alla *Guide d'autodéfense juridique: Face à la police / Face à la justice* [<https://infokiosques.net/spip.php?article538>]: "In questa guida, il termine "poliziotto" è usato in modo intercambiabile con qualsiasi tipo di agente o poliziotto, indipendentemente dal grado o dallo status [...]".

informazioni nell'economia e nella politica globale non possono che incoraggiarle. In effetti, sappiamo già che non si preoccupano di fare controlli incrociati sulle persone. Ma cosa sappiamo delle pratiche legali e illegali di coloro che ci sono più vicini?

Inoltre, come possiamo essere sicuri che ciò che è autorizzato oggi lo sarà anche domani? I governi cambiano, così come le leggi e le situazioni. E questo può accadere con estrema rapidità, come molti hanno potuto constatare con l'applicazione dello stato di urgenza in Francia per due anni nel 2015⁴⁰ prima che alcune misure venissero inserite nel diritto comune.⁴¹ Se non dobbiamo nascondere il fatto che visitiamo regolarmente un sito web di attivisti, ad esempio, come facciamo a sapere cosa succederà se è collegato a un processo repressivo? Le tracce *lasciate* sul computer... potrebbero essere utilizzate come prove incriminanti.

Mettere in atto pratiche di protezione dei dati quando riteniamo di non averne bisogno direttamente le rende anche più "normali", più accettabili e meno sospette. Le persone che non hanno altra possibilità di sopravvivenza se non quella di nascondere le proprie attività digitali ne saranno senza dubbio grate.

In generale, limitiamo le nostre azioni non appena sappiamo che altri potrebbero ascoltarci, guardarci o leggerci. Canteremmo sotto la doccia se sapessimo che c'è una microspia? Impareremmo a ballare se le telecamere fossero puntate su di noi? Scriveremmo una lettera intima con la stessa libertà se qualcuno ci leggesse alle spalle? Avere cose da nascondere non è solo una questione di legalità, ma anche di intimità.

In questo modo, le società di controllo vedono ognuno di noi come una potenziale minaccia da monitorare. Nascondersi è quindi una questione *politica e collettiva*, se non altro per mettere i bastoni tra le ruote a chi vorrebbe che fossimo sempre esposti e identificabili.

Tutto ciò può indurci a pensare che non vogliamo essere controllabili da nessun "Grande Fratello". Sia che esista già, sia che ne anticipiamo la comparsa, la cosa migliore che possiamo fare è assicurarci che non possa usare tutti i meravigliosi strumenti che la tecnologia moderna ci offre - o lui stesso - contro di noi.

Quindi *abbiamo anche noi qualcosa da nascondere, se non altro per coprire le nostre tracce!*

Capire per poter scegliere

Questa guida è un tentativo di descrivere l'intimità (o meglio, la sua mancanza) in termini comprensibili nel mondo digitale, e di mettere in chiaro alcune idee preconcepite per capire meglio a cosa ci stiamo esponendo quando usiamo un determinato strumento.

In questo modo è possibile individuare le "soluzioni", che possono essere pericolose se non si conoscono i loro limiti.

Leggendo queste poche pagine, potreste avere l'impressione che nulla sia davvero sicuro con un computer; ebbene, è vero. E non lo è. Ci sono strumenti e usi appropriati. E alla fine, la domanda spesso non è tanto "dobbiamo o non dobbiamo usare queste tecnologie?", quanto piuttosto "quando e come dobbiamo (o non dobbiamo) usarle?".

⁴⁰. Wikipedia, 2017, *Stato di emergenza in Francia* [https://fr.wikipedia.org/wiki/Etat_d%27urgence_in_Francia].

⁴¹. Repubblica Francese, 2021, *Loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement* [<https://www.vie-publique.fr/loi/279661-loi-30-juillet-2021-prevention-terrorisme-et-renseignement>].

Prendersi il tempo per capire

I software sono progettati per essere il più possibile accessibili e facili da usare. Allo stesso modo, l'accelerazione dei computer e delle connessioni a Internet rende il loro funzionamento quasi istantaneo, quasi impercettibile. Grazie alla diffusione delle reti Wi-Fi, non abbiamo più bisogno di collegare i nostri dispositivi ai cavi per scambiare dati.

Questa semplificazione degli strumenti suggerisce che capire come funzionano è superfluo. Purtroppo, questo significa anche che dobbiamo fidarci e delegare molte decisioni a esperti che prendiamo in parola. L'apprendimento e la comprensione richiedono tempo e pazienza, ma ci danno anche potere e autonomia.

Come leggere questa guida

Questa guida è un tentativo di raccogliere e condividere ciò che abbiamo imparato in anni di pratica, errori, riflessioni e discussioni.

Per rendere tutto più facile da digerire, abbiamo diviso tutto ciò che volevamo raccontare in due volumi. Poiché la parte *offline* è un prerequisito essenziale per comprendere le problematiche della parte *online*, questi due volumi sono stati riuniti in un unico libro.

Un tomo "offline"

Un primo volume, dedicato all'uso *offline* del computer, è stato pubblicato nel 2010. Prima ancora di pensare a collegare i nostri computer, questa prima puntata dà un'occhiata più da vicino al funzionamento di queste macchine. Vedremo *che le* possibilità di controllo e sorveglianza *attraverso gli* strumenti digitali sono innominabili.

Un tomo online

Come suggerisce il nome, questa seconda puntata si concentrerà sull'uso dei computer online, cioè collegati tra loro. Un vasto programma...

Almeno nei Paesi ricchi, l'uso di Internet è diventato uno stile di vita. Controllare la posta elettronica, scaricare file e ottenere informazioni online fanno ormai parte della vita quotidiana di molti di noi. Chiunque potrebbe dire che, in un certo senso, *sa cos'è* Internet. Diciamo che quasi tutti sono in grado di utilizzarlo per alcuni scopi comuni.

Il nostro obiettivo in questo secondo volume, tuttavia, non sarà quello di definire nei minimi dettagli *che cos'è* Internet. Al massimo, forniremo alcuni elementi di comprensione sufficienti a consentire la navigazione - l'ambiguità del termine, che si riferisce tanto alla "navigazione in rete" quanto alla possibilità di orientarsi in uno spazio complesso con l'aiuto di strumenti adeguati.

Gettarsi via

Ancora una volta, partiamo per un viaggio nelle acque torbide del mondo digitale. Ogni volume sarà diviso in tre parti. La prima parte preparerà la scena e spiegherà i concetti di base, fornendo una comprensione generale. La seconda parte tratterà i casi d'uso tipici. Infine, la terza e ultima parte descriverà in dettaglio gli strumenti necessari per implementare le politiche di sicurezza discusse nella seconda parte, nonché il loro utilizzo.

I riquadri forniranno dettagli che si discostano dal testo:



PRECISIONE

Questo tipo di riquadro fornisce esempi o dettagli aggiuntivi che sono facoltativi da leggere.



PER SAPERNE DI PIÙ...

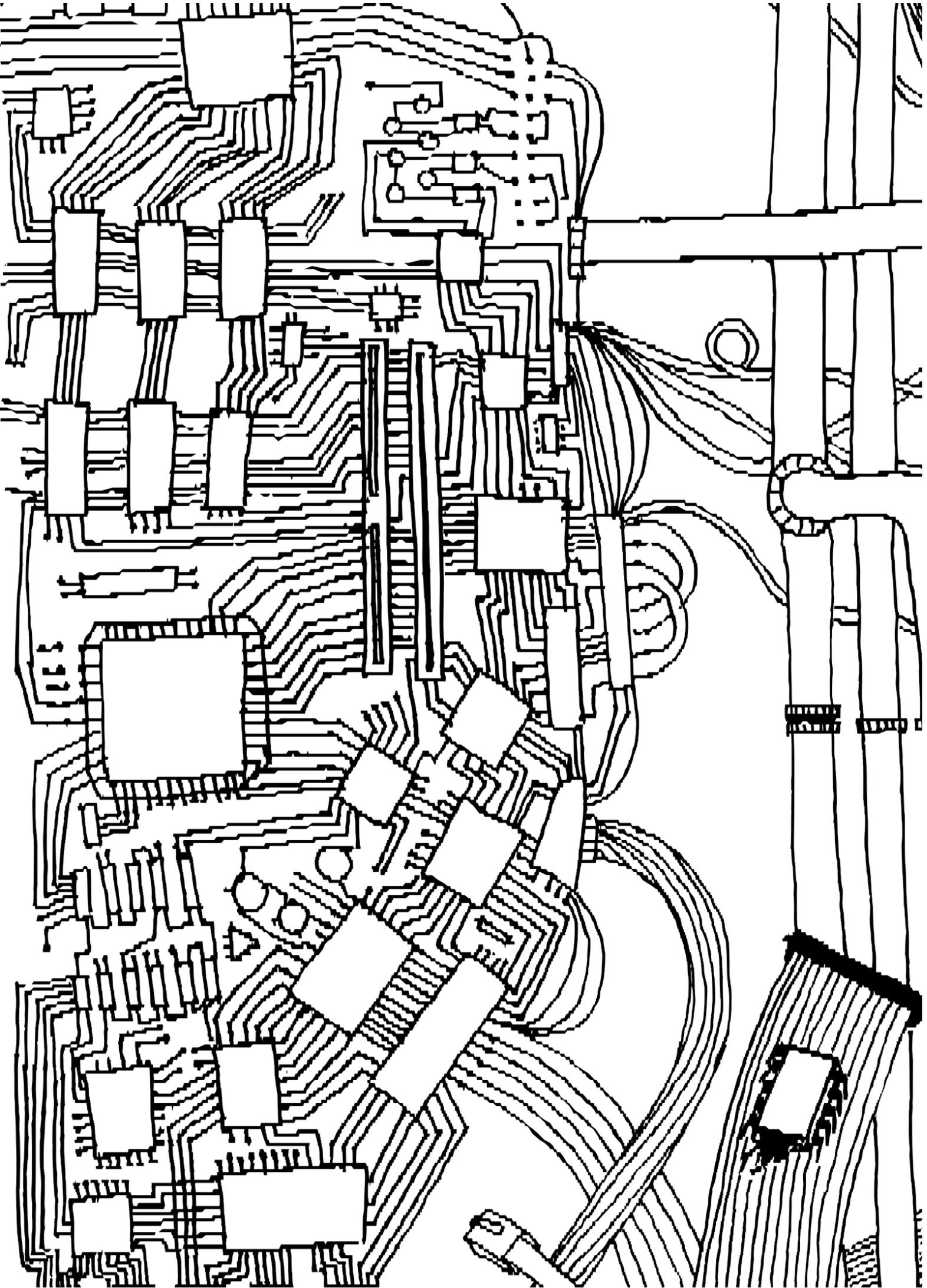
Qui ci saranno indicazioni per andare più lontano, per chi ha voglia di fare escursioni fuori pista.

*

**

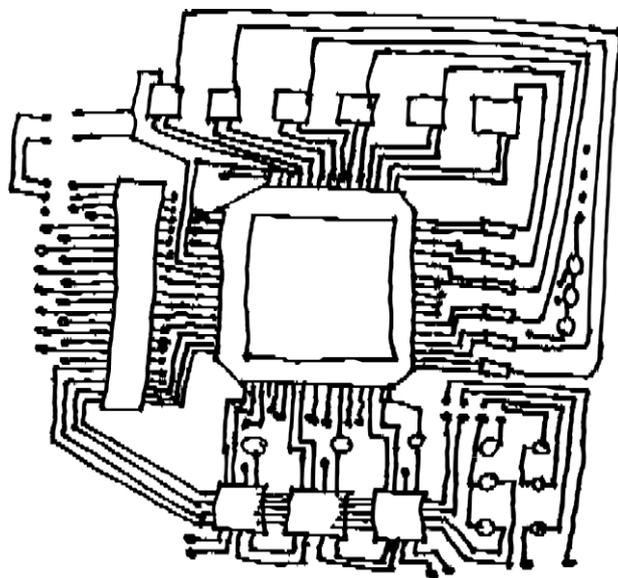
Non solo le tecnologie si evolvono molto rapidamente, ma potremmo aver commesso degli errori o scritto delle falsità in queste pagine. Cercheremo di mantenere aggiornate queste note su <https://guide.boum.org/>.

Adattare le nostre pratiche all'uso del mondo digitale è quindi necessario se vogliamo, o dobbiamo, prestare attenzione al suo impatto. Ma il viaggio, da solo, ha poco significato. Vi invitiamo quindi a costruire la vostra zattera digitale, a salire a bordo con gusto e a non dimenticare di portare con voi questa guida e qualche razzo di soccorso per inviare i vostri commenti e le vostre idee sui *casi d'uso* a guide@boum.org.



VOLUME 1

Collegamenti esterni



PRIMA PARTE

Comprensione

Introduzione

Data la complessità degli strumenti informatici e digitali, la quantità di informazioni che si devono ingerire nel tentativo di acquisire alcune pratiche di autodifesa può sembrare enorme. Lo è certamente per chi cerca di capire tutto in una volta...

Questo primo volume si concentrerà quindi sull'uso di un computer "offline". - potremmo anche dire *prima di qualsiasi connessione*. Ma si tratta anche di conoscenze più generali che si applicano *indipendentemente dal fatto che il computer sia collegato o meno a una rete*. Quindi, fino al secondo volume, lasceremo da parte le minacce specificamente legate all'uso di Internet e delle reti.

Per questo pezzo *off-line*, come per gli altri, ci soffermeremo sulle nozioni di base e sulle loro implicazioni in termini di sicurezza/riservatezza/privacy.¹ Dopo aver analizzato casi d'uso concreti, vedremo alcune ricette pratiche.

Un'ultima nota prima di entrare nel vivo: *l'illusione della sicurezza è di gran lunga peggiore della chiara consapevolezza della debolezza*. Prendiamoci quindi il tempo di leggere le prime parti prima di saltare sulle nostre tastiere o di gettare i nostri computer fuori dalla finestra.

1. L'idea è quella di fare appello a una nozione un po' vaga: qualcosa che ruota attorno alla possibilità di decidere cosa rivelare, a chi rivelarlo e cosa tenere segreto; qualcosa che includa anche una certa attenzione a sventare i tentativi di penetrare questi segreti. Il termine utilizzato è *privacy*. Nessuna parola francese sembra appropriata per trasmettere tutto il significato che vorremmo dare a questa nozione. Altrove ci si imbatte spesso nel termine "sicurezza", ma il suo uso corrente ci spinge a evitarlo.

Nozioni di base sul computer

Prima di tutto, le cose da fare.

Un *computer* non è un cappello da mago in cui si possono riporre i conigli e tirarli fuori quando servono, e che può aprire una finestra dall'altra parte del mondo con la semplice pressione di un tasto.

Un computer è un insieme di componenti più o meno complessi, collegati tra loro da connessioni elettriche, cavi e talvolta onde radio. Tutto questo *hardware* memorizza, trasforma e replica i segnali per manipolare le informazioni che vediamo su un bello schermo con tanti pulsanti da cliccare.

Capire come si integrano questi componenti principali, comprendere le basi del loro funzionamento, è il primo passo verso la comprensione dei punti di forza e di debolezza di queste macchine, alle quali affidiamo molti dei nostri dati.

1.1 Macchine per l'elaborazione dei dati

I computer sono macchine inventate per elaborare i dati. Ciò significa che sono in grado di registrare, analizzare e classificare dati in quantità molto elevate e molto rapidamente.

Nel mondo digitale, copiare i dati costa solo qualche microwatt, in altre parole non molto. Dobbiamo quindi considerare che *mettere le informazioni su un computer* (e questo è ancora più vero quando si tratta di una rete) *significa accettare che queste informazioni possano sfuggirci senza che ce ne accorgiamo*.

Questa guida può aiutare a ridurre i rischi, ma dobbiamo affrontare questa realtà.

1.2 L'attrezzatura

Il nostro computer, somma di componenti interconnessi, è innanzitutto un'accumulazione di oggetti che possiamo toccare, spostare, modificare e rompere.

L'accoppiata *schermo/tastiera/tower* (o CPU), o laptop, è comoda quando si vuole semplicemente collegare i fili nei punti giusti. Ma per scoprire cosa sta succedendo ai nostri dati, dobbiamo dare un'occhiata più da vicino.

Stiamo parlando del contenuto di un cosiddetto *personal computer*, talvolta chiamato PC. Ma altre macchine hanno gli stessi componenti e sono anch'esse computer: telefoni cellulari, "box" di connessione a Internet, tablet, lettori MP3, registratori di cassa, contatori comunicanti Linky o Gazpar ¹ computer di bordo, oggetti connessi di ogni tipo, *ecc.*

1. I contatori comunicanti Linky e Gazpar sono i sostituti dei contatori storici di elettricità e gas - Wikipedia, 2021, *Compteur communicant* [https://fr.wikipedia.org/wiki/Compteur_communicant].

1.2.1 La scheda madre



Una scheda madre

Un computer è costituito principalmente da componenti elettronici. La *scheda madre* è un grande circuito stampato che collega la maggior parte di questi elementi attraverso l'equivalente di fili elettrici. Alla scheda madre sono collegati, come minimo, un processore, una barra RAM, un sistema di archiviazione (disco rigido o altra memoria), un firmware per avviare il computer e altre schede e periferiche, a seconda delle necessità.

Qui di seguito daremo una rapida occhiata a ciascuno di questi elementi per darvi un'idea di chi fa cosa, cosa che vi tornerà molto utile in seguito.

1.2.2 Il processore



Un chip di microprocessore Intel Pentium 60 MHz nel suo alloggiamento

Il processore (noto anche come CPU, per unità di *elaborazione centrale*) è il componente che gestisce l'elaborazione dei dati.

L'esempio più concreto del funzionamento di un processore è la calcolatrice. In una calcolatrice si inseriscono i dati (numeri) e le operazioni da eseguire su di essi (addizione, moltiplicazione o altro) prima di esaminare il risultato. Questo risultato può essere utilizzato come base per ulteriori calcoli.

Un processore funziona esattamente nello stesso modo. Dati i dati (che possono essere un elenco di operazioni da eseguire), esegue i processi richiesti in una catena. Questo è tutto ciò che fa, ma lo fa molto velocemente.

Ma se il processore è solo una calcolatrice, come può elaborare informazioni diverse dai numeri, come testi, immagini, suoni o movimenti del mouse?

Semplicemente trasformando tutto ciò che non lo è in un numero, utilizzando un codice precedentemente definito. Per un testo, questo potrebbe essere A = 65, B = 66 e così via. Una volta definito questo codice, possiamo *digitalizzare* le nostre informazioni. Con il codice precedente, possiamo trasformare "GUIDA" in 71 85 73 68 69.

Questa serie di numeri rappresenta le lettere che compongono la nostra parola. Ma il processo di digitalizzazione comporta sempre una perdita di informazioni. In questo esempio, stiamo perdendo la specificità della scrittura a mano, anche se le cancellature e le lettere esitanti sono altrettante "informazioni". Passare le cose al setaccio del mondo digitale significa inevitabilmente perdere pezzi.

Oltre ai dati, anche le operazioni che il processore deve eseguire (le sue *istruzioni*) sono codificate sotto forma di numeri. Un programma è quindi una serie di istruzioni, manipolate come qualsiasi altro dato.



PRECISIONE

All'interno del computer, tutti questi numeri sono rappresentati da stati elettrici: assenza di corrente o presenza di corrente. Esistono quindi due possibilità, i famosi 0 e 1 che si vedono ovunque. È per questo che si parla di linguaggio binario (*bi-nauta*), la cui unità di misura è il *bit*². Infine, l'elaborazione dei dati avviene con l'aiuto di un bel fascio di fili e di diversi miliardi di *transistor* (interruttori, non molto diversi da quelli usati per accendere o spegnere la luce in cucina).

Non tutti i processori funzionano allo stesso modo. Alcuni sono stati progettati per essere più efficienti in determinati tipi di calcolo, altri per consumare meno energia possibile e così via. Inoltre, non tutti i processori hanno esattamente le stesse istruzioni. Esistono grandi famiglie di processori, note come *architetture*. Questo è importante, perché un processore con una determinata architettura sarà generalmente in grado di eseguire solo programmi progettati per quell'architettura.

La maggior parte dei personal computer è basata sull'architettura x86-64 (nota anche come x64, AMD64 o Intel 64).³ (nota anche come x64, AMD64 o Intel 64), mentre molti telefoni e altri minicomputer utilizzano l'architettura ARM.

2. Per maggiori informazioni, si veda [Wikipedia, 2014, Bit](https://fr.wikipedia.org/wiki/Bit) [https://fr.wikipedia.org/wiki/Bit].

3. Fino agli anni 2010, alcuni personal computer utilizzavano una versione precedente dell'architettura x86, in cui i dati manipolati erano codificati su 32 bit, rispetto ai 64 bit della versione x86-64. Questi vengono chiamati processori a 32 o 64 bit.

1.2.3 RAM

La *memoria ad accesso casuale* (RAM) viene spesso fornita sotto forma di *stick di memoria* e collegata direttamente alla scheda madre.



Moduli di memoria diversi

La RAM memorizza tutti i software e i documenti aperti all'accensione del computer. È qui che il processore recupera i dati da elaborare e memorizza i risultati delle operazioni. Praticamente tutte le informazioni elaborate dal computer passano quindi attraverso la RAM in forma direttamente utilizzabile e quindi non criptata.

La RAM è collegata al processore e consente di leggere, scrivere e modificare i dati molto rapidamente, in base alle esigenze del processore.

La chiamiamo *RAM* in contrapposizione alla *memoria di sola lettura* (disco rigido, chiavetta USB, disco SSD, ecc.): a differenza di questi componenti, i dati in essa contenuti diventano illeggibili dopo alcuni minuti o ore (a seconda del modello) quando la RAM non viene più alimentata.

1.2.4 Disco rigido o SSD

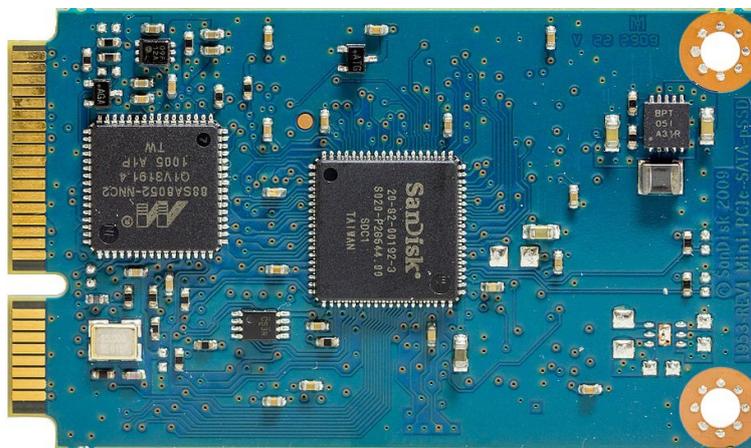


Un disco rigido da 3 pollici e mezzo

Poiché la RAM viene cancellata non appena l'alimentazione si esaurisce, il computer ha bisogno di un altro posto per memorizzare dati e programmi tra un'accensione e l'altra. È qui che entra in gioco *la memoria persistente o di sola lettura*: una memoria in cui le informazioni scritte rimangono anche senza alimentazione.

A tal fine, si utilizza un supporto di memorizzazione come un *disco rigido* o un dischetto. *SSD*.

Il termine disco rigido si riferisce generalmente ai dischi rigidi rotanti, noti anche come *dischi rigidi magnetici* o *dischi rigidi meccanici*. Questi dischi rigidi a rotazione hanno spesso la forma di un guscio metallico contenente diversi dischi che ruotano senza fermarsi, come un giradischi in miniatura. Su questi dischi sono presenti minuscoli pezzi di ferro e sulla parte superiore di ogni disco sono presenti delle *testine di riproduzione*. Grazie ai campi magnetici, queste rilevano e modificano la posizione dei pezzi di ferro. È la posizione dei pezzi di ferro che codifica le informazioni da memorizzare.



Un'unità SSD interna

A causa dei loro movimenti meccanici, i dischi rigidi a rotazione sono lenti. Per questo motivo, negli ultimi anni, più della metà dei supporti di memorizzazione venduti sono SSD o *Solid State Drive* (o dischi elettronici o dischi a stato solido), piuttosto che dischi rigidi rotativi.⁴ Le unità SSD funzionano con un altro tipo di memoria: la memoria *flash*, lo stesso tipo utilizzato nelle *chiavette USB* e nelle *schede SD*. In un'unità SSD, i dati vengono memorizzati utilizzando diverse centinaia di interruttori miniaturizzati. Questa memoria interamente elettronica è circa 25 volte più veloce di un disco rigido rotante.

I dischi rigidi rotazionali e le unità SSD possono memorizzare *molte più informazioni* della RAM, ma sono molto più lenti.

L'informazione viene memorizzata sotto forma di *bit*, di cui esistono multipli g a r g e a b s e y t e s r a l ⁵ ad esempio, la capacità di un disco rigido, spesso espressa in

(GB), terabyte (TB),

ecc. possono essere quantificate semplicemente andando a pagina 16.

Le informazioni memorizzate su un disco (disco rigido o SSD) sono spesso documenti, ma anche programmi con tutti i dati necessari, come i file temporanei, i registri di sistema, i file di backup, di configurazione, ecc.

Il disco utilizzato conserva quindi una memoria quasi permanente e quasi esaustiva di tutti i tipi di tracce che parlano di noi, di ciò che facciamo, con chi e come, non appena usiamo un computer.

4. Q4, 2021, *Quota di mercato SSD* [<https://www.t4.ai/industry/ssd-market-share>].

5. *Wikipedia*, 2017, *Byte* [<https://fr.wikipedia.org/wiki/Octet>].

1.2.5 Altre periferiche

Con un processore, un po' di RAM e un supporto di memorizzazione, avete già un computer. Non molto loquace, però. Quindi di solito si aggiungono altre *periferiche*, come schermo, tastiera, mouse, scheda di rete (cablata o wireless), lettore di schede micro SD e *così via*.

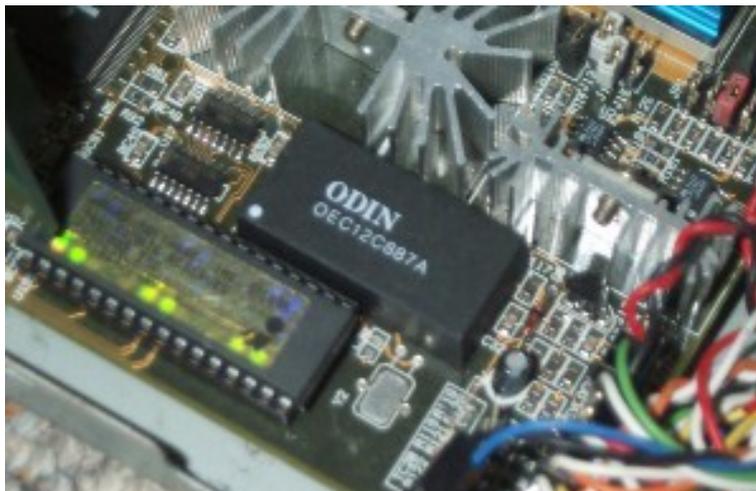
Molte di queste periferiche sono collegate tramite USB (*Universal Serial Bus*), uno standard che consente di collegare stampanti, tastiere, mouse, dischi rigidi aggiuntivi, adattatori di rete o le cosiddette "chiavette USB".

Il collegamento tra il processore e le varie periferiche USB è assicurato da un insieme specifico di chip, chiamato *chipset*. Il chipset è saldato sulla scheda madre o addirittura integrato nello stesso alloggiamento del processore.

La maggior parte dei chipset odierni integra periferiche aggiuntive progettate per fornire ambienti sicuri per il sistema operativo del computer e l'esecuzione dei programmi. Queste includono il Management Engine (ME) di Intel e il Platform Security Processor (PSP) di AMD. Queste periferiche sono spesso fonte di preoccupazione, in quanto il loro funzionamento non è trasparente e talvolta possono essere utilizzate come backdoor sui computer che ne sono dotati.⁶ sui computer che ne sono dotati.

Altre periferiche possono richiedere l'aggiunta di una scheda aggiuntiva, detta *scheda figlia*, come nel caso della maggior parte degli adattatori Wi-Fi.

1.2.6 Firmware della scheda madre



Un chip firmware su una scheda madre

Per avviare il computer, è necessario fornire al processore un programma iniziale, in modo che possa caricare i programmi da eseguire successivamente.

Questo piccolo software, chiamato *firmware*⁷ è contenuto in un chip di memoria collegato alla scheda madre. Si tratta di una memoria *flash*, come quella delle chiavette USB o dei dischi SSD.

Il firmware storico della maggior parte dei personal computer si chiama BIOS (*Basic Input/Output System*). Dal 2012,

6. Questi dispositivi funzionano con un software che può contenere una *backdoor*, ossia una funzione che consente di accedere segretamente al software o addirittura a computer, senza che l'utente ne sia consapevole.

7. Il firmware può essere chiamato anche *firmware*, microcodice, software interno o software incorporato.

sempre più computer utilizzano un nuovo standard chiamato UEFI (*Unified Extended Firmware Interface*).

Tra le altre cose, questo primo programma eseguito dal computer consente di scegliere la posizione del sistema operativo che si desidera utilizzare. Di solito viene caricato dal disco rigido, ma può anche provenire da una chiavetta USB, da un CD o da un DVD o persino dalla rete.

prossimo
pagina.



PER SAPERNE DI PIÙ...

Per fare un giro del firmware di un computer, è possibile seguire l'*interfaccia di configurazione del firmware di Enter* nello strumento *Start su CD, DVD o chiavetta USB* (vedere pagina 108).

1.3 Elettricità, campi magnetici, rumore e onde radio

Dopo aver dato una rapida occhiata a ciò che lo compone, passiamo alla riservatezza delle informazioni che circolano all'interno di un computer.

Innanzitutto, la maggior parte delle informazioni circola sotto forma di correnti elettriche. Non c'è quindi motivo per cui non si possa installare l'equivalente di un *amperometro* per misurare il flusso di corrente e quindi essere in grado di ricostruire i dati manipolati dal computer in una forma o nell'altra.

Inoltre, ogni corrente elettrica che scorre tende a emettere un campo magnetico. Questi campi magnetici possono irradiare una distanza di diversi metri o più.⁸ È quindi possibile, se si hanno i mezzi, ricostruire il contenuto di uno schermo o ciò che è stato digitato su una tastiera, anche da dietro un muro, dalla strada o dall'appartamento adiacente. I ricercatori sono riusciti a registrare i tasti digitati su normali tastiere cablate a partire dalle loro emissioni elettromagnetiche, fino a 20 metri di distanza.⁹

Lo stesso tipo di operazione è possibile osservando i lievi disturbi generati dal computer sulla rete elettrica in cui è collegato.¹⁰

Altri esperimenti che utilizzano un microfono per ascoltare il rumore dei componenti elettronici del computer e della sua alimentazione hanno permesso, in determinate condizioni, di decifrare le chiavi di crittografia contenute nel computer bersaglio.¹¹ Nel frattempo sono state apportate correzioni al software coinvolto per complicare questo tipo di attacco.

Infine, alcune periferiche (tastiere, mouse, cuffie, ecc.) funzionano *in modalità wireless*. Comunicano con il computer tramite onde radio che possono essere captate e decodificate da chiunque si trovi nelle vicinanze.

In sintesi, anche se un computer non è collegato a una rete e qualsiasi programma sia in esecuzione su di esso, è comunque possibile per esperti ben attrezzati "ascoltare" ciò che accade all'interno.

8. Nel 1995, Berke Durak è riuscito a catturare le onde elettromagnetiche [<http://lambda-diode.com/electronics/tempest/>] emesse dalla maggior parte dei componenti del suo computer utilizzando un semplice *walkman* in grado di ricevere radio (link in inglese).

9. Martin Vuagnoux e Sylvain Pasini hanno prodotto alcuni video spaventosi [<https://lasecwww.epfl.ch/keyboard/>] per illustrare il loro articolo del 2009 *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*.

10. Nel 1998, Paul Kocher, Joshua Jaffe e Benjamin Jun hanno pubblicato un rapporto [<https://www.ra.mbus.com/wp-content/uploads/2015/08/DPATechInfo.pdf>] che spiega le varie tecniche di analisi del consumo energetico.

11. Clément Bohic, 2013, *Chiffrement : il suffirait d'écouter le processeur pour décoder les clefs*, [silicon.fr](http://www.silicon.fr) [<https://www.silicon.fr/chiffrement-ecouter-processeur-decoder-clefs-91686.html>].

1.4 Software

Al di là della somma degli elementi fisici che compongono un computer, dobbiamo considerare anche gli elementi meno tangibili: il software.

Ai tempi dei primi computer, ogni volta che si dovevano eseguire diverse operazioni di elaborazione, era necessario un intervento fisico per modificare la disposizione di cavi e componenti. Oggi, invece, non è più così: le operazioni necessarie per eseguire questi processi sono diventate dati come tutti gli altri. Questi dati, detti *programmi*, vengono caricati, modificati e manipolati da altri programmi.

Un insieme di programmi per svolgere un determinato compito è chiamato *software*. È quindi l'interazione di migliaia di software tra loro che consentirà di svolgere i compiti complessi per i quali i computer sono oggi generalmente utilizzati.

L'effetto prodotto quando si fa clic su un pulsante è quindi l'avvio di una catena di eventi, una somma impressionante di calcoli che si traducono in pulsazioni elettriche che modificano un oggetto fisico. È come le vibrazioni della membrana di un altoparlante per riprodurre un suono, uno schermo che modifica i suoi LED per visualizzare una nuova pagina o un disco SSD che attiva o disattiva microinterruttori per creare la sequenza binaria di dati che costituirà un *file*.

1.4.1 Il sistema operativo

Lo scopo di un *sistema operativo* è innanzitutto quello di consentire ai vari programmi software di condividere l'accesso ai componenti hardware del computer e di comunicare tra loro. Inoltre, un sistema operativo viene generalmente fornito con un software, almeno per consentire l'avvio di altri software.

La parte fondamentale di un sistema operativo è il suo *kernel*, che coordina l'uso dell'hardware da parte di altri software.

Per ogni componente hardware del computer che si desidera utilizzare, il kernel attiva un programma chiamato *driver*. Esistono driver per i dispositivi di input (tastiera, mouse, ecc.), per i dispositivi di output (schermo, stampante, ecc.) e per i dispositivi di archiviazione (DVD, chiavetta USB, ecc.).

Il kernel gestisce anche l'esecuzione dei vari programmi, assegnando a ciascuno di essi parti della RAM del processore e del tempo di calcolo.

Oltre al kernel, i sistemi operativi odierni - come Windows, macOS o GNU/Linux - includono anche numerosi strumenti (o utility), nonché ambienti desktop grafici che consentono di utilizzare il computer semplicemente facendo clic sui pulsanti.

Il sistema operativo è solitamente memorizzato sul disco rigido. Tuttavia, è anche possibile utilizzare un sistema operativo memorizzato su una chiavetta USB o masterizzato su un DVD. In quest'ultimo caso si parla di sistema *live*.

1.4.2 Applicazioni

Le *applicazioni* sono programmi software che consentono di eseguire le operazioni desiderate dal computer. Ne sono un esempio Mozilla Firefox per la navigazione web, LibreOffice per l'automazione d'ufficio e VLC per la riproduzione di musica e video.

Ogni sistema operativo definisce un metodo specifico per l'accesso delle applicazioni all'hardware, ai dati, alla rete o ad altre risorse. Le applicazioni che si vogliono utilizzare devono quindi essere adattate al sistema operativo del computer su cui si desidera utilizzarle.

1.4.3 Le librerie

Piuttosto che riscrivere pezzi di programma in ogni applicazione per fare la stessa cosa, questi pezzi sono raggruppati in *librerie*, che i programmi software condividono.

Esistono librerie per l'affichaggio grafico (che garantiscono la coerenza di ciò che viene visualizzato sullo schermo), per la lettura o la scrittura di formati di file, per l'interrogazione di alcuni servizi di rete e così via.

Se non si scrive software da soli, raramente si ha bisogno di visitare queste librerie. Tuttavia, può essere utile sapere che esistono, se non altro perché un problema (come un errore di programmazione) in una libreria può avere ripercussioni su tutto il software che la utilizza.

1.4.4 Pacchetti

I sistemi operativi GNU/Linux possono essere organizzati in modo diverso a seconda della loro distribuzione.¹² Alcune distribuzioni (come Debian o Tails, su cui si basa la maggior parte degli strumenti presentati in questa guida) funzionano con *pacchetti*.

Il software (*sistemi operativi, applicazioni o librerie*) viene quindi installato tramite pacchetti. Un pacchetto è composto da diversi file che, tra l'altro, permettono di eseguire il programma, specificano se dipende da altri software o da altri pacchetti, permettono di configurarlo, forniscono la documentazione, ne verificano l'autenticità, ecc.

Il sistema può essere gestito con un software che automatizza l'installazione, la disinstallazione e l'aggiornamento dei pacchetti. Tale software è chiamato *gestore di pacchetti*. In generale, i pacchetti di una distribuzione sono disponibili su Internet nei cosiddetti *repository*. Il gestore di pacchetti recupera da questi repository i pacchetti necessari, che sono specifici per ogni distribuzione.

1.5 Memorizzazione dei dati

Abbiamo visto che un disco rigido (o una chiave USB) può essere utilizzato per memorizzare i dati tra un'accensione e l'altra del computer.

Ma per potersi orientare, i dati vanno disposti in un certo modo: un armadio senza ripiani in cui si accumulano fogli di carta non è necessariamente la forma più efficiente di archiviazione.

1.5.1 Spartito

Proprio come è possibile inserire diversi ripiani in un mobile, è possibile "tagliare" un disco rigido in diverse *partizioni*.

Ogni scaffale può avere un'altezza diversa e una classificazione diversa, a seconda che si vogliono mettere libri o fascicoli, in ordine alfabetico o cronologico.

Allo stesso modo, su un disco rigido, ogni partizione può essere di dimensioni diverse e contenere una modalità di organizzazione diversa: questo si chiama *file system*.

12. La distribuzione di un sistema operativo è una versione di esso adattata a usi o esigenze specifiche. Ciò può avvenire, ad esempio, per renderlo particolarmente leggero o più facile da usare, ma anche per funzioni speciali (per una particolare azienda o strumento). Ogni distribuzione riunisce un insieme adattato e coerente di software, dal sistema alle applicazioni, con vari gradi di funzionalità.

1.5.2 Sistemi di file

Un file system serve a recuperare le informazioni dalla nostra enorme mole di dati, proprio come l'indice di un libro di cucina vi porta direttamente alla pagina giusta per leggere la ricetta del banchetto serale.

Si noti, tuttavia, che l'eliminazione di un file non cancella il contenuto del file, ma si limita a rimuovere una riga dall'indice. Se si scorrono tutte le pagine, si riuscirà sempre a trovare la propria ricetta, a patto che la pagina non sia stata riscritta - questo punto verrà sviluppato più avanti.

[pagina]
42

Si possono immaginare migliaia di formati diversi per l'archiviazione dei dati e quindi esistono molti file system diversi. *La formattazione* si riferisce alla creazione di un file system definito su un supporto.

Poiché è il sistema operativo che dà ai programmi l'accesso ai dati, un file system è spesso fortemente legato a un particolare sistema operativo.



PRECISIONE

Per citarne solo alcuni: NTFS e FAT32 sono i tipi solitamente utilizzati dai sistemi operativi Windows; *ext* (*ext2*, *ext4*) è spesso utilizzato da GNU/Linux; HFS, HFS+ e HFSX sono utilizzati da macOS.

Una delle conseguenze è che su un determinato computer possono esserci spazi di memoria non riconosciuti dal sistema operativo e quindi non facilmente accessibili.

Tuttavia, è possibile leggere un file system sconosciuto *a priori* al sistema in uso, purché si utilizzi il software appropriato. Windows, ad esempio, è in grado di leggere una partizione *ext3*, se è installato il software appropriato.

1.5.3 Formati dei file

[pagina]
30

I dati che manipoliamo sono generalmente raggruppati sotto forma di file. Un file ha un contenuto - i dati - e dei metadati, cioè un nome, una posizione (la cartella in cui si trova), una dimensione e altri dettagli a seconda del file system utilizzato.

Ma all'interno di ogni file, i dati stessi sono organizzati in modo diverso, a seconda della loro natura e del software utilizzato per manipolarli. Per distinguerli, si parla di *formati* di file.

In generale, un codice, talvolta chiamato *estensione*, viene posto alla fine del nome di un file per indicarne il formato. È possibile scegliere un'estensione o un'altra e modificarla. Tuttavia, questo è principalmente a scopo informativo e non significa che la modifica dell'estensione cambi il formato del file.

Alcuni esempi di estensioni: per la musica, spesso utilizzeremo i formati MP3 o Ogg; per un documento di testo di LibreOffice, sarà OpenDocument Text (ODT); per le immagini, potremo scegliere tra JPEG, PNG e altri; *e così via*.

[pagina]
39

Come il software, i formati possono essere *aperti* o *proprietary*. *I formati aperti* sono definiti pubblicamente, tra l'altro per non limitarne l'uso a un singolo software.

Alcuni formati *proprietary* sono stati studiati attentamente per renderli utilizzabili da altri software, ma la loro comprensione rimane spesso imperfetta. È il caso del vecchio formato Microsoft Word (DOC) o di Adobe Photoshop (PSD).

1.5.4 Memoria virtuale (*swap*)

In teoria, tutti i dati a cui il processore deve accedere, e quindi tutti i programmi e i documenti che apre, dovrebbero trovarsi nella RAM. Ma per poter aprire molti programmi e documenti contemporaneamente, i moderni sistemi operativi imbrogliano: quando è necessario, scambiano pezzi di RAM con uno spazio dedicato sul disco rigido. Questo è noto come "memoria virtuale" o "spazio *di swap*".

Quindi il sistema operativo fa la sua parte per garantire che il processore abbia sempre a disposizione i dati a cui vuole accedere nella RAM. La memoria virtuale è un esempio di spazio di archiviazione a cui non pensiamo necessariamente, salvato sul disco rigido come un grande file contiguo (con Windows e talvolta con GNU/Linux) o in una partizione separata (con GNU/Linux).

Torneremo sui problemi posti da queste questioni di formato e spazio di archiviazione dal punto di vista della riservatezza dei dati nella prossima sezione.

Tracce su ogni piano

Il normale funzionamento di un computer lascia molte tracce di ciò che si fa su di esso. A volte queste informazioni *sono necessarie* per il funzionamento del computer. Altre volte, queste informazioni vengono raccolte per consentire al software di essere "più pratico".

2.1 In RAM

Come abbiamo visto, il primo luogo in cui vengono memorizzate le informazioni in un computer è la scheda di memoria. RAM.

Finché il computer è acceso, contiene tutte le informazioni di cui il sistema ha bisogno. Pertanto, conserva necessariamente molte tracce: battute di tasti (comprese le password), file aperti e altri eventi vari che hanno scandito la fase di risveglio del computer.

Prendendo il controllo di un computer acceso, non è molto difficile trasferire tutte le informazioni contenute nella RAM, ad esempio su una chiavetta USB o su un altro computer in rete. E prendere il controllo di un computer può essere semplice come collegare un *iPod* improvvisato quando il proprietario è girato di spalle.¹ Una volta recuperata, la grande quantità di informazioni contenute nella RAM - ad esempio su chi sta utilizzando il computer - può essere sfruttata.

Abbiamo anche visto che questi dati diventano illeggibili dopo lo spegnimento del computer. Tuttavia, ciò richiede più o meno tempo e può bastare a un malintenzionato per avere il tempo di recuperare ciò che è presente. Questo è noto come *attacco cold boot*: l'idea è quella di copiare il contenuto della RAM prima che abbia avuto il tempo di cancellarsi, in modo da sfruttarlo in seguito. È persino tecnicamente possibile portare la memoria di un computer appena spento a una temperatura molto bassa, nel qual caso il suo contenuto può sopravvivere per diverse ore o addirittura giorni.²

Tuttavia, per funzionare, questo attacco deve essere eseguito molto presto dopo lo spegnimento. Inoltre, se si utilizzano alcuni programmi di grandi dimensioni (ad esempio, il ritocco di un'immagine enorme con Adobe Photoshop o GIMP) prima di spegnere il computer, è probabile che le tracce lasciate in precedenza nella RAM vengano sovrascritte. Inoltre, esistono programmi software appositamente progettati per sovrascrivere il contenuto della RAM con dati casuali appena prima di spegnere il computer.

1. Fernand Lone Sang, Vincent Nicomette, Yves Deswarte, Loïc Dufлот, 2011, *DMA*

attacchi peer-to-peer e contromisure [https://www.sstic.org/media/SSTIC2011/SSTIC-actes/attaques_d_ma_peer-to-peer_et_contremesures/SSTIC2011-Article-attaques_dma_peer-to-peer_et_contr_emesures-lone-sang_dufлот_nicomette_deswarte.pdf]. Maximilian Dornseif, 2004, *posseduto da un iPod* [<https://web.archive.org/web/20100326020818/http://md.hudora.de/presentations/#firewire-pacsec>].

2. J. Alex Halderman *et al*, 2008, *Lest We Remember: Cold Boot Attacks on Encryption Keys* [<https://citp.princeton.edu/memory/>].

47

[página
na 25

[página
44

[página
na 47

[página
na 47

[página
na 25

[página

2.2 In memoria virtuale

ses parte del disco rigido per supportare la RAM. Ciò accade in particolare quando il computer è molto utilizzato, ad esempio quando si lavora con immagini di grandi dimensioni, ma anche in molti altri casi, in modo imprevedibile.

La conseguenza più fastidiosa di questa operazione molto pratica è che il computer scriverà informazioni potenzialmente sensibili dalla RAM al disco rigido, *che rimarranno leggibili anche dopo lo spegnimento del computer.*

- ⌋ Con un computer configurato nel modo standard, è quindi illusorio credere
 - ⌋ che un documento letto da una chiave USB, anche se aperto con un software
 - ⌋ portatile, non lascerà mai tracce sul disco rigido.
-
- ⌋ Per impedire a chiunque di accedere a questi dati, è possibile utilizzare un
 - ⌋ sistema operativo configurato per criptare la memoria virtuale.

2.3 Guardare e ibernare

La maggior parte dei sistemi operativi consente di mettere in "pausa" un computer. Questa funzione è utilizzata soprattutto con i computer portatili, ma è valida anche per i desktop.

Esistono due tipi principali di "pausa": la veglia e l'ibernazione.

2.3.1 Il giorno prima

Lo standby (noto anche come *sospensione della RAM* o *sospensione*) consiste nello spegnere il maggior numero possibile di componenti del computer, pur mantenendo l'alimentazione per un rapido riavvio.

Come minimo, la RAM continuerà a essere utilizzata per memorizzare tutti i dati su cui si stava lavorando, comprese le password e le chiavi di crittografia.

- ⌋ In breve, un computer in modalità standby non offre la stessa protezione contro
- ⌋ l'accesso ai dati di un computer acceso.

2.3.2 Ibernazione

L'ibernazione, nota anche come *sospensione su disco*, consiste nel salvare tutta la RAM sul disco rigido e poi spegnere completamente il computer. Al successivo avvio, il sistema operativo rileva l'ibernazione, copia il backup nella RAM e ricomincia a lavorare da lì.

- ⌋ Nei sistemi GNU/Linux, la memoria viene solitamente copiata nella
- ⌋ memoria virtuale (*swap*). Su altri sistemi, può trovarsi in un file di grandi dimensioni, spesso *nascosto*.

Poiché l'intero contenuto della RAM viene poi scritto sul disco rigido, ciò significa che tutti i programmi e i documenti aperti, le password, le chiavi di crittografia e così via, possono essere recuperati da chiunque acceda al disco rigido. A patto che non sia stato riscritto nulla su di esso.

- ⌋ Tuttavia, questo rischio è limitato dalla crittografia del disco rigido: la
- ⌋ passphrase è necessaria per accedere al backup della RAM.

2.4 Giornali

I sistemi operativi scrivono una storia dettagliata di ciò che fanno nei loro *registri di sistema*.

Questi registri aiutano il funzionamento del sistema operativo e possono consentirci di correggere problemi di configurazione o *bug*.

Tuttavia, questi registri memorizzano anche dati che possono sollevare problemi di privacy. Ad esempio, registrano :

- la data, l'ora e il nickname dell'utente che effettua il login a ogni accensione del computer;
- marca e modello di qualsiasi supporto rimovibile (disco esterno, chiave USB, ecc.) collegato;
- stampa della data e del numero di pagine ;
- nome del software, data e ora di installazione o disinstallazione di un'applicazione.

Per impostazione predefinita, tutti questi registri vengono memorizzati a tempo indeterminato sul disco rigido del computer, tranne nel caso dei sistemi *live*, che li memorizzano nella RAM.

2.5 Backup automatici e altri elenchi

Oltre a questi registri, è possibile che sul computer rimangano altre tracce anche dei file eliminati. Anche se i file e il loro contenuto sono stati effettivamente eliminati, qualche parte del sistema operativo o di un altro programma può deliberatamente mantenerne traccia.

Ecco alcuni esempi:

- un elaboratore di testi può mantenere un riferimento al nome di un file eliminato nel menu "documenti recenti". A volte, può anche conservare i file temporanei con il contenuto del file in questione. Esistono decine di programmi che funzionano in questo modo;
- Quando si utilizza una stampante, il sistema operativo spesso copia il file in attesa nella "coda di stampa". Una volta svuotata la coda, il contenuto di questo file non sarà scomparso dal disco rigido;
- In Windows, quando si collega un'unità rimovibile (chiavetta USB, disco rigido esterno, scheda SD o DVD), il sistema spesso ne analizza prima il contenuto per suggerire il software adatto alla lettura: questa scansione automatica lascia un elenco di tutti i file presenti sul supporto utilizzato, anche se non viene consultato nessuno dei file in esso contenuti.

È difficile trovare una soluzione adeguata a questo problema. Un file, anche se perfettamente cancellato, probabilmente continuerà a esistere sul computer per qualche tempo in una forma diversa. Una ricerca dei dati grezzi sul disco mostrerà se esistono o meno copie di questi dati, a meno che non siano solo referenziati o memorizzati in una forma diversa, ad esempio compressa.

Infatti, solo sovrascrivendo l'intero disco e installando un nuovo sistema operativo si può essere sicuri che tutte le tracce di un file siano state rimosse. D'altra parte, l'uso di un sistema *live*, il cui team di sviluppo presta particolare attenzione a questo problema, garantisce che queste tracce non vengano lasciate in nessun altro luogo se non nella RAM. Per saperne di più, si veda più avanti.

pagina

139

pagina

113

2.6 Metadati

Oltre alle informazioni contenute in un file, esistono anche informazioni che lo accompagnano, non necessariamente visibili a prima vista: data di creazione, nome del software utilizzato, computer, ecc. Questi "dati sui dati" sono comunemente chiamati "metadati". Questi "dati sui dati" sono comunemente chiamati "metadati".

[pagi
na 24
-----] Una parte dei metadati viene registrata dal file system: il nome del file, la data e l'ora della sua creazione e delle sue modifiche e spesso molte altre cose. Queste tracce vengono lasciate sul computer (il che può essere un problema di per sé), ma il più delle volte non vengono scritte sul file.

[pagi
na 24
-----] D'altra parte, molti formati di file memorizzano anche metadati all'interno del file. Questi metadati vengono distribuiti insieme al file quando viene copiato su una chiavetta USB, inviato per e-mail o pubblicato online. Queste informazioni possono essere conosciute da chiunque abbia accesso al file.

I metadati registrati dipendono dal formato e dal software utilizzato. La maggior parte dei formati di file audio consente di registrare il titolo del brano e l'interprete. Gli elaboratori di testo o i PDF registrano il nome dell'autore, la data e l'ora di creazione e talvolta anche la cronologia completa delle ultime modifiche.³ Quindi, potenzialmente, informazioni che pensavate di aver cancellato.

I formati immagine come TIFF o JPEG sono probabilmente i più importanti: questi file fotografici creati da una fotocamera digitale o da un telefono cellulare contengono metadati in formato EXIF. Questi possono includere la marca, il modello e il numero di serie della fotocamera utilizzata, nonché la data, l'ora e talvolta anche le coordinate geografiche dello scatto, senza dimenticare una versione a metà natura dell'immagine. Sono stati questi metadati a porre fine alla corsa di John McAfee, fondatore ed ex capo dell'omonima società di sicurezza informatica.⁴ Inoltre, tutte queste informazioni tendono a rimanere anche dopo che il file è passato attraverso un software di fotoritocco. Il caso della miniatura è particolarmente interessante: molte foto disponibili su Internet contengono ancora la totalità di una foto ritagliata, o addirittura volti "sfocati".⁵ o anche volti "sfocati".⁶

Per la maggior parte dei formati di file aperti, tuttavia, è disponibile un software per esaminare ed eventualmente rimuovere i metadati.

pagina
185

_pagina
24

3. Deblock Fabrice, 2006, *Quand les documents Word trahissent la confidentialité* [<https://web.archive.org/web/20190913142445/http://www.journaldunet.com/solutions/0603/060327-indiscretions-word.shtml>].

4. Big Browser, 2012, *Vice de forme - L'errore che ha portato all'arresto di John McAfee* [https://www.lemonde.fr/big-browser/article/2012/12/12/vice-de-forme-la-bourde-qui-a-mene-a-l-arrestation-de-john-mcafee_5986399_4832693.html].

5. Esistono anche motori di ricerca di metadati, come *Stolen Camera Finder* [<https://www.stolencamerafinder.com/>], ad esempio.

6. Maximillian Dornseif e Steven J. Murdoch, 2004, *Hidden Data in Internet Published Documents* [<http://events.ccc.de/congress/2004/fahrplan/files/316-hidden-data->

slides.pdf].

Software dannoso, bug e altre spie

Ogni sistema operativo lascia tracce, almeno quando è in funzione. Oltre a queste tracce, sui nostri computer possiamo trovare tutta una serie di *bug*. Possono essere installati a nostra insaputa (consentendoci, ad esempio, di recuperare password o contatti e-mail), oppure possono essere sistematicamente presenti nel software che installiamo.

Queste cimici possono essere utilizzate in una varietà di tecniche di sorveglianza, da Dalla "lotta alla pirateria" del software proprietario, alla raccolta di dati per lo *spam* e altre truffe, alla registrazione mirata di persone, pagina 39. ¹e altre truffe.

La portata di questi dispositivi aumenta drasticamente non appena il computer è connesso a Internet. Sono facili da installare se non si fa nulla di particolare per proteggersi, e i dati raccolti possono essere recuperati a distanza.

Tuttavia, le persone che raccolgono queste informazioni sono ugualmente pericolose: dipende dal caso, dalle loro motivazioni e dai loro mezzi. Autori di violenza domestica ²GAFAM ³ che tracciano i dati degli utenti di Internet a fini pubblicitari, i gendarmi di Saint-Tropez o la *National Security Agency* degli Stati Uniti... tutte queste persone o strutture sono spesso in competizione tra loro e non formano un insieme coerente.

Per accedere ai nostri computer, non tutti hanno accesso agli stessi mezzi o agli stessi strumenti: ad esempio, lo spionaggio industriale è uno dei motivi principali della sorveglianza più o meno legale. ⁴e, nonostante le apparenze ⁵non pensate che Microsoft stia dando tutti i trucchi del mestiere alla polizia francese.

3.1 Contesto legale

Tuttavia, le forze dell'ordine e i servizi segreti francesi hanno ora i mezzi per impostare una sorveglianza informatica completa nella più completa legalità, utilizzando diverse delle "cimici" presentate di seguito.

1. *Lo spam* è una comunicazione elettronica non richiesta, di solito.

2. Catherine Armitage, 2014, *Spyware's role in domestic violence* [<https://www.theage.com.au/technology/technology-news/spywares-role-in-domestic-violence-20140321-358sj.html>] parla dell'uso di *malware* e altri strumenti tecnologici da parte degli autori di violenza domestica. (in).

3. GAFAM è l'acronimo delle cinque grandi società statunitensi - Google, Apple, Facebook, Amazon e Microsoft - che dominano il mercato digitale.

4. Per avere un'idea delle problematiche legate allo spionaggio industriale: Wikipedia, 2014, *Spionaggio industriale* [https://fr.wikipedia.org/wiki/Espionnage_industriel].

5. Microsoft, in collaborazione con Interpol, ha prodotto un toolbox chiamato COFEE (Com-Forensic Evidence Extractor) a disposizione delle forze di polizia di quindici Paesi. Korben, 2009, *Cofee - La clé sécurité de Microsoft vient-d'apparaître sur-la-toile.html* [<https://korben.info/cofee-la-cle-securite-de-microsoft-vient-d-apparaître-sur-la-toile.html>].

La legge del 2016 "che rafforza la lotta contro la criminalità organizzata, il terrorismo e il loro finanziamento e migliora l'efficienza e le garanzie della procedura penale"⁶ include disposizioni legali che consentono l'installazione di microspie per registrare e comunicare ciò che viene colpito sullo schermo o ciò che le varie periferiche (tastiera, webcam, scanner, cellulare...) trasmettono al computer.

L'"installazione" di queste cimici è autorizzata, a distanza o entrando nell'abitazione della persona monitorata per installare gli strumenti necessari.

⁷ Il juge des libertés et de la détention (giudice della libertà e della custodia) può richiederlo durante le indagini preliminari e in flagranza; il juge d'instruction (giudice istruttore) durante le inchieste giudiziarie.⁸ Queste misure si applicano non solo agli atti di "terrorismo" (come la "proliferazione di armi di distruzione di massa"), ma anche a una serie di reati commessi da più persone ("bande organizzate"). Questi possono andare dal favoreggiamento della "circolazione e del soggiorno illegale di uno straniero in Francia", all'"organizzazione criminale" di una "organizzazione criminale".

"distruzione, degrado e deterioramento della proprietà".⁹

La legge sull'intelligence del 2015¹⁰ conferisce più o meno gli stessi poteri¹¹ ai "servizi di intelligence specializzati" di "ricercare, raccogliere, utilizzare e mettere a disposizione del Governo informazioni relative a questioni geopolitiche e strategiche, nonché minacce e rischi che possono influire sulla vita della Nazione".¹²

3.2 Malware

Software dannoso¹³ (noto anche come *malware*) è un software sviluppato allo scopo di causare danni: raccogliere informazioni, ospitare informazioni illegali, trasmettere spam e *così via*. I virus informatici, i worm, i trojan, gli *spyware*, i *rootkit* e i *keylogger* fanno tutti parte di questa famiglia. Alcuni programmi possono appartenere a più di una di queste categorie contemporaneamente.

pagi

na

35

3.2.1 Sfruttare le vulnerabilità

Per installarsi su un computer, alcuni malware sfruttano le vulnerabilità del sistema operativo o delle applicazioni.¹⁴ o nelle applicazioni. Si basano su errori di progettazione o di programmazione per dirottare il flusso del programma a proprio vantaggio. Purtroppo, tali "falle di sicurezza" sono state riscontrate in moltissimi programmi software e se ne scoprono sempre di nuove, sia da parte di chi cerca di correggerle sia da parte di altri che cercano di sfruttarle.

6. Légifrance, 2016, *loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale* [<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032627231/>].

7. Légifrance, 2019, *Code de procédure pénale*, articolo 706-102-1 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624/2019-06-01/].

8. Légifrance, 2019, *Code de procédure pénale*, articolo 706-95-12 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270130/2019-06-01/].

9. Légifrance, 2017, *Code de procédure pénale*, articoli 706-73 e 706-73-1 [https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006138138/].

10. Légifrance, 2015, *loi n° 2015-912 du 24 juillet 2015 relative au renseignement* [<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899/>].

11. Légifrance, 2017, *Code de la Sécurité Intérieure*, articolo L853-2 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043887476/].

12. Légifrance, 2015, *Code de la Sécurité Intérieure*, articolo L811-2 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939233/].

13. L'intera sezione è in gran parte ispirata al passaggio dedicato all'argomento nella *Guida all'autodifesa con sorveglianza* [<https://ssd.eff.org/fr/module/comment-puis-je-me-prot%C3%A9ger-anti-malware>] della *Electronic Frontier Foundation*.

14. Secondo l'*Internet Storm Center* [<https://isc.sans.edu/survivaltime.html>], entro il 2021, un sistema operativo su cui non sono stati installati gli aggiornamenti di sicurezza sarà compromesso in meno di un'ora se collegato direttamente a Internet.

3.2.2 Ingegneria sociale

Un altro metodo comune è quello di invogliare l'utente del computer a lanciare il malware nascondendolo in un software apparentemente innocuo. Ad esempio, su un sito di social media legato alla rivoluzione siriana, un semplice link a un video ha portato gli utenti a scaricare un virus contenente un *keylogger*.¹⁵

Gli avversari non hanno quindi bisogno di trovare gravi vulnerabilità nel software comune. È particolarmente difficile assicurarsi che i computer condivisi da molte persone, o i computer in luoghi pubblici come una biblioteca o un cybercafé, non siano stati corrotti: basta infatti una sola persona un po' meno vigile per essere ingannati...

3.2.3 Camouflage

Inoltre, la maggior parte del malware "serio" non lascia segni immediatamente visibili della sua presenza e può persino essere molto difficile da rilevare. Forse il caso più complicato è quello delle vulnerabilità precedentemente sconosciute, chiamate

"vulnerabilità zero-day"¹⁶ Si tratta di vulnerabilità che il software antivirus difficilmente riconoscerebbe, poiché non sono ancora state catalogate. Questo è esattamente il tipo di sfruttamento delle vulnerabilità zero-day che VUPEN ha venduto all'NSA nel 2012.¹⁷

Il malware può essere nascosto in punti insospettabili del computer: ad esempio, i processori Intel hanno recentemente incluso un Management Engine (ME). Nel 2017 sono state scoperte diverse vulnerabilità di sicurezza nel firmware di questo motore di gestione.

¹⁸ Permettono l'installazione di malware completamente impercettibili che resistono agli aggiornamenti del sistema operativo e hanno accesso all'intero processore e alla RAM.¹⁹

3.2.4 Capacità

Questi programmi possono essere utilizzati per eseguire un'ampia gamma di operazioni: ottenere numeri di carte di credito o password, inviare spam, contribuire ad attaccare un server saturandolo di richieste e *così via*. Possono anche utilizzare il microfono, la webcam o altre periferiche del computer. Esiste un vero e proprio mercato specializzato dove è possibile acquistare tali programmi, personalizzati per diversi scopi.

Ma possono anche essere utilizzati per spiare organizzazioni o individui specifici.²⁰ per esempio, esfiltrare documenti memorizzati sul computer (anche documenti criptati, se sono stati decriptati in qualche momento), o distruggendo i dispositivi di anonimizzazione su Internet.

15. Eva Galperin *et al*, 2014, *Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campagne* [https://www.eff.org/files/2013/12/28/quantum_of_surveillance4d.pdf].

16. Wikipedia, 2016, *Zero-day vulnerabilità* [https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_zero-day].

17. Grégoire Fleurot, 2013, *Espionnage : Vupen, l'entreprise française qui bosse pour la NSA* [<https://www.slate.fr/france/77866/vupen-nsa-espionnage-exploits>].

18. Guillaume Louel, 2017, *New Intel ME security flaw!*, Hardware.fr [<https://www.hardware.fr/news/15297/new-security-flaw-intel-me.html>].

19. Mark Ermolov, Maxim Goryachy, 2018, *How to Hack a Turned-off Computer, or Running Unsigned Code in Intel ME*, blackhat.com [<https://www.blackhat.com/docs/eu-17/materials/eu-17-Goryachy-How-To-Hack-A-Turned-Off-Computer-Or-Running-Unsigned-Code-Intel-Management-Engine-wp.pdf>] (in inglese).

20. Ad esempio, un attacco mirato alle istituzioni georgiane, attribuito alla Ministero della Giustizia della Georgia e altri, 2012, *Cyber Espionage Against Georgian Government* [<https://web.archive.org/web/20200601112146/https://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf>].



PRECISIONE

Per fare un esempio dagli Emirati Arabi Uniti, un attivista per i diritti umani, Ahmed Mansour, è stato vittima di un attacco mirato al suo smartphone²¹. Gli è stato inviato un SMS contenente un link a un virus. Questo virus permetteva alla persona che lo controllava di utilizzare la fotocamera, il microfono e di monitorare le attività del telefono della vittima in qualsiasi momento. L'attacco è stato sventato e analizzato grazie a Citizen Lab.

[pagina

31

I servizi segreti e i poliziotti francesi sono legalmente autorizzati a utilizzare questo software, il che significa sicuramente che lo possiedono. Una suite di software spia attribuita ai servizi segreti francesi è stata scoperta, tra l'altro, in Iran.

22.

3.2.5 Rischio e prevenzione

Nessuno sa quanti computer siano infettati da malware, ma alcuni stimano che il 20-50% dei computer Windows sia infetto.²³ È quindi molto probabile che si trovi del malware su qualsiasi Windows che si pensa di utilizzare. Finora, l'utilizzo di un sistema operativo minoritario (come GNU/Linux) ha ridotto in modo significativo il rischio di infezione, poiché questi sistemi hanno meno probabilità di essere presi di mira, in quanto lo sviluppo di *malware* specifici è economicamente meno redditizio.

Ecco alcuni modi per limitare i rischi:

- non installare (o utilizzare) alcun software proveniente da fonti sconosciute: non fidatevi del primo sito web che incontrate²⁴;
- prestare attenzione agli avvisi del sistema operativo che segnalano che il software non è sicuro o che è necessario un aggiornamento della sicurezza;
- infine, ridurre la possibilità di installare nuovo software: limitando l'uso dell'account di amministrazione e il numero di persone che vi hanno accesso.

3.3 Attrezzatura per spie

Gli avversari che vogliono mettere le mani sui segreti contenuti nei nostri computer possono usare il malware, come abbiamo appena visto, ma possono altrettanto facilmente usare lo spyware. Questi gadget non possono competere con quelli di James Bond!

[pagina

32

Esiste un'intera gamma di hardware più o meno facilmente reperibili che possono essere utilizzati per intromettersi o esfiltrare informazioni da un computer, praticamente a qualsiasi livello. In seguito alla pubblicazione di documenti riservati della NSA da parte di Edward Snowden, il giornale tedesco *Der Spiegel* ha pubblicato un vero e proprio catalogo dello spionaggio informatico.²⁵

21. Andréa Fradin, 2016, "Pegasus", l'arma di un'oscura azienda israeliana che fa tremare Apple [https://www.nouvelobs.com/rue89/rue89-surveillance/20160826.RUE3689/pegasus-l-arme-d-u-ne-israeliano-azienda-fantasy-that-shakes-apple.html].

22. Martin Untersinger, 2015, *Dino, le nouveau programme-espion développé par des francophones*, Le Monde.fr [https://www.lemonde.fr/pixels/article/2015/06/30/dino-le-nouveau-programme-espion-developpe-par-des-francophones_4664675_4408996.html].

23. SafetyDetectives, 2021, *Statistiche e tendenze: antivirus e sicurezza informatica 2021* [https://fr.safetydetectives.com/blog/antivirus-statistics-it/#review-4].

24. Questo consiglio vale anche per gli utenti GNU/Linux. Nel dicembre 2009, il progetto *gnome*-Il sito web *look.org* ha distribuito un *malware* [https://lwn.net/Articles/367874/] presentato come screensaver. Era scaricabile come pacchetto Debian da insieme ad altri screensaver e sfondi.

25. Der Spiegel, 2013, *Grafico interattivo: Il catalogo delle spie della NSA* [https://www.spiegel.de/international/world/a-941262.html].

Senza entrare in un elenco esaustivo, questo catalogo comprende connettori USB falsi, che consentono di ritrasmettere sotto forma di onde radio ciò che li attraversa; piccoli chip installati nei cavi che collegano lo schermo o la tastiera al computer, che fanno lo stesso, in modo che gli avversari possano captare ciò che state digitando o vedendo da una distanza di sicurezza. Infine, c'è una pletera di spyware installati nel computer, sul disco rigido, nella memoria o sulla tastiera.

firmware, ecc.

pagina 20

Il quadro non è molto incoraggiante: un controllo meticoloso del computer richiederebbe di smontarlo, con pochissime possibilità di riassembly in modo che possa funzionare di nuovo. Una risposta potrebbe essere quella di tenere il computer con sé o in un luogo che si ritiene sicuro. Detto questo, non tutte queste attrezzature sono disponibili per tutti i tipi di avversari. Inoltre, non ci sono prove che l'uso di tali apparecchiature sia diventato comune, per ragioni di costo, installazione o altri parametri.

Diamo un'occhiata più da vicino ai *keylogger*, che possono essere classificati sia come spyware che come malware.

3.4 Keylogger o registratori di battute di tastiera

I *keylogger*, che possono essere "hardware" o "software", hanno la funzione di registrare furtivamente tutto ciò che viene digitato sulla tastiera di un computer, per poter trasmettere questi dati all'agenzia o alla persona che li ha installati.²⁶

Una volta installati, la loro capacità di registrare le battute dei tasti mentre vengono digitati su

Una tastiera bypassa quindi qualsiasi dispositivo di crittografia e consente l'accesso diretto a frasi, password e altri dati sensibili a pagina 47.

I *keylogger* hardware sono dispositivi collegati alla tastiera o al computer. Possono avere l'aspetto di adattatori, schede di espansione all'interno del computer (PCIe o mini PCIe) o addirittura essere integrati nella tastiera.²⁷ Sono quindi difficili da individuare se non li si cerca in modo specifico...

Nel caso di una tastiera wireless, non c'è nemmeno bisogno di un *keylogger* per recuperare i tasti digitati: basta captare le onde emesse dalla tastiera per comunicare con il ricevitore e quindi violare la crittografia utilizzata, che nella maggior parte dei casi è piuttosto debole.²⁸ Da una distanza minore, è comunque possibile registrare e recuperare i dati.

decodificare le onde elettromagnetiche emesse dalle tastiere cablate, comprese quelle integrate nei computer portatili...

I *keylogger* software sono molto più diffusi, perché possono essere installati in remoto (tramite una rete, un malware o altro) e in genere non richiedono l'accesso fisico al computer per recuperare i dati raccolti (ad esempio, possono essere inviati periodicamente via e-mail). La maggior parte di questi programmi registra anche il nome dell'applicazione corrente, la data e l'ora di esecuzione e le sequenze di tasti ad essa associate.

Nel 2012 la polizia italiana ha utilizzato un software *keylogger* per indagare su una stazione radio anarchica.²⁹ Un agente di polizia statunitense è stato condannato per aver installato

26. Elettronica Frontiera Foundation, 2021, *Keylogger* [<https://web.archive.org/web/20220928165559/https://ssd.eff.org/fr/glossary/enregistreur-de-frappe>].

27. Molti modelli sono disponibili al banco, ad esempio: un adattatore USB [<https://web.archive.org/web/20210611153039/https://www.ebay.fr/itm/224463276889?hash=item34430dcb59%3Ag%3Ay8QAAOSwFpddVMrk>] o un chip tastiera [<https://web.archive.org/web/20210611153634/https://www.ebay.fr/itm/224463702020?hash=item3443144804%3Ag%3ARWgAAOSwQKdcrmjy>].

28. Tom Espiner, 2007, *Microsoft wireless keyboard hacked from 50 metres* [<https://www.zdnet.co.uk/home-and-office/networking/microsoft-wireless-keyboard-hacked-from-50-metres/>].

29. Croce Nera Anarchica, 2018, *Resoconto udienze Scripta Manent aprile-luglio* [<https://www.autistici.org/cna/2018/09/13/resoconto-enze-scripta-manent-aprile-luglio/>] (in italiano).

un *keylogger* sul computer di lavoro della moglie, che lavorava presso il tribunale³⁰.

L'unico modo per individuare i *keylogger* hardware è quello di familiarizzare con questi dispositivi e di effettuare regolarmente un controllo visivo della macchina, dentro e fuori. Anche se il catalogo dell'NSA pubblicato alla fine del 2013 riporta la difficoltà di individuare dispositivi di keylogging appena più grandi di un'unghia. Per i *keylogger* software, gli indizi sono gli stessi di altre minacce informatiche.

pagi

3.5 Piattaforme di indagine digitale

na

32

I poliziotti dispongono di hardware e software specifici per estrarre e analizzare il contenuto di dischi, chiavette USB o schede SD, nonché il contenuto della memoria ad accesso casuale dei computer.³¹ dei computer. Questi vengono forniti da aziende specializzate in digital forensics.³² I loro software possono, ad esempio, generare un riepilogo grafico dell'utilizzo del computer, effettuare ricerche per parola chiave, ripristinare i dati cancellati o decifrare le password. Tali piattaforme esistono anche per gli *smartphone*³³.

pagi

3.6 Stampa dei problemi?

na

18

Pensavamo di aver scoperto tutte le sorprese che i nostri computer ci riservano... ma anche le stampanti cominciano ad avere i loro piccoli segreti.

3.6.1 Un po' di steganografia

pagi

na

42

Prima cosa da sapere: molti stampatori di fascia alta firmano i loro lavori³⁴. Questa firma steganografica³⁵ La firma steganografica, nota come *watermarking*, si basa su lievissimi dettagli di stampa, spesso invisibili a occhio nudo, che vengono inseriti in ogni documento. Essi consentono di identificare con certezza la marca, il modello e, in alcuni casi, il numero di serie della macchina utilizzata per stampare un documento. Diciamo "con certezza", perché questi dettagli servono proprio a questo: a individuare la macchina dal suo lavoro.

In effetti, questo è uno dei modi in cui è stata trovata la persona che nel giugno 2017 ha rilasciato documenti *top secret della NSA* sull'hackeraggio delle elezioni americane del 2016 da parte di hacker russi. I segni della stampante utilizzata per immaginare i documenti riservati erano ancora presenti quando sono stati pubblicati dal giornale *The Intercept*.³⁶

Sui documenti rimangono anche altri tipi di usura, e questo vale per tutte le stampanti. Con l'età, infatti, le testine di stampa si spostano, compaiono lievi errori, le parti si usurano e tutto ciò crea gradualmente una firma specifica della stampante. Proprio come la balistica può identificare un'arma da fuoco da un proiettile, così è possibile

30. Jerome Vosgien, 2019, *Un policier installa un keylogger sul computer della moglie* [<http://news.sophos.com/en-fr/2014/01/13/policier-installe-keylogger-ordinateur-epouse/>].

31. Cindy Casey, 2019, *RAM Analysis Memory Forensics* [[https://www.bucks.edu/media/bccc_medialibrary/con-ed/itacademy/fos2019/Casey-RAM-Forensics-\(1\).pdf](https://www.bucks.edu/media/bccc_medialibrary/con-ed/itacademy/fos2019/Casey-RAM-Forensics-(1).pdf)] (in inglese).

32. Wikipedia, 2021, *Informatica forense* [https://fr.wikipedia.org/wiki/Informatique_l%C3%A9_gale].

33. Wikipedia, 2021, *Cellebrite* [<https://fr.wikipedia.org/wiki/Cellebrite>].

34. La *Electronic Frontier Foundation* cerca di mantenere un [elenco di produttori e modelli di stampanti indiscrete](https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots) [<https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots>].

35. Per saperne di più sulla steganografia, si consiglia di leggere questo articolo di [Wikipedia](https://fr.wikipedia.org/wiki/St%C3%A9ganographie), 2014, *Steganography* [<https://fr.wikipedia.org/wiki/St%C3%A9ganographie>].

36. Robert Graham, 2017, *Come The Intercept ha fatto uscire allo scoperto il vincitore del reality* [<https://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html>].

utilizzare questi difetti per identificare una stampante da una pagina che è stata emessa.

Per proteggersi in parte da questo, è interessante sapere che i dettagli dell'impressione non resistono a ripetute fotocopie: fotocopiare la pagina stampata, poi fotocopiare la fotocopia risultante, basta a far scomparire tali firme. D'altra parte... siamo sicuri di lasciarne altre, perché le fotocopiatrici hanno difetti, e talvolta firme steganografiche, simili a quelle delle stampanti. Insomma, stiamo girando in tondo, e il problema diventa scegliere *quali* tracce lasciare...

3.6.2 La memoria, di nuovo...

Alcune stampanti sono sufficienti per essere più vicine a un vero computer che a un tampone d'inchiostro. Possono creare problemi anche su un altro piano, poiché sono dotate di una

RAM: come quella del PC, tiene traccia dei documenti che sono stati elaborati per tutto il tempo in cui la macchina è accesa... o finché un documento non sovrascrive.

La maggior parte delle stampanti laser ha una capacità di memoria di circa dieci pagine. I modelli più recenti, o quelli con scanner integrato, possono contenere diverse migliaia di pagine di testo...

Peggio ancora: alcuni modelli, spesso utilizzati per le grandi tirature come nel caso della I centri di fotocopiatrice, a volte, hanno dischi rigidi interni, ai quali l'utente non ha accesso, e che conservano tracce - e questa volta, anche dopo lo spegnimento di

Alcune illusioni sulla sicurezza

Bene. Stiamo iniziando a capire le tracce che possiamo lasciare in modo invano e le informazioni che i malintenzionati potrebbero recuperare.

Non resta che mettere in discussione alcune idee preconcrete.

4.1 Software proprietario, open source, libero

Come abbiamo visto, il software può fare molte cose che non vogliamo che faccia. È quindi essenziale fare il possibile per ridurre questo problema. Da questo punto di vista, il software libero è molto più affidabile di quello proprietario: vedremo perché.

4.1.1 La metafora della torta

Per capire la differenza tra software libero e software proprietario, spesso si usa la metafora della torta. Per preparare una torta, occorre una ricetta: un elenco di istruzioni da seguire, di ingredienti da utilizzare e di processi di trasformazione da eseguire. Allo stesso modo, la ricetta di un software si chiama "codice sorgente". È scritto in un linguaggio progettato per essere compreso dagli esseri umani. Questo La ricetta viene poi trasformata in un codice che può essere compreso dall'elaboratore, proprio come la preparazione di una torta ci dà la possibilità di mangiarla.

Il software proprietario è disponibile solo "pronto da mangiare", come una torta industriale senza ricetta. È quindi molto difficile conoscere gli ingredienti: si può fare, ma il processo è lungo e complicato. Inoltre, rileggere una sequenza di diversi milioni di addizioni, sottrazioni, letture e scritture in memoria, per ricostruirne lo scopo e il funzionamento, è tutt'altro che la prima cosa che si vorrebbe fare su un computer.

Il software libero, invece, viene fornito con la propria ricetta per chiunque voglia capire o modificare il funzionamento del programma. È quindi più facile sapere cosa si sta dando in pasto al processore e quindi cosa succederà ai dati.

4.1.2 Software proprietario: blind trust

Il software proprietario è quindi un po' come una scatola sigillata: si può vedere che fa quello che si vuole, ha una bella interfaccia grafica, ecc. *Ma non si possono conoscere i dettagli del suo funzionamento.* Ma non si può sapere nei dettagli come funziona. Non sappiamo se fa solo quello che gli chiediamo o se fa anche altre cose. Per scoprirlo, dovremmo essere in grado di studiare il suo funzionamento, cosa difficile da fare senza il suo codice sorgente... quindi non ci resta che fidarci *ciecamente*.

Windows e macOS, i primi, sono enormi scatole ermeticamente sigillate in cui sono installate altre scatole altrettanto ermeticamente sigillate (da Microsoft Office agli antivirus...) che possono fare molte cose diverse da quelle che chiediamo loro.

In particolare, possono fornire informazioni che questi programmi software raccoglierebbero su di noi, o addirittura consentire l'accesso all'interno del computer. Per esempio, con le backdoor incluse nel software¹ incluse nel software, che chi ha la chiave potrebbe usare per entrare nel nostro computer. Poiché è impossibile sapere come è scritto il sistema operativo, tutto è immaginabile.

È un'illusione per la sicurezza affidare la riservatezza e l'integrità dei nostri dati a programmi di cui siamo obbligati a fidarci a occhi chiusi. E l'installazione di altri software che dichiarano sulla confezione di occuparsi di questa sicurezza per noi, quando il loro funzionamento non è più trasparente, non può risolvere il problema.

1.3 Il vantaggio di avere la ricetta: il software libero

La maggiore fiducia che possiamo avere in un sistema *libero* come GNU/Linux è dovuta principalmente al fatto che abbiamo la "ricetta" per realizzarlo. Ma non dimentichiamo che non c'è nulla di magico: il software libero non lancia alcun "incantesimo di protezione" sui nostri computer.

Tuttavia, GNU/Linux offre maggiori possibilità di rendere i computer un po' più sicuri da usare, non da ultimo rendendo possibile la configurazione del sistema fin nei minimi dettagli. Troppo spesso questo richiede un know-how relativamente specialistico, ma almeno è possibile.

Inoltre, il modo in cui viene prodotto il software open-source è difficilmente compatibile con l'introduzione di backdoor: si tratta di un processo di produzione collettivo, piuttosto aperto e trasparente, che coinvolge un'ampia varietà di persone. Non è quindi facile per i malintenzionati introdurre accessi segreti.

Tuttavia, fate attenzione al software descritto come *open source*. Questi ultimi danno anche accesso alla loro "ricetta", ma i loro metodi di sviluppo sono più chiusi e opachi. La modifica e la redistribuzione di questi software sono nel peggiore dei casi vietate, nel migliore dei casi formalmente autorizzate, ma rese molto difficili nella pratica. Poiché solo il team che sta dietro al software potrà partecipare al suo sviluppo, possiamo presumere che in pratica nessuno leggerà il suo codice sorgente in dettaglio... e quindi nessuno verificherà realmente il suo funzionamento.

È il caso, ad esempio, di TrueCrypt, il cui sviluppo è stato interrotto nel maggio 2014. Si trattava di un software di crittografia il cui codice sorgente era disponibile, ma il cui sviluppo era chiuso e la cui licenza limitava la modifica e la redistribuzione. Ai nostri fini, il fatto che il software sia *open source* dovrebbe essere visto più come un punto di vendita che come una garanzia di fiducia.

Solo che... la distinzione tra software libero e *open source* è sempre più sfumata: le persone impiegate da Intel, Google e altri scrivono gran parte del software libero più importante, e non sempre si guarda con attenzione a ciò che scrivono. Per esempio, ecco le statistiche delle organizzazioni che impiegano le persone che sviluppano il kernel di Linux (che è libero). Sono espresse come percentuale del numero totale di linee di codice sorgente modificate in un determinato periodo.² :

1. Sul tema delle "backdoor", si veda l'articolo di Wikipedia, 2014, *Backdoor* [https://fr.wikipedia.org/wiki/Porte_d%C3%A9rob%C3%A9e].

2. Jonathan Corbet, 2021, *Alcune statistiche sullo sviluppo di 5.12*, Linux Weekly News [<https://lwn.net/Articles/853039>].

Organizzazioni	Percentuale
Linaro	17,4 %
Intel	11,5 %
Red Hat	5,5 %
Google	4,2 %
(Sconosciuto)	4,2 %
NVIDIA	4,1 %
(Nessuno)	3,8 %
Realtek	3,3 %
SUSE	2,9 %
MediaTek	2,9 %
Braccio	2,3 %
Marvell	2,2 %
AMD	2,1 %
Pengutronix	2,0 %
<i>ecc.</i>	

Non è quindi impossibile che qualcuno che ha scritto parte del software in un angolo, e che gode della fiducia della "comunità Open Source", possa aver integrato parti di codice dannose. L'NSA (un'agenzia di intelligence statunitense) ha è stato così in grado di creare e far convalidare uno standard crittografico contenente una vulnerabilità che consente di aggirare la crittografia di alcuni protocolli sicuri.³

Se utilizzate solo software libero fornito da una distribuzione GNU/Linux non commerciale come Debian o Tails, è improbabile che ciò accada, ma è una possibilità. In questo caso, potete fare affidamento sulle persone che lavorano alla distribuzione per studiare il funzionamento dei programmi in essa integrati.

Tuttavia, questa fiducia può essere valida solo se rimaniamo vigili su ciò che installiamo sul nostro sistema. Ad esempio, su Debian, i pacchetti ufficiali della distribuzione sono "Questo permette di verificarne l'origine. Ma se si installano pacchetti o estensioni di Firefox trovati su Internet senza verificarli, si corre il rischio di tutti i rischi menzionati per il malware.

Per concludere: *gratuito o meno, non esiste un singolo software che possa garantire la privacy dei nostri dati*; esistono solo pratiche associate all'uso di determinati software. Un software scelto perché ci sono elementi che ci permettono di riporre un certo livello di fiducia in esso.

4.2 La password di un account non protegge i suoi dati

Tutti i sistemi operativi recenti (Windows, macOS, GNU/Linux, *ecc.*) offrono la possibilità di avere diversi account utente sullo stesso computer. Ma è importante ricordare che le password che talvolta proteggono questi account non sono una garanzia di riservatezza dei dati.

Certo, è comodo avere un proprio spazio, con le proprie impostazioni (segnalibri, sfondo, *ecc.*), ma chi vuole accedere a tutti i dati del computer non ha problemi: semplicemente ricollegandosi al computer, sarà possibile accedere a tutti i dati del computer.

computer, sarà in grado di accedere a tutti i dati presenti sul computer. il disco rigido su un altro computer, o avviandolo con un altro sistema operativo, pag. 22 avrebbe accesso a tutti i dati scritti su quel disco rigido.

Quindi, anche se l'uso di account e password separati può avere alcuni vantaggi (come la possibilità di bloccare lo schermo quando ci si assenta per qualche minuto), è importante tenere presente che non protegge realmente i dati.

3. Julien Lausson, 2013, *La NSA è sospettata di aver manomesso uno standard crittografico* [<http://www.numerama.com/politique/26979-la-nsa-est-suspectee-d-avoir-altere-un-standard-cryptog-raphique.html>].

4.3 Informazioni sulla "cancellazione" dei file

Abbiamo già detto che il contenuto di un file diventato inaccessibile o invisibile non è scomparso nel nulla. Ora spiegheremo perché.

pagi

na

24

4.3.1 L'eliminazione di un file non cancella il suo contenuto...

... e può essere molto facile da trovare.

Infatti, quando si "cancella" un file mettendolo nel *Cestino* e poi svuotandolo, si dice semplicemente al sistema operativo che il contenuto di questo file non è più di interesse per l'utente. Il sistema cancella quindi la sua voce nell'indice dei file esistenti. Il sistema può quindi riutilizzare lo spazio occupato da questi dati per scrivere qualcos'altro.

Ma possono passare settimane, mesi o anni prima che questo spazio venga *effettivamente* utilizzato per nuovi file e che i vecchi dati scompaiano. Nel frattempo, se si guarda direttamente a ciò che è scritto sul disco rigido, si trova il contenuto dei file "cancellati". Si tratta di un'operazione abbastanza semplice, automatizzata da numerosi programmi di "recupero" o "ripristino" dei dati.⁴

4.3.2 L'inizio della soluzione: riscrivere i dati più volte

Una volta che i nuovi dati sono stati riscritti nello spazio del disco rigido, diventa difficile trovare quelli che c'erano prima. Ma questo non significa che sia impossibile: quando il computer riscrive 1 su 0, è più simile a 0,95, e quando riscrive 1 su 1, è più simile a 1,05...⁵... allo stesso modo in cui si può leggere su un blocco note ciò che è stato scritto su una pagina strappata, grazie alle depressioni create sulla pagina bianca sottostante.

D'altra parte, diventa molto difficile, se non impossibile, recuperarli quando vi si riscrive sopra più volte con dati casuali. Il modo migliore per rendere inaccessibile il contenuto di questi file "cancellati" è quindi quello di utilizzare un software che si assicuri di riscriverli più volte. Questo è noto come

"cancellare" i dati.

4.3.3 Alcuni limiti alle possibilità di riscrittura

Anche se è possibile riscrivere più volte in una determinata posizione del disco rigido per rendere inaccessibili i dati in essa contenuti, ciò non garantisce la loro completa scomparsa dal disco.

Dischi "moderni"

I dischi odierni riorganizzano il loro contenuto in modo "intelligente": una parte del disco viene riservata per sostituire i posti che diventerebbero difettosi. Queste operazioni di sostituzione sono difficili da individuare, quindi non si può mai essere sicuri che il punto in cui si sta riscrivendo sia effettivamente quello in cui il file "cancellato" è stato scritto in origine.

Nel caso delle chiavette USB e dei dischi SSD (*Solid State Drive*), si può persino dire che, nella maggior parte dei casi, si sta riscrivendo in una posizione diversa. La memoria *flash* utilizzata dalle chiavette USB e dai dischi SSD smette di funzionare correttamente dopo un certo numero di volte.

4. È il caso, ad esempio, di **PhotoRec** [https://www.cgsecurity.org/wiki/PhotoRec_FR].

5. Peter Gutmann, 1996, *Cancellazione sicura di dati da memorie magnetiche e a stato solido* [http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html].

scrittura⁶Questi contengono chip che riorganizzano automaticamente il loro contenuto, distribuendo le informazioni nel maggior numero possibile di luoghi diversi.

Tenendo conto di questi meccanismi, diventa difficile garantire che i dati che si desidera distruggere siano effettivamente scomparsi.

Tuttavia, aprire un disco rigido per esaminarne le viscere richiede tempo e notevoli risorse materiali e umane. Non tutti sono in grado di fare questo investimento, non sempre.

Per i chip di memoria *flash* su chiavetta USB o unità SSD, anche se non è immediato, l'operazione è molto più semplice: è sufficiente un saldatore e un dispositivo per leggere direttamente i chip di memoria. Quest'ultimo può essere acquistato per circa \$1,500.⁷

Sistemi di file

Anche se il contenuto di un file è stato perfettamente cancellato, possono rimanere tracce altrove, che possono essere dovute al file system.

In effetti, i file system odierni tengono traccia delle modifiche successive dei file

"log".
Questi file system sono quindi detti "registrato".

La registrazione è stata introdotta per migliorare la robustezza dei file system. Dopo un arresto improvviso del computer, consente al sistema di riprendere semplicemente le ultime operazioni eseguite, invece di dover setacciare l'intero disco per correggere le incongruenze. Ma può anche lasciare una traccia di file che si vorrebbe veder scomparire.



PRECISIONE

Windows utilizza i file system NTFS e ReFS, che sono di tipo journaled. In GNU/Linux, ext4 è il file system più usato. Per impostazione predefinita, registra solo i nomi dei file e altri metadati, ma non il loro contenuto.

Alcuni file system hanno altre caratteristiche che lasciano il segno:

- *snapshot* possibili con i moderni file system (NTFS, ReFS, Btrfs, ecc.);
- caching in cartelle temporanee con file system di rete (come NFS) ;
- ecc.

Quello che non sappiamo

Per quanto riguarda i CD-RW o i DVD±RW (riscrivibili), sembra che non sia stato condotto alcuno studio serio sull'efficacia della riscrittura per rendere i dati irrecuperabili. Le raccomandazioni attuali sono quindi di distruggere metodicamente i supporti di questo tipo che possono aver contenuto dati da cancellare.⁸

6. Wikipedia, 2020, SSD [https://fr.wikipedia.org/wiki/SSD].

7. Il PC-3000 Flash [https://www.acelab.eu.com/pc3000flash.php] viene venduto come un strumento professionale per il recupero di dati da dispositivi flash danneggiati.

8. NIST, 2014, Linee guida per la sanificazione dei media [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf].

4.3.4 Tante altre volte, quando "cancelliamo"

È importante notare che i file non si eliminano semplicemente mettendoli nel *Cestino*. Ad esempio, quando si utilizza l'opzione "Cancella le mie tracce" nel browser Firefox, non si fa altro che eliminare i file. Sebbene i dati non siano più accessibili a Firefox, è ancora possibile accedervi direttamente dal disco rigido.

Infine, vale la pena sottolineare che *la riformattazione di un disco rigido non elimina il contenuto che vi si trovava*. Come l'eliminazione dei file, rende disponibile solo lo spazio in cui si trovava il contenuto, ma i dati rimangono fisicamente presenti sul disco finché non vengono sovrascritti. Allo stesso modo, distruggere il catalogo di una biblioteca non fa sparire i libri sugli scaffali.

Ciò significa che i file possono essere recuperati anche dopo la riformattazione, con la stessa facilità con cui sarebbero stati semplicemente "cancellati".⁹

4.3.5 E non lasciare tracce?

Purtroppo non esiste un modo semplice per risolvere radicalmente il problema. La soluzione meno difficile al momento è quella di utilizzare il computer dopo averlo avviato con un sistema *live* configurato per utilizzare solo la RAM, come Tails. In questo caso, è possibile non scrivere nulla sul disco rigido, né sulla memoria virtuale (*swap*), e conservare le informazioni solo nella RAM (quindi solo finché il computer rimane acceso).

4.4 Software portatile: una falsa soluzione

Il "software portatile" è un software che non è installato su un sistema operativo specifico, ma può essere avviato da una chiavetta USB o da un disco rigido esterno e quindi portato con sé, in modo da poterlo utilizzare su qualsiasi computer.

Tuttavia, a differenza dei sistemi *live*, questi programmi utilizzano il sistema operativo installato sul computer in cui devono essere utilizzati (nella maggior parte dei casi, sono progettati per Windows).

L'idea alla base è quella di garantire che abbiate sempre a portata di mano il software di cui avete bisogno, personalizzato in base alle vostre esigenze. Ma "portarsi dietro il proprio ufficio" non è necessariamente il modo migliore per preservare la riservatezza dei dati.

Ammettiamolo: questi programmi non proteggono le persone che li utilizzano più di quanto non faccia il software "non portatile".

4.4.1 Problemi principali

Queste soluzioni "chiavi in mano" pongono quindi alcuni problemi piuttosto spiacevoli.

Le tracce rimarranno sul disco rigido

Se il software è stato reso "portatile" correttamente, non dovrebbe lasciare alcuna traccia sul disco rigido del computer su cui viene utilizzato. Ma in realtà il software non ha mai il controllo assoluto. Dipende in larga misura dal sistema operativo.

su cui è impiegato, che potrebbe aver bisogno di scrivere memoria virtuale (*swap*) sul disco rigido, o di registrare varie tracce di ciò che fa nei suoi log e in altri "documenti recenti". Tutto questo rimarrà sul disco rigido.

9. Anche **PhotoRec** [https://www.cgsecurity.org/wiki/PhotoRec_FR] offre questo tipo di funzionalità.

Non c'è motivo di fidarsi di un sistema sconosciuto

Abbiamo già visto che molti sistemi non fanno quello che dovrebbero. Tuttavia, poiché il software portatile utilizzerà il sistema installato sul computer su cui viene lanciato, soffrirà di tutti i bug e di altri malware.

che potrebbero essere presenti.

Non sappiamo chi li abbia compilati né come.

Le modifiche apportate al software per renderlo portatile sono raramente controllate, e di solito non dagli stessi autori del software. Di conseguenza, è ancora più probabile che questo software contenga falle di sicurezza, introdotte per errore o deliberatamente, rispetto alle versioni non portabili.

In seguito, esamineremo i criteri da tenere in considerazione quando si sceglie il software da installare o scaricare.

Un modo per proteggere i dati: crittografia

La *crittografia* è la branca della matematica che si occupa specificamente della protezione dei messaggi. Fino al 1999, l'uso delle tecniche crittografiche era vietato al grande pubblico. Ora è diventato legale, tra l'altro per consentire ai commercianti di Internet di essere pagati senza che i numeri delle carte di credito dei loro clienti vengano rubati.

La *crittoanalisi* è il campo della "rottura" delle tecniche crittografiche, ad esempio per recuperare un messaggio che era stato protetto.¹

La protezione dei messaggi presenta tre aspetti:

- **riservatezza**: evitare occhi indiscreti ;
- **autenticità**: garantire la fonte del messaggio ;
- **integrità**: per garantire che il messaggio non sia stato modificato.

Si possono volere tutte e tre le cose allo stesso tempo, ma anche solo una o l'altra. Una persona che scrive un messaggio *confidenziale* può voler negare la paternità (e quindi che non possa essere *autenticato*). Possiamo anche immaginare di voler certificare la provenienza (*autenticità*) e l'*integrità* di un comunicato ufficiale che sarà distribuito pubblicamente (e quindi tutt'altro che *riservato*).

Nel seguito parleremo di *messaggi*, ma le tecniche crittografiche possono essere applicate a qualsiasi numero, e quindi a qualsiasi dato, una volta digitalizzato.

La crittografia non mira a nascondere i messaggi, ma a proteggerli. Per nascondere i messaggi è necessario utilizzare tecniche steganografiche.

(come quelli utilizzati dalle stampanti citate in precedenza, o addirittura alla crittografia ripudiabile), che non approfondiremo in questa sede.

pagina 36

pagina 52

5.1 Proteggere i dati da occhi indiscreti

La crittografia è il modo più serio per garantire che i dati possano essere compresi solo da chi "sa". I bambini che usano i codici per scambiarsi le parole, o i soldati che comunicano i loro ordini, lo hanno capito molto bene!

La crittografia di un file o di un supporto di memorizzazione lo rende illeggibile a chiunque non sia in possesso del codice di accesso (spesso una *passphrase*). Sarà

1. Per una buona panoramica dei vari metodi - noti come "attacchi" - comunemente utilizzati nella crittoanalisi, si rimanda alla pagina di [Wikipedia, 2020, Cryptanalysis \[https://fr.wikipedia.org/wiki/Cryptanalysis\]](https://fr.wikipedia.org/wiki/Cryptanalysis).

È ancora possibile accedere ai contenuti, ma i dati assomiglieranno a una serie di numeri casuali, rendendoli incomprensibili e inutilizzabili.

Spesso usiamo i termini "*criptare*" e "*decriptare*" invece di "*cifrare*" e "*decifrare*", il che può generare confusione. Tuttavia, preferiamo evitare l'anglicismo *crypter* e riservare *decrypt* all'operazione che consiste nel vanificare un sistema di cifratura (cioè "decifrare" un messaggio senza conoscere il codice segreto di cifratura).

5.1.1 Come funziona?

In linea di massima, esistono solo tre idee principali per capire come criptare i messaggi².

La prima idea: la *confusione*. La relazione tra il messaggio originale (non cifrato) e il messaggio cifrato deve essere oscurata. Un esempio molto semplice è il "cifrario di Cesare", che consiste nello spostare ogni lettera del testo in chiaro di tre caratteri dell'alfabeto:

testo in chiaro :	AS SAU T	IN	A	ORA
	↓↓↓↓↓	↓↓↓↓↓	↓↓↓	↓↓↓↓↓
testo cifrato:	DVVDXW	GDQV	XQH	KHXUH

A + 3 lettere =
D

Solo che con il cifrario di Cesare è facile analizzare le frequenze delle lettere e trovare le parole.

La seconda grande idea è la *diffusione*. Si tratta di spezzare il messaggio per renderlo più difficile da riconoscere. Un esempio di questa tecnica è la trasposizione in colonne. Per una diffusione a tre punti, dividiamo il testo in tre righe e lo trascriviamo colonna per colonna:

1	2	3	4	5	6							
A	S	S	A	U	T							
DANSU							IN					
↓												
LEI							HI					
EI							UI					
RI							EI					

→ distribuzione in 3 punti

1	2	3	4	5	6
ADE SA		SNE AS		UUR TNE	
H				U	

Quelli che chiamiamo *algoritmi di cifratura* sono le diverse tecniche utilizzate per trasformare il testo originale. Per quanto riguarda la *chiave di cifratura*, nel caso del cifrario di Cesare, ad esempio, è il numero di caratteri di offset (3, in questo caso) o, nella tecnica broadcast, il numero di righe nelle colonne. Il valore di questa chiave è variabile: avremmo potuto decidere di utilizzare colonne di 2 righe o un offset di 6 caratteri.

Questo ci porta alla terza grande idea: *il segreto sta solo nella chiave*. Dopo alcuni millenni, abbiamo capito che è una cattiva idea dare per scontato che nessuno sarà in grado di capire l'algoritmo di crittografia: prima o poi qualcuno lo capirà. È molto più facile tenere segreta una semplice chiave di crittografia o una passphrase che un intero algoritmo.

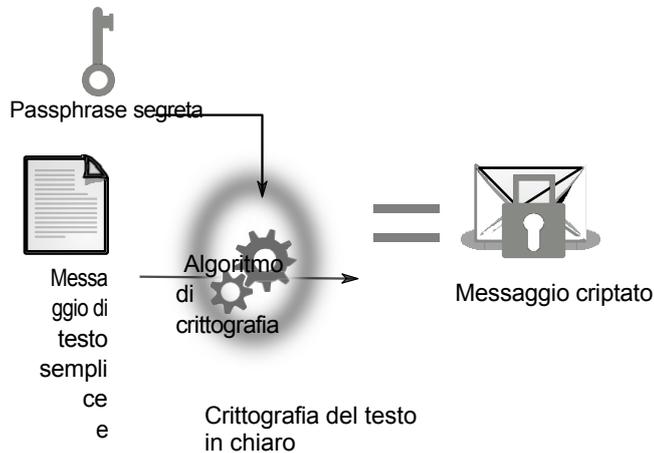
Al giorno d'oggi, l'algoritmo può essere trovato in modo molto dettagliato su Wikipedia, consentendo a chiunque di verificare che non ha particolari punti deboli, ovvero che l'unico modo per decifrare un messaggio criptato è quello di avere la *chiave che* è stata utilizzata con esso.

² Quello che segue è un adattamento molto parziale del fumetto di Jeff Moser sull'algoritmo AES [https://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html].

5.1.2 Volete un disegno?

In concreto, per garantire la *riservatezza* dei nostri dati, utilizziamo due operazioni: la crittografia, per proteggere i dati, e la decrittografia, per poterli leggere. Queste operazioni sono eseguite da software come GnuPG.

Primo passo: la crittografia



Per un esempio pratico, prendiamo il seguente messaggio ³ :

Gli spaghetti sono nella credenza.

Dopo aver crittografato questo messaggio utilizzando il software GnuPG con l'algoritmo AES-256 e, come passphrase, "questo è un segreto", si ottiene, per esempio ⁴ :

```
----- INIZIO MESSAGGIO PGP -----  
  
jA0ECQMCRM01mTSIONRg01kBWGQI76cQ0ocEvdBhX6BM2AU6aYSPYmSj8ihFX      u  
wV1GVraWuwEt4XnLc3F+0xT3EaXINMhdH9oydA92WDkaqPEnjsWQs/   oSCeZ3WxoB  
9 mf9y6jzqozEHw==  
=T6eN  
----- FINE MESSAGGIO PGP -----
```

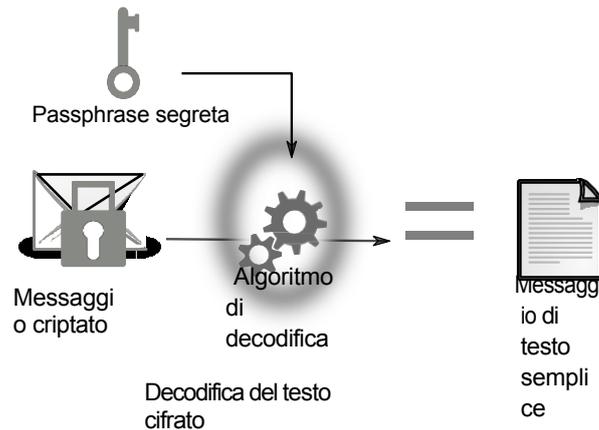
Ecco come appare un testo dopo la crittografia: il suo contenuto è diventato completamente incomprensibile. I dati "in chiaro", leggibili da tutti, sono stati trasformati in un altro formato, illeggibile da chiunque non abbia la passphrase.

Seconda fase: decodifica

Per decifrare, suffraghiamo nuovamente GnuPG, questa volta con il nostro testo cifrato. GnuPG ci chiederà la passphrase utilizzata per criptare il nostro messaggio e, se questa è corretta, otterremo finalmente le informazioni che ci mancavano per preparare il pranzo.

3. Questo messaggio è della massima importanza strategica per i clienti che invitate a casa vostra. È quindi fondamentale crittografarlo. A parte gli scherzi, se cifriamo solo i messaggi "sensibili", allora tutti i messaggi cifrati che inviamo sono sospetti; da qui l'importanza di cifrare anche i messaggi innocui.

4. Anche se lo stesso messaggio viene criptato con la stessa passphrase, il risultato è diverso ogni volta che l'operazione viene ripetuta: per evitare che chiunque possa confrontare i messaggi criptati (senza conoscere la passphrase) per scoprire se corrispondono o meno allo stesso messaggio in chiaro, vengono introdotti dati casuali per rendere ogni messaggio criptato unico e distinto dagli altri.



5.1.3 Per un disco rigido...

Se si desidera che tutti i dati inseriti in un supporto di memorizzazione (disco rigido, chiave USB, ecc.) siano crittografati, il sistema operativo dovrà eseguire operazioni di crittografia e decrittografia "al volo".

Ciò significa che ogni volta che i dati devono essere letti dal disco rigido, vengono decifrati durante il percorso in modo che il software che ne ha bisogno possa accedervi. Viceversa, ogni volta che un'applicazione software chiede di scrivere dei dati, questi vengono crittografati prima di arrivare sul disco rigido.

Affinché queste operazioni funzionino, la chiave di crittografia deve rimanere nella RAM per tutto il tempo in cui il supporto deve essere utilizzato.

pagi

na

18

Inoltre, la chiave di crittografia non può essere modificata. Una volta utilizzata per criptare i dati sul disco, la chiave diventa indispensabile per rileggerli. Per cambiare la chiave, bisognerebbe rileggere e riscrivere tutti i dati sul disco...

Per evitare questa noiosa operazione, la maggior parte dei sistemi utilizzati per crittografare i supporti di memorizzazione ha un trucco: la chiave di crittografia è in realtà un grande numero casuale, che viene a sua volta crittografato utilizzando una *passphrase*.⁵ Questa versione criptata della chiave di crittografia viene solitamente scritta sul supporto di memorizzazione all'inizio del disco, come "*intestazione*" dei dati crittografati.

Con questo sistema, cambiare la passphrase diventa semplice, poiché è sufficiente modificare questa *intestazione* (cosa che di solito viene fatta automaticamente da questi sistemi di crittografia).

5.1.4 Sintesi e limiti

La crittografia è il modo perfetto per proteggere i vostri dati⁶ crittografando tutto o parte del disco rigido, qualsiasi altro supporto di memorizzazione (chiavetta USB, CD, ecc.) o le vostre comunicazioni. Inoltre, i computer moderni sono abbastanza potenti da permetterci di rendere la crittografia una routine, anziché riservarla a circostanze speciali o a informazioni particolarmente sensibili (altrimenti si identifica immediatamente quest'ultima come importante, mentre è meglio dissolverla nella massa).

pagina

249

5. Il sistema LUKS, utilizzato in GNU/Linux, consente persino di utilizzare diverse versioni criptate della chiave di crittografia. Ciascuna di queste versioni può essere cifrata con una *passphrase* diversa, consentendo a più persone di accedere agli stessi dati senza dover ricordare lo stesso segreto.

6. Un articolo di Rue89 sulle rivelazioni di Snowden sull'impotenza dell'NSA di fronte alle minacce di guerra. crittografia: Marie Gutbub, 2014. *War crimes and data decryption: new revelations from Snowden* [<https://www.nouvelobs.com/rue89/rue89-monde/20141229.RUE7224/crimes-de-guerre-e-et-decryptage-de-donnees-nouvelles-revelations-de-snowden.html>].

Una passphrase può essere utilizzata per crittografare un intero disco rigido e/o per fornire a determinate persone una parte crittografata con la propria passphrase. È anche possibile criptare singoli file, e-mail o allegati, con una passphrase ancora diversa.

Tuttavia, pur essendo uno strumento potente ed essenziale per la sicurezza delle informazioni, la **crittografia presenta dei limiti**, che devono essere tenuti presenti quando la si utilizza.

Come spiegato in precedenza, quando si accede a dati crittografati, occorre tenere presente due cose. In primo luogo, una volta decifrati, i dati rimangono *almeno nella RAM*. In secondo luogo, finché i dati devono essere crittografati o decrittografati, la RAM contiene anche la *chiave di crittografia*.

Chiunque sia in possesso della chiave di crittografia può leggere *tutto ciò che è crittografato con essa* e può anche usarla per crittografare i dati.

È necessario tenere a mente i seguenti punti:

- Il sistema operativo e il software hanno accesso ai dati e alla chiave di crittografia tanto quanto noi, quindi tutto dipende da quanto ci si fida di loro di loro.
- quindi installate solo software di cui vi fidate.
- Chiunque acceda fisicamente al computer quando è acceso, ha paghe e l'accesso di fatto al contenuto della RAM. Quando un disco crittografato viene **attivato**, contiene, in chiaro, i dati su cui si sta lavorando da quando si è acceso il computer (anche se crittografati su disco). Ma soprattutto, come già detto, contiene la chiave di crittografia, che può essere copiata. È quindi meglio prendere l'abitudine di spegnere il computer e disattivare (smontare, espellere) i dischi crittografati quando non vengono utilizzati.
- In alcuni casi, può essere necessario fornire soluzioni hardware per interrompere l'alimentazione in modo rapido e semplice. ⁷ dischi criptati diventano di nuovo inaccessibili senza la passphrase, a meno che non si *freddi* pagina **27** attacco di avvio.
- È anche possibile che sul **computer** sia stato installato un keylogger che registra la passphrase.

Inoltre, la matematica utilizzata negli algoritmi crittografici è talvolta difettosa. E molto più spesso il software che li applica presenta punti deboli o errori. Alcuni di questi problemi possono, da un giorno all'altro, rendere possibile la decrittazione in pochi clic di dati criptati con quella che si pensava fosse la migliore protezione disponibile. ⁸...

Esiste anche un certo **limite "legale"** ai possibili attacchi. In Francia, chi cripta i propri dati è tenuto a fornire il codice di accesso alle autorità giudiziarie quando queste lo richiedono, come spiega l'articolo 434-15-2 del Codice Penale ⁹ :



È punito con tre anni di reclusione e una multa di 270.000 euro chiunque sia a conoscenza dell'accordo segreto di decrittazione di un mezzo crittografico che potrebbe essere stato utilizzato per preparare, agevolare o commettere un crimine o un delitto, se rifiuta di consegnare tale accordo all'autorità giudiziaria o di darvi attuazione, in risposta alle richieste di tale autorità emesse ai sensi dei titoli II e III del libro I^{er} del codice penale. Procedura.

7. Per questo motivo, può essere consigliabile non lasciare la batteria collegata in un computer portatile quando non viene utilizzato. È quindi sufficiente rimuovere il cavo di alimentazione per spegnerlo.

8. Blog di Zythom, 2015, *Il disco rigido criptato* [<https://zythom.fr/2015/03/le-disque-dur-chiffre/>].

9. Il termine giuridico è "crittologia". Una ricerca su questa parola su [Légifrance](https://www.legi-france.gouv.fr) [<https://www.legi-france.gouv.fr>] fornirà un elenco esaustivo di testi giuridici in questo campo.

Se il rifiuto avviene quando la consegna o l'attuazione dell'accordo avrebbe permesso di evitare la commissione di un crimine o di un reato o di limitarne gli effetti, la pena è aumentata a cinque anni di reclusione e a una multa di 450.000 euro.¹⁰

Si noti che le parole "*susceptible*" e "*sur les réquisitions*" significano che la legge è abbastanza vaga da richiedere a chiunque detenga dati criptati di vuotare il sacco. Potrebbero chiederci la passphrase di un supporto che non è nostro... e che non avremmo. Tuttavia, la polizia, anche nella persona di un OPJ¹¹ deve ottenere l'autorizzazione preventiva di un magistrato.¹² Dall'altra parte della Manica, una legislazione doganale simile fa sì che Muhammad Rabbani, direttore dell'organizzazione CAGE, possa rischiare la prigione per essersi rifiutato di consegnare le sue password alla frontiera.¹³

Contrariamente alle aspettative di molti¹⁴ ¹⁵il tribunale ha respinto l'argomentazione del "diritto a non incriminarsi" a difesa della mancata comunicazione dell'accordo di decrittazione. Ha sostenuto che "questi dati, già fissati su un supporto, esistono indipendentemente dalla volontà dell'indagato".¹⁶ Inoltre, la Divisione Penale della Corte di Cassazione francese ha stabilito che "il codice di sblocco di un telefono cellulare può costituire una chiave di decrittazione, se il telefono è dotato di un dispositivo crittografico".¹⁷

Alcune tecniche combinano anche la crittografia e la steganografia per rendere impercettibile la presenza di dati crittografati: si tratta della cosiddetta "crittografia ripudiabile", della "plausible deniability" o della "deniable encryption".¹⁸ *crittografia negabile*". Software come VeraCrypt¹⁹ offrono questa funzione, che in teoria consentirebbe di negare l'esistenza di dati criptati a un'autorità giudiziaria, evitando così di essere costretti a rivelare la passphrase ai sensi dell'articolo 434-15-2. Tuttavia, non esiste ancora un caso in cui si possa negare l'esistenza di dati criptati. Tuttavia, non esiste ancora una giurisprudenza in materia e l'uso della crittografia ripudiabile non esclude la possibilità che i tribunali siano in grado di dimostrare l'esistenza di dati crittografati con altri mezzi. È quindi necessaria una certa cautela.

Dal 2014²⁰ i poliziotti hanno anche il diritto di requisire chiunque vogliano.

". di essere informati delle misure applicate per la protezione dei dati" e "di fornire loro informazioni che consentano di accedere ai dati".²¹

10. Légifrance, 2016, *Codice penale*, articolo 434-15-2 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032654251/2016-06-05].

11. Ufficiale di polizia giudiziaria.

12. Les Numériques, 2020, *Rifiutare di sbloccare il proprio smartphone alla polizia, un'infrazione in alcuni casi* [<https://www.lesnumeriques.com/telephone-portable/refuser-le-deverrouillage-d-e-son-smartphone-a-la-police-une-infraction-dans-certains-cas-n155755.html>].

13. Birkbeck Law Review, 2018, *In Conversazione con Muhammad Rabbani, CAGE* [<https://web.archive.org/web/20211102115950/http://www.bbklr.org/blog/in-conversation-with-muhammad-rabbani-cage>].

14. Maître Éolas, 2014, *Allô oui j'écoute* [<https://www.maitre-eolas.fr/post/2014/03/08/All%C3%B4-oui-j-%C3%A9coute#c173067>].

15. La Quadrature du Net, 2018, *Le Conseil constitutionnel restreint le droit au chiffrement* [<https://www.laquadrature.net/2018/04/04/le-conseil-constitutionnel-restreint-le-droit-au-chiffrement>].

16. Conseil constitutionnel, 2018, *decisione n. 2018-696 QPC del 30 marzo 2018*. [<https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm>].

17. Légifrance, 2021, *Corte di Cassazione, Divisione Penale, 3 marzo 2021, 19-86.757, Non pubblicato* [<https://www.legifrance.gouv.fr/juri/id/JURITEXT000043252997>].

18. Wikipedia, 2020, *Plausibile negabilità (crittologia)* [[https://fr.wikipedia.org/wiki/D%C3%A9finition_de_plausible_d%C3%A9niabilit%C3%A9_\(cryptologie\)](https://fr.wikipedia.org/wiki/D%C3%A9finition_de_plausible_d%C3%A9niabilit%C3%A9_(cryptologie))].

19. Sito ufficiale di VeraCrypt [<https://www.veracrypt.fr/>].

20. Légifrance, 2014, *Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme* [<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000029754374>].

21. Légifrance, *Codice di procedura penale*, articolo 57-1 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032655328].

Ciononostante, alcune persone si rifiutano di dare il proprio consenso alla cifratura e lo rivendicano in nome del diritto di rimanere in silenzio e di non incriminarsi.²² Così come altri rifiutano di fornire il proprio DNA, il che è anche - in misura minore - penalmente riprovevole.

5.2 Garantire l'integrità dei dati

Abbiamo visto alcuni modi per garantire la *riservatezza* dei nostri dati. Tuttavia, può anche essere importante essere in grado di garantire la loro *integrità*, cioè di verificare che non siano stati alterati nel corso del processo (per errore o per maliziosamente, ad esempio per introdurre bug). Potremmo anche voler garantire che il *contenuto* dei nostri dati, pagina 32.

5.2.1 Potenza del chopper

La maggior parte delle tecniche per garantire l'integrità o l'autenticità si basa su strumenti matematici che la crittografia ha ribattezzato "funzioni di hash".

Questi funzionano come *minatori*, in grado di ridurre qualsiasi cosa in minuscoli pezzi. E se il nostro chopper funziona abbastanza bene da essere usato nella crittografia, sappiamo che :

- con i piccoli pezzi, è impossibile ricostituire l'oggetto originale senza provare ogni oggetto sulla Terra;
- lo stesso oggetto, una volta tritato, produrrà sempre gli stessi piccoli pezzi;
- la probabilità che due oggetti diversi producano esattamente gli stessi pezzetti è astronomicamente bassa.

Quando queste proprietà sono soddisfatte, è sufficiente confrontare i piccoli pezzi di due oggetti per vedere se sono identici.

I pezzetti che escono dal nostro tritacarne sono più comunemente noti come "a". *checksum* o *impronta digitale*. Di solito è scritto in una forma che assomiglia a :

```
f9f5a68a721e3d10baca4d9751bb27f0ac35c7ba
```

Il nostro tritacarne funziona con dati di qualsiasi dimensione e forma: possiamo ridurre in piccoli pezzi - cioè calcolare le loro impronte digitali - un'immagine, un CD, un software *e così via*. Così, ad esempio, invece di confrontare direttamente il contenuto di due DVD byte per byte, operazione che potrebbe essere lunga e noiosa, possiamo semplicemente confrontare le loro impronte digitali per determinare se sono identiche.

Questo non significa che il nostro chopper sia magico. È facile immaginare che quando si riduce qualsiasi cosa a cubetti della stessa dimensione, si possono ottenere gli stessi cubetti da due oggetti diversi. Questo si chiama *collisione*. Fortunatamente, la probabilità che tali collisioni matematiche si verifichino per caso è astronomicamente bassa, a meno che non esistano algoritmi in grado di provarle... cosa che è già accaduta con diverse funzioni hash dopo alcuni anni di ricerca, come la funzione SHA-1²³ per esempio. In questo caso, la terza proprietà della funzione hash non è più rispettata e il suo utilizzo dovrebbe essere interrotto.

22. Le Parisien, 2018, *Un gardé à vue peut garder le silence mais doit donner les codes de son smartphone* [<https://www.leparisien.fr/faits-divers/un-garde-a-vue-peut-garder-le-silence-mais-doit-donner-les-codes-de-son-smartphone-16-04-2018-7667613.php>].

23. Marc Stevens *et al*, 2017, *Annuncio della prima collisione SHA-1*, Google Security Blog [<https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>].

5.2.2 Verifica dell'integrità del software

Facciamo un esempio: Ana ha scritto un programma e lo distribuisce su CD, che si trovano nei club di utenti GNU/Linux. Bea vuole usare il programma di Ana, ma si rende conto che sarebbe stato molto facile per un'amministrazione malintenzionata sostituire uno dei CD di Ana con del malware.

Non può ritirare un CD direttamente da Ana, che vive in un'altra città. D'altra parte, ha incontrato Ana qualche tempo fa e conosce la sua voce. Così le telefona e Ana le fornisce la *somma di controllo* del contenuto del CD, che ha calcolato con una funzione di hash sicura:

CD di Ana	→	94d93910609f65475a189d178ca6a45f
	funzione hash	22b50c95416affb1d8feb125dc3069d0

Bea può quindi confrontarlo con quello generato dal CD acquistato, utilizzando la stessa funzione di hash:

Il CD di Bea	→	94d93910609f65475a189d178ca6a45f
	funzione hash	22b50c95416affb1d8feb125dc3069d0

Poiché le checksum sono identiche, Bea è felice, perché è sicura di utilizzare lo stesso CD fornito da Ana.

Il calcolo di queste checksum non richiede molto più tempo della riproduzione dell'intero CD... al massimo qualche minuto.

Ora mettiamoci nei panni di Carole, che è stata pagata per prendere il controllo del computer di Bea a sua insaputa. Per farlo, vuole creare un CD che assomigli a quello di Ana, ma che contenga un malware.

Carole inizia procurandosi il CD originale di Ana. Poi modifica il CD per includere il malware. Questa prima versione assomiglia molto all'originale. Potrebbe ingannare chi non è attento, ma sa che Bea controllerà la somma di controllo del CD prima di installare il programma che contiene.

Poiché Ana utilizza una funzione di hash che non presenta difetti noti, a Carole non resta che provare un numero enorme di variazioni sui dati del suo CD, nella speranza di ottenere una *collisione*, ossia la stessa somma di controllo di Ana.

Sfortunatamente per lei, e fortunatamente per Bea, anche con un gran numero di computer potenti e anche se vi dedicasse molto tempo, le possibilità di successo di Carole rimarrebbero astronomicamente basse.²⁴

È quindi sufficiente ottenere un'*impronta digitale*, o una *somma di controllo*, attraverso intermediari fidati per verificare l'integrità dei dati. La sfida consiste quindi nell'ottenere queste impronte digitali con mezzi fidati, cioè nel poterle verificare l'*autenticità*...

24. Per mettere le cose in prospettiva, con una funzione di hash attualmente considerata sicura (SHA- 256, per esempio), anche se Ana avesse un miliardo di miliardi di computer, ciascuno in grado di calcolare dieci miliardi di checksum al secondo, e li facesse calcolare per un periodo di tempo equivalente all'attuale età dell'universo (quindici miliardi di anni), sarebbe ancora *molto lontana dall'aver* una ragionevole possibilità di trovare una collisione!

Tuttavia, questo non tiene conto dei possibili progressi futuri della crittoanalisi che potrebbero scoprire punti deboli nella funzione hash utilizzata e proporre algoritmi più efficienti per consentire a Carole di portare a termine il suo attacco in un tempo ragionevole.

5.2.3 Controllare la password

Un altro esempio di utilizzo delle funzioni di hash riguarda la verifica dell'*autenticità* di una richiesta di accesso.

Se l'accesso a un computer è protetto da password, ad esempio quando si accede a GNU/Linux²⁵ il computer deve essere in grado di verificare che la password inserita sia quella corretta. Tuttavia, le password non vengono memorizzate in chiaro sul computer, altrimenti sarebbe troppo facile ottenerle.

Ma come fa il computer a garantire che la password digitata sulla tastiera sia corretta?

Quando si sceglie una password per il computer, il sistema utilizza una funzione di hash per registrare un'impronta della password. Per verificare l'accesso, il sistema "taglia" la password inserita nello stesso modo. E se le impronte digitali sono uguali, ritiene che la password sia quella giusta.

È quindi possibile verificare che la password corrisponda, senza conservare la password stessa!

5.3 Simmetrico, asimmetrico?

Le tecniche di crittografia menzionate finora si basano su un'unica chiave segreta, utilizzata sia per la crittografia che per la decrittografia. Si tratta della cosiddetta crittografia *simmetrica*.

Questo è in contrasto con la crittografia *asimmetrica* che, nel contesto della cifratura, non utilizza la stessa chiave per criptare e decriptare un messaggio. Conosciuta anche come "crittografia a chiave pubblica", è utilizzata principalmente per le comunicazioni online e sarà discussa in dettaglio nel secondo volume.

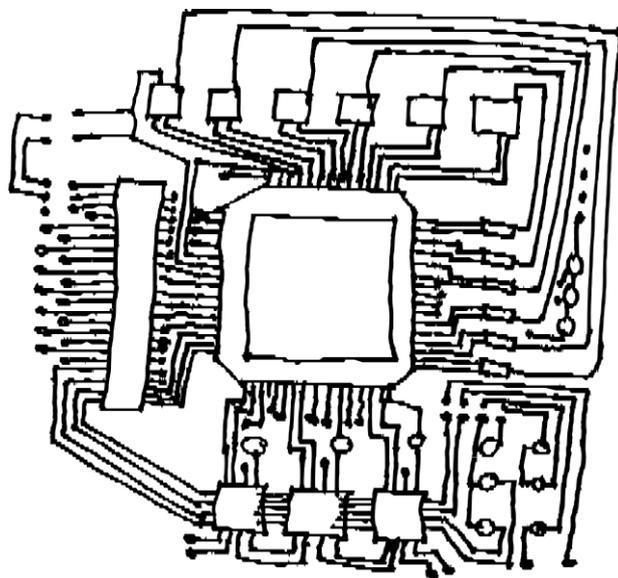
Una delle proprietà più interessanti della crittografia asimmetrica, che può essere menzionata brevemente in questa sede, è la sua capacità di produrre *firme digitali*. Come la sua controparte cartacea, la firma digitale può essere utilizzata per apporre un segno di riconoscimento ai dati.

Queste firme digitali, che utilizzano la crittografia asimmetrica, sono il modo più semplice per verificare l'origine del software. Le useremo più avanti...

[pagina

249

25. Ricordate che le password non servono a proteggere i dati [pagina 41]!



PARTE SECONDA

Scegliere le risposte giuste

Introduzione

A dire il vero, questo primo capitolo e la comprensione di come funzionano i computer sono sufficienti per gettare nel panico chiunque... Ma nascondere la testa sotto la sabbia non è una soluzione adeguata: abbiamo già scartato l'idea di non avere nulla da nascondere. La negazione non vi rende meno esposti a rischi o minacce.

Dopo aver letto questo libro, ripenserete sicuramente ai film d'azione in cui l'eroina nasconde il suo computer in una cassaforte della biblioteca che si apre quando si estraggono alcuni libri con una combinazione speciale... e lo scoraggiamento può avere la meglio su di voi.

Fortunatamente c'è un'altra soluzione: leggere il resto della guida! Questa nuova sezione presenta situazioni tipiche, chiamate *casi d'uso*, e suggerisce pratiche e strumenti adatti a ciascuna situazione.

Fiducia e riduzione del rischio

Le nozioni di *fiducia* e di *riduzione del rischio* sono utili quando si sceglie come utilizzare gli strumenti digitali. In questo capitolo esamineremo il sesso, la droga e il rock'n'roll, contesti in cui queste nozioni sono già state prese in considerazione. Come la tecnologia digitale, queste pratiche possono essere divertenti, ma spesso comportano dei rischi.

6.1 Riduzione del rischio

Lavorare in un cantiere o in un ufficio;
condividere gioielli per piercing, giocattoli sessuali o
spazzolini da denti; collegarsi a Internet o utilizzare
strumenti digitali;
salire su un'auto o andare in bicicletta...

Tutte queste pratiche comportano dei rischi... che possono essere ridotti!

Come dice Act Up: "informazione = potere". In effetti, la conoscenza e la comprensione ci permettono di trarre più piacere correndo meno rischi, nella consapevolezza che il rischio zero non esiste. La nozione di rischio è relativa e comprende così tanti aspetti diversi che è necessario discuterne per comprenderli e definirli.¹

La diffusione di informazioni sui rischi connessi è tanto più importante se si considera che quando un virus è presente, sia nell'organismo che nel computer, non è detto che vi siano segni visibili. Per questo motivo, dal punto di vista della salute, è consigliabile non aspettare i sintomi prima di intervenire e sottoporsi a screening regolari. Oppure, sul fronte digitale, gli aggiornamenti regolari aiutano a ridurre il rischio di infezione correggendo le falle di sicurezza.

Molte persone dedicano il loro tempo a facilitare la riduzione del rischio: distribuendo opuscoli informativi, ma anche profilattici, *pagliette* o tappi per le orecchie. Allo stesso modo, si sviluppano software, si scrive documentazione e si organizzano workshop sull'autodifesa e sull'intimità digitale.

Rendere l'uso della crittografia facile come indossare un elmetto; conoscere il clitoride come la RAM;
per rendere Tor facile da usare come i tappi per le orecchie;
Perché, a conti fatti, masturbarsi e cercare immagini di sfondo per ore e ore rende la vita più piacevole e non dovrebbe essere rischioso!

1. Ecco perché negli anni '90, nel campo delle tossicodipendenze, si è smesso di parlare di *prevenzione* e si è iniziato a parlare di *riduzione del danno* [<http://www.keep-smiling.com/?p=259>]. Nel campo della sessualità, si è smesso di usare il termine "*sesso sicuro*" e si è iniziato a usare il termine "*safer sex*".

6.2 Una storia di fiducia

Fidarsi di apparecchiature, software e reti digitali è come fidarsi di un meccanico: si può credere o meno. Allo stesso modo, ci si può fidare più o meno di un team di sviluppo software.²

Questa super applicazione cripta completamente tutti i vostri dati! Questo casco protegge la vostra testa in caso di incidente!

Non preoccupatevi, non ho corso alcun rischio!

Affermazioni di questo tipo non sono sufficienti per costruire un rapporto di fiducia. È meglio fare domande, guardare oltre l'ovvio.

Se un'applicazione dichiara di criptare completamente i dati, potremmo chiederci quale sia il sistema di crittografia e se questo metodo sia approvato dalle comunità di cui ci fidiamo. Potremmo anche chiederci se si tratta di marketing ingannevole.

Allo stesso modo, quando condividiamo la sessualità, possiamo discutere di ciò che consideriamo un'assunzione di rischio e di quali siano i nostri limiti, le nostre pratiche o il nostro rapporto con la riduzione del rischio e lo screening.

Porsi le seguenti domande aiuta a valutare la fiducia che si può avere in uno strumento:

- Perché è stato sviluppato questo strumento?
- È libero?
- Qual è il suo modello di business?
- A chi deve rendere conto?

Ma non si tratta solo di rischio e fiducia. Si tratta di un rischio solo quando non c'è l'intenzione di danneggiare persone, gruppi, idee, *ecc.*

Il rischio è quello di rovinarsi le mani tirando fuori i rovi senza guanti, la minaccia è il capo che mette in secondo piano i suoi dipendenti sindacalizzati; il rischio di guidare in stato di ebbrezza è quello di avere un incidente, la minaccia è quella di vedersi revocare la patente; il rischio, quando non si è fatto un backup, è di perdere tutti i dati se un disco rigido si blocca, e la minaccia è che la polizia perquisisca il luogo di attività militante dove sono conservati; il rischio è un bug del software che manda in crash il computer, la minaccia è Cambridge Analytica, che utilizza i dati dell'account Facebook per influenzare i risultati delle elezioni.

Naturalmente la questione è più complessa: ci sono rischi di minacce e le minacce possono generare rischi!

La questione della minaccia non è solo individuale, poiché la mancata adozione di determinate precauzioni può esporre le persone con cui comunichiamo.

2. Questa domanda di fiducia può essere posta a qualsiasi specialista: giornalisti, medici, agricoltori, falegnami, ingegneri, poliziotti, negozianti, tatuatori, muratori, piloti (di aerei, treni, autobus, *ecc.*), *urbanisti*, parrucchieri, architetti, farmacisti, insegnanti, artisti, bagnini, infermieri, panettieri, vivaisti e donne che lavorano nel settore pubblico.), *urbanisti*, parrucchieri, architetti, farmacisti, insegnanti, artisti, bagnini, infermieri, panettieri, politici, postini, strizzacervelli, receptionist (presso CAF, MSA, Pôle emploi, *ecc.*), contabili, rappresentanti di commercio, venditrici, *ecc.*), contabili, rappresentanti di commercio, veterinari, responsabili delle risorse umane, scienziati, artigiani, cuochi, guardie di sicurezza, banchieri, operai, sportivi, allenatori, tecnici elettronici, educatori, assistenti sociali e *così via*.

Valutazione del rischio

Quando ci si chiede quali siano le misure da mettere in atto per proteggere i dati o le comunicazioni digitali, ci si rende subito conto che si sta andando in un vicolo cieco.

In realtà, anche le soluzioni che potremmo mettere in atto hanno i loro svantaggi: a volte sono una vera e propria seccatura da implementare, mantenere o utilizzare; a volte abbiamo la possibilità di scegliere tra varie tecniche, nessuna delle quali soddisfa pienamente le "specifiche" che ci siamo prefissati; a volte sono troppo nuove per essere sicuri che funzionino davvero; *e così via*.

Dovremmo quindi iniziare a porci alcune semplici domande, al fine di stabilire un *modello di minacce*¹ cioè l'identificazione e la prioritizzazione delle minacce potenziali.

7.1 Cosa vogliamo proteggere?

Ciò che vogliamo proteggere rientra generalmente nell'ampia categoria delle *informazioni*: ad esempio, il contenuto dei messaggi di posta elettronica, i file di dati (foto, volantini, rubriche) o l'esistenza stessa della corrispondenza tra tale persona e tale persona.

La parola "proteggere" copre esigenze diverse:

- **riservatezza**: nascondere le informazioni da occhi indesiderati ;
- **integrità**: mantenere le informazioni in buone condizioni e impedire che vengano alterate a nostra insaputa;
- **accessibilità**: garantire che le informazioni rimangano accessibili a chi ne ha bisogno.

Per ogni serie di informazioni da proteggere, è necessario definire i requisiti di riservatezza, integrità e accessibilità. Dato che queste esigenze sono generalmente in conflitto, sarà necessario stabilire delle priorità e trovare dei compromessi, e andarci piano con la capra (affamata) e il cavolo (molto appetitoso)...

7.2 Da chi vogliamo proteggerci?

Si pone presto la questione delle capacità delle persone che potrebbero essere alla ricerca di ciò che vogliamo proteggere: genitori invadenti, compagni di classe che potrebbero molestare, ladri che vogliono recuperare i dati bancari, un ex coniuge violento alla ricerca di mezzi di controllo o di ricatto, gerarchie troppo curiose, la polizia incaricata di sedare un movimento sociale, funzionari pubblici che vogliono proteggere i loro dipendenti, ecc. Ci si chiede quali siano le capacità delle persone che potrebbero essere alla ricerca di ciò che vogliamo proteggere.

1. Vedi [Electronic Frontier Foundation, 2019, Il tuo piano di sicurezza](https://ssd.eff.org/fr/mod_ule/your-security-plan) [https://ssd.eff.org/fr/mod_ule/your-security-plan].

controllo dei lavoratori migranti ²GAFAM che tracciano e vendono dati personali, servizi di intelligence incaricati di schedare massicciamente una comunità o una tendenza politica, ecc.

Ma non è facile sapere cosa possano fare effettivamente i più qualificati, né di quali risorse e budget dispongano. Seguendo i telegiornali, e attraverso vari altri mezzi, possiamo vedere che la situazione varia molto a seconda di chi abbiamo di fronte. Tra i genitori, i gendarmi locali e la *National Security Agency* (NSA) degli Stati Uniti, c'è un ampio divario nella gamma di azioni, mezzi e tecniche impiegate.

La questione dei mezzi degli avversari è piuttosto ampia.

Esistono **mezzi giudiziari**: ad esempio, la possibilità che una rogatoria autorizzi la polizia a sequestrare le apparecchiature informatiche, o il fatto che vi venga richiesto di fornire la vostra chiave di crittografia.

Allo stesso tempo, alcune organizzazioni, come la SDAT ³ o la DGSE ⁴. Nulla è certo sulle loro capacità: quanto sono avanzate nella violazione della crittografia? Sono a conoscenza di eventuali falle non rivelate nei loro metodi, che permetterebbero loro di leggere i dati? Su questi argomenti, ovviamente, non c'è modo di sapere con certezza cosa possano fare queste entità.

Occorre anche tenere conto **delle risorse finanziarie**. Alcune tecnologie di sorveglianza sono costose e non tutti i servizi di intelligence possono permetterselo, né saranno disponibili per ogni indagine. Considerando che il bilancio annuale della DGSE era di 880 milioni di euro nel 2021 e che quello della NSA era stimato in

10,8 miliardi di dollari (!) nel 2013, non giocano nello stesso campionato.

C'è anche la questione dei **mezzi politici**: ad esempio, fino a che punto lo Stato francese può collaborare con la NSA?

D'altra parte, proteggere completamente un computer è un compito impossibile. Si tratta quindi di porre ostacoli a coloro che potrebbero essere alla ricerca delle nostre informazioni. Quanto più grandi sono i mezzi di queste persone, tanto più numerosi e solidi devono essere i bastoni.

Valutare il rischio significa chiedersi quali dati si vogliono proteggere e da chi. Da qui si può cercare di capire quali sono i mezzi a disposizione di chi potrebbe essere interessato e definire una *politica di sicurezza* di conseguenza.

2. Si veda l'articolo di Ritimo: [10 menaces contre les migrant-es et les réfugié-es](https://www.ritimo.org/10-menaces-contre-les-migrant-es-et-les-refugie-es) [https://www.ritimo.org/10-menaces-contre-les-migrant-es-et-les-refugie-es].

3. Dipartimento di polizia francese dedicato alla lotta al terrorismo, cfr. [Wikipedia, 2021, Sous-direction anti-terroriste](https://fr.wikipedia.org/wiki/Sous-direction_anti-terroriste) [https://fr.wikipedia.org/wiki/Sous-direction_anti-terroriste].

4. Servizio di intelligence francese, vedi [Wikipedia, 2017, Direction générale de la Sécurité](https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_S%C3%A9curit%C3%A9_ext%C3%A9rieure) [esterno](https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_S%C3%A9curit%C3%A9_ext%C3%A9rieure) [https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_S%C3%A9curit%C3%A9_ext%C3%A9rieure].

Definizione di una politica di sicurezza

Una catena è forte solo quanto il suo anello più debole. Non ha senso installare tre enormi catenacci su una porta blindata accanto a una finestra fatiscante. Allo stesso modo, la crittografia di una chiavetta USB è di scarsa utilità se i dati in essa memorizzati vengono utilizzati su un computer, che ne conserverà le tracce *non criptate* sul disco rigido.

Questi esempi ci insegnano qualcosa: queste "soluzioni" mirate non servono a nulla se non fanno parte di un insieme di pratiche coerentemente articolate. Inoltre, le informazioni che vogliamo proteggere sono spesso legate a pratiche che non rientrano nell'ambito degli strumenti digitali. Ecco perché

Dobbiamo quindi valutare i rischi a livello globale ed elaborare risposte adeguate.

In modo globale, ma *situato*: una data situazione corrisponde a un insieme singolare di problemi, rischi, know-how... e quindi possibilità di azione. Non esiste una soluzione unica che risolva ogni problema con un colpo di bacchetta magica. L'unica strada percorribile è l'apprendimento sufficiente per poter immaginare e attuare una politica di sicurezza adeguata alla propria situazione.

8.1 Una questione di compromesso

I dati e le comunicazioni digitali possono sempre essere protetti *meglio*. Le possibilità di attacco e sorveglianza sono illimitate, così come i dispositivi disponibili per proteggersi da esse. Tuttavia, ogni protezione aggiuntiva che vogliamo mettere in atto richiede uno sforzo in termini di apprendimento e di tempo: non solo uno sforzo iniziale per iniziare, per installare la protezione, ma anche, molto spesso, un'ulteriore complessità d'uso, tempo speso a digitare passphrase, a eseguire procedure noiose e ripetitive, a concentrare la nostra attenzione sulla tecnica piuttosto che sull'uso che vorremmo fare degli strumenti digitali.

In ogni situazione, quindi, si tratta di trovare un **compromesso** adeguato, tra la facilità d'uso e il livello di protezione desiderato.

A volte, questo compromesso semplicemente **non esiste**. Lo sforzo necessario per proteggersi da un rischio plausibile sarebbe troppo doloroso ed è meglio correre quel rischio o, semplicemente, non usare strumenti digitali per archiviare certi dati o parlare di certe cose. Esistono altri mezzi, la cui efficacia è stata dimostrata da tempo: alcuni manoscritti sono sopravvissuti per secoli, sepolti in vasi conservati nelle grotte...

8.2 Cosa fare?

L'obiettivo è quello di rispondere alla seguente domanda: quale insieme di pratiche e strumenti dovrebbe proteggermi in modo sufficiente dai rischi valutati sopra?

[pagina

63

Per farlo, possiamo partire dalle nostre pratiche attuali e porci le seguenti domande:

1. Di fronte a una politica di sicurezza di questo tipo, quali angoli di attacco utilizzerebbero i miei avversari?
2. Quali mezzi devono usare i miei avversari?
3. Queste risorse sono disponibili per i miei avversari?

Se la risposta alla terza domanda è "sì", prendetevi il tempo di informarvi sulle soluzioni che potrebbero proteggervi da questi attacchi, e poi immaginate i cambiamenti nella pratica che queste soluzioni e la politica di sicurezza che ne deriva comporterebbero. Se questo vi sembra fattibile, rimettetevi nei panni dei vostri avversari e ponetevi nuovamente le domande di cui sopra.

Ripetete questo processo di riflessione, ricerca e immaginazione fino a trovare un percorso praticabile, un compromesso accettabile.

Se non siete sicuri, potete sempre chiedere a qualcuno più preparato e affidabile di mettersi nei panni dell'avversario: sarà felice di vedere che avete fatto la maggior parte delle riflessioni da soli, il che lo incoraggerà sicuramente ad aiutarvi sui punti che rimangono fuori dalla vostra portata.

8.3 Alcune regole

Prima di esaminare più da vicino i casi concreti e le politiche di sicurezza che potrebbero essere messe in atto, ci sono alcuni principi fondamentali, alcune grandi famiglie di scelte.

8.3.1 Complesso vs. semplice

Quando si tratta di sicurezza, una soluzione semplice è sempre preferibile a una complessa.

In primo luogo, perché una soluzione complessa offre un maggior numero di "superfici d'attacco", vale a dire un maggior numero di punti in cui possono verificarsi problemi di sicurezza...

In secondo luogo, perché più una soluzione è complessa, più conoscenze sono necessarie per immaginarla, implementarla e mantenerla, oltre che per esaminarla e valutarne la pertinenza e i problemi. Ciò significa che, in linea di massima, più una soluzione è complessa, meno sarà sottoposta all'attento esame, anche esterno, necessario per stabilirne la validità.

Infine, molto semplicemente, una soluzione complessa che non rientra completamente nello spazio mentale di chi l'ha sviluppata ha maggiori probabilità di generare problemi di sicurezza derivanti da interazioni complesse o casi speciali difficili da individuare.

Ad esempio, piuttosto che passare ore a configurare dispositivi per proteggere un computer particolarmente sensibile dalle intrusioni di rete, si potrebbe anche staccare la spina. A volte si può anche rimuovere fisicamente la scheda di rete...

8.3.2 Elenco autorizzato, elenco bloccato

Quando si viene a conoscenza di una minaccia, il riflesso abituale è quello di cercare di prevenirla. Ad esempio, una volta scoperto che un particolare software lascia tracce delle vostre attività in una determinata cartella, la pulite regolarmente. Finché non si scopre che lo stesso software lascia tracce anche in un'altra cartella, e così via.

Questo è il principio dell'elenco bloccato ¹ un elenco di cartelle in cui sono memorizzati file temporanei, software che inviano segnalazioni e *così via*. Questo elenco viene ampliato man mano che vengono fatte nuove scoperte e spiacevoli sorprese; su questa base, cerchiamo di fare del nostro meglio per proteggerci da ognuna di queste minacce. In altre parole, un elenco bloccato funziona sulla base della *fiducia ma in casi certi*.

Il principio della lista autorizzata ² è l'opposto: è un principio di *diffidenza, tranne che in certi casi*. Tutto è vietato, *tranne* ciò che è esplicitamente autorizzato. I file non possono essere memorizzati sul disco rigido, se non in un determinato luogo e in un determinato momento. L'accesso alla rete è vietato ai software, ad eccezione di alcuni software ben selezionati.

pagina

131

Questo per quanto riguarda le basi.

Qualsiasi politica di sicurezza basata sul principio dell'*elenco di blocco* ha un grosso problema: tale elenco non è mai completo, poiché tiene conto solo dei problemi già identificati. Mantenere aggiornato un elenco di blocco è un compito infinito e senza speranza; che lo si faccia da soli o lo si deleghi a persone con conoscenze informatiche specialistiche, è inevitabile che qualcosa venga trascurato.

Il problema è che, nonostante i loro difetti, gli strumenti basati sull'approccio delle *liste bloccate* sono numerosi (come vedremo), a differenza di quelli basati sul metodo *delle liste autorizzate*, che di conseguenza ci sono meno familiari.

L'implementazione dell'approccio dell'*elenco autorizzato* richiede uno sforzo iniziale che, pur essendo significativo, viene rapidamente ricompensato. Imparare a usare un sistema *attivo* che non scrive nulla sul disco rigido senza che gli venga chiesto di farlo richiede un po' di tempo. Ma una volta fatto questo, si può dire addio alle lunghe e inefficienti sessioni di pulizia del disco rigido che devono sempre essere ripetute, perché si basano sul principio dell'*elenco bloccato*.

pagina

113

Un altro esempio è il software antivirus, progettato per impedire l'esecuzione di programmi dannosi. Poiché funzionano in base al principio dell'elenco bloccato, i loro database devono essere costantemente aggiornati, poiché sono sistematicamente obsoleti. Una risposta a questo problema, con l'approccio dell'*elenco autorizzato*, consiste nell'impedire l'esecuzione di qualsiasi programma che non sia stato preventivamente registrato, oppure nel limitare le possibilità di azione di ciascun programma. Anche queste tecniche, note come *Mandatory Access Control*, richiedono la manutenzione di elenchi, ma si tratta di elenchi *autorizzati* e il sintomo di un elenco obsoleto sarà il malfunzionamento del software, piuttosto che la pirateria informatica.

È quindi molto meglio, ove possibile, affidarsi a liste autorizzate più ampie possibile, in modo da poter fare molte cose interessanti con i computer, con un certo grado di sicurezza. E, quando non esiste un elenco autorizzato appropriato, affidarsi a solide liste bloccate di provenienza nota, tenendo presente il problema intrinseco di questo metodo; liste bloccate che alla fine contribuiremo a completare, condividendo le nostre scoperte.

8.3.3 Nessuno è infallibile

Su Internet si dice spesso che "la maggior parte dei problemi del computer si trova tra la sedia e la tastiera". ³ Dietro questa espressione sprezzante nei confronti delle persone che utilizzano gli strumenti si nasconde una realtà: nessuno è infallibile e l'errore umano è sempre una possibilità.

1. A volte si parla anche di "lista nera".

Le espressioni "lista nera" e "lista bianca" possono evocare una dimensione razzista, sia nei termini stessi che nella loro struttura gerarchica. Abbiamo quindi scelto di sostituire questi due termini con "lista bloccata" e "lista autorizzata". Purtroppo, la maggior parte dei programmi, dei manuali d'uso e di altra documentazione tecnica utilizza ancora questi termini. È per questo che si trova costretta a menzionarli.

2. A volte si parla anche di "lista bianca".

3. Wiktionary, 2020, *Tra la sedia e la tastiera*

[https://fr.wiktionary.org/wiki/entre_la_c_haise_et_le_clavier].

Alcune pratiche possono essere diabolicamente efficienti... finché non si commette un errore. Poiché alla fine siamo destinati a commetterne uno, è meglio anticiparlo piuttosto che pagarne le conseguenze.⁴

Ad esempio, immaginate una chiavetta USB contenente documenti riservati. Anche se siete molto attenti a non lasciarla in giro, potrebbe essere lasciata su un tavolo... e poi collegata e utilizzata da qualcuno che l'ha scambiata per un'altra, in una macchina di cui non vi fidate. La crittografia della chiave prima di archiviare documenti riservati avrebbe ridotto notevolmente i rischi.

In breve, non siamo robot. È meglio avere solide protezioni materiali che imporre a noi stessi una vigilanza illimitata, e questo ci dà anche tranquillità.

8.3.4 Nulla è eterno

Una volta definita una politica di sicurezza, non dimenticate di rivederla di tanto in tanto! Il mondo della sicurezza informatica si evolve molto rapidamente e una soluzione considerata ragionevolmente sicura oggi potrebbe essere facilmente attaccabile l'anno prossimo.

Non dimentichiamo nemmeno, nelle nostre politiche di sicurezza, che è importante monitorare la vita del software da cui dipendiamo: i suoi problemi, con un impatto sulla sicurezza; i suoi aggiornamenti, con sorprese talvolta buone o cattive... Tutto questo richiede un po' di tempo e tanto vale pianificarlo fin dall'inizio.

4. In inglese si usa l'espressione "better safe than sorry". L'equivalente francese di "mieux vaut prévenir que guérir".

Casi d'uso

Basta con la teoria, illustriamo questi concetti con alcuni *casi d'uso*: in base a situazioni date, suggeriremo come definire una politica di sicurezza appropriata. Molte delle soluzioni tecniche adottate saranno spiegate.

nella sezione seguente, a cui facciamo riferimento se necessario.

Pagina 95

Essendo tutti ambientati nel contesto offline di questo primo volume, questi casi d'uso avranno una qualità artificiale: tutti presuppongono che i computer in gioco non siano mai connessi alle reti, e in particolare a Internet.

Caso d'uso: un nuovo inizio, per fermarsi pagare il pifferaio

(o come ripulire il computer dopo anni di utilizzo spensierato)

9.1 Contesto

Prendiamo un computer che è stato utilizzato senza particolari precauzioni per diversi anni. Questa macchina presenta senza dubbio uno o più dei seguenti problemi:

1. il suo disco conserva tracce indesiderate del passato ;
2. il sistema operativo è un software proprietario (ad esempio Windows), e infestato da malware.

pagina
27
pagina 31

D'altra parte, i file problematici vengono memorizzati in modo perfettamente trasparente. Infatti, questo computer viene utilizzato per varie attività (alcune delle quali perfettamente legali) come :

- ascoltare musica e guardare film da Internet ;
- aiutare i migranti privi di documenti a preparare i loro dossier per la prefettura;
- progettare un bel biglietto d'auguri per la nonna ;
- Creare documenti amministrativi falsi che semplificano notevolmente alcune procedure (gonfiare le buste paga quando si è stanchi di vedersi rifiutare un appartamento in affitto dopo l'altro);
- tenere aggiornati i conti della famiglia;
- produrre testi, musica o video "terroristici". Ovvero, secondo la definizione europea di terrorismo ¹ minacciare "di provocare una distruzione massiccia [...] di un'infrastruttura [...] suscettibile [...] di produrre perdite economiche [...]".

nomici". Ad esempio, con l'obiettivo di "costringere indebitamente autorità pubbliche o un'organizzazione internazionale di compiere o astenersi dal compiere qualsiasi atto". Ad esempio, le persone impiegate da Orange che, durante una rissa, minacciano di disattivare il sistema di fatturazione, consentendo così a tutti di effettuare chiamate gratuite.

1. Unione Europea, 2017, *Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta al terrorismo, che sostituisce la decisione quadro 2002/475/GAI del Consiglio e modifica la decisione 2005/671/GAI del Consiglio*, articolo 3 [<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32017L0541&qid=1495634630652>].

9.2 Valutazione dei rischi

9.2.1 Cosa vogliamo proteggere?

[pigi
na 63
-----]

Applichiamo al caso in esame le categorie definite quando abbiamo parlato di valutazione del rischio: -----

- riservatezza: per evitare che un occhio indesiderato cada troppo facilmente sulle informazioni memorizzate nel computer;
- integrità: impedire che le informazioni vengano modificate a nostra insaputa;
- accessibilità: garantire che le informazioni rimangano accessibili quando necessario.

Qui l'accessibilità e la riservatezza sono le priorità assolute.

9.2.2 Da chi vogliamo proteggerci?

Si tratta di una domanda importante: a seconda della risposta, la politica di sicurezza appropriata può variare da una cosa all'altra.

Gesto generoso, conseguenze legali

Questo computer potrebbe essere sequestrato durante una perquisizione.

Ad esempio, vostro figlio ha generosamente dato un grammo di *erba* ad alcuni amici che, dopo essere stati scoperti, hanno informato la polizia della provenienza della roba... dopodiché la procura ha perseguito vostro figlio per traffico di droga. Da qui la perquisizione.

In questi casi, è probabile che il computer venga esaminato dalla polizia, mettendo a rischio l'obiettivo della riservatezza. I mezzi che potrebbero essere utilizzati vanno dai gendarmi di Saint-Tropez che accendono il computer e fanno clic, all'esperto forense che esamina più da vicino il contenuto del disco. D'altra parte, è improbabile che in questo caso vengano utilizzati mezzi extra-legali, in quanto generalmente riservati ai servizi speciali e alle forze armate.

Furto con scasso

Questo computer potrebbe essere rubato durante un furto.

A differenza della polizia, le persone che hanno rubato il vostro computer probabilmente se ne fregano dei vostri segreti e non vi denunceranno. Nel peggiore dei casi, vi ricatteranno per riavere i vostri dati. Tuttavia, è improbabile che si impegnino a fondo per trovare i vostri dati sul disco del computer.

9.3 Definizione di una politica di sicurezza

[Poniamoci ora le domande indicate nella metodologia, mettendoci nei panni degli avversari. -----]

Tutto ciò che segue si applica ai computer offline. Se il computer è collegato a una rete, sono possibili altre situazioni e modalità di attacco che verranno analizzate nel secondo volume di questa guida.

[page
231
-----]

9.3.1 Mettetevi nei panni degli avversari

Primo passo: quando bastano per guardare

1. L'approccio più pratico: collegare il disco a un altro computer, esaminarne il contenuto e scoprire tutti i nostri piccoli segreti.

2. Risorse necessarie: un altro computer permetterà ai gendarmi di Saint-Tropez di trovare la maggior parte dei nostri segreti; un esperto forense sarà anche in grado di trovare i file che pensavamo fossero stati cancellati.
3. Credibilità dell'attacco: alta.

Dovremo quindi adattare le nostre pratiche. La crittografia del disco è la risposta più ovvia a questo tipo di attacco: l'installazione e l'utilizzo di un sistema crittografato è ormai un'operazione di routine.
semplice.

I passi per arrivarci sarebbero quindi :

1. Eseguire un sistema *attivo* per eseguire le seguenti operazioni in un ambiente relativamente sicuro:
 - salvare temporaneamente i file che devono sopravvivere alla pulizia su un disco esterno criptato o su una chiave USB;
 - espellere/rimuovere e scollegare il dispositivo di archiviazione esterno;
 - cancellare "realmente" l'intero disco **interno** del computer.
2. Installare un sistema operativo open source, specificando al programma di installazione che deve essere crittografia del disco, compresa la memoria virtuale (*swap*).
3. Ricopiare i dati precedentemente salvati sul nuovo sistema.
4. Mettere in atto ciò che serve per eliminare i file in modo "sicuro", in modo da...
5. Eliminare il contenuto dei file sul supporto di backup temporaneo, che potrebbe essere riutilizzato in futuro.

Poi, di tanto in tanto, assicurarsi che i dati cancellati senza particolari precauzioni non possano essere recuperati in seguito. È anche importante assicurarsi che il sistema sia regolarmente aggiornato, per tappare eventuali "buchi di sicurezza".
potrebbe utilizzare un malware.

Per eseguire questi passaggi, fare riferimento alle seguenti ricette:

- criptare un disco esterno o una chiave USB (vedere pagina 145) ;
- utilizzare un sistema *in tensione* (vedere pagina 113) ;
- salvare i dati (vedere pagina 151) ;
- cancellare "per davvero" (vedere pagina 139);
- installare un sistema criptato (vedere pagina 119) ;
- mantenere il sistema aggiornato (vedere pagina 175).

Secondo passo: il cassetto del comò non era criptato

1. Angolo di attacco: l'equivalente dei file che stiamo cercando di proteggere potrebbe trovarsi nella stanza accanto, nel terzo cassetto della cassettiera, su carta o su una chiavetta USB.
2. Mezzi necessari: perquisizione, furto con scasso o altra visita senza preavviso.
3. Credibilità dell'attacco: alta, poiché è proprio questo il tipo di situazione da cui stiamo cercando di proteggerci.

Anche in questo caso, si può notare che una politica di sicurezza deve essere considerata nel suo complesso. pagina 65 Senza un minimo di coerenza nelle pratiche, non ha senso preoccuparsi di digitare

passphrase per un tempo pari a quello di un giorno senza pane.

È quindi giunto il momento di riordinare i documenti nella cassettiera e di ripulire le chiavette USB, i CD o i DVD contenenti dati che ora si intende crittografare:

- salvare i dati su un supporto crittografato;
- per le chiavette USB e i dischi esterni: cancella il loro contenuto per davvero;
- per CD e DVD: distruggere e smaltire i residui;
- decidere cosa fare dei dati precedentemente salvati: copiarli o archivarli.

Terza fase: la legge come mezzo di coercizione

1. Angolo di attacco: la polizia ha il diritto di chiedere l'accesso alle informazioni criptate, come spiegato nel capitolo sulla crittografia.
2. Mezzi necessari: sufficiente perseveranza nell'indagine per applicare questa legge.
3. Credibilità dell'attacco: probabile, già utilizzato in diverse occasioni, anche per casi di stupefacenti.²

Se la polizia chiede l'accesso a dati criptati, la domanda pratica è: le informazioni contenute nel computer rappresentano un rischio maggiore rispetto al rifiuto di fornire la passphrase? Dopodiché, dipende da come ci si sente. Il fatto di cedere in questa situazione non pregiudica l'utilità di criptare il disco: per lo meno, permette di sapere cosa è stato rivelato, quando e a chi.

Tuttavia, sebbene rivelare la propria passphrase sia una decisione personale, può avere conseguenze più ampie. Ad esempio, per altre persone i cui pseudonimi sono citati in documenti archiviati sul nostro computer, o se in un procedimento legale tutte le persone, tranne una, rivelano la propria passphrase. In ultima analisi, la scelta di rivelare o meno la propria passphrase non è una questione individuale e può quindi essere presa in considerazione da più persone. Può anche darsi *che, per principio*, non si voglia rivelare la propria passphrase, anche *se non si ha nulla da nascondere*.

Detto questo, potrebbe essere una buona idea organizzarsi per vivere una situazione del genere in modo meno delicato: il nuovo obiettivo potrebbe essere quello di avere un disco sufficientemente "pulito" in modo che non sia un disastro se ci si arrende alla legge, o se si scopre una falla nel sistema crittografico utilizzato.

Come primo passo, è spesso possibile scendere a compromessi sull'accessibilità dei file relativi a progetti conclusi, che spesso non saranno più necessari. Questo aspetto sarà affrontato nel caso d'uso dell'archiviazione, che potrà essere studiato in seguito.

C'è poi la questione della compartimentazione: non tutte le nostre attività richiedono lo stesso livello di sicurezza e non vogliamo necessariamente che siano tutte collegate alla nostra identità civile o allo stesso pseudonimo. Sarebbe possibile aumentare il livello complessivo di sicurezza per tutte le nostre attività, ma questo potrebbe essere troppo oneroso. Quindi, la *compartimentazione* potrebbe essere più appropriata. Occorre poi specificare le rispettive esigenze di riservatezza di queste diverse attività e, da lì, stabilire quali, essendo più "sensibili" di altre, debbano avere un trattamento preferenziale.

Il prossimo caso d'uso esaminerà questo trattamento preferenziale, ma per ora è meglio finire di leggere questo!

9.3.2 Altri angoli di attacco da considerare

Oltre a queste situazioni, esistono diversi altri possibili punti di attacco contro una politica di sicurezza di questo tipo.

Primo angolo di attacco: una falla nel sistema di crittografia utilizzato

Come già spiegato in queste pagine, ogni sistema di sicurezza prima o poi viene violato. Se l'algoritmo di crittografia utilizzato viene violato, probabilmente farà notizia, tutti lo sapranno e sarà possibile reagire.

Ma se è la sua implementazione nel kernel di Linux a non essere funzionante, non passerà l'esame.

2. Cour de Cassation française, 2020, *Arrêt de la chambre criminelle du 13 octobre 2020* [<https://www.courdecassation.fr/decision/5fca302e5b008f80d3ad3a35>].

non su *Libération*, e c'è da scommettere che solo gli specialisti di sicurezza informatica ne saranno a conoscenza.

Quando non si hanno a che fare con queste persone, un modo per tenersi aggiornati è quello di iscriversi agli annunci di sicurezza di Debian.³ Le e-mail ricevute in questo modo sono scritte in inglese, ma è possibile trovare la traduzione in francese - se disponibile - sulla pagina "Informazioni sulla sicurezza" del progetto Debian.⁴ La pagina del progetto Debian, dove sono elencati gli annunci di sicurezza. La difficoltà, quindi, sarà quella di interpretarli...

Detto questo, anche se il sistema di crittografia utilizzato è "rotto", gli avversari devono comunque saperlo... I gendarmi di Saint-Tropez probabilmente non lo sapranno, ma un esperto forense sì.

Inoltre, per quanto riguarda la fantascienza, ricordiamo che è difficile sapere quanto siano avanti i militari e le agenzie governative come la NSA in questo campo.

Secondo angolo di attacco: attacco a freddo

1. Angolo di attacco: l'attacco a freddo è descritto nel capitolo sui binari.
2. Mezzi necessari: accesso fisico al computer mentre è illuminato o spento da poco.
3. Credibilità dell'attacco: per quanto ne sappiamo, questo attacco non è mai stato utilizzato, almeno pubblicamente, dalle autorità. La sua credibilità è quindi molto bassa.

pagina
27

Può sembrare superfluo proteggersi da questo attacco nella situazione qui descritta. Tuttavia, è meglio adottare subito delle buone abitudini, piuttosto che trovarsi di fronte a spiacevoli sorprese tra qualche anno. Quali abitudini? Eccone alcune che rendono più difficile questo attacco:

- spegnere il computer quando non viene utilizzato;
- se si utilizza un computer fisso, assicurarsi che l'alimentazione possa essere interrotta rapidamente e facilmente, ad esempio mediante un interruttore multiplo facilmente accessibile;
- se si utilizza un computer portatile e se possibile, rimuovere la batteria (è poi sufficiente scollegare il cavo di alimentazione per spegnere la macchina);
- rendere più difficoltoso e lungo l'accesso al vano RAM del computer, ad esempio incollandolo/saldandolo.

Terzo angolo di attacco: l'occhio e la videosorveglianza

Con il sistema crittografato ideato nel primo passo, la riservatezza dei dati a pagina 72 si basa sulla segretezza della passphrase. Se viene digitata di fronte a una telecamera di videosorveglianza, gli avversari che hanno accesso a questa telecamera o alla sua

Un eventuale registratore potrebbe scoprire questo segreto, quindi sequestrare il computer e accedere ai dati. Più semplicemente, in un bar, un occhio attento potrebbe vedere la passphrase mentre viene digitata.

L'impostazione di un attacco di questo tipo richiede il monitoraggio delle persone che utilizzano il computer, fino a quando una di esse non digita la passphrase nel posto sbagliato. Questa operazione può richiedere tempo e denaro.

Per proteggersi da un attacco di questo tipo, è necessario:

- scegliere una passphrase lunga e difficile da ricordare "al volo" da parte di un osservatore;

pagina
103

3. La mailing list si chiama [debian-security-announce](https://lists.debian.org/debian-security-announce/) [https://lists.debian.org/debian-security-announce/].

4. <https://www.debian.org/security/index.fr.html>

- prima di digitare la passphrase, controllare che non vi siano occhi indesiderati (umani o elettronici) nell'ambiente circostante;
- nascondere la tastiera utilizzando lo schermo nel caso di un computer portatile, oppure utilizzando una cover⁵.

Quarto angolo di attacco: la parte non criptata e il firmware

pagina
119

Come spiegato nella ricetta dedicata, un sistema crittografato non è interamente crittografato: il piccolo software che chiede la passphrase per crittografare il *resto dei* dati all'avvio è memorizzato in chiaro nella parte del disco nota come */boot*. Un malintenzionato che abbia accesso al computer può facilmente modificare questo software per installare un *keylogger* in pochi minuti. Il *keylogger* memorizza la passphrase mentre viene digitata e la recupera in un secondo momento o la invia semplicemente in rete.

pagi
na
31

Se questo attacco viene sferrato in anticipo, gli avversari saranno in grado di decriptare il disco quando sequestreranno il computer, ad esempio durante una perquisizione.

Tutto sommato, i mezzi necessari per questo attacco sono abbastanza limitati: *a priori*, non è necessario essere una supereroina per accedere, per qualche minuto, alla stanza in cui risiede il computer.

Tuttavia, per quanto riguarda la situazione descritta per questo caso d'uso, questo attacco non sembra essere il più probabile.

PRECISIONE

Un modo per proteggersi da questo attacco è quello di memorizzare i programmi di avvio, compresa la piccola cartella non crittografata (*/boot*), su un supporto esterno, come una chiavetta USB, che verrà conservata in modo permanente in un luogo più sicuro del computer. È l'*integrità* di questi dati, non la loro *riservatezza*, che deve essere protetta. Ciò richiede una grande abilità e rigore, che non approfondiremo in questa sede.

Queste pratiche alzano la posta in gioco per gli avversari, ma rimane un ma: una volta ottenuto l'accesso fisico al computer, se */boot* non è accessibile, e quindi non modificabile, è possibile effettuare lo stesso tipo di attacco al firmware della macchina (BIOS o UEFI). È un po' più difficile perché il modo per farlo dipende dal modello di computer utilizzato, ma è possibile. Non conosciamo alcun modo pratico per proteggersi da questo attacco.

Quinto angolo di attacco: il malware

pagina
31

Nel capitolo precedente abbiamo visto che il software installato su un computer a nostra insaputa può rubare i dati. In questo caso, tale software è in grado di trasmettere la chiave di crittografia del disco agli avversari, in modo che possano accedere ai dati crittografati non appena ottengono l'accesso fisico al computer.

L'installazione di malware sul sistema Debian in questione richiede un livello di abilità superiore rispetto agli attacchi studiati in precedenza, ma anche una maggiore preparazione. Un attacco di questo tipo è quindi fantascientifico, almeno per quanto riguarda questa situazione. In altre situazioni, potrebbe essere necessario essere estremamente cauti sull'origine dei dati e del software che si iniettano nel computer.

pagina
131

A tal fine, la ricetta per l'installazione del software fornisce alcuni utili suggerimenti su come installare un nuovo software in modo pulito. Il secondo volume di questa guida, dedicato alle reti, mostra che una connessione a Internet aggiunge molti nuovi angoli di attacco da cui è possibile introdurre malware.

5. Nel documentario *Citizen Four* di Laura Poitras, si vede Edward Snowden che si copre il computer per digitare la sua passphrase.

Sesto angolo di attacco: la forza bruta

Attaccare un sistema crittografico con la "forza bruta", cioè cercando la passphrase testando tutte le possibili combinazioni una per una, è il modo più semplice e più lento. Ma quando non è possibile implementare nessun altro tipo di attacco...

Per il nostro disco criptato nella prima fase, questo tipo di attacco richiede un'enorme quantità di tempo (molti anni) e/o denaro, e competenze avanzate... almeno se la passphrase è solida.

Si potrebbe pensare che se un'organizzazione è disposta a mobilitare così tante fonti per accedere ai nostri dati, farebbe bene a mettere in atto uno degli altri attacchi elencati sopra, meno costosi e altrettanto efficaci. In particolare, potrebbero andare direttamente dalla persona interessata e chiedere la passphrase, cordialmente o meno...



Disegno tratto da XKCD, tradotto da noi (<https://xkcd.com/538/>).

Caso d'uso: lavorare su un documento sensibile

10.1 Contesto

Dopo un nuovo inizio, il computer utilizzato per completare questo progetto a pagina 71 è stato dotato di un sistema crittografato. Bene. Poi si presenta la necessità di lavorare su un progetto a parte, più "sensibile", per esempio:

- è necessario redigere un opuscolo;
- è necessario tracciare un'affiche;
- un libro deve essere creato e poi esportato in formato PDF;
- una fuga di informazioni deve essere organizzata per rivelare le terribili pratiche di un'azienda;
- un film deve essere montato e masterizzato su DVD.

In tutti questi casi, i problemi da risolvere sono più o meno gli stessi.

Dato che sarebbe troppo complicato aumentare nuovamente il livello generale di sicurezza informatica, si è deciso di riservare un trattamento speciale a questo particolare progetto.

10.1.1 Convenzioni di vocabolario

Nel seguito, ci riferiremo ad essi come :

- *file di lavoro*: tutti i file necessari alla produzione dell'opera (immagini o *rushes* utilizzati come base, documenti registrati dal software utilizzato, ecc.);
- *il lavoro*: il risultato finale (volantino, affiche, ecc.).

In breve, la materia prima e il prodotto finito.

10.2 Valutazione dei rischi

Cerchiamo ora di definire i rischi che comporta lavorare con un documento sensibile.

10.2.1 Cosa vogliamo proteggere?

Applichiamo le categorie definite quando abbiamo parlato di valutazione del rischio al caso in esame. in questione.

pagina 63:

- riservatezza: per evitare che un occhio indesiderato scopra troppo facilmente il lavoro e/o i file di lavoro;
- integrità: per evitare che questi documenti vengano modificati a nostra insaputa;

- **accessibilità:** garantire che questi documenti rimangano accessibili quando necessario. In questo caso, l'accessibilità e la riservatezza sono priorità assolute.

Accessibilità, perché l'obiettivo principale è completare l'opera. Se dovessimo recarci al Polo Nord per farlo, il progetto rischierebbe seriamente di cadere nelle crepe (ghiacciate).

E quando si parla di riservatezza, tutto dipende da come viene pubblicizzato il lavoro. Diamo quindi un'occhiata più da vicino.

Lavori limitati

Se il contenuto dell'opera non è completamente pubblico, o addirittura perfettamente segreto, l'idea è quella di nascondere sia l'opera *che* i file di lavoro.

Lavoro distribuito pubblicamente

Se il lavoro deve essere pubblicato, la questione della riservatezza si riduce all'anonimato.

In questo caso, sono soprattutto i file di lavoro a dover essere nascosti sotto il tappeto: scoprirli su un computer suggerisce fortemente che i suoi proprietari hanno creato l'opera... con conseguenze potenzialmente spiacevoli.

Ma non è tutto: se l'opera, o le sue versioni intermedie, sono memorizzate su questo computer (PDF, *ecc.*), la loro data di creazione è molto probabilmente registrata nel file system e nei metadati. Il fatto che questa data sia precedente a

La pubblicazione dell'opera può facilmente portare gli oppositori a trarre conclusioni scomode sulla sua genealogia.

10.2.2 Da chi vogliamo proteggerci?

Prendiamo le minacce descritte nel caso d'uso "un nuovo inizio": il computer utilizzato per creare l'opera può essere rubato dalla polizia o durante un furto.

10.3 Qual è il sistema operativo migliore per lavorare sul documento?

10.3.1 Decidete quale software vi serve

La prima domanda è: quale software verrà utilizzato per questo progetto?

- Se il software necessario gira sotto GNU/Linux, continuiamo a leggere questo capitolo per esplorare le opzioni disponibili.
- Se questi programmi funzionano solo su Windows (o Mac OS), vale la pena di verificare se esistono programmi simili per Debian GNU/Linux. Se esistono, provateli per vedere se sembrano funzionare per questo progetto.
- Se solo il software Windows è davvero soddisfacente, è un peccato. Ma abbiamo trovato un modo praticabile per limitare i danni. Diamo quindi un'occhiata a come si presenta questo metodo, ignorando i paragrafi successivi, dedicati a GNU/Linux.

10.3.2 Utilizzare un sistema amnesico *dal vivo* per lasciare il minor numero di tracce possibile

Si potrebbe immaginare di configurare finemente un sistema Debian criptato per mantenere il minor numero possibile di tracce delle nostre attività sul disco rigido. Il problema

di questo approccio è che si tratta di un tipo di "lista bloccata". Abbiamo spiegato
66 i limiti di questo approccio: non importa quanto tempo si spende, non importa quanta
esperienza si mette a disposizione,

Anche con una conoscenza particolarmente approfondita del funzionamento interno del
sistema operativo, si dimentica sempre una piccola opzione ben nascosta.

giorni di tracce indesiderate a cui non avevamo pensato.

Un capitolo è dedicato all'installazione di un sistema Debian criptato, ma non copre
tutti i metodi per limitare le tracce. Fortunatamente, alcuni sistemi *live*
amnesiac funzionano secondo il principio della "lista autorizzata": a meno che non
sia esplicitamente richiesto, non vengono lasciate tracce sul disco rigido.

Sulla base della sola riservatezza, il sistema *live* batte di gran lunga gli altri.
D'altra parte, se il suo principale vantaggio è l'amnesia, questo può talvolta
essere uno svantaggio. Ad esempio, se il nostro sistema *live* preferito non
fornisce un software essenziale per il progetto, dovrete installarlo a ogni avvio,
cosa che fortunatamente può essere fatta automaticamente.

Se l'utilizzo di un sistema *live* è quindi la soluzione più sicura, è anche la meno
difficile da implementare, vista la difficoltà di installare un sistema Debian che
lascia poco

traccia. Nella sezione seguente, esamineremo un criterio di sicurezza basato
su questa soluzione.

Va notato che è anche possibile installare un sistema Debian in una macchina
virtuale per soddisfare esigenze simili, ma questa soluzione è meno adatta e quindi non
verrà descritta qui. La documentazione è disponibile online, anche se è importante
prendere le stesse precauzioni di compartimentazione per Debian descritte nel
capitolo sulla creazione di una macchina virtuale Windows.

pagina

pagina

119

pagina

113

prossimo

pagina.

pagina

163

10.4 Lavorare su un documento sensibile... su un sistema *attivo*

[página 79] Dopo aver preparato la scena all'inizio di questo caso d'uso e aver deciso di utilizzare un *sistema attivo*, ora dobbiamo implementare questa soluzione... ed esaminarne i limiti.

10.4.1 Scaricare e installare il sistema *live*

Non tutti i sistemi *live* sono progettati per un uso "sensibile". È quindi importante scegliere un sistema appositamente progettato per (tentare di) non lasciare traccia sul disco rigido del computer su cui viene utilizzato. Questa guida si concentra e documenta il sistema *live* Tails.

Se non si dispone già di una copia dell'ultima versione del sistema *live* Tails, seguire le istruzioni per scaricare e installare un sistema *live* "discreto" (vedere pagina 114).

Una volta installato il dispositivo Tails sulla nostra chiave, possiamo, se lo desideriamo, creare uno spazio di archiviazione criptato per salvare alcuni documenti o impostazioni. A tale scopo, prendere il sistema *live* precedentemente installato e avviarlo (vedere pagina 107). Quindi seguire le istruzioni per la creazione e la configurazione di un volume persistente in Tails (vedere pagina 116).

10.4.2 Installare qualsiasi software aggiuntivo

Se avete bisogno di utilizzare un software non installato in Tails e non volete reinstallarlo ogni volta, seguite la ricetta per l'installazione di software aggiuntivo persistente in Tails (vedere pagina 117).

10.4.3 Utilizzo del sistema *live*

Ogni volta che si desidera lavorare sul documento, è necessaria la chiave contenente il sistema *live* e la sua persistenza crittografata per avviarlo (vedere pagina 107). È quindi necessario attivare il volume persistente (vedere pagina 116).

10.4.4 Cancellare i dati

Una volta completato il progetto e stampato o pubblicato online (vedere pagina 285), è possibile archiviarlo (vedere pagina 89). È quindi necessario eliminare il volume persistente (vedere pagina 116) contenente i dati.

10.4.5 C'è ancora molto da fare

Dobbiamo ancora ripulire i metadati (vedi pagina 88) e studiare i limiti del nostro approccio (vedi pagina 88).

10.5 Lavorare su un documento sensibile... in Windows

[página 79] Avendo preparato la scena all'inizio di questo caso d'uso, e nonostante tutti i problemi legati all'uso di Windows, cerchiamo ora di limitare un po' i danni.

10.5.1 Punto di partenza: un colino e una scatola di cerotti secchi.

Partiamo da un computer dotato, nel modo più convenzionale, di un disco rigido su cui è stato installato Windows. Non ci soffermeremo qui su questa situazione, poiché la prima parte di questo libro ha abbondantemente descritto i numerosi problemi che essa pone. In breve, un colabrodo pieno di falle nella sicurezza.

Possiamo quindi immaginare di attaccare qualche toppa su questo colino ¹. Facciamo un rapido giro.

Un disco rigido può essere smontato e nascosto. È vero. Ma ci sono momenti in cui è in uso, a volte per giorni o settimane. Questa patch si basa su due ipotesi un po' azzardate:

- *Siamo fortunati.* Basta infatti che l'incidente (perquisizione, furto con scasso, ecc.) avvenga nel momento sbagliato perché tutta la riservatezza desiderata si riduca a nulla.
- *La nostra disciplina è perfettamente rigorosa.* Infatti, se ci si dimentica, o non ci si prende il tempo, di "mettere via" il disco rigido quando non serve più, e a quel punto si verifica un incidente, il gioco è fatto.

Esistono anche strumenti per la crittografia dei dati in Windows. Per quanto ci si possa fidare di questi strumenti, resta il fatto che essi si basano necessariamente sulle funzioni offerte dalla scatola nera di Windows. In ogni caso, Windows avrà accesso *in chiaro* ai nostri dati e nessuno sa cosa potrebbe farne.

Per concludere questo piccolo tour nella corte dei miracoli, aggiungiamo che l'unica "soluzione" possibile in questo caso sarebbe un approccio a liste bloccate,

la cui inefficacia è già stata spiegata sopra

pagina 66

Ora è il momento di mettersi all'opera.

10.5.2 Secondo passo: racchiudere Windows in uno scomparto (quasi) stagno

Quella che comincia a sembrare una soluzione seria sarebbe far funzionare Windows in un compartimento stagno, con una porta aperta, quando necessario e con cognizione di causa, per consentirgli di comunicare con il mondo esterno in modo strettamente limitato.

In altre parole, impostare una soluzione basata su una logica di *elenco autorizzato*: nulla può entrare o uscire da Windows *a priori* e, a partire da questa regola generale, le *eccezioni* vengono autorizzate caso per caso, tenendo conto del loro impatto.

La *virtualizzazione* ² consente di configurare questo tipo di sistema. Si tratta di un insieme di tecniche hardware e software che consentono di eseguire diversi sistemi operativi separatamente su un unico computer, (quasi) come se fossero in esecuzione su macchine fisiche separate.

Oggi è relativamente facile eseguire Windows **all'interno di un computer**, un sistema GNU/Linux, interrompendo così l'accesso alla rete.

- e, in particolare, isolandolo da Internet.



Nota bene: è consigliabile leggere l'intero capitolo prima di precipitarsi nelle ricette pratiche; la descrizione dell'ipotesi che segue è piuttosto lunga e i suoi limiti vengono esplorati alla fine del capitolo, dove vengono prese in considerazione le contromisure. Sarebbe un peccato passare quattro ore a seguire queste ricette, prima di rendersi conto che una soluzione completamente diversa sarebbe, in realtà, più appropriata.

Iniziamo riassumendo l'ipotesi proposta.

1. [Archivio INA, La passoire des Shadoks](https://www.youtube.com/watch?v=1Duiup2tWKA) [https://www.youtube.com/watch?v=1Duiup2tWKA]
2. Per ulteriori informazioni, consultare la pagina [Wikipedia, 2020, Virtualizzazione](https://fr.wikipedia.org/wiki/Virtualizzazione) [https://fr.wikipedia.org/wiki/Virtualizzazione].

pagina
71

L'idea è quindi quella di eseguire Windows in un compartimento stagno *a priori*, **all'interno** di un sistema Debian crittografato come quello impostato dopo aver letto il caso d'uso precedente. Quello che fungerà da disco rigido di Windows è in realtà un file di grandi dimensioni memorizzato sul disco rigido del nostro sistema Debian crittografato.

Installare il gestore di macchine virtuali

È quindi necessario seguire la ricetta per l'installazione di Virtual Machine Manager (vedere pagina 163). Questo software verrà utilizzato per avviare Windows in un compartimento stagno.

Installazione di un Windows "pulito" nel Gestore macchine virtuali

Prepariamo un'immagine *pulita* del disco virtuale: per farlo, seguite la ricetta per l'installazione di Windows virtualizzato (vedere pagina 165). Questa ricetta spiega come installare Windows nel Gestore macchine virtuali, interrompendo fin dall'**inizio** l'accesso alla rete.

Da quel momento in poi, Windows viene chiamato sistema *ospite* dal sistema Debian criptato, che è il sistema *host*.

Installare il software necessario in Windows "pulito"

Potreste anche installare tutto il software *non promettente* di cui avete bisogno per creare i vostri lavori premeditati in questo momento nel vostro Windows "pulito".³ In questo modo eviterete di doverlo rifare all'inizio di ogni nuovo progetto... e, speriamo, eviterete di usare un'immagine "sporca" di Windows per un nuovo progetto, un giorno, quando il tempo sta per scadere.

Poiché l'*ospite* di Windows non può lasciare la scatola per recuperare i file, è necessario inviargli i file di installazione del software necessari dall'"esterno".

Torneremo su questo punto più avanti, quando gli invieremo file di ogni tipo. Per il momento, dato che stiamo preparando un'immagine "pulita" di Windows da usare come base per ogni nuovo progetto, non confondiamo tutto e accontentiamoci di inviargli solo ciò che è necessario per installare il software desiderato e non compromettente.

Creiamo una cartella sul sistema host chiamata *Windows Software* e copiamo **solo il file** i file necessari per installare il software desiderato.

Condividere quindi questa cartella con il *guest* Windows. A tale scopo, seguire la ricetta per la condivisione di una cartella con un sistema virtualizzato (vedere pagina 171).

E per quanto riguarda l'installazione di software all'interno di Windows *guest*: chiunque sia abbastanza esperto di Windows da leggere queste pagine è, senza dubbio, più competente di chi sta scrivendo queste righe.



Nota bene: una volta completato questo passaggio, **non** si deve fare **nient'**altro in questo Windows virtualizzato.

Eeguire un'istantanea di Windows "pulito"

Ora facciamo un'*istantanea* della macchina virtuale *pulita* che abbiamo appena preparato. In altre parole, salviamo il suo stato in un angolo. In futuro, questa istantanea servirà come punto di partenza per ogni nuovo progetto.

È quindi necessario seguire la ricetta per l'acquisizione di un'istantanea di una macchina virtuale (vedere pagina 168).

3. Ad esempio, se si vuole nascondere il fatto che si fanno film, avere un software di editing video può essere compromettente.

Nuovo progetto, nuovo inizio

Supponiamo che stiate iniziando un nuovo progetto che richiede Windows; ecco come procedere:

1. Ripristinare l'istantanea della macchina virtuale contenente l'installazione di Windows.
2. La macchina virtuale può ora essere avviata nel suo scomparto sigillato. Verrà utilizzata **esclusivamente** per il nuovo progetto e ora diventa una macchina virtuale *sporca*.
3. All'interno di questa nuova macchina virtuale *di vendita*, viene creato un nuovo utente Windows. Il nome assegnato deve essere diverso **ogni volta che** si avvia un nuovo progetto e questo utente sarà utilizzato **esclusivamente** per questo nuovo progetto. Questo perché il software tende a registrare il nome dell'utente attivo nei metadati dei file salvati, pag. 30 e che è meglio evitare di fare controlli incrociati sfortunati.

I dettagli tecnici del primo passo sono spiegati nella ricetta per il ripristino dello stato di una macchina virtuale da un'istantanea (vedere pagina 168). Per quanto riguarda la creazione di un nuovo utente sulla versione di Windows in uso, chi sta leggendo questa pagina sarà sicuramente in grado di trovarlo nel *Pannello di controllo*.

Ora che abbiamo un compartimento stagno, vediamo come aprire le porte al suo interno in modo selettivo, a seconda delle necessità.

Come si inviano i file all'utente guest di Windows? Poiché l'utente *guest* di Windows non è autorizzato a lasciare la casella per recuperare i file, può essere necessario inviargli i file dall'"esterno", ad esempio :

- materiale grezzo (*bozze*, immagini o testi provenienti da altre fonti);
- software necessari per il nuovo progetto e non presenti nell'immagine virtuale "pulita" appena ripristinata.

Abbiamo già visto come farlo, ma in un caso molto specifico: l'installazione di nuovo software in un Windows *guest* "pulito". La condivisione di file con un Windows "sporco" richiede una maggiore attenzione e precauzioni, che ora analizzeremo.

La procedura è leggermente diversa, a seconda del supporto su cui si trovano originariamente i file da importare (CD, DVD, chiavetta USB, cartella sul disco rigido del sistema crittografato), ma le precauzioni abituali sono le stesse:

- Windows deve avere accesso **solo** ai file che si desidera importare e basta. Non si deve dare accesso a una cartella contenente un'accozzaglia di file relativi a progetti che non dovrebbero sovrapporsi. Se questo significa iniziare una fase di selezione e riordino, ben venga.
- Quando Windows deve *leggere* (copiare) i file contenuti in una cartella, gli viene concesso l'accesso *in sola lettura* a tale cartella. Meno diritti si concedono a Windows per scrivere qua e là, meno tracce fastidiose lascerà.

Per evitare di mescolare le spazzole, si consiglia di :

- creare **una singola** cartella di importazione per ogni progetto ;
- nominare questa cartella nel modo più esplicito possibile; ad esempio:
Cartella leggibile da Windows ;
- non condividere mai cartelle diverse da questa con l'*ospite* Windows.

Le spiegazioni pratiche sono fornite nella ricetta per l'invio di file al sistema virtualizzato (vedere pagina 171).

Come si fa a far uscire i file dal Windows sigillato? Per impostazione predefinita, il *guest* Windows non è autorizzato a lasciare tracce al di fuori del suo compartimento stagno. Ma quasi inevitabilmente, arriva il momento in cui è necessario far uscire i file da esso, e a quel punto è necessario autorizzarlo esplicitamente. Ad esempio :

- per portare un file PDF esportato alla casella di copia o alla stampante;
- per proiettare il film appena uscito in DVD.

A tal fine, esporremo questi file in una cartella vuota, dedicata a questo scopo, e memorizzata su un volume crittografato che può essere :

- una chiave USB criptata, attivata sotto Debian digitando la passphrase corrispondente;
- il disco rigido della Debian criptata, che qui funge da ufficio del sistema *host*.

Questa cartella dedicata sarà condivisa con il *guest* Windows. Sottolineiamo le parole **vuoto** e **dedicato**: Windows sarà in grado di leggere e modificare tutto ciò che si trova in questa cartella e sarebbe un peccato permettergli di leggere i file, quando l'unica cosa da fare è esportare un file.

Se è necessario masterizzare un DVD, è possibile farlo da Debian.

Per evitare di mescolare i pennelli e limitare il contagio, si consiglia di :

- creare **una singola** cartella di esportazione per ogni progetto ;
- nominare questa cartella nel modo più esplicito possibile; ad esempio: *Cartella in cui Windows può scrivere* ;
- non condividere mai con l'*ospite* Windows altre cartelle oltre a questa, a parte la cartella di importazione consigliata nel paragrafo precedente.

Le ricette per la condivisione di una cartella con un sistema virtualizzato (vedere pagina 171) e per la crittografia di una chiave USB (vedere pagina 145) spiegano come procedere nella pratica.

Quando il progetto è terminato

Una volta terminato il progetto, è il momento di pulire, ma prima :

1. il lavoro risultante viene esportato sul supporto appropriato (carta, DVD, ecc.), con l'aiuto del paragrafo precedente, che spiega come produrre file dal sistema operativo *guest* Windows ;
2. I file di lavoro vengono archiviati, se necessario (il caso d'uso seguente riguarda proprio questo aspetto).

Poi è il momento della grande pulizia, eliminando il maggior numero possibile di tracce del progetto completato dal sistema *host*:

- l'immagine del disco virtuale viene ripristinata allo stato "pulito" utilizzando la ricetta per il ripristino dello stato di una macchina virtuale da un'istantanea (vedere pagina 168);
- dopo un ultimo controllo che tutto ciò che deve essere conservato sia stato archiviato altrove, le cartelle condivise con Windows vengono eliminate "per davvero" (vedere pagina 141);
- Le tracce lasciate sul disco rigido vengono cancellate "per davvero" (vedere pagina 143).

Un altro nuovo progetto?

Se arriva un nuovo progetto che richiede l'uso di Windows, **non** riutilizziamo lo stesso *sporco* Windows. Torniamo invece alla fase "nuovo progetto, nuovo inizio".

pagina
89

pagina
preceden
te

10.5.3 Terza fase: possibili attacchi e contromisure

L'ipotesi che abbiamo appena descritto si basa sull'utilizzo, come sistema *host*, una Debian criptata. Tutti gli attacchi a questa Debian criptata sono quindi applicabili alla presente soluzione. Ora è il momento di studiare gli attacchi che possono essere utilizzati contro questo sistema.

Tracce lasciate sulla nostra Debian criptata

La maggior parte delle tracce più evidenti di questo progetto sono separate dal resto del sistema: tutti i file di lavoro sono memorizzati nel file contenente l'immagine del disco virtuale. Il nome della macchina virtuale, la sua configurazione e i periodi di utilizzo, invece, lasceranno altre tracce sul nostro sistema Debian.

Se si verifica un disastro durante l'esecuzione del progetto, il disco rigido del computer utilizzato contiene i file di lavoro all'interno dell'immagine del disco virtuale.

Se la catastrofe si verifica in seguito Poiché l'immagine del disco virtuale viene ripulita correttamente al termine del progetto, se la catastrofe si verifica in seguito (cedimento alla legge, scoperta di un problema nel sistema crittografico), le tracce residue sul disco rigido saranno meno evidenti e meno numerose che se si fosse proceduto in modo ordinario.

Anche se la catastrofe si verifica dopo la fine del progetto, cioè dopo la bonifica, il progetto è stato completato.

Come spiega l'inizio di questo caso d'uso a pagina 79, il principale inconveniente del metodo qui descritto è che si basa sul principio della lista bloccata, un principio molto criticato su queste pagine... e a pagina 66 rimarranno quindi sempre tracce indesiderate, a cui non avevamo pensato, sull'hard disk del computer utilizzato, oltre a quelle che ormai conosciamo bene: log a pagina 27, memoria ad accesso casuale e "virtuale", backup automatici.

Se, nonostante queste preoccupazioni, l'ipotesi che abbiamo appena descritto sembra essere una compromesso accettabile, è ora necessario scoprire le limitazioni condivise da tutte le soluzioni considerate in questo caso d'uso.

In caso contrario, andiamo a scavare.

Andare oltre

Si ipotizzi che uno degli attacchi descritti nella terza fase del caso d'uso a pagina 74

Un "nuovo inizio" sembra credibile. In caso di successo, il contenuto del disco rigido crittografato del sistema *host* del disco rigido del sistema *host* sarebbe leggibile, in chiaro, dall'aggressore. Ma è bene ricordare che questi file di lavoro sono contenuti nel disco virtuale.

immagine utilizzata dal nostro *ospite* Windows... che è un file insulso memorizzato sul disco rigido del sistema *host*. Questi file di lavoro, insieme a qualsiasi traccia registrata dal software utilizzato in Windows, diventano quindi leggibili dall'aggressore.

Esamineremo due modi per limitare i danni. Uno è un "elenco bloccato", l'altro è un "elenco autorizzato".

Memorizzazione dell'immagine del disco virtuale fuori dal disco rigido del sistema *host*
Un'idea è quella di memorizzare l'immagine del disco virtuale utilizzata dal sistema Windows *guest* fuori dal disco rigido del sistema *host*. Ad esempio, su un disco rigido esterno crittografato. In questo modo, anche se il disco del sistema *host* viene decriptato, i nostri file di lavoro rimangono inaccessibili... a patto che il disco rigido esterno che li contiene non sia alla portata dell'avversario in quel momento.

Si tratta di un approccio di tipo "elenco bloccato", con tutti i problemi che ciò comporta. pagina 66 I file di lavoro e il sistema Windows non vengono salvati sul disco fisso.

sul sistema *host*. Non dimenticate però che questi dati verranno utilizzati dal Virtual Machine Manager, che a sua volta gira sul sistema *host*. Come spiegato nel capitolo "Tracce a tutti i livelli", varie tracce rimarranno quindi inevitabilmente **sul disco rigido interno** del computer in uso.

Per seguire questo percorso :

- scoprire i limiti condivisi da tutte le soluzioni considerate in questo caso d'uso;
- vedere la ricetta per la crittografia di un disco rigido esterno.

La controparte di questo approccio "elenco bloccato" è una soluzione "elenco autorizzato", che combina l'uso di un sistema *live* e la memorizzazione dell'immagine del disco virtuale su un disco rigido esterno crittografato.

Per seguire questo percorso :

- scoprire i limiti condivisi da tutte le soluzioni considerate in questo caso d'uso;
- Vedere la ricetta per la crittografia di un disco rigido esterno e la ricetta per l'utilizzo di un sistema *live*.

10.6 Pulire i metadati del documento finito

Una volta completato il documento, lo esportiamo in un formato adatto allo scambio di documenti - ad esempio, un PDF per stampare un testo, un file AVI o MKV per pubblicare un video su Internet, *ecc.*

Supponiamo di pubblicare il nostro documento senza prendere ulteriori precauzioni. Gli oppositori che non lo gradiscono probabilmente inizieranno a scaricare il documento alla ricerca di qualsiasi metadato che possa collegarlo alle persone che lo hanno prodotto.

Nonostante le precauzioni già prese, è bene ripulire i metadati eventualmente presenti.

10.7 Limiti comuni a queste politiche di sicurezza

Qualsiasi politica di sicurezza basata su questo caso d'uso è vulnerabile a una serie di attacchi, indipendentemente dal fatto che utilizzi un sistema *live* o il famigerato Windows.

Gli angoli di attacco del capitolo Nuovi inizi esaminano alcuni degli attacchi immaginabili, più o meno fantascientifici, a seconda del tempo, del luogo, dei protagonisti e delle circostanze. È giunto il momento di rileggerli con occhi nuovi.

Inoltre, nella sezione "Problemi" di questo volume sono stati trattati in termini relativamente generali alcuni metodi di sorveglianza, che può essere utile rivisitare alla luce della situazione concreta che stiamo trattando; in particolare, citiamo i temi dell'elettricità, dei campi magnetici e delle onde radio, nonché gli effetti di varie cimici.

Caso d'uso: archiviazione di un progetto completato

11.1 Contesto

Un progetto delicato sta per essere completato; ad esempio, un libro è stato progettato e stampato a pagina 79, oppure un film è stato montato, compresso e masterizzato su DVD.

In generale, non sarà più necessario avere un accesso permanente ai file di lavoro (iconografia ad alta risoluzione, *rushes* non compressi). D'altra parte, può essere utile poterli recuperare in un secondo momento, ad esempio per una riedizione, una versione aggiornata, ecc.

Poiché più un sistema viene usato frequentemente, più è probabile che venga *attaccato*, è meglio estrarre le informazioni usate raramente dal computer che si usa ogni giorno. Inoltre, è più facile negare qualsiasi collegamento con i file quando sono memorizzati su una chiavetta USB nel bosco, piuttosto che quando sono memorizzati sul disco rigido del computer.

11.2 È davvero necessario?

La prima domanda da porsi prima di archiviare tali file è: è *davvero* necessario conservarli? Quando un'informazione non è più disponibile, per quanto ci si sforzi, nessuno sarà in grado di fornirla, e a volte questa è la soluzione migliore.

11.3 Valutazione dei rischi

11.3.1 Cosa vogliamo proteggere?

Cosa succede ai requisiti definiti quando abbiamo parlato di valutazione del rischio a pagina 63, applicati a questo caso?

- riservatezza: per evitare che un occhio indesiderato cada troppo facilmente sulle informazioni archiviate;
- integrità: impedire che le informazioni vengano modificate a nostra insaputa;
- accessibilità: garantire che le informazioni rimangano accessibili quando necessario.

In questo caso, l'accessibilità è secondaria rispetto alla riservatezza: l'idea dell'archivage è quella di fare un compromesso, rendendo l'accesso ai dati più difficile *per tutti*, per offrire loro una migliore riservatezza.

11.3.2 Da chi vogliamo proteggerci?

I rischi previsti nel nostro "nuovo inizio" sono validi anche in questo caso: una pagina 71

furto con scasso, una ricerca per motivi non direttamente legati alle informazioni che desideriamo proteggere.

A questi rischi si aggiunge la possibilità che il libro o il film prodotto possa scontentare qualche commissario, ministro, amministratore delegato o simili. Succede. Diciamo:

- questa autorità è venuta a conoscenza di indizi che la portano a sospettare chi ha commesso il capolavoro;
- Questa autorità è in grado di inviare una coorte di poliziotti nelle prime ore del mattino a casa di sospetti criminali.

Un'intrusione così intempestiva comporterà, come minimo, il sequestro dell'hardware informatico eventualmente rinvenuto. L'apparecchiatura sarà poi consegnata a un esperto di computer, che eseguirà una sorta di autopsia per scoprire i dati memorizzati... o che sono stati memorizzati.

pagina

na

42

11.4 Metodo

Il metodo più semplice attualmente è :

1. creare una chiave USB o un disco rigido esterno crittografato (vedere pagina 145);
2. copiare i file da archiviare su questo dispositivo ;
3. cancellare e sovrascrivere il contenuto dei file di lavoro (vedere pagina 139).

Una volta eseguite queste operazioni, la chiave o il disco rigido possono essere conservati in un luogo diverso dal computer che si utilizza più spesso.

I CD o i DVD potrebbero essere presi in considerazione per il loro basso costo, ma è più complesso criptare correttamente i dati su questi supporti rispetto alle chiavette USB, che sono ormai comuni e facili da ottenere.

11.5 Quale passphrase?

pagina

103

Poiché i file saranno archiviati in forma crittografata, sarà necessario scegliere una passphrase. Tuttavia, dato che lo scopo è l'archiviazione, questa passphrase non sarà usata molto spesso. E una passphrase usata raramente rischia di essere dimenticata... rendendo praticamente impossibile l'accesso ai dati.

Esistono diverse soluzioni possibili a questo problema.

11.5.1 Scrivete la passphrase da qualche parte

La difficoltà sta nel sapere dove scriverla, dove conservarla per poterla ritrovare... senza che altri possano trovarla e identificarla come una passphrase.

11.5.2 Utilizzare la stessa passphrase del sistema giornaliero.

pagina

119

La passphrase per il vostro sistema giornaliero, se è crittografato, è quella che digitate regolarmente e che probabilmente ricordate.

D'altra parte:

- se si è costretti a rivelare la passphrase comune, diventa possibile anche l'accesso all'archivio;

- è necessario avere **un elevato livello di fiducia** nei computer utilizzati per accedere agli archivi. In caso contrario, la passphrase può essere "rubata" a vostra insaputa e utilizzata per leggere non solo le informazioni archiviate, ma anche tutti i dati memorizzati sul vostro computer di tutti i giorni.

11.5.3 Condividere il segreto con altri

Un segreto può essere condiviso da più persone. Ciò richiede la presenza di più persone per accedere al contenuto archiviato. Questo aspetto deve essere valutato: può complicare il compito, sia per gli accessi desiderati che per quelli indesiderati.

pagina
157

11.6 Un disco rigido? Una chiave? Diverse chiavi?

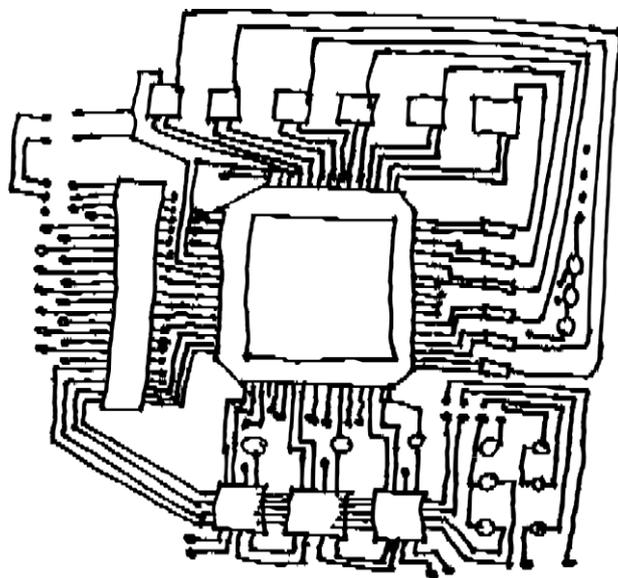
In base alle scelte fatte in precedenza, in particolare per quanto riguarda le passphrase, ci si può chiedere quale supporto utilizzare. Da un punto di vista tecnico, la soluzione più semplice al momento è quella di utilizzare un'unica passphrase per ogni supporto.

Un disco rigido esterno può contenere più dati di una chiavetta USB e quindi a volte è necessario: per archiviare un progetto video, ad esempio.

Archiviare più progetti sullo stesso supporto semplifica il compito, ma rende difficile separare i progetti in base ai livelli di riservatezza desiderati. Infatti, chi può accedere agli archivi di un progetto ha accesso anche agli altri, il che non è necessariamente auspicabile.¹

Inoltre, se la passphrase è un segreto condiviso, tanto vale facilitare l'accesso alle persone che condividono il segreto, disponendo di un supporto che possono trasmettersi reciprocamente.

1. Il tema della compartimentazione è sviluppato nel capitolo sulle identità contestuali. [pagina 246].



TERZA PARTE

Strumenti

Introduzione

In questa terza sezione spiegheremo come applicare in pratica alcune delle idee sopra esposte.

Questa sezione è un'appendice tecnica alle sezioni precedenti. Una volta compreso

Una volta scelte le risposte di pagina 59 che fanno al caso vostro, resta da chiedersi "Come si fa?", a cui questa appendice fornisce alcune risposte.

Per la maggior parte delle ricette presentate in questa guida, si presuppone che si utilizzi GNU/Linux con il desktop GNOME; queste ricette sono state scritte e testate sotto Debian GNU/Linux versione 11 (soprannominata Bullseye) ¹ e Tails versione 5 ² (*The Amnesic Incognito Live System*).

Tuttavia, questi sono generalmente adattabili ad altre distribuzioni basate su Debian, come Ubuntu ³ o Linux Mint ⁴.

Se non utilizzate ancora GNU/Linux, potete consultare il caso d'uso di un nuovo avvio o utilizzare un sistema live.

a

71 o utilizzare un sistema *attivo*.

Le procedure sono presentate passo per passo e, laddove possibile, viene spiegato il significato delle azioni proposte.

L'ordine in cui ogni ricetta viene descritta è importante. A meno che non sia indicato diversamente, si raccomanda di non saltare un passaggio e poi tornare indietro. Il risultato potrebbe essere molto diverso da quello atteso.

Infine, è importante utilizzare la versione più aggiornata di questa guida, poiché il software si evolve. È possibile trovarla sul sito web <https://guide.boum.org/>.

1. <https://www.debian.org/releases/bullseye/index.fr.html>
2. <https://tails.boum.org/index.fr.html>
3. <https://www.ubuntu-fr.org/>
4. <https://linuxmint.com/>

Utilizzo di un terminale

🔄 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: Da quindici a trenta minuti.*

Un personal computer viene spesso utilizzato facendo clic su menu e icone. Tuttavia, c'è un altro modo per "parlare" con lui: digitando pezzi di testo chiamati "comandi". La chiave per digitare questi comandi si chiama

Ad esempio, il "terminale", la "*shell*" o la "linea di comando".

Per quanto possibile, questa guida cerca di evitare l'uso di questo strumento, che può essere piuttosto confuso se non si è abituati. Tuttavia, il suo utilizzo si è rivelato talvolta indispensabile.

12.1 Che cos'è un terminale?

Una spiegazione dettagliata dell'uso delle righe di comando va oltre lo scopo di questa guida, ma Internet è pieno di tutorial e corsi che fanno proprio questo.¹ Tuttavia, ci è sembrato necessario fornire alcune nozioni di base sul loro utilizzo.

Iniziamo quindi aprendo un terminale: sul desktop di GNOME 3, aprete la panoramica delle attività premendo (su Mac), quindi digitate **terminale** e fate clic su **Terminale**. Si aprirà una finestra che mostra :

```
IDENTIFICATORE@ NOME-MACCHINA :~$
```

Alla fine c'è un quadrato, chiamato "cursore", che corrisponde al punto in cui si inserisce il testo del comando. In concreto, con l'identificatore *rabouane* su una macchina chiamata *debian*, si vedrà :

```
rabouane@debian:~$
```

Da questo stato, noto come "prompt dei comandi", è possibile digitare direttamente i comandi che si desidera far eseguire al computer.

L'effetto finale di questi comandi è spesso lo stesso che si ottiene facendo clic nel punto giusto di un'interfaccia grafica.

Per esempio, se si scrive **firefox** nel terminale appena aperto e poi si scrive **Invio** (o **↵**) per aprire il browser web *Firefox*.

Tuttavia, non saremo in grado di inserire un nuovo comando nel nostro terminale finché non chiuderemo il browser. Avremmo potuto fare esattamente la stessa cosa

1. Tra gli altri, una [pagina su ubuntu-en.org](https://doc.ubuntu-fr.org/console) [https://doc.ubuntu-fr.org/console] che a sua volta termina con altri collegamenti.

Per farlo, premere  ( su Mac) e digitare `navig`, quindi fare clic su *Firefox ESR*.

Ai fini di questa guida, il vantaggio principale del terminale è che consente di eseguire azioni che nessun'altra interfaccia grafica attualmente offre.

12.2 Informazioni sui controlli

I comandi sono come ordini impartiti al computer tramite il terminale. Queste "righe di comando" hanno un linguaggio proprio, con parole, lettere e sintassi proprie. È quindi utile fare alcune osservazioni su questo argomento.

12.2.1 Sintassi

Prendiamo ad esempio questo comando, `sfill`, che esegue più o meno le stesse operazioni di `nautilus-wipe`, uno strumento grafico che verrà presentato più avanti:

pagina
143

```

┌───┐ sfi  ┌─┐ ┌─┐ ┌───┐ /home
ll      opzion opzion argomento
ordine  e      e

```

In questa riga di comando, possiamo vedere, in ordine :

- il *comando* che chiamiamo è `sfill`. Il comando è solitamente un programma installato nel sistema;
- due *opzioni*, `-l` e `-v`, che modificano il comportamento del programma `sfill`. Queste possono essere opzionali a seconda del programma (e iniziano con uno o due trattini per distinguerle);
- un *argomento di tipo* `/home` che specifica su cosa lavorerà il comando. Possono essercene diversi o nessuno, a seconda del comando.

Ciascuno di questi elementi deve essere separato dagli altri da uno (o più) spazi. Quindi c'è uno spazio tra il comando e la prima opzione, tra la prima opzione e la successiva, tra l'ultima opzione e il primo argomento, tra il primo argomento e gli argomenti successivi *e così via*.

Non c'è alcun mistero quando si tratta di conoscere le opzioni e gli argomenti di un comando: ognuno di essi ha normalmente una *pagina man*. Per accedervi, è sufficiente digitare `man` seguito dal nome del comando nel Terminale, quindi premere *Invio*.

 o ). Questi ultimi, tuttavia, possono risultare di difficile comprensione a causa della loro restituire

aspetti tecnici e talvolta sono disponibili solo in inglese.

12.2.2 Inserimento di un percorso di file

Quando si utilizza un terminale, è spesso necessario specificare cartelle e file. Il termine "percorso" viene utilizzato per descrivere la cartella e la sottocartella in cui si trova un file. Per separare una cartella dal suo contenuto, si usa il carattere `/` (pronunciato "slash").

Per fare un esempio, ecco il *percorso* del documento `recette.txt` nel file

Cartella Documenti della cartella personale dell'account Alligator:

```
/ home/ alligatore/ documenti/ ricette. txt
```

Poiché molti comandi prevedono come argomenti i nomi dei file, diventa presto noioso digitare a mano i loro percorsi completi. Esiste tuttavia un modo più semplice per inserire un percorso: quando si afferra l'icona di un file con il mouse e la si trascina per rilasciarla sul terminale, il suo percorso viene scritto nel punto in cui si trova il cursore.

Tuttavia, questo funziona solo con i file o le cartelle "reali". Si otterrà un nome strano che non funzionerà, ad esempio, con i file del cestino, l'icona della *cartella personale* sul desktop o le icone delle chiavette USB.

12.2.3 Esecuzione

Una volta digitato un comando, si chiede al computer di "eseguirlo".
premeendo il tasto *Invio* (↵) oppure (ritorno).

12.2.4 Ordine di fine o di interruzione

L'esecuzione dei comandi richiede tempi variabili. Al termine, il terminale torna sempre allo stato in cui si trovava prima dell'esecuzione del comando, il "prompt dei comandi":

```
rabouane@debian:~$
```

Si dice quindi che il terminale "restituisce".

Se si desidera interrompere l'esecuzione di un comando prima che sia terminato, è possibile premere il tasto **Ctrl**, e tenendo premuto il tasto premere sul **C**. In questo modo il comando si interrompe immediatamente, come avviene quando chiudere la finestra di un programma.

12.2.5 Tipografia

La maggior parte dei simboli utilizzati per inserire comandi completi sono simboli comuni. Quando un comando utilizza il simbolo "-", si tratta di un "trattino".

che si può ottenere digitando (su una tastiera francese) il key **Pe**: un "' (apostrofo destro). **4**.

Altri simboli sono raramente utilizzati al di fuori del terminale, ma sono disponibili sulle tastiere standard. Sono anche indicati sulla tastiera e sono accessibili con il tasto pulsante **Alt** a destra, ha preso nota **Alt Gr**. Qui, sulla base della tastiera di un PC di

Lo standard francese, la corrispondenza di alcuni tasti con i simboli che scrivono e i loro nomi (in questa guida ne verranno utilizzati pochissimi):

Chiav	Risultati	Nome del simbolo
Alt		
Gr + 2	~	tilde
Alt Gr + 3	#	hash
Alt Gr + 4	{	tutore sinistro
Alt Gr + 5	[gancio sinistro
Alt Gr + 6		<i>tubo</i>
Alt Gr + 8	\	backslash
Alt Gr + 0	@	a
Alt Gr +)]	gancio dritto
+ =	}	tutore destro

12.2.6 Nomi da sostituire

A volte, specifichiamo che daremo un nome a qualcosa che abbiamo trovato, in modo da poterlo riutilizzare in seguito. Ad esempio, diremo che l'identificatore è LOGIN. Diciamo che stiamo lavorando con l'identificatore daisy. Quando si scrive "digita LOGIN, sostituendo LOGIN con l'ID del tuo account", in realtà si digita paquerette.

12.3 Privilegi amministrativi

Alcuni comandi che modificano il sistema richiedono diritti amministrativi. In questo modo si avrà accesso illimitato all'intero sistema, con tutti i rischi che ciò comporta.

Per eseguire un comando con diritti amministrativi, anteporre `pkexec` al nome del comando. Una finestra richiederà la password prima di eseguire il comando.

12.4 Avvertenze

Ancor più che per le ricette citate in precedenza, i comandi devono essere digitati con la massima precisione. Dimenticare uno spazio, omettere un'opzione, sbagliare un simbolo o essere imprecisi in un argomento cambia il significato del comando.

E poiché il computer fa *esattamente* ciò che gli viene richiesto, se si cambia il comando, farà *esattamente il contrario*...

12.5 Un esercizio

Creeremo un file vuoto chiamato "essai", che poi cancelleremo (senza sovrascrivere il suo contenuto).

In un terminale, inserire il comando :

```
> test al tatto
```

E premere *Invio* () o () per far sì che il computer lo esegua.

Il comando `touch` crea un file vuoto; l'*argomento* `essai` fornisce il nome del file. Non vengono utilizzate opzioni.

È quindi possibile verificare che questo file sia stato creato lanciando il comando `ls` (che sta per "list"):

```
> ls
```

Una volta emesso il comando, il computer risponde con un elenco. Su quello utilizzato per il test, questo dà :

```
Uffici
o test
```

`Bureau` è il nome di una cartella già esistente, mentre `essai` è il nome del file appena creato. Un altro computer potrebbe aver risposto con molti altri file oltre a `Bureau` ed `essai`.

Il comando `ls` risponde solo a un altro modo per vedere cos'altro è disponibile. Facendo clic sull'icona della *cartella personale* sul desktop, si vedrà apparire una nuova icona nel browser dei file, che rappresenta il file di *prova* appena creato.

Ora cancelleremo questo file. La riga di comando per farlo ha la sintassi generale :

```
rm [ opzioni ] CANCELLARE IL NOME DEL FILE
```

Useremo l'opzione `-v` che, nel contesto di questo comando, chiede al computer di essere "prolisso" sulle azioni che sta per eseguire.

Per inserire il nome del file da eliminare, utilizzeremo il suggerimento dato in precedenza per indicare il percorso del file. Quindi, si inserisce il nome del file da eliminare:

- digitare `rm -v` nel nostro terminale,
- digitare uno spazio per separare l'opzione `-v` dal resto,

- nella finestra *Cartella personale*, trascinare l'icona del file di prova e rilasciarla nel terminale.

Al termine di questa operazione, dovremmo ottenere qualcosa di simile a :

```
> rm -v '/ home/ LOGIN/ essai'
```

È quindi possibile premere il tasto *Invio* (↵) o (se si noti che l'ordinateur risponde:

```
"home/ LOGIN/ test" cancellato
```

Questo indica che il file richiesto è stato cancellato. È comunque possibile verificare la sua assenza eseguendo un nuovo `ls` :

```
> ls
```

Si può notare che non ci sono `test` nell'elenco restituito dal comando. Sullo stesso computer di prima, questo dà ora :

```
Ufficio
```

E l'icona deve essere scomparsa anche dal browser dei file. A quanto pare, il file è stato quindi cancellato, anche se, come spiegato in [Paragrafo 1](#), la sua pagina [42](#) contenuto esiste ancora sul disco. Poiché si trattava di un file vuoto chiamato "essai", non è un grosso problema. possiamo dire

12.6 Attenzione alle tracce!

La maggior parte delle *shell* salva automaticamente le righe di comando digitate in un file di "cronologia". Questo è comodo per recuperare in seguito i comandi utilizzati, ma lascia anche un file di "cronologia" sul disco. traccia delle nostre attività.

La *shell* standard di Debian si chiama `bash`. Con `bash`, per disabilitare temporaneamente la registrazione della cronologia nel terminale che si sta utilizzando, è sufficiente fare :

```
> non impostato HISTFILE
```

Inoltre, i comandi vengono memorizzati nel file nascosto `.bash_history` (situato nella *cartella personale*). Per questo motivo, di tanto in tanto, si consiglia di ripulirlo.

pagina
141

12.7 Ulteriori informazioni

La prima esperienza con questa finestra piena di caratteri piccoli potrebbe essere l'inizio di una lunga passione. Per coltivarla, non c'è niente di meglio che prendersi il tempo di leggere il tutorial "Linux in modalità testo: consolati!"² dal libro *Linux aux petits oignons*, o la sezione "La console, ça se mange?"³ nel tutorial "Riprendete il controllo con Linux!"

2. <https://fr.calameo.com/read/005322362565c72e1efe8>

3. <https://web.archive.org/web/20210920080224/https://sdz.tdct.org/sdz/reprenez-le-controllo-a-l-aide-de-linux.html#Laconsoleasemange>

Scegliere una passphrase

🔄 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.*

🕒 *Durata: Circa dieci minuti.*

Una "passphrase" è un segreto utilizzato per proteggere dati criptati. Questo è ciò che si usa per criptare un disco rigido o dei documenti, o anche, com'è vedremo nel secondo volume di questo libro, chiavi crittografiche.

Usiamo il termine "frase" piuttosto che "password", perché una singola parola, per quanto bizzarra e complicata, è molto meno resistente di una semplice frase di più parole. Si ritiene che una passphrase sia composta da almeno dieci parole. Ma più sono, meglio è!

Un criterio importante che a volte viene trascurato: una buona passphrase è quella che si può ricordare.¹ Questo elimina la necessità di scriverla su carta, un grave errore che rende obsoleto il valore della creazione di una passphrase concreta. Ma, cosa altrettanto importante, una buona passphrase deve essere il più possibile difficile da indovinare. Quindi evitiamo la passphrase composta da 15 parole di caratteri casuali che dimenticherete appena 15 minuti dopo averla trovata, tanto quanto il testo di una hit da discoteca degli anni '80.

Una tecnica per trovare una buona passphrase difficile da indovinare, ma non per questo meno facile da ricordare, è quella di creare una frase che non provenga da un testo esistente. Infatti, che si tratti del testo di una canzone, di un verso di una poesia o di una citazione di un libro, strumenti come il Progetto Gutenberg² rendono sempre più facile testare frasi d'accesso tratte dalla letteratura esistente.³

Tuttavia, l'uso dell'espressione "passphrase" può indurre a scegliere una frase che abbia un senso, con lo svantaggio di perdere la casualità che rafforza la sicurezza della password.

Per creare una passphrase bisogna quindi usare l'immaginazione; ecco alcuni consigli sulle buone abitudini da adottare quando si sceglie una passphrase:

1. Scegliere dieci parole a caso che non hanno nulla a che fare l'una con l'altra, ad esempio aprendo uno o più libri a caso e tenendo la prima parola su cui cadono gli occhi.

1. Randall Munroe, 2014, *Complessità delle password* [<https://xkcd.lapin.org/index.php?number=936>].

2. Wikipedia, 2017, *Progetto Gutenberg* [https://fr.wikipedia.org/wiki/Projet_Gutenberg].

3. Dan Goodin, 2013, *How the Bible and YouTube are fueling the next frontier of password cracking* [<https://arstechnica.com/security/2013/10/how-the-bible-and-youtube-are-fueling-the-next-frontier-of-password-cracking/>].

2. Spesso i software richiedono l'inserimento di numeri o caratteri speciali. È quindi possibile trovare le cose da modificare in queste parole. Sappiate che questo passaggio non è affatto necessario dal punto di vista della sicurezza e rischia soprattutto di rendere la frase più difficile da ricordare. Ciò può comportare l'aggiunta di espressioni gergali, parole di lingue diverse, l'inserimento di lettere maiuscole o spazi dove non ci si aspetterebbe, la sostituzione di caratteri con altri, la possibilità di dare sfogo alla propria fantasia in fatto di ortografia *e così via*.
3. Create un mnemonico per ricordarlo. Esempio: ricamo
una struttura narrativa con queste parole può aiutare a ricordare la frase di passaggio.

È meglio utilizzare solo i caratteri presenti su tutte le varianti di tastiera; in altre parole, evitare i caratteri accentati o altri simboli specifici delle lingue locali. In questo modo si possono evitare problemi di tasti mancanti o difficili da trovare, e soprattutto di codifica errata dei caratteri, se dobbiamo digitare la nostra passphrase su una tastiera diversa da quella a cui siamo abituati.



PER SAPERNE DI PIÙ...

È anche possibile utilizzare il gestore di password KeePassXC (vedere pagina 355) per generare una passphrase di dieci parole casuali.

Per impostazione predefinita, questo strumento include un elenco di parole in inglese, ma è possibile specificare un altro elenco di parole⁴ aggiungendolo, sotto forma di un semplice file di testo contenente una parola per riga, alla cartella `/usr/share/keepassxc/wordlists`. Questa operazione deve essere eseguita come superutente.

Quindi, avviare KeePassXC e andare al menu *Strumenti*, quindi *Generatore di password*. Nella scheda *Passphrase*, è possibile scegliere l'elenco di parole da utilizzare (se ne sono disponibili diverse) e il numero di parole. La passphrase generata appare in alto.

Il numero di parole necessarie per rendere una passphrase difficile da indovinare varia a seconda della dimensione dell'elenco di parole. L'indicatore *Entropia*, situato a destra, sotto la passphrase, dà quindi una misura di questa difficoltà: maggiore è l'entropia, meglio è. Una buona passphrase richiede un'entropia di circa 128 bit.

Ad esempio, trovate dieci parole a caso:

sembrano ponte freno payante in uscita struzzo date licenze degauchir
piller

Se un programma richiede l'aggiunta di simboli o numeri, è possibile creare frasi senza complicarsi troppo la vita. Ad esempio:

Sembler ponte frein payante. Fuori struzzo, licenze dater! degauchir
+piller-1984

E possiamo immaginare una frase, con queste parole, che serva da mnemonico:

Può sembrare che giocare a bridge metta i bastoni tra le ruote, perché non è gratis. Tirate fuori il vostro struzzo e date le vostre licenze! Pianificare e saccheggiare, senza supervisione

4. Ad esempio, si può utilizzare l'elenco di parole francesi proposto da mbelivo [https://raw.githubusercontent.com/mbelivo/diceware-wordlists-en/master/wordlist_fr_5d.txt]. Tuttavia, è necessario adattarlo al formato utilizzato da KeePassXC, cosa che si può fare con il comando eseguito in un terminale dalla cartella in cui si trova il file in questione:
`cut -d' ' -f2 < wordlist_fr_5d.txt > wordlist_fr_5d_keepassxc.txt`

Si può quindi scegliere di utilizzare solo l'elenco di parole casuali o la frase completa come passphrase. In quest'ultimo caso, tuttavia, dovrete fare attenzione all'uso di caratteri speciali, come già detto.

Una volta che i dati sono stati crittografati con la nuova passphrase, è bene utilizzarla una decina di volte per decifrare i dati. È anche possibile scriverla su un foglio di carta al momento della creazione, per essere sicuri di ricordarla quando la si usa per la prima volta (naturalmente, sarà necessario distruggere il foglio in seguito). In questo modo potrete insegnare alle vostre dita a digitare questa nuova frase e quindi memorizzarla mentalmente e fisicamente.

Infine, non dimentichiamo che se trovare una passphrase di questo tipo non è facile, è necessario trovarne una diversa per ogni supporto da crittografare. Utilizzare la stessa passphrase, o peggio la stessa password, per una serie di cose diverse, può rivelarsi disastroso se viene rivelata.

Inoltre, non si dovrebbe mai utilizzare una passphrase come password per un servizio online che viene utilizzato anche per bloccare un segreto crittografico. Infatti, se questo servizio online venisse violato, la nostra passphrase sarebbe nota agli hacker e potenzialmente venduta ad altri.

Avvio da CD, DVD o CD-ROM Chiave USB

C Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

⌚ *Durata: Da un minuto a venti minuti circa.*

Qui vedremo come avviare un computer da un supporto esterno, come un CD di installazione Debian o un sistema *live* su una chiavetta USB.

A volte, soprattutto sui computer moderni, è abbastanza semplice. Altre volte, invece, è un po' sconcertante...

Quando si avvia un computer, il firmware (BIOS o UEFI)

e eseguito
primo.

na **20**. Come abbiamo visto, è questo che consente di scegliere la periferica che si desidera utilizzare. (disco rigido, chiavetta USB, CD o DVD, ecc.) in cui si trova il sistema operativo da avviare.



vien
per

pagi

14.1 Prova ingenuamente

Iniziare a inserire il supporto esterno, quindi (ri)avviare il computer. A volte funziona da solo. In questo caso, siete fortunati: non c'è bisogno di leggere il resto del capitolo!

14.2 Tentativo di selezione una tantum del dispositivo di avvio

Con i firmware recenti, spesso è possibile scegliere un dispositivo di avvio caso per caso. Ma questo non è sempre possibile, soprattutto per alcuni computer dotati di Windows (dalla versione 8 in poi), per i quali la gestione è più complicata. Tra le altre cose, dovrete disabilitare il *Secure Boot*¹ e probabilmente cercare su Internet come avviare una chiavetta USB con questo particolare modello di computer.

(R)avviare il computer, osservando attentamente i primi messaggi che appaiono sullo schermo. Cercate i messaggi in inglese che assomigliano a:

- Premere [KEY] per selezionare il dispositivo di avvio temporaneo
- [TASTO] = Menu di avvio
- [TASTO] per accedere al menu di selezione MultiBoot

Questi messaggi indicano di utilizzare il tasto KEY per selezionare un dispositivo di avvio.

Questa chiave è spesso **F2** o **F12** o **F9** o **Scappare**.

Sui Mac esiste una possibilità equivalente a questa: subito dopo l'allu-
computer, tenere premuto il tasto **alt** (a volte anche

1. [Come disabilitare l'avvio sicuro](https://doc.ubuntu-fr.org/desactiver_secure_boot) [https://doc.ubuntu-fr.org/desactiver_secure_boot].

opzioni) marcato (). Dopo un po', si dovrebbe vedere la scritta *Startupmanager*².

Ma torniamo ai nostri PC. Spesso il firmware va troppo veloce, quindi non si ha il tempo di leggere il messaggio, capirlo e premere il tasto. Una volta individuato il tasto giusto, riavviate la macchina e premete il tasto in questione (non tenendolo premuto, ma premendolo e rilasciandolo più volte) non appena il computer si accende.

Se tutto va bene, un messaggio come questo affiche :

```
+-----+
| Menu di avvio |
+-----+
|
| 1: Dispositivi rimovibili
| 2: Disco rigido
| 3: DVD - ROM
| 4: Avvio della rete
|
|      |<Invio impostazione
|
+-----+
```

Se funziona, il gioco è fatto. Scegliete la voce giusta in questo menu, spostandovi con le frecce della tastiera [↑] e [↓], quindi premete *Invio* ([↵]) o *ritorno*.

Spesso dobbiamo indovinare il termine usato dal firmware per indicare il nostro dispositivo. Ad esempio, per avviare una chiavetta USB, selezionare *Dispositivi rimovibili*. Il computer si avvierà dal dispositivo selezionato. Non è necessario continuare a leggere!

14.3 Modifica dei parametri del firmware



Il firmware viene utilizzato per configurare il funzionamento dell'hardware del computer. È buona norma non apportare tante modifiche tutte insieme, ma annotarle su un foglio di carta. In questo modo, se il computer smette di funzionare, si può tornare indietro. In caso di dubbio, uscire senza salvare e ricominciare.

Se la scelta di un dispositivo di avvio temporaneo non funziona, è necessario entrare nel firmware per impostare manualmente l'ordine di avvio. Il firmware verifica i dispositivi nell'ordine configurato e avvia il primo sistema operativo trovato. Lo scopo di questa modifica è di mettere i nostri supporti esterni in cima a questo elenco.

Per rendere le cose un po' più interessanti, i programmi del firmware sono quasi tutti diversi, quindi è impossibile dare una ricetta che funzioni sempre.³

14.3.1 Entrare nell'interfaccia di configurazione del firmware

Ancora una volta, si tratta di (ri)avviare il computer osservando attentamente i primi messaggi che appaiono sullo schermo. Cercate i messaggi in inglese che assomigliano a :

- Premere [KEY] per accedere all'impostazione
- Impostazione: [KEY]
- [TASTO] = Impostazione
- Accedere al BIOS premendo [KEY]

2. http://support.apple.com/kb/HT1310?viewlocale=fr_FR

3. Le esercitazioni illustrate per alcuni BIOS sono disponibili su [questa pagina](https://www.hiren.info/pages/bios-boot-cdrom) [https://www.hiren.info/pages/bios-boot-cdrom].

- Premere [KEY] per accedere all'impostazione del BIOS
- Premere [KEY] per accedere al BIOS
- Premere [KEY] per accedere alla configurazione del sistema
- Per l'impostazione premere [KEY]

Questi messaggi indicano di utilizzare il tasto KEY per accedere al firmware.

Questa chiave è spesso (←) Inc () Del () F2 () F1, F10, F12, Escap, () Sch () e (→) () Cancellare () o () rso met () i mes

Ecco una tabella che riassume le chiavi di accesso al firmware di alcuni comuni produttori di computer ⁴.

I tasti del produttore osservati	
Acer	F1, F2, Canc, ellare
Compaq	
Dell	
Fujitsu	F1
HP	F10
IBM	F2, F10, F12, Escap, e
Lenovo	F2
NEC	F1 Ingresso ()
Packard Bell	F1, ↓
Samsung	F2
Sony	F1
Toshiba	F2, F12, Escap, Cancellare, e

Spesso il firmware va troppo veloce e non si ha il tempo di leggere il messaggio, capirlo e premere il tasto. Una volta individuato il tasto giusto, riavviare la macchina premendo il tasto in questione (senza tenere premuto il tasto, ma premendolo e rilasciandolo più volte). A volte il computer si perde e si blocca. In questo caso, riavviare e riprovare...

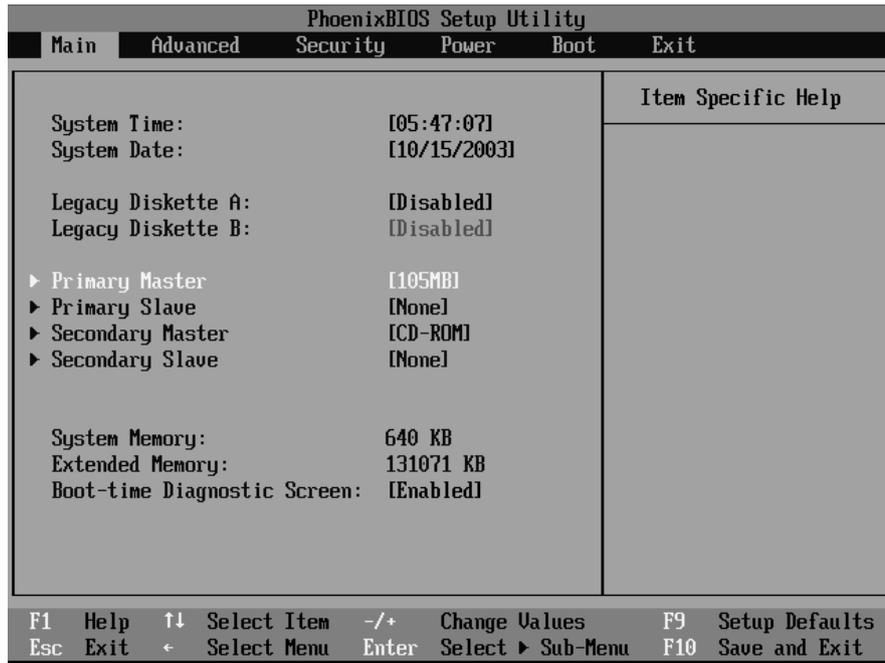
Se al posto del messaggio desiderato compare un'immagine, è possibile che il firmware sia configurato per visualizzare un logo anziché questi messaggi. Provare premere Scappare o su Sch (←) o (→) per visualizzare i messaggi.

Se il computer si avvia troppo rapidamente per poter leggere i messaggi affiche, a volte è possibile premere il tasto Break key (spesso in alto, a destra della tastiera) per bloccare lo schermo. Premendo nuovamente un tasto qualsiasi è possibile per "scongellare" lo schermo.

14.3.2 Utilizzo dell'interfaccia di configurazione del firmware

Una volta entrati nel firmware, lo schermo è spesso blu o nero, pieno di menu e a volte il mouse non funziona. Di solito, un'area in basso o a destra dello schermo spiega come navigare tra le opzioni, come cambiare scheda e così via. Spesso è in inglese: help è "aiuto", key è "chiave", select è "seleziona", value è "valore" e modify è "modifica". Di solito vengono descritti anche i tasti da usare per muoversi, ad esempio ← ↑ ↓ →: Muovi (in inglese, "move"). Queste sono le frecce della tastiera ↓ | e | ↑ | e/o ← | e | →. A volte è utile anche la Tab (←) o (→).

4. Tim Fisher, 2019, *BIOS Setup Utility Access Keys for Popular Computer Systems* [<https://web.archive.org/web/20200227083303/https://www.lifewire.com/bios-setup-utility-access-keys-for-popular-computer-systems-2624463>] (archivio), e Michael Stevens Tech, 2014, *How accedere a accedere/entrare Scheda madre BIOS* [https://web.archive.org/web/20201128221653/http://michaelstevensstech.com/bios_manufacturer.htm] (archivio).



Una schermata del BIOS

14.3.3 Modificare la sequenza di avvio

L'idea è quella di rovistare fino a trovare qualcosa che contenga la parola e si presenta come :

- Primo dispositivo di avvio
- Ordine dello stivale
- Gestione dell'avvio
- Sequenza di avvio

In caso contrario, provare qualcosa come Advanced BIOS Features o Advanced features.

Una volta trovato l'input giusto, è necessario capire come modificarlo. Ad esempio, Invio: Seleziona o +/- : Valore. L'obiettivo è quello di mettere al primo posto il CD/DVD o la chiave USB, a seconda di quale sia l'avvio desiderato.

A volte è necessario inserire un sottomenu. Ad esempio, se è presente un menu Ordine di avvio e viene scritto in Invio: Selezionare la guida, premere Invio () a  o una volta selezionato il menu.

Altre volte, le opzioni possono essere modificate direttamente. Ad esempio, se c'è un'opzione come Primo dispositivo di avvio ed è scritta nel campo +/- : Valore, premere il tasto

 o  il tasto finché non viene visualizzato il valore corretto, ad esempio IDE DVDROM. A volte si usa invece il tasto Pagina giù,  () e Pagina precedente (,  o ) sono utilizzati. Talvolta anche, come F5 e F6. Altre volte, invece, questi tasti vengono utilizzati per spostare il dispositivo in alto e in basso in un elenco corrispondente all'ordine di avvio.

14.3.4 Scelta della nuova configurazione

Una volta scelto il supporto giusto per l'avvio, è necessario chiedersi se lo si vuole lasciare per sempre o meno. Se si desidera lasciarlo, può essere utile posizionare il disco interno al secondo posto nella sequenza di avvio. In questo modo, se il supporto posizionato per primo è assente, il computer si avvierà da quel disco.

Se non si include il disco interno nella sequenza di avvio, il computer non si avvierà da esso, anche in assenza di un CD, un DVD o una chiave USB.

Tuttavia, lasciare che il computer si avvii su un supporto esterno può avere conseguenze spiacevoli: diventa un po' più facile per un malintenzionato avviarlo utilizzando questo supporto, ad esempio, per portare a termine un attacco.

È vero che il firmware può essere utilizzato per impostare una password di accesso al computer, che deve essere inserita prima dell'avvio. Ma non ha senso fare affidamento su questa protezione: nella maggior parte dei casi, questa protezione può essere facilmente aggirata, ad esempio rimuovendo la batteria dalla scheda madre per alcuni minuti.

14.3.5 Salvare e uscire

Una volta impostata la nuova configurazione, salvare e uscire. Ancora una volta, leggete la guida a video, ad esempio F10: Salva. A volte può essere necessario premere uno o più tasti

timeescoanp per ottenere il menu giusto. Verrà quindi visualizzato un messaggio che chiede (in

English)^e se si è sicuri di voler salvare e uscire. Ad esempio:

```
+-----+
|Conferma dell'                                impostazione |
+-----+
|
| Salva la configurazione e uscire ora |
|
|      |<Sì                <No>          |
|
+-----+
```

Vogliamo salvare, quindi selezioniamo Sì e premiamo *Invio*.

(or).

Utilizzo di un sistema *live*

🔄 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

🕒 **Durata:** Da trenta minuti a un'ora, più circa trenta minuti di download.

Un sistema *live* è un sistema GNU/Linux che funziona senza essere installato sul disco rigido interno del computer.

Si noti che questo non significa che non ci saranno tracce sul disco interno:

Ad esempio, molti sistemi *live* utilizzano la memoria virtuale (*swap*) se ne rilevano la possibilità. Inoltre, alcuni sistemi *live* consentono l'accesso automatico al contenuto del disco interno, che potrebbe lasciare dei residui.

tracce.

15.1 Sistemi *live* discreti

D'altra parte, alcuni sistemi *live* sono appositamente progettati per (tentare di) non lasciare traccia sul disco rigido del computer su cui vengono utilizzati, a meno che non venga loro espressamente richiesto di farlo. È il caso, ad esempio, di Tails (*The Amnesic Incognito Live System*).

A quel punto (se le persone dietro al sistema *live* hanno fatto le cose per bene) non viene scritto nulla sul disco interno. Tutto ciò che viene fatto dal sistema *live* sarà

solo nella RAM, che viene più o meno cancellata per davvero quando il computer viene spento, almeno dopo un certo periodo di tempo.

L'uso di questi sistemi *live* è quindi uno dei modi migliori per utilizzare un computer senza lasciare tracce. Qui vedremo come ottenere un sistema *live* e come avviarlo.

Il modo abituale per utilizzare un sistema *live* è installarlo su una chiavetta USB o masterizzarlo su un DVD.

In genere è consigliabile utilizzare Tails su una chiavetta USB: ciò consente di utilizzare alcune funzionalità non disponibili su DVD, come gli aggiornamenti automatici e lo spazio persistente.

Tuttavia, dato che è possibile scrivere dati su una chiavetta USB, ma non su un DVD, questo rende possibile per i malintenzionati modificare il nostro sistema *live* per registrare, ad esempio, le nostre password o i tasti premuti. Se, per questi motivi, si sceglie di utilizzare un DVD, è necessario assicurarsi di aggiornarlo manualmente, altrimenti si utilizzerà un

sistema con vulnerabilità-note!

15.2 Scaricare, controllare e installare Tails

Qui spiegheremo come scaricare l'ultima versione di Tails dal sito ufficiale e come verificarne l'autenticità prima di installarla su una chiavetta USB o di masterizzarla su un DVD. Ci basiamo principalmente sulla procedura guidata ufficiale disponibile sulla pagina web <https://tails.boum.org/install/index.fr.html>, che offre diverse documentazioni a seconda del sistema operativo in uso.

Se avete già un'installazione dell'ultima versione di Tails, potete semplicemente duplicarla. Per farlo, seguite lo strumento di clonazione di Tails.

Nota: questa guida fornisce ulteriori spiegazioni sulla verifica dell'autenticità dell'immagine di Tails. Quando si arriva alla sezione "Verifica del download" della documentazione ufficiale di Tails, fare riferimento alla parte di questo capitolo dedicata alla verifica dell'autenticità del sistema live.

15.2.1 Scaricare Coda

Tails può essere scaricato in due modi: direttamente *tramite* un browser web (in HTTPS) o utilizzando BitTorrent.

Qualunque sia il metodo utilizzato, è necessario disporre di un'immagine su disco del sistema Tails ¹ immagine del sistema Tails e la corrispondente firma OpenPGP per verificarne l'autenticità.

Con un browser web, i due file devono essere scaricati separatamente, mentre BitTorrent li recupera contemporaneamente.

In ogni caso, è necessario seguire la [procedura guidata di installazione di Tails \[https://tails.boum.org/install/index.en.html\]](https://tails.boum.org/install/index.en.html) per il sistema operativo in uso.

15.2.2 Verificare l'autenticità del sistema live

La procedura guidata di installazione ufficiale di Tails (se non si utilizza il metodo della riga di comando) offre uno strumento automatico per verificare l'integrità del file scaricato. Esso indica di fare clic sul pulsante *Seleziona il download...* e quindi esegue un controllo iniziale dell'immagine scaricata. In particolare, garantisce che ² che l'immagine corrisponda esattamente a quella distribuita dal sito Tails. Tuttavia, **non protegge** da un attacco al sito Tails.

L'immagine del sistema *live* che abbiamo appena scaricato è firmata digitalmente con OpenPGP. Utilizzeremo questa firma per verificarne l'autenticità in modo più robusto. Se non avete ancora scaricato questa firma, potete ottenerla facendo clic sul collegamento *OpenPGP signature* nella sezione *Check your download*, quindi su *OpenPGP signature* nel riquadro che appare.

Successivamente, è necessario scaricare la chiave OpenPGP per la firma di Tails. A tale scopo, sempre nella sezione *Controlla il download*, fare clic prima su *Firma OpenPGP* per visualizzare il riquadro corrispondente (se non è già visibile), quindi fare clic su *Chiave di firma OpenPGP*. Questa chiave è associata all'indirizzo tails@boum.org.

Una volta scaricata, importiamo questa chiave pubblica OpenPGP nel portachiavi del desktop. È quindi possibile verificare l'impronta digitale di questa chiave facendo doppio clic su di essa in *Kleopatra*. L'impronta digitale osservata dalle persone che hanno scritto questa guida è la seguente (supponendo che si tratti di una copia originale che abbiamo tra le mani):

1. Un'immagine del disco è un *file di archivio* contenente una copia identica di un sistema di archiviazione (CD, DVD, disco rigido, chiavetta USB, ecc.). Viene spesso utilizzata per trasferire e duplicare i file di installazione del sistema. Un'immagine disco può avere diversi formati, come .img o .iso (detta immagine ISO).

2. Il modello di minaccia affrontato dal sistema di verifica dei download di Tails è documentato [sul sito web Tails \[https://tails.boum.org/contribute/design/download_verification/\]](https://tails.boum.org/contribute/design/download_verification/).

A490 D0F4 D311 A415 3 E2B B7CA DBB8 02 B2 58 AC D84F

Se l'impronta osservata è uguale a questa, è possibile verificare la firma digitale dell'immagine. *Kleopatra* può afficher *Impossibile verificare i dati Signatura creata su [...]* Con il certificato: *Sviluppatori Tails (chiave di identità offline a lungo termine)*

pagina
345

<tails@boum.org> (DBB8 02B2 58AC D84F). Questo significa che il file è effettivamente protetto dalla chiave in questione, ma che non abbiamo confermato l'autenticità di questa chiave... non è un problema perché abbiamo solo verificato la sua impronta digitale.

Se la firma è valida, c'è un'alta probabilità che il download di Tails appena eseguito sia valido. Innanzitutto, la sua integrità è stata verificata, quindi l'immagine è esattamente identica a quella proposta dal sito. Inoltre, è firmata con una chiave la cui impronta digitale può essere verificata in questa guida, cioè altrove rispetto al sito di Tails. Poiché la probabilità che il sito e la guida siano stati corrotti nello stesso modo è molto, molto bassa, si può continuare con l'installazione.

15.2.3 Installare Tails sul supporto scelto

Tornare alla [procedura guidata di installazione di Tails \[https://tails.boum.org/install/index.en.html\]](https://tails.boum.org/install/index.en.html) per trovare le istruzioni per installare Tails su una chiavetta USB per il nostro sistema operativo.

Se invece preferite installare Tails su DVD, andate alla [pagina dedicata \[https://tails.boum.org/install/dvd/index.fr.html\]](https://tails.boum.org/install/dvd/index.fr.html).

15.3 Clonazione o aggiornamento di una chiave Tails

Una volta che si dispone di un DVD o di una chiave USB con Tails, è possibile duplicarla, ad esempio per creare una chiave USB con persistenza corrispondente a una nuova identità contestuale, per regalare una chiave Tails a un conoscente o per aggiornare una chiave USB contenente una versione precedente di Tails.

pagina
preceden
te.

Per farlo, seguiamo la documentazione ufficiale di Tails, disponibile su qualsiasi DVD o chiave Tails, anche senza una connessione a Internet.

Avviare prima Tails. Quindi fare doppio clic *sull'icona della documentazione di Tails* sul desktop. Cercate la sezione *Download, installazione e aggiornamento*, quindi la sezione *Installazione tramite clonazione da un'altra voce di Tails*. Fare clic su *Per PC* o *Per Mac*, a seconda del computer in uso. Seguire i passaggi indicati.

questa
pagina

Per aggiornare la chiave così creata, è necessario seguire la pagina *Aggiornamento automatico*, che si trova alla voce *Aggiornamento di una chiavetta USB Tails*.

15.4 Avvio su un sistema live

Una volta completata la copia o la masterizzazione, è possibile riavviare il computer, lasciando il supporto del sistema *live* all'interno, e verificare che la copia abbia funzionato. A condizione, ovviamente, di aver configurato il firmware del computer per l'avvio sul supporto corretto: per maggiori dettagli, consultare la ricetta che spiega come avviare il sistema su un supporto esterno.

All'avvio, Tails presenta una schermata che consente di scegliere, tra le altre opzioni, la lingua di affichage e il layout della tastiera.

pagina
107

15.5 Utilizzo della persistenza Tails

[questa
pagina

Quando si utilizza Tails da una chiavetta USB, è possibile creare un volume persistente crittografato nello spazio libero della chiavetta.

I dati contenuti in questo volume persistente vengono sottoposti a backup e rimangono disponibili da una sessione Tails all'altra. Il volume persistente può essere utilizzato per eseguire il backup di file personali, chiavi di crittografia, configurazioni o software non installati di default in Tails.

[questa
pagina
[questa
pagina

Una volta creato il volume persistente, si può scegliere se attivarlo o meno a ogni avvio di Tails.

Infine, è possibile eliminarlo quando non è più necessario accedere ai dati in esso contenuti.

Tuttavia, l'uso di un volume persistente non è privo di conseguenze in termini di tracce lasciate. Per questo motivo è necessario iniziare a leggere la pagina di avvertimento sull'uso della persistenza.

A tale scopo, fare doppio clic sull'icona della *documentazione di Tails* sul desktop. Cercate la sezione *Come iniziare con Tails* e fate clic su *Avvertenze sullo storage persistente*, che si trova appena sotto la voce *Storage persistente*.

15.5.1 Creazione e configurazione di un volume persistente

Lo scopo di questa ricetta è creare e configurare un volume persistente su una chiave Tails.

Per farlo, seguiremo la documentazione ufficiale di Tails, disponibile su qualsiasi chiavetta USB o DVD di Tails, anche senza una connessione a Internet.

[pagina
preceden
te.

Avviare prima Tails. Quindi fare doppio clic sull'icona *Tails Documentation* sul desktop. Cercare la sezione *Primi passi con Tails* e fare clic su *Archiviazione persistente*. In questa pagina di documentazione, seguire le sezioni *Creare uno storage persistente* e *Configurare uno storage persistente*.

Se si dispone già di un volume persistente e si desidera semplicemente modificarne i parametri, come la passphrase, passare direttamente alla sezione *Argomenti avanzati* in fondo alla pagina di riepilogo della documentazione.

15.5.2 Attivare e utilizzare un volume persistente

Lo scopo di questa ricetta è attivare il volume persistente appena creato sulla nostra chiave Tails.

Per farlo, seguiremo la documentazione ufficiale di Tails, disponibile su qualsiasi chiavetta USB o DVD di Tails, anche senza una connessione a Internet.

[pagina
preceden
te.

Avviare prima Tails. Quindi fare doppio clic sull'icona *Tails Documentation* sul desktop. Cercare la sezione *Primi passi con Tails* e fare clic su *Persistent storage*. In questa pagina di documentazione, seguire la sezione *Utilizzo dello storage persistente*.

15.5.3 Eliminare un volume persistente

Lo scopo di questa ricetta è eliminare il volume persistente precedentemente creato sulla nostra chiave Tails.

Per farlo, seguiremo la documentazione ufficiale di Tails, disponibile su qualsiasi chiavetta USB o DVD di Tails, anche senza una connessione a Internet.

[pagina
preceden
te.

Avviare prima Tails. Sul desktop, fare doppio clic sull'icona *Tails Documentation*. Cercare la sezione *Primi passi con Tails*, fare clic su *Elimina archiviazione persistente* sotto la voce *Archiviazione persistente*, quindi seguire questa pagina di documentazione.

15.5.4 Installazione di software persistente aggiuntivo in Tails

Tails contiene software adatto alla maggior parte delle attività comuni di Internet e di creazione di documenti. Tuttavia, per progetti specifici, potrebbe essere necessario installare in Tails un software specifico, come quello per la progettazione e la simulazione di circuiti elettronici.

Quando Tails è installato su una chiavetta USB, è possibile impostare un volume persistente in modo che uno o più programmi specifici vengano installati automaticamente a ogni avvio.

Trovare il nome del pacchetto da installare Abbiamo bisogno del nome esatto del pacchetto da installare. Per trovarlo, seguite la ricetta [Trova un pacchetto](#). Ad esempio, il nostro software di progettazione di circuiti elettronici è fornito dal pacchetto `geda`.

pagina
135

Installazione del software aggiuntivo Per installare il pacchetto così identificato, seguiremo la documentazione ufficiale di Tails, disponibile in qualsiasi chiavetta USB o DVD di Tails, anche senza connessione a Internet.

Avviare prima Tails. Sul desktop, fare doppio clic sull'icona della *documentazione di Tails*. Cercate la sezione *Primi passi con Tails*, fate clic su *Installa software aggiuntivo* e seguite questa pagina di documentazione.

pagina
115

Installazione di un sistema crittografato

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Un giorno, con diversi periodi di attesa (a volte lunghi).*

Abbiamo visto che tutti i computer - ad eccezione di alcuni sistemi *live* - lasciano tracce ovunque, di file aperti, lavori eseguiti, connessioni a Internet e così via. Abbiamo anche visto che un modo per esporre un po' meno dati memorizzati sul computer e le tracce che lasciamo su di esso è quello di criptare l'intero sistema su cui *pagina* stiamo lavorando.

È possibile installare un sistema operativo GNU/Linux, come Debian o *pagina* 22 Ubuntu, su una parte crittografata del disco rigido. A ogni avvio, il computer richiederà una passphrase, dopodiché sbloccherà la crittografia del disco, consentendo l'accesso a i dati, consentendo così l'avvio del sistema. Senza questa passphrase, chiunque voglia consultare il contenuto del disco si troverà di fronte a dati indecifrabili. Questo è ciò che intendiamo fare in questa ricetta.

L'installazione di un nuovo sistema operativo può cancellare tutti i dati presenti sul disco rigido. Il primo passo consiste nel fare un backup dei dati che si desidera conservare. Poi, se si ritiene che il disco rigido contenga dati sensibili, è possibile cancellarli "per davvero" per renderne il recupero il più difficile possibile.

pagina
151
pagina
139

16.1 Limiti



Attenzione: questa semplice installazione criptata non risolve tutti i problemi di riservatezza con un colpo di bacchetta magica. Protegge i dati solo in determinate condizioni.

16.1.1 Limiti di un sistema criptato

Raccomandiamo vivamente la seguente lettura di base:

- il capitolo sulla crittografia (e le sue limitazioni),
- il caso d'uso di un nuovo inizio, che esamina in dettaglio i limiti pratici di tale sistema e i possibili attacchi ad esso.

a pagina 47
pagina
71

Senza di ciò, l'installazione di un sistema crittografato può creare un falso senso di sicurezza, che può portare a molti problemi.

16.1.2 Limiti di una nuova installazione

Quando si installa un nuovo sistema, si parte da zero. Non c'è un modo semplice per verificare che il supporto di installazione utilizzato sia affidabile e non contenga malware, ad esempio. Potreste scoprirlo solo *in un secondo momento*, e allora potrebbe essere troppo tardi...

16.1.3 Limiti alla manipolazione delle apparecchiature

L'uso di un sistema operativo libero come Debian ha uno svantaggio: i produttori di hardware in genere vi prestano poca attenzione. Può quindi essere difficile, se non impossibile, utilizzare un computer o una delle sue periferiche con Debian.

[pagina
na 20]

La situazione è migliorata negli ultimi anni: il funzionamento dell'hardware tende a diventare più omogeneo e, soprattutto, la diffusione dei sistemi open-source spinge sempre più i produttori a contribuire, direttamente o indirettamente, a garantire il funzionamento del proprio hardware.¹

Tuttavia, prima di sostituire un sistema operativo, è bene assicurarsi che l'hardware necessario funzioni correttamente, utilizzando un sistema *live*. Il sistema Tails, ad esempio, è basato su Debian. L'hardware che funziona con uno di essi dovrebbe quindi funzionare senza troppe difficoltà con l'altro. Si tenga presente, tuttavia, che Tails include un firmware non libero, mentre per averlo in Debian è necessario installarlo esplicitamente.

[pagina
113
questa
pagina]

16.2 Scaricare il supporto di installazione

Il modo più semplice per installare il sistema è utilizzare una chiavetta USB, un CD o un DVD. Debian offre diverse varianti, quindi è una buona idea iniziare a scegliere il metodo più adatto alla propria situazione.

16.2.1 Con o senza firmware non libero?

[pagi
nā 20]

Per funzionare, alcune periferiche del computer richiedono il "firmware" del sistema. Ma non sempre sono disponibili versioni gratuite...

Un micro-cosa?

Si tratta di programmi che vengono eseguiti su chip elettronici all'interno del dispositivo, anziché sul processore del computer. È il caso, ad esempio, del programma che controlla il movimento delle parti meccaniche di un disco rigido o il funzionamento del sistema radio di una scheda Wi-Fi. Non ci rendiamo necessariamente conto della loro esistenza, poiché la maggior parte dell'hardware viene consegnata con il firmware già installato.

[pagi
na
16]

Per altre periferiche, invece, il sistema operativo deve inviare il firmware a un componente durante l'inizializzazione.

Il firmware gratuito viene fornito con il programma di installazione Debian. Poiché la maggior parte dei firmware non è libera, dobbiamo fornire al programma di installazione qualsiasi firmware non libero necessario per far funzionare il computer: questo è tipicamente il caso di alcune schede Wi-Fi.

Un'altra storia di compromesso

[pagi
na
39]

Se installiamo il nostro sistema crittografato su un computer portatile, è molto probabile che sia necessario un firmware aggiuntivo per far funzionare il Wi-Fi o anche per avere un'immagine di buona qualità.

1. Per alcuni hardware, i problemi possono derivare da errori nel funzionamento del firmware integrato. Questi problemi vengono talvolta corretti dagli aggiornamenti forniti dai produttori. Può quindi essere una buona idea aggiornare il firmware (BIOS o UEFI), il *controller incorporato* o altri componenti prima di procedere all'installazione. Purtroppo queste procedure differiscono troppo da un hardware all'altro per poter essere descritte in dettaglio in questo libro, ma in genere si possono trovare sul sito web del produttore...

Su un computer fisso senza Wi-Fi, è abbastanza plausibile che il nostro sistema crittografato funzioni correttamente senza necessariamente avere un firmware non libero.

Anche se non abbiamo prove del suo utilizzo, è possibile che il firmware proprietario di una scheda Wi-Fi possa spiarcì a nostra insaputa... ma senza firmware non funziona. Ancora una volta, si tratta di una questione di compromesso.

16.2.2 Immagine dell'installazione di rete

Il modo più rapido è quello di utilizzare un'immagine di installazione di rete. Questa contiene solo le prime parti del sistema. Il programma di installazione scarica quindi il software da installare da Internet. Il computer su cui si desidera installare Debian deve quindi essere collegato a Internet, preferibilmente tramite un cavo di rete (e non tramite *Wi-Fi*, che raramente funziona all'interno del programma di installazione).

Esistono diversi file (chiamati anche "immagini") che contengono una copia del file immagine di installazione, a seconda dell'architettura del processore. Nella maggior parte dei casi, è necessario scaricare quella che termina con `amd64-i386-netinst.iso`, nota come multi-architettura, adatto sia alle architetture a 32 che a 64 bit e in grado di funzionare con tutte le architetture dei processori.

sulla maggior parte dei computer domestici prodotti dopo il 2006².

Scegliere tra :

- la versione completamente gratuita³
- la versione contenente il firmware non libero⁴.

16.2.3 L'immagine con l'ambiente grafico

Se non è possibile collegare a Internet il computer su cui si vuole installare Debian, si può scaricare un'immagine contenente l'intero sistema di base e il consueto ambiente grafico. Ciò richiede l'accesso a un masterizzatore DVD o a una chiavetta USB di almeno 4 GB.

Come per l'immagine di installazione di rete, è necessario scegliere tra ⁵ :

- la versione completamente gratuita⁶
- la versione contenente il firmware non libero⁷.

Per l'installazione è necessario solo il primo DVD. Il nome del file da scaricare termina con `-amd64-DVD-1.iso` (64-bit).

16.3 Controllare l'ingombro dell'immagine di installazione

È buona norma assicurarsi che il download dell'immagine sia andato a buon fine controllando l'impronta digitale del programma di installazione, per garantirne l'integrità e l'autenticità.

age⁴⁷ procederà in due fasi: la prima ne garantirà l'integrità, la seconda l'autenticità.

autenticità.

Per farlo, è necessario avviare un sistema già installato. Se avete accesso a un computer GNU/Linux, come quello di un amico, siete a posto. Se invece avete solo un sistema *live*, per esempio, potete installare l'immagine

2. I computer portatili che utilizzano l'architettura del processore ARM [pagina 16] stanno comparando, ma gli autori di questa guida non ne hanno mai provato uno.

3. <https://cdimage.debian.org/cdimage/release/current/multi-arch/iso-cd/>

4. <https://cdimage.debian.org/cdimage/unofficial/non-free/cd-including-firmware/current/multi-arch/iso-cd/>

5. Questi DVD funzionano con i computer dotati di architettura di processore x86-64, cioè la stragrande maggioranza dei computer prodotti dopo il 2012.

6. <https://cdimage.debian.org/debian-cd/current/amd64/iso-dvd/>

7. <https://cdimage.debian.org/immaggi/ufficiali/non-free/immaggio-includenti->

scaricato su una chiavetta USB, quindi verificare l'impronta digitale dal sistema *attivo*.

Per verificare l'integrità e l'autenticità dell'immagine ISO, sono necessari due piccoli file:

- il checksum SHA512SUMS ;
- la firma di questa somma di controllo SHA512SUMS.sign.

Scaricateli dalla pagina in cui avete trovato l'immagine ISO qui sopra facendo clic con il tasto destro del mouse e selezionando *Save link target as....*

16.3.1 Verificare l'integrità dell'immagine di installazione

pagina
161

A tal fine, seguire lo strumento `checksum`. Sarà necessario calcolare la somma di controllo SHA512 dell'immagine di installazione (l'immagine ISO) e verificare che corrisponda a quella contenuta nel file `SHA512SUMS`.

16.3.2 Verificare l'autenticità dell'immagine di installazione

Se il controllo di integrità ha avuto successo, cioè se le due checksum calcolate coincidono, si può continuare il processo per verificarne l'autenticità. Infatti, gli avversari potrebbero fornire supporti di installazione e checksum corrotti. Il controllo precedente ci mostrerebbe semplicemente che il file scaricato è quello disponibile sul sito web, non quello che speriamo di avere.

Il secondo volume spiega come garantire l'autenticità del programma di installazione scaricato, poiché l'impronta digitale è firmata con GnuPG, che utilizza la crittografia asimmetrica. Sono necessari i seguenti strumenti:

- Scaricate la chiave pubblica utilizzata per firmare il supporto di installazione da <https://keyserver.ubuntu.com/pks/lookup?op=get&search=0xdf9b9c49eaa9298432589d76da87e80d6294be9b> e salvatela con  e poi *Salva* con nome `debian.asc` come nome del file e *salvare*.
- Importare questa chiave nel portachiavi di Office. Controllare l'impronta digitale:
 - se si ha accesso a un'installazione Debian affidabile, si può installare il pacchetto `debian-keyring`, quindi utilizzare un terminale e digitare il seguente comando:

```
gpg -- keyring /usr/share/keyrings/debian - role -
Ctrl-g-pngo- default - portachiavi --
S impronta digitale debian -
cd@lists.debian.org
```

- se ci si fida del libro tra le mani, si afferma che la stampa è: DF9B 9C49 EAA9 2984 3258 9D76 DA87 E80D 6294 BE9B.

- Controllare la firma del file `SHA512SUMS`, contenuta nel file `SHA512SUMS.sign` precedentemente scaricato. La notifica deve afficher *Signature valide manon affidabili dellachieve di firma del CD Debian* `<debian-cd@lists.debian.org> su [...]`.

16.4 Preparare il supporto per l'installazione

Una volta selezionata, scaricata e verificata l'immagine del supporto di installazione, non resta che installarla su una chiavetta USB, un CD o un DVD.

16.4.1 Creare una chiave USB di installazione

Se avete una chiavetta USB vuota, o contenente solo dati che non desiderate, e avete accesso a un sistema basato su GNU/Linux, come Debian o Tails, questa è l'opzione più veloce.⁸ o Tails, questa è l'opzione più veloce.

pagina
113

8. Occasionalmente, il computer potrebbe non riuscire ad avviarsi dalla chiavetta USB prodotta seguendo le istruzioni descritte qui. Tuttavia, da quanto abbiamo potuto sperimentare con



Attenzione: tutti i dati della chiave andranno persi. D'altra parte, se questa chiave non fosse inizialmente criptata, sarebbe possibile effettuare un'analisi.

per trovare i file il cui contenuto non è stato sovrascritto in precedenza...

pagina 42

Aprire i dischi dalla panoramica delle attività: premete  ( su Mac), quindi digitate e fare clic su *Dischi*.

Una volta aperto Dischi, è possibile inserire la chiavetta USB. Nell'elenco a sinistra dovrebbe comparire una voce corrispondente. Fare clic su di essa per selezionarla.

Quindi fare clic sul menu  nell'angolo in alto a destra () e selezionare *Ripristina immagine disco...*. In *Immagine da ripristinare*, selezionare l'immagine ISO scaricata in precedenza. Fare clic su *Avvia ripristino...*

Una finestra chiede *Vuoi davvero scrivere l'immagine del disco sul dispositivo?* Verificare che le dimensioni e il modello del dispositivo in questione corrispondano alle dimensioni e al modello della nostra chiave USB. In caso affermativo, fare clic su *Ripristina*.

Verrà quindi richiesta la password di amministrazione. Digitare la password e *autenticarsi* per iniziare a scrivere la chiave di installazione. Al termine del ripristino, fare clic su  per espellere la chiave.

16.4.2 Masterizzare l'immagine di installazione su CD o DVD

Se non si dispone di una chiave USB o di un sistema GNU/Linux, è possibile masterizzare l'immagine di installazione su un CD o un DVD.

Il file scaricato è una "immagine ISO", cioè un formato di file che la maggior parte dei programmi di masterizzazione riconosce come "immagine CD grezza". In generale, se si inserisce un disco vuoto nell'unità, il software di masterizzazione si occuperà di trasformare l'immagine scrivendola sul disco vuoto - almeno, funziona con Tails, e più in generale con Debian o Ubuntu.

In Windows, se non è già stato installato un software in grado di masterizzare immagini ISO, il programma gratuito *InfraRecorder*⁹ (che farà al caso vostro).

16.5 L'installazione stessa

Per installare Debian criptata dal supporto di installazione (CD, DVD o chiavetta USB), è necessario avviarlo seguendo la ricetta corrispondente.

pagina

Da qui può iniziare l'installazione vera e propria: concedetevi un po' di tempo e qualche cruciverba, perché il computer sarà in grado di lavorare a lungo senza una particolare supervisione.

107

Nel caso di un'immagine di installazione di rete, verificare che il cavo che collega il computer alla rete sia ben collegato. Se si tratta di un computer portatile, verificare che il cavo di alimentazione sia collegato, poiché durante l'installazione non vengono visualizzati avvisi di batteria scarica.

Il programma di installazione Debian ha la sua documentazione¹⁰. Se si hanno dubbi sui passi descritti di seguito, può valere la pena di darvi un'occhiata. Inoltre, per la maggior parte delle scelte che ci chiede di fare, il programma di installazione suggerisce automaticamente una risposta che di solito funziona...

Al momento in cui scriviamo, le chiavi create in questo modo da Tails sembrano funzionare correttamente .

9. <http://infrecorder.org/>

10. Il manuale di installazione è disponibile in diverse versioni [<https://www.debian.org/releases/stable/installmanual.en.html>]. Seguiremo quella corrispondente all'architettura del processore [pagina 16].

16.5.1 Avvio del programma di installazione

Avviare dal supporto di installazione (CD, DVD o chiave USB). Appare il *menu di installazione di Debian GNU/Linux*. Premere il tasto

Immettere (↵) o (⏎) per avviare il resto del programma di installazione.

Se si è scelto un CD multi-architettura, l'opzione selezionata automaticamente dal programma di installazione sarà normalmente *Installazione grafica* e sarà disponibile un'opzione di *installazione a 32 bit*; in questo caso, il programma di installazione ha rilevato che il processore è compatibile con l'architettura amd64, che offre una serie di vantaggi in termini di sicurezza.

[pagina
na]

16

16.5.2 Selezionare la lingua e il layout della tastiera

- Dopo un po' di pazienza, appare un menu denominato *Seleziona una lingua*: il programma di installazione propone di scegliere una lingua per il resto dell'installazione. Selezionate il *francese*. Per passare alla fase successiva, selezionare ogni volta *Continua*.
- Un menu chiede di specificare il Paese, per regolare l'adattamento del sistema. Scegliete la vostra posizione geografica.
- In *Configura tastiera*, la scelta predefinita *francese* è appropriata se si dispone di una tastiera francese "azerty".
- Il programma di installazione carica quindi i file necessari.

16.5.3 Firmware e hardware di rete

Dopo un tempo di caricamento, il programma di installazione di Debian rileverà le schede di rete presenti nel computer.

Come abbiamo visto in precedenza, alcuni hardware richiedono al sistema un firmware per funzionare.

Se il supporto di installazione è stato precedentemente preparato con il firmware necessario per il sistema, apparirà una schermata che chiederà di accettare un CONTRATTO DI LICENZA DEL SOFTWARE o simile. Dopo averlo letto, si può rispondere *Sì* per continuare l'installazione.

Se il supporto di installazione contiene solo programmi gratuiti, è possibile che venga visualizzato un messaggio che indica un elenco di *file del firmware mancanti*: si tratta di programmi del firmware non gratuiti utili per il computer, ma non forniti dal supporto di installazione. Il programma di installazione suggerisce di inserire un supporto rimovibile che li contenga. Selezionando *No* si potrà proseguire con l'installazione senza installare questi elementi del firmware non gratuiti.¹¹ Scegliendo *Sì*, invece, si indica al programma di installazione di cercare i file o i pacchetti contenenti tali firmware sui dispositivi disponibili, tornando così alla scelta precedente di un'installazione completamente gratuita.

[pagina
120]

[pagina
120]

¹¹. Il microcodice mancante può essere installato in un secondo momento dopo l'attivazione dei repository. non libero [pagina 136].



PER SAPERNE DI PIÙ...

È possibile preparare un dispositivo di questo tipo copiando i programmi firmware più comuni raccolti dalla comunità Debian in un archivio [<https://cdimage.debian.org/cdimage/unofficial/non-free/firmware/bullseye/current>] da decomprimere in una directory del firmware nella radice di una chiave USB formattata in FAT.

Questo archivio *del firmware* è disponibile in tre versioni, corrispondenti a tre diversi tipi di compressione (.cpio.gz, .tar.gz o .zip). A seconda del formato o dei formati che il nostro sistema è in grado di decomprimere, sceglieremo il file corrispondente. Se non conoscete la risposta a questa domanda, potete scaricare tutti e tre i file finché non ne trovate uno che potete decomprimere. Come per l'immagine ISO, è consigliabile verificare l'integrità (vedere pagina 122) e l'autenticità (vedere pagina 122) di ogni file scaricato.

Se il messaggio appare di nuovo, la chiave non contiene il necessario¹². Non è compito di questa guida indicare come ottenere tutti i firmware che possono essere utili. Infine, non esitate a rispondere *No...* Nella maggior parte dei casi, l'installazione proseguirà senza ulteriori problemi, grazie alla connessione cablata, che fa a meno del firmware necessario per il funzionamento della scheda Wi-Fi.

16.5.4 Configurazione di rete e nome della macchina

- Il programma di installazione richiede un po' di tempo per configurare la rete. Se il computer dispone di diverse schede di rete, è necessario scegliere quella che si intende utilizzare per l'installazione. La scelta predefinita è generalmente quella giusta, se si tratta di una scheda di rete *Ethernet*.
- Viene quindi richiesto il *nome della macchina*. Scegliete un nome piccolo per il vostro computer, tenendo presente che questo nome sarà visibile in rete e potrà apparire anche nei file creati o modificati con il sistema che state installando. Potrebbe quindi essere una buona idea dargli un nome generico, come ad esempio *debian*.
- Il programma di installazione chiede quindi un *Dominio*. Senza entrare troppo nei dettagli, è meglio lasciare questo campo vuoto (cioè eliminare tutto ciò che il programma può aver precompilato).

16.5.5 Creare utenti e scegliere le password

Il programma di installazione chiede ora di scegliere la *password di root*. Si tratta di una password necessaria per eseguire operazioni di amministrazione del computer: aggiornamenti, installazione di software, modifiche importanti del sistema, ecc.

Tuttavia, è più semplice risparmiare una password in più e permettere al primo account creato sul sistema di avere il diritto di eseguire operazioni di amministrazione¹³ richiedendo nuovamente la password. Per fare ciò, è sufficiente non inserire una password per "root": basta lasciare la casella vuota e scegliere *Continua*, poi di nuovo *Conferma password*.

- In *Nome completo del nuovo utente*, scegliere il nome associato al primo account creato sul sistema. Questo nome verrà spesso registrato nei documenti creati o modificati in questa sessione, quindi può essere utile scegliere un nuovo pseudonimo.

12. Per esempio, i nomi dei file che iniziano con b43 sono firmware per un particolare tipo di scheda Wi-Fi e non sono ridistribuiti direttamente da Debian. Per farli funzionare, è necessario provare a installare uno dei seguenti pacchetti una volta che il sistema è operativo: `firmware-b43-installer`, `firmware-b43-lpky-installer` o `firmware-b43legacy-installer`.

13. Questa modalità è chiamata *sudo*, perché nel terminale sarà possibile, aggiungendo `sudo` all'inizio di Sulla linea, eseguire un comando come *root*, cioè come superutente.

- In *Login per l'account utente*, scegliere un *login* per questo account. È precompilato, ma può essere modificato. Il programma di installazione avverte, nel caso in cui si voglia modificarlo, che deve iniziare con una lettera minuscola ed essere seguito da un numero qualsiasi di numeri e lettere minuscole.
- Il programma di installazione chiede una password per l'utente. Si tratta della persona che avrà il diritto di amministrare il computer, se si è deciso di non inserire una password.
"root" in precedenza. (Non dimenticate di trovare un modo per ricordare questa password).

16.5.6 Partizionamento dei dischi

[pagina]
20

Se il supporto di installazione è stato avviato in modalità UEFI, il programma di installazione potrebbe chiedere: *"Forzare l'installazione UEFI?"* Questo significa che ha rilevato un altro sistema già installato sul disco rigido, che utilizza la "modalità di compatibilità del BIOS" (l'antenato di UEFI) per l'avvio. Dal momento che stiamo comunque per cancellare tutte le tracce di questo vecchio sistema e mettere Debian al suo posto, possiamo rispondere *Sì* a questa domanda.



PER SAPERNE DI PIÙ...

La probabilità di avere un problema con UEFI è molto bassa, ma alcune schede madri o firmware problematici potrebbero funzionare meglio in modalità di compatibilità BIOS.

Se alla fine dell'installazione il sistema non si avvia in UEFI, si può riavviare l'installazione rispondendo *No* a questa domanda, per installare Debian in modalità di compatibilità BIOS.

Il supporto all'installazione avvia quindi lo strumento di partizionamento. Rileva le partizioni presenti e propone di modificarle.

- Nel menu *Metodo di partizionamento*, selezionare *Assistito - usa un intero disco con LVM crittografato*.
- In *Disco da partizionare*, selezionare il disco su cui installare Debian GNU/Linux. Se si vuole rimuovere il sistema attualmente installato, questo è solitamente il primo disco dell'elenco. La dimensione del disco è un'indicazione della sua idoneità, in modo da non provare a installare Debian sulla chiavetta USB contenente il programma di installazione, per esempio.
- Il programma di installazione offre quindi una scelta di *schemi di partizionamento*. Selezionare *Tutto in una partizione*.
- Il programma di installazione avverte che verrà applicato lo schema di partizionamento corrente, che sarà irreversibile. Ora che è stato eseguito il backup di ciò che si desidera conservare, rispondere *Sì* a *Scrivi le modifiche sui dischi e configurare LVM?*
- Il programma di installazione sostituirà quindi il vecchio contenuto del disco con dati casuali. Questa operazione richiede molto tempo, diverse ore su un disco di grandi dimensioni, e lascia molto tempo per fare altre cose!
- Il programma di installazione chiede quindi una *passphrase segreta*. Scegliete una buona passphrase e digitatela, quindi confermate la passphrase digitandola una seconda volta.
- Il programma di installazione propone quindi la dimensione da utilizzare sul disco in *Quantità di spazio sul gruppo di volumi per il partizionamento assistito*. È possibile mantenere il valore predefinito, che corrisponde alla dimensione massima utilizzabile del disco.
- Il programma di installazione mostra un elenco di tutte le partizioni che verranno create. È possibile fidarsi di esso lasciando *Terminare il partizionamento e applicando le modifiche* selezionate.

[pagina]
103

- Il programma di installazione avverte che scriverà le modifiche sul disco. L'intero disco è già stato riempito di dati casuali, quindi se conteneva dati importanti è già stato cancellato. Rispondere *Sì* a *Le modifiche devono essere applicate ai dischi?* Il programma di installazione crea quindi le partizioni, operazione che potrebbe richiedere un po' di tempo.

16.5.7 Installazione di base del sistema

Il programma di installazione installerà ora un sistema Debian GNU/Linux minimale. Lasciate che faccia il resto...

16.5.8 Configurazione dello strumento di gestione dei pacchetti

A seconda della versione del programma di installazione utilizzato, possono essere poste domande diverse:

- Se il programma di installazione chiede *se scansionare i supporti di installazione diversi da quello usato per avviare il programma di installazione*, la scelta predefinita, *No*, è appropriata.
- Se il programma di installazione chiede *se utilizzare un mirror in rete*, la scelta predefinita, *No*, è appropriata. Tuttavia, se si dispone di una buona connessione a Internet, è possibile scegliere *Sì*: in questo modo verrà installata una versione aggiornata.

Se si utilizza un'installazione di rete (nota anche come "*netinst*", per *installazione di rete*), o se si è risposto *Sì* alla domanda precedente, il programma di installazione chiederà da quale server scaricare il file :

- Il programma di installazione chiede innanzitutto di scegliere il *Paese del mirror dell'archivio Debian*. Selezionare il paese in cui ci si trova.
- Viene quindi richiesto il *mirror dell'archivio Debian* da utilizzare. La scelta predefinita è, *deb.debian.org*, è molto buono.
- Il programma di installazione chiede se è necessario un *proxy HTTP*. Lasciare vuoto.
- Il programma di installazione scarica quindi i file necessari per continuare.

16.5.9 Selezione del software

La domanda successiva riguarda la *configurazione del concorso di popolarità* e chiede *Vuoi partecipare allo studio statistico sull'uso dei pacchetti?* Risposta *No*, a meno che non si accetti di fornire a Debian un elenco del software installato.

¹⁴.

Il programma di installazione chiede quindi quale *software installare*. Di solito suggerisce i seguenti: *Ambiente desktop Debian*, *GNOME* e le *solite utility di sistema*.



PER SAPERNE DI PIÙ...

La maggior parte degli strumenti descritti in questa guida si basa sull'ambiente desktop GNOME. Tuttavia, GNOME è un po' esigente in termini di potenza e altri ambienti più leggeri saranno più adatti a computer non molto potenti: *LXDE*, *Xfce* o *MATE*.

14. Comunicare l'elenco dei software installati in Debian facilita il lavoro delle persone che sviluppano e mantengono questa distribuzione, dando loro una visione dei software più utilizzati. Inoltre, fa capire loro che questo software è importante per noi e che vogliamo che continui a essere mantenuto in Debian. Tuttavia, l'elenco dei software che utilizziamo è ancora un dato personale: se ci sono violazioni della sicurezza sui server di Debian, questi dati potrebbero essere divulgati. Inoltre, rispondere *No* a questa domanda è anche parte della costruzione di una cultura politica collettiva di rifiuto di comunicare i nostri dati personali e di opposizione alla governance dei numeri.

Il programma di installazione scarica quindi il resto del sistema Debian GNU/Linux (o lo recupera dal supporto di installazione) e lo installa. Ci vuole molto tempo, quindi c'è tutto il tempo per fare altre cose.

È possibile che i servizi di sistema debbano essere riavviati al momento dell'aggiornamento. Se il programma di installazione suggerisce di *riavviare automaticamente i servizi al momento dell'aggiornamento*, è possibile rispondere *Sì* per evitare che il sistema chieda ogni volta la conferma manuale.

16.5.10 Installazione del programma di avvio GRUB

Se si è scelto di installare Debian in modalità UEFI, il programma di installazione installa automaticamente il programma di avvio GRUB, che consente di avviare GNU/Linux.

Altrimenti, il programma di installazione propone di installare GRUB in una parte del disco rigido chiamata "settore di avvio":

- Alla domanda *Installare il programma di avvio GRUB sul disco principale*, rispondere *Sì*.
- Il programma di installazione chiede quindi il *dispositivo in cui verrà installato il programma di avvio*. Scegliere il disco rigido interno, che di solito è */dev/sda*. In caso di dubbio, un buon indizio è quello di scegliere il primo disco dell'elenco il cui nome contiene *ata* o *sata*.

Al termine, il programma di installazione suggerisce di riavviare il computer, verificando che il supporto di installazione (CD, DVD, chiave USB) non sia più inserito al momento del riavvio. Selezionare *Continua*.

16.5.11 Riavviare il nuovo sistema

Il computer si avvia quindi sul nuovo sistema. A un certo punto, chiede la passphrase su una schermata nera: "Please unlock disk". Digitare la passphrase e premere

premere *Invio* () o  alla fine¹⁵.

Dopo aver avviato alcuni programmi, appare una schermata con le parole *debian 11* e il nome dell'account precedentemente inserito. Selezionare quest'ultimo, quindi inserire la password associata.

Ecco un nuovo sistema criptato Debian pronto all'uso. Se non ne avete mai usato uno prima, potrebbe essere una buona idea farci un giro per familiarizzare. La panoramica delle attività, che si può aprire facendo clic su *Attività* nell'angolo in alto a sinistra dello schermo o premendo il tasto  ( su Mac), dà accesso ai molti pacchetti software già installati. Per trovare un programma, si può digitare una parola che ne descrive la funzione (ad esempio, *immagine* per trovare i programmi che lavorano con le immagini). Per visualizzare tutti i software installati, fare clic su  in basso a sinistra. Le pagine di aiuto contenenti numerosi suggerimenti e trucchi sono accessibili digitando *Aiuto* nella panoramica delle attività.

16.6 Impostazione del repository principale dei pacchetti Debian

Una volta completata l'installazione, a seconda dell'immagine usata per installare Debian, potrebbe essere necessario andare in *Software e aggiornamenti* per aggiornare il repository principale dei pacchetti Debian.

15. Se non vi sentite molto a vostro agio con la digitazione, vi capiterà spesso di commettere un errore di battitura nelle prime frasi. Non preoccupatevi degli errori ripetuti e continuate a farlo finché non riuscite a scrivere la frase senza errori... dopo un po' di tempo, la cosa si sarà "abituata" e gli errori di battitura saranno sempre più rari. Detto questo, non fa male controllare di aver capito bene.

non abbia inavvertitamente lasciato la chiave  abbassato, nel qual caso potremmo andare avanti all'infinito sulla tastiera, ma non è ancora possibile sbloccare il disco rigido.

Per fare ciò, afferire alla panoramica delle attività premendo  ( su Mac), quindi digitare `software` e fare clic su *Software e aggiornamenti*. Nella scheda *Software Debian*, selezionare *Ufficialmente supportato (principale)*. Poiché questo software modifica i programmi di cui ci fidiamo, siamo rassicurati dal fatto che ci chieda la nostra password.

Se si è usata un'immagine su DVD per installare Debian, è necessario disattivare anche questo repository in modo che il sistema non lo usi più. Per farlo, nella scheda *Altro software*, deselezionare tutte le righe che iniziano con `cdrom:`. Se non si fa questo, Debian insisterà affinché il supporto di installazione sia sempre inserito nel computer, in modo da poter aggiornare l'elenco dei software disponibili.

Per chiudere la finestra *Software e aggiornamenti*, fare clic sul pulsante *Chiudi*. È possibile che appaia una finestra di *informazioni sul software non aggiornata*, in tal caso fare clic su *Aggiorna*. Viene visualizzata una finestra di aggiornamento *della cache* che mostra l'avanzamento del download degli elenchi di pacchetti disponibili. Questa finestra e la finestra *Software e aggiornamenti* si chiudono automaticamente al termine dell'aggiornamento.

16.7 Qualche idea per non perdere il filo del discorso

Ora può essere utile imparare a salvare i dati... e a cancellarli. "per davvero".

È anche importante imparare a mantenere il sistema aggiornato. I problemi del software vengono scoperti regolarmente ed è importante installare le correzioni non appena sono disponibili.

pagina
151
pagina
139
pagina
175

16.8 Documentazione su Debian e GNU/Linux

Ecco alcuni riferimenti alla documentazione su Debian e GNU/Linux:

- La guida di riferimento di Debian official ¹⁶;
- La pagina iniziale della documentazione ufficiale Debian ¹⁷;
- Manuale dell'amministratore Debian ¹⁸.

È disponibile molta documentazione su come usare GNU/Linux. Se spesso sono molto utili, sono, come molte cose su Internet, purtroppo di qualità non uniforme. In particolare, molte di esse smettono di funzionare quando una parte del sistema viene modificata, o hanno scarsa considerazione per la privacy che ci aspettiamo dal nostro sistema. Dobbiamo quindi pensare in modo critico e cercare di capirli prima di applicarli.

Detto questo, ecco alcuni altri riferimenti a wiki e forum:

- Il wiki ufficiale Debian ¹⁹ (parzialmente tradotto dall'inglese);
- Il forum francese su Debian `debian-fr.org` ²⁰;

16. <https://www.debian.org/doc/manuals/debian-reference/index.fr.html>

17. <https://www.debian.org/doc/user-manuals.fr.html>

18. <https://debian-handbook.info/browse/fr-FR/stable/>

19. <https://wiki.debian.org/fr/FrontPage>

20. <https://www.debian-fr.org/>

Scelta, verifica e installazione del software

Questa sezione offre alcune ricette per la gestione del software:

- Quali sono i criteri di scelta del software? A volte è necessario scegliere un software per svolgere un determinato compito e ci si può perdere nella moltitudine di soluzioni disponibili... In questo capitolo esamineremo alcuni criteri per aiutarvi a prendere la decisione giusta.
- Come si trova e si installa il software con Debian? Quando si vogliono eseguire nuove operazioni con il computer, è necessario installare nuovo software. In questo capitolo vi daremo alcuni suggerimenti su come trovare ciò che state cercando in Debian.
- Come si installano i pacchetti su Debian? A volte si ha bisogno di *pacchetti* che completino il software o che abbiano uno scopo proprio.
- Come si accede ai repository Debian? Il software scaricato dal sistema Debian è memorizzato nei cosiddetti *repository*. Sebbene i repository forniti con Debian contengano quasi tutto il software necessario, a volte è utile aggiungerne di nuovi.

pagina 22

questa
pagina

pagina
134

pagina
135
pagina
136

17.1 Criteri di selezione

C *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

C *Durata: Da mezz'ora a un'ora.*

Quando si tratta di scegliere un software per svolgere un determinato compito, è facile perdersi nella moltitudine di soluzioni disponibili. Ecco alcuni criteri per aiutarvi a prendere la decisione giusta.

I vantaggi dell'utilizzo di software libero rispetto a quello di software proprietario o addirittura di *open source* è già stato spiegato. Il resto di questo testo si concentrerà quindi esclusivamente sul software libero disponibile.

17.1.1 Distribuzione

In genere è preferibile installare il software fornito dalla distribuzione GNU/Linux (ad esempio Debian). Le ragioni principali sono due.

Innanzitutto, una questione pratica: la distribuzione fornisce gli strumenti per installare e aggiornare, in modo più o meno automatizzato, un insieme di pacchetti software; ci avvisa quando uno dei pacchetti software che stiamo usando deve essere aggiornato, ad esempio per correggere una falla di sicurezza. Ma non appena si installa un software non fornito dalla distribuzione, bisogna pensare ad aggiornarlo da soli, a tenere il passo con le falle di sicurezza che vengono scoperte, a gestire le dipendenze tra i software e così via. Tutto ciò richiede impegno, tempo e abilità.

D'altra parte, una questione di politica di sicurezza: quando scegliete la vostra distribuzione GNU/Linux, avete implicitamente deciso di riporre una certa fiducia in un insieme di persone, in un processo di produzione. L'installazione di software non fornito dalla vostra distribuzione implica una decisione simile su un nuovo gruppo di persone, un nuovo processo produttivo. Una decisione del genere non va presa alla leggera: quando si decide di installare un software non fornito dalla propria distribuzione, si amplia l'insieme di persone e processi di cui ci si fida, aumentando così i rischi. Ad esempio, senza alcune precauzioni, potreste ritrovarvi a scaricare rapidamente un virus.

61 17.1.2 Maturità

Il richiamo della novità è spesso una trappola: un software in pieno sviluppo può contenere problemi importanti che non sono ancora stati scoperti.

Quando è possibile, è meglio scegliere un software che è stato sviluppato attivamente e che ha raggiunto un certo livello di maturità. Nei software sviluppati e in uso da almeno qualche anno, è probabile che i problemi più gravi siano già stati scoperti e corretti... comprese le falle di sicurezza.

Per scoprirlo, si può consultare la storia del software. Di solito è possibile trovarla sul sito web del software cercando termini come *historique*, *release*, *news* o *changelog*. Se ci sono molti aggiornamenti, soprattutto recenti, significa che il software è ancora in fase di manutenzione.

17.1.3 Processi produttivi e comunità

L'etichetta di *software libero* è un criterio essenzialmente legale, che non deve mai essere sufficiente a ispirare fiducia.

Naturalmente, il fatto che il software sia sottoposto a una licenza libera apre la possibilità di metodi di sviluppo che ispirino fiducia. Ma le persone che sviluppano il software possono benissimo, intenzionalmente o meno, scoraggiare la cooperazione e lavorare in isolamento. Cosa importa se il programma è *legalmente* libero, se di fatto nessun altro leggerà mai il suo codice sorgente?

Dobbiamo quindi dare una rapida occhiata al processo di produzione del software, utilizzando le seguenti domande per valutare il dinamismo del processo:

- Chi sviluppa? Una persona, più persone, un intero team?
- Il numero di persone che contribuiscono al codice sorgente sta aumentando o diminuendo?
- Lo sviluppo è attivo? Non stiamo parlando di velocità pura, ma di reattività, follow-up a lungo termine e resilienza. Lo sviluppo del software è una gara di resistenza, non uno *sprint*.

E sugli strumenti di comunicazione collettiva su cui si basa lo sviluppo (mailing list e chat room, per esempio):

- È possibile accedere facilmente alle discussioni che guidano lo sviluppo del software?
- Queste discussioni riuniscono molte persone?
- Queste persone partecipano al suo sviluppo o lo usano semplicemente?
- Qual è l'atmosfera? Calma piatta, silenzio tombale, gioiosa cacofonia, agghiacciante serietà, braccia aperte, ostilità implicita, tenera complicità? (Ma anche: battute sessiste, commenti razzisti?).
- Il volume delle discussioni negli ultimi mesi/anni è diminuito o aumentato? Più che il volume grezzo, è importante la percentuale di messaggi che ricevono risposte: un software maturo, stabile e ben documentato non sarà necessariamente fonte di discussioni, ma se non c'è nessuno a rispondere alle domande dei neofiti, questo può essere un brutto segno.

- Avete feedback o suggerimenti per il miglioramento? Se sì, vengono presi in considerazione?
- Le risposte sono sempre date da un numero ristretto di persone, oppure esistono pratiche di auto-aiuto più diffuse?

17.1.4 Popolarità

La popolarità è un criterio difficile quando si parla di software. Il fatto che la stragrande maggioranza dei desktop sia attualmente basata su Windows non indica in alcun modo che Windows sia il miglior sistema operativo disponibile.

Tuttavia, se questo software non viene utilizzato da molte persone, ci sono dubbi sulla sua redditività a lungo termine: se il team di sviluppo dovesse smettere di lavorarci, che ne sarebbe di lui? Chi ne prenderebbe il testimone?

Una regola generale è quella di scegliere un software utilizzato da un numero sufficientemente ampio di persone, ma non necessariamente il più diffuso.

Per misurare la popolarità di un'applicazione software, si possono utilizzare gli stessi criteri descritti in precedenza per il dinamismo della "comunità" formatasi intorno ad essa. Si può anche guardare alla valutazione di un'applicazione in *Logiciels*, basandosi non solo sul punteggio ma anche sul numero di persone che hanno votato. Ad esempio, un'applicazione con tre stelle e 295 voti sarà preferita a una con cinque stelle ma solo 19 voti. Debian pubblica anche i risultati del suo concorso di popolarità.¹ Questo ci permette di confrontare non solo il numero di persone che hanno installato un determinato software, ma anche, cosa ancora più importante, l'evoluzione della sua popolarità nel tempo.

17.1.5 Passato di sicurezza

Si può anche dare un'occhiata al tracker della sicurezza² offerto da Debian. Se si cerca un programma per nome, si troverà un elenco dei problemi di sicurezza che sono stati scoperti e, in alcuni casi, risolti.

Se questo software ha una storia di sicurezza perfettamente pulita, potrebbe significare: o che non interessa a nessuno, o che il software è scritto in modo estremamente rigoroso.

Se sono state scoperte falle di sicurezza nel software studiato, ci sono diverse implicazioni, alcune delle quali contraddittorie.

Queste vulnerabilità sono state scoperte e corrette:

- quindi non esistono più, *a priori*;
- Quindi una persona si è preoccupata di trovarli e un'altra di correggerli: possiamo supporre che si stia prestando attenzione a questo problema.

Ma queste scappatoie esistevano:

- il software potrebbe essere stato scritto senza che la sicurezza fosse una preoccupazione particolare;
- altre scappatoie possono rimanere scoperte o, peggio ancora, non pubblicate.

Per affinare la nostra intuizione riguardo a questo software, può essere una buona idea guardare al criterio del "tempo". Per esempio, non è drammatico se alcuni difetti sono stati scoperti all'inizio dello sviluppo di un prodotto software, e se non ne sono stati scoperti per alcuni anni, allora possiamo attribuirli a degli errori.

1. [Debian.org, 2014, Debian Popularity Contest](http://popcon.debian.org/) [http://popcon.debian.org/].

2. Il team di sicurezza di Debian mantiene informazioni per ogni pacchetto, che possono essere visualizzate *sul tracker di sicurezza* [https://security-tracker.debian.org/tracker/], dove è possibile effettuare una ricerca per nome del software.

di gioventù. Al contrario, se sono state scoperte regolarmente nuove falle, per anni e fino a tempi molto recenti, è molto probabile che il software abbia ancora molti problemi di sicurezza totalmente sconosciuti... o non pubblicati. Così come un numero relativamente alto di difetti, anche recenti, può indicare una comunità di sviluppatori attiva ed essere un segnale migliore rispetto all'assenza di difetti di sicurezza per un software con cui pochi hanno a che fare.

17.1.6 Team di sviluppo

Chi ha scritto il software? Chi si occupa della manutenzione? Una volta che siamo riusciti a rispondere a queste domande, ci sono una serie di indizi che possono aiutarci a determinare quanta fiducia possiamo riporre nel team di sviluppo. Per esempio:

- Le stesse persone hanno scritto anche un altro software che utilizziamo già ampiamente; le nostre impressioni su quest'altro software sono del tutto pertinenti a questo studio.
- I membri del team di sviluppo hanno indirizzi che terminano con @debian.org e quindi hanno il diritto di modificare il software fornito da Debian GNU/Linux; se usiamo questa distribuzione, ci fidiamo già de facto di queste persone.
- I membri del team di sviluppo hanno indirizzi che terminano con @google.com, il che dimostra che Google li paga; mentre non ci sono dubbi sulle loro capacità tecniche, è discutibile quanto il loro lavoro sia controllato a distanza dal loro datore di lavoro, che non si può fidare di sapere cosa stanno facendo quando si tratta dei nostri dati personali.

17.2 Trovare e installare il software

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

 *Durata: Da cinque minuti (se si conosce il nome del software) a mezz'ora (se si parte da zero), più il tempo di download e installazione (da pochi secondi a diverse ore, a seconda delle dimensioni del software da installare e della velocità della connessione).*

A volte conosciamo già il nome del software (noto anche come *applicazione*) che vogliamo installare - perché ci è stato raccomandato, perché lo abbiamo trovato su Internet - e vogliamo sapere se è in Debian. Altre volte, invece, conosciamo solo il compito che vorremmo far svolgere al software. In ogni caso, il database dei software disponibili in Debian risponderà sicuramente alle vostre domande.

pagina
131

Per aiutarvi a fare la scelta giusta quando sono disponibili diversi pacchetti software per eseguire lo stesso compito, consultate il capitolo sui criteri di selezione del software.

- Aprire l'applicazione *Software*: afficher la vue d'ensemble des Activités en ap- puy sur la touche  ( su Mac), quindi digitare *logic* nella barra di ricerca e fare clic su *Logiciels*.
- Esistono poi due tecniche per trovare un'applicazione:
 - oppure fare clic sull'icona  nell'angolo in alto a sinistra. Digitare il nome dell'applicazione nella barra di ricerca. È anche possibile digitare parole chiave, ma non sempre le descrizioni delle applicazioni sono tradotte in francese. Con una conoscenza di base dell'inglese, è spesso una buona idea provare le parole chiave in quella lingua.
 - oppure selezionare una categoria in fondo alla pagina (ad esempio, *Giochi*).
- Vengono visualizzati i risultati della ricerca. Facendo clic sull'icona di un software, appare la sua descrizione.

pagina
23

Una volta trovato il software desiderato, è possibile installarlo. È necessario essere connessi a Internet, poiché il software viene installato da pacchetti scaricati online dai cosiddetti *repository*.

- Fate clic sul pulsante *Installa* sotto il logo e il titolo del software.

- Poiché stiamo per installare una nuova applicazione, ci viene chiesta la password.
- Il software installa la nuova applicazione.
- Uscire dall'applicazione *software*.

17.3 Trovare e installare un pacchetto Debian

☞ Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

🕒 Tempo: dieci minuti, più il tempo di download e di installazione (da pochi secondi a diverse ore, a seconda delle dimensioni dei pacchetti da installare e della velocità di connessione).

I pacchetti sono talvolta necessari. I pacchetti possono essere usati per installare il software, ma possono anche essere usati per integrare il software o avere uno scopo proprio.

Per installare i pacchetti, è possibile utilizzare il software *Synaptic Package Manager*.

17.3.1 Trovare un pacchetto Debian

- Aprire il *Gestore dei pacchetti*: visualizzare l'insieme delle attività premendo il tasto  ( su un Mac), quindi selezionare il pacchetto e cliccare su *Gestore dei pacchetti Synaptic*.
- Poiché il gestore di pacchetti consente di modificare il software installato sul computer e quindi di scegliere i programmi a cui affidarsi, è rassicurante che chieda la password per l'apertura.
- Una volta entrati nel gestore dei pacchetti, iniziamo a ricaricare l'elenco dei pacchetti disponibili facendo clic sull'icona  *Reload*. Il gestore dei pacchetti scarica quindi le informazioni più recenti sui pacchetti disponibili da un server Debian.
- Esistono poi due tecniche per la ricerca di un pacchetto:
 - oppure fare clic sull'icona  *Search* sul lato destro della barra degli strumenti. Verificare che *Descrizione e Nome* siano selezionati in *Cerca in*. Digitare parole chiave o il nome di un'applicazione nella casella di *ricerca* (ad es. "Dizionario tedesco di openoffice"). Raramente le descrizioni di applicazioni meno convenienti sono tradotte in francese. Con un po' di inglese di base, spesso vale la pena di provare le parole chiave in quella lingua;
 - Cliccate su *Categoria* nella colonna di sinistra e scegliete la categoria che vi sembra più appropriata per il pacchetto.
- I risultati della ricerca o i pacchetti della categoria vengono visualizzati in un elenco. Facendo clic sul nome di un pacchetto, la sua descrizione appare nel riquadro in basso. A questo punto non resta che installare il pacchetto corrispondente.

17.3.2 Selezionate il pacchetto da installare

Per l'installazione vera e propria del pacchetto di cui sopra, ci sono diversi modi di procedere, a seconda che si voglia usare la versione predefinita, disponibile nei repository ufficiali della propria distribuzione, o un pacchetto proveniente da un altro repository, ad esempio per avere una versione più recente.

Per installare la versione predefinita

Normalmente, il pacchetto desiderato si trova da qualche parte nell'elenco dei pacchetti. Una volta trovata la riga corrispondente, fate clic con il tasto destro del mouse e nel menu che appare scegliete *Seleziona per l'installazione*.

A volte, affinché il pacchetto funzioni correttamente, è necessario installare altri pacchetti. Ad esempio, se diversi programmi utilizzano lo stesso pacchetto,

in modo che venga installato una sola volta, non è contenuto in ogni pacchetto software, ma esiste separatamente e viene richiamato dai pacchetti software. Se il pacchetto da installare dipende da altri pacchetti, il gestore apre una finestra che chiede se è necessario *apportare altre modifiche*. In generale, questi suggerimenti sono pertinenti e si possono accettare facendo clic su *Aggiungi alla selezione*.

Per installare una versione specifica

questa
pagina

A volte si desidera installare una versione particolare di un pacchetto tra quelle disponibili, ad esempio se si sono aggiunti repository specifici. Invece di scegliere *Seleziona per l'installazione* dal menu contestuale, selezionate il pacchetto desiderato facendo clic con il tasto sinistro del mouse sul suo nome, senza fare clic sulla casella di controllo. Andare quindi al menu a discesa *Pacchetto* e selezionare *Forza* versione. Selezionate il file versione desiderata. Se questa opzione è disattivata in grigio, significa che non è disponibile, poiché esiste una sola versione del pacchetto. Il resto rimane invariato.

17.3.3 Applicare le modifiche

Gli ultimi due passaggi possono essere ripetuti per installare più pacchetti contemporaneamente. Una volta preparate le installazioni, non resta che avviarle facendo clic su *Applica* nella barra degli strumenti. Il gestore di pacchetti apre quindi una finestra di *riepilogo*, in cui vengono elencate tutte le operazioni da eseguire. Dopo una rapida occhiata per assicurarsi di non aver commesso errori, fate clic su *Applica*.

Il gestore dei pacchetti scarica quindi i pacchetti da Internet, li verifica e li installa. Occasionalmente, il gestore può indicare che non è stato possibile verificare alcuni pacchetti: **questa informazione non va presa alla leggera**. In tal caso, è meglio annullare il download, fare clic su *Ricarica* nel menu principale e ripetere l'operazione di selezione dei pacchetti. Se il messaggio appare di nuovo, potrebbe essere il risultato di un attacco, di un guasto tecnico o di un problema di configurazione. Ma è meglio astenersi dall'installare nuovi pacchetti finché non si è individuata la fonte del problema.

Infine, se tutto è andato bene, il gestore di pacchetti mostra una finestra che indica che *le modifiche sono state applicate* e si può fare clic su *Chiudi*. Infine, chiudete il gestore di pacchetti per evitare che finisca in altre mani.

17.4 Aggiungere depositi

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

Durata: Da un quarto d'ora a mezz'ora.

I pacchetti Debian contenenti i programmi si trovano nei cosiddetti *repository*. Sebbene i repository forniti con Debian contengano quasi tutto il software di cui si può avere bisogno, a volte è utile :

- installare software più recente di quello contenuto nell'ultima versione stabile di Debian, noto come *backport*;
- installare software *non libero* (ad esempio, firmware) o software fornito da terzi (ad esempio, il browser Tor).



Attenzione: aggiungere un nuovo repository Debian a un computer significa decidere di fidarsi delle persone che lo mantengono. Mentre i repository *backport* di cui stiamo parlando sono mantenuti da membri Debian, questo non è il caso di molti altri repository. La decisione di fidarsi non deve essere presa alla leggera: se il repository in questione contiene *malware*, potrebbe essere possibile installarlo sul computer senza nemmeno accorgersene.

pagina
32

17.4.1 Software aperto e aggiornamenti

Aprire *Software e aggiornamenti*: per farlo, accedere alla panoramica delle attività premendo  ( su Mac), quindi digitare `softw` e cliccare su *Software e aggiornamenti*.

17.4.2 Disabilitare i supporti di installazione locali

Come accennato nel capitolo precedente, a seconda dell'immagine di installazione usata per installare Debian, il sistema di gestione dei pacchetti può richiedere che il supporto di installazione sia sempre collegato al computer, in modo da poter aggiornare l'elenco dei pacchetti disponibili.

Per evitare questo problema, disabilitate i repository per questo supporto di installazione: nella scheda *Altro software*, deselezionate tutte le righe che iniziano con `cdrom`.

pagina
128

17.4.3 Configurare la posizione del repository

Per installare il software backported

Fare clic sulla scheda *Altro software*, quindi sul pulsante *Aggiungi*. Nella riga *APT*, inserire la directory APT da

```
deb http:// deb.debian.org/debian/bullseye-backports main
```

aggiungere:

In questo caso, la *versione del repository* è *bullseye-backports* e la *categoria* è *principale*. A questo punto, fare clic su  *Aggiungere una fonte di aggiornamento*.

Poiché questo software modifica i programmi di cui ci fidiamo, siamo rassicurati dal fatto che ci chieda la nostra password.

Per installare software non libero o di terze parti

- Nella scheda *Software Debian*, selezionare in base alle proprie esigenze
 - *contrib* per aggiungere software di terze parti ;
 - *non-free* per aggiungere software non libero.

Poiché questo software modifica i programmi di cui ci fidiamo, siamo rassicurati dal fatto che ci chieda la nostra password.

17.4.4 Aggiornare i pacchetti disponibili

Per chiudere la finestra *Software e aggiornamenti*, fare clic sul pulsante *Chiudi*. È possibile che appaia una finestra di *informazioni sul software non aggiornata*, in tal caso fare clic su *Aggiorna*. Viene visualizzata una finestra di aggiornamento *della cache* che mostra l'avanzamento del download degli elenchi di pacchetti disponibili. Questa finestra e la finestra *Software e aggiornamenti* si chiudono automaticamente al termine dell'aggiornamento.

Per installare un pacchetto dai backport, seguite lo strumento di installazione di un pacchetto e scegliete di installare una versione particolare quando si presenta la domanda.

pagina
135

Eliminare i dati "per davvero"

Nella sezione Comprensione abbiamo visto che quando si elimina un file, il suo contenuto ^{pagina 42} non viene realmente eliminato. Tuttavia, esistono programmi che permettono di cancellare i file e il loro contenuto, o almeno di tentare di farlo, con l'opzione ^{di} `rm -P` ^{limiti spiegati in precedenza.} ^{pagina 42}

18.1 Un po' di teoria

18.1.1 Il metodo Gutmann

La documentazione del pacchetto `secure-delete`, che utilizzeremo nella prossima ricetta, ispirata a una pubblicazione di Peter Gutmann del 1996 ¹ ci dice:

Il processo di eliminazione funziona come segue:

1. *la procedura di sovrascrittura (in modalità sicura) sostituisce il contenuto del file [...]. Dopo ogni passaggio, la cache del disco viene svuotata;*
2. *il file viene troncato, in modo che un utente malintenzionato non sappia quali blocchi del disco appartengono al file;*
3. *il file viene rinominato, in modo che un utente malintenzionato non possa trarre conclusioni sul contenuto del file eliminato dal suo nome;*
4. *infine, il file viene eliminato. [...]*²

Per un disco rigido magnetico di meno di 20 anni ³ è sufficiente sovrascrivere i dati un paio di volte con dati casuali.

Il NIST (*National Institute of Standards and Technology*, l'ente governativo statunitense che definisce i protocolli di sicurezza utilizzati, tra l'altro, dalle amministrazioni di quel Paese) ha pubblicato uno studio del 2006 dell'NSA, che sembra concludere che sui dischi rigidi magnetici recenti i dati sono così strettamente incollati tra loro che diventa praticamente impossibile eseguire un'analisi magnetica per trovare tracce di dati cancellati. ⁴ dall'NSA, che sembra concludere che sui dischi rigidi magnetici recenti i dati sono così strettamente incollati tra loro che diventa praticamente impossibile eseguire un'analisi magnetica per trovare tracce di dati cancellati.

Di conseguenza, nelle ricette che seguono, ci limiteremo ad alcune riscritture casuali.

Tuttavia, questo metodo non è adatto ai dischi SSD. Oggi i dischi SSD tendono a sostituire i dischi rigidi...

Ancora una volta, si tratta di trovare il giusto compromesso, caso per caso, tra velocità ^{pagina 65}

1. Peter Gutmann, 1996, *Cancellazione sicura di dati da memorie magnetiche e a stato solido* [http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html].

2. Fonte: file `file README.gz` da `secure-delete` da `installato` sua Debian a `/usr/share/doc/secure-delete`.

3. Utilizzando la tecnologia PRML [<https://fr.wikipedia.org/wiki/PRML>], introdotta nel 1990 [<http://www.datadoctor.biz/datarecoverybook/chapter-2.html>] (in inglese).

4. NIST, 2006, *Linee guida per la sanificazione dei supporti*.
[<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-88.pdf>].

e il livello di protezione desiderato, a seconda delle dimensioni dei dati da sovrascrivere, dell'età del disco rigido e della fiducia riposta nel NIST.

18.1.2 Per chiavette USB, dischi SSD e altre memorie *flash*

Per le chiavette USB e altri dispositivi di memoria *flash*, come le schede SD o i dischi SSD, uno studio del 2011 ha mostrato che la situazione era davvero problematica. ⁵ ha dimostrato che la situazione è davvero problematica.

Questo studio dimostra che è impossibile, per quante volte un file venga riscritto, essere sicuri che tutto il suo contenuto sia stato sovrascritto. Anche se questo rende i dati inaccessibili semplicemente inserendo la chiave, essi sono ancora visibili a chiunque guardi direttamente nei chip della memoria *flash*.

L'unico metodo che ha funzionato in modo costante è stato quello di riscrivere l'intera chiavetta USB più volte. Nella maggior parte dei casi sono sufficienti due passaggi, ma su alcuni modelli sono state necessarie venti riscritture prima che i dati scomparissero definitivamente.

[pagina
145] Sulla base di queste osservazioni, la risposta preventiva sembra essere la crittografia sistematica delle chiavette USB, un'operazione che rende davvero difficile estrarre informazioni direttamente dai chip di memoria *flash*. E per quanto riguarda la pulizia a posteriori, nonostante i suoi limiti, la sovrascrittura completa protegge ancora dagli attacchi puramente software.

L'unico modo per rendere illeggibili i dati su questi supporti è distruggerli fisicamente.

18.1.3 Altri limiti alla cancellazione "sicura"

Potrebbero esserci ancora informazioni sul file che possono essere utilizzate per recuperarlo, soprattutto se si utilizza un file system con journaling come *ext4*, Btrfs, HFS+, ReFS, NTFS, un sistema di scrittura, una compressione o un backup (su disco, ad esempio con RAID o tramite rete). ⁶ o tramite rete). Vedere la Parte 1.



[pagina
43]

18.2 Su altri sistemi

Abbiamo visto che è illusorio, se si utilizza un sistema operativo proprietario, cercare una vera *privacy*. Sebbene esistano software che presumibilmente cancellano i file con il loro contenuto su Windows e macOS, è molto più difficile fidarsi.

[pagina
39]

18.3 Andiamo

I contenuti possono essere eliminati:

- dei singoli file (vedi pagina successiva) ;
- di un'intera periferica (vedi pagina a fianco);
- dei file precedentemente eliminati (vedere pagina 143).

5. Michael Wei e altri, 2011, *Cancellazione affidabile dei dati dalle unità a stato solido basate su flash* [http://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf].

6. RAID è l'acronimo di *Redundant Array of Independent Disks*.

Dischi indipendenti). È un sistema che distribuisce i dati su più dischi per migliorare le prestazioni, la sicurezza o la tolleranza ai guasti (Wikipedia, 2021, *RAID (informatica)*) [[https://fr.wikipedia.org/wiki/RAID_\(informatica\)](https://fr.wikipedia.org/wiki/RAID_(informatica))].

18.4 Eliminazione di file... e del loro contenuto

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

 *Durata: Cinque minuti di preparazione, poi da pochi secondi a diverse ore di attesa, a seconda delle dimensioni del file da eliminare e del metodo utilizzato.*

Ecco come sbarazzarsi dei file, facendo attenzione a renderne illeggibile il contenuto.

 **Attenzione:** questo metodo funziona solo con i dischi rigidi meccanici. Dopo aver sovrascritto il contenuto dei file su una chiavetta USB (o su qualsiasi altro supporto di archiviazione che utilizza una memoria *flash*, come una scheda SD o un disco SSD), è molto probabile che i file siano ancora scritti in una regione inaccessibile del dispositivo!

18.4.1 Installare il software necessario

Se non l'avete ancora fatto, installate il pacchetto `nautilus-wipe` (vedere pagina 135), quindi riavviate il computer.

Questo pacchetto è presente in Tails per impostazione predefinita.

18.4.2 Eliminazione dei file e del loro contenuto dal browser dei file

In coda

Per eliminare i file e il loro contenuto con Tails, consultare la documentazione facendo clic sull'icona *Tails Documentation* sul desktop. Nell'indice che si apre, cercate la sezione *Crittografia e privacy* e fate clic sulla pagina *Eliminazione sicura dei file e pulizia dello spazio su disco*.

Con una Debian criptata

Per eliminare i file e il loro contenuto dal Browser dei file, navigare fino al file, fare clic con il tasto destro del mouse e selezionare *Sovrascrivi*. Si apre una finestra che chiede di confermare l'eliminazione e propone alcune *opzioni*.

È possibile scegliere il numero di passaggi da effettuare per coprire i dati sul dispositivo, nonché alcune opzioni di comportamento durante la cancellazione dei dati. Le opzioni predefinite sono sufficienti per i dischi rigidi magnetici.

Quindi fare clic su *Sovrascrivi*. Al termine dell'eliminazione, viene visualizzato il messaggio *Sovrascrittura riuscita*.

si apre la finestra che indica che *l'elemento o gli elementi sono stati sovrascritti con successo*.

18.5 Eliminare un intero disco "per davvero"

Prima di smaltire un disco rigido, riciclarlo, reinstallare un sistema pulito a pagina 71 o inviare un computer rotto al servizio di assistenza post-vendita, è forse opportuno ostacolare le persone che vogliono recuperare il computer. i dati che conteneva. La soluzione migliore è riscrivere l'intero disco con dati casuali.

Prima di utilizzare questa ricetta, pensateci due volte e fate un accurato backup dei dati da memorizzare. Se applicata correttamente, rende i dati molto difficili da recuperare, anche analizzando il disco in laboratorio.

pagina
151

18.6 Cancellare l'intero contenuto di un disco

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

 Tempo: Cinque minuti di preparazione, poi diverse ore di attesa a seconda delle dimensioni del disco.

[successivo] Per cancellare un intero volume (disco o partizione), utilizzare il comando `shred` per
pagina. sovrascrive tre volte l'intero set di dati con dati casuali. Oltre a cancellare i file, questo comando copre lo spazio cancellato in modo tale da rendere praticamente impossibile trovare quello che c'era prima.

[pagina] Per coprire il contenuto di un disco, dovete essere lontani da esso... se
113 contiene il sistema operativo che usate normalmente, dovete mettere il disco rigido in un altro computer o usare un sistema *live*. `shred` è uno strumento standard, quindi qualsiasi sistema *live* dovrebbe andare bene.

Il comando è molto semplice. È sufficiente conoscere la posizione del dispositivo (il suo percorso) che si desidera eliminare e avere pazienza, poiché il processo richiede diverse ore.

18.6.1 Trova il percorso del dispositivo

Innanzitutto, è necessario essere in grado di identificare il percorso utilizzato dal sistema operativo per designare il supporto di memorizzazione che si desidera cancellare.

Se si desidera cancellare un'unità interna, scollegare innanzitutto eventuali dischi rigidi esterni, chiavette USB, lettori di schede di memoria o altri dispositivi di archiviazione collegati al computer. In questo modo, da un lato si evita che vengano cancellati per errore, dall'altro si facilita la ricerca dell'unità interna.

Naturalmente, non si dovrebbe fare questo se si vuole rendere inaccessibile il contenuto di un'unità esterna.

Aprire l'utilità di gestione del disco

Aprire i dischi: visualizzare l'insieme delle attività premendo il tasto  ( su un Mac), quindi selezionare il disco e cliccare su *Dischi*.

Trova il percorso del dispositivo

La sezione a sinistra mostra l'elenco dei dischi noti al sistema. È possibile fare clic su uno qualsiasi di essi per visualizzare ulteriori informazioni sul lato destro. Le icone, le dimensioni e i nomi dei dischi dovrebbero aiutare a identificare quello che si sta cercando.

Se questo non basta, si può dare un'occhiata all'organizzazione della partizione, osservando la tabella che appare sul lato destro:

- se il disco da cancellare contiene un sistema GNU/Linux non criptato, devono essere presenti almeno due partizioni, una con file system *Swap*, l'altra solitamente *Ext3* o *Ext4*;
- se il disco da cancellare contiene un sistema GNU/Linux criptato, devono esserci almeno due partizioni, una con file system *Ext2* e l'altra *LUKS* ;
- se il disco da cancellare contiene un sistema Windows, devono essere presenti una o più partizioni contrassegnate da *NTFS* o *FAT*.

Inoltre, il dispositivo corrispondente al disco interno è solitamente il primo dell'elenco.

Una volta trovato e selezionato il disco, è possibile leggere il percorso del disco nell'angolo in basso a destra, accanto all'etichetta *Dispositivo*.

Il percorso del dispositivo inizia con `/dev/` seguito da tre lettere ed eventualmente da un numero; nella maggior parte dei casi i primi caratteri sono `sd`, `hd` o `mmcblk`: per esempio, `/dev/sdx1`. Annotate il percorso da qualche parte, senza il numero (ad esempio, `/dev/sdx`): dovrete scriverlo in seguito, al posto di `LE-PÉRIPHÉRIQUE`.



Attenzione: questo percorso potrebbe non essere sempre lo stesso. È meglio ripetere questa breve procedura dopo aver riavviato il computer, aver collegato o scollegato una chiave USB o un disco rigido. In questo modo si eviteranno spiacevoli sorprese... come la perdita del contenuto di un altro disco rigido.

18.6.2 Eseguire il comando `shred`

Aprire un terminale: aprire la panoramica delle attività premendo `⌘` (Mac), quindi digitare `terminale` e fare clic su *Terminale*.

Inserite il seguente comando, sostituendo `THE-DEVICE` con il percorso del dispositivo determinato in precedenza:

```
pkexec shred -n 3 -v LE-PÉRIPHÉRIQUE
```

Se si preferisce usare il metodo originale di Gutmann (più lungo e forse più sicuro), sostituire `-n 3` con `-n 25` nella riga di comando.

Una volta digitato e controllato il comando, premere il tasto *Invio* o `return`. Viene richiesta una password, poiché questo comando richiede i privilegi di amministrazione di pagina 99; inserirla. Il comando `shred` scriverà sul terminale, cosa che farà (poiché gli è stato chiesto di farlo aggiungendo l'opzione `-v` al comando `shred`, che significa, nel contesto di *questo* comando, che il computer deve essere "verboso").

- cioè "loquace"):

```
shred: / dev/ sdb : pass 1/3 ( random)...
shred: / dev/ sdb : passaggio 2/3 (
casuale)... shred: / dev/ sdb : passaggio
3/3 ( casuale)...
```

Al termine della procedura, il terminale visualizza nuovamente il segno `$`, che simboleggia il prompt dei comandi. A questo punto il terminale può essere chiuso.

18.6.3 Riutilizzare il disco

Attenzione: questo metodo non cancella solo i dati di un intero volume, ma anche quelli di un altro volume,

Al termine dell'operazione, il disco non ha più una tabella di partizione o un file `system`. Per riutilizzarlo, è necessario creare almeno una nuova partizione e il relativo file `system`,

utilizzando ad esempio l'applicazione Dischi. pagina 24

18.7 Rendere irrecuperabili i dati precedentemente cancellati

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

 **Tempo:** Cinque minuti di preparazione, poi da alcuni minuti a diverse ore di attesa, a seconda delle dimensioni del disco da pulire e del metodo utilizzato.

Quando i file sono già stati eliminati senza particolari precauzioni, i dati che contenevano sono ancora presenti sul disco. Lo scopo di questa ricetta è quello di recuperare i dati rimasti, sovrascrivendo lo spazio libero sul disco rigido. Questo metodo non elimina i file visibili nel browser dei file.



Attenzione: come gli altri modi per eliminare un file "per davvero", questo non funziona con alcuni file system "intelligenti" che, per essere più efficienti, non mostrano tutto lo spazio libero al software incaricato di sovrascriverne le tracce. Non ci si deve fidare di questo metodo nemmeno per le chiavette USB, le schede SD o i dischi SSD, preferendo coprire più volte la totalità dei dati in essi contenuti.

pagina

43

pagina

142

In coda

Il pacchetto `nautilus-wipe` è già installato in Tails per impostazione predefinita. È quindi sufficiente consultare la documentazione, facendo clic sull'icona *Tails Documentation* sul desktop. Quindi, nell'indice che si apre, cercate la sezione *Crittografia e privacy* e fate clic sulla pagina *Eliminazione sicura dei file e pulizia dello spazio su disco*.

Con una Debian criptata

Se non l'avete ancora fatto, installate il pacchetto `nautilus-wipe` (vedere pagina 135), quindi riavviate il computer.

Quindi, aprire un browser di file e navigare fino al disco che si desidera pulire. Fate clic con il tasto destro del mouse nella parte destra del browser dei file e selezionate *Sovrascrivi spazio libero su disco*. Si apre una finestra che chiede di confermare l'eliminazione dello spazio disponibile sul disco e propone alcune *opzioni*.

È possibile scegliere il numero di passaggi da effettuare per recuperare i dati dal dispositivo, nonché alcune opzioni di comportamento durante la cancellazione dei dati. Le opzioni predefinite sono sufficienti per i dischi magnetici di oggi.

Quindi fare clic su *Sovrascrivi lo spazio disponibile su disco*. La sovrascrittura potrebbe richiedere del tempo. In alcuni casi, è richiesta la password di amministrazione.

Si noti che all'interno della cartella viene creato un file chiamato `tmp.XXXXXXXXXX`. `Nautilus Wipe` creerà questo file all'interno e ne aumenterà le dimensioni il più possibile, in modo da utilizzare tutto lo spazio libero disponibile, quindi lo sovrascriverà in modo sicuro. Una volta completata l'eliminazione, si apre una finestra *Sovrascrittura riuscita*, in cui viene indicato che

Lo spazio disponibile su disco nella partizione o nel dispositivo "... è stato sovrascritto con successo.

Partizionare e crittografare un disco rigido

Ora analizzeremo la crittografia di un dispositivo, al fine di memorizzare i dati in modo riservato.

Una volta che un disco è stato crittografato, è possibile accedere ai dati in esso contenuti solo dopo aver inserito una passphrase per decifrarlo. Per ulteriori informazioni

Per ulteriori informazioni, consultare la sezione sulla crittografia.

pagina 47

Quando viene inserita la passphrase, il sistema ha accesso ai dati del dispositivo in questione, quindi non digitate la passphrase in un punto qualsiasi, ma solo-

su computer e sistemi in cui si ha sufficiente fiducia.

pagina 65

Non solo avranno accesso ai dati decrittati, ma sul computer rimarranno anche tracce della presenza del dispositivo. Per questo motivo, si consiglia di si usa su un sistema GNU/Linux criptato o su un PC criptato.

che

un sistema *vivo* amnesico.

pagina

Può trattarsi di un disco rigido, di un'unità SSD, di una chiavetta USB, di una scheda SD o anche solo di una parte di uno di questi dispositivi. In effetti, un disco rigido o una chiavetta USB possono essere tagliati in diversi pezzi indipendenti, noti come

119

pagina

113

punteggi.

pagina 23

Nel seguito, se non diversamente specificato, il termine disco si riferisce sia ai dischi rigidi interni che a quelli esterni, o a qualsiasi tipo di dispositivo di memoria *flash*, come una chiavetta USB, un drive SSD o una scheda SD.

Se si vuole avere un posto sul disco dove mettere i dati che non saranno riservati e a cui si può accedere su computer non affidabili, si può dividere il disco in due partizioni:

1. una partizione non criptata, dove vengono memorizzati solo dati non riservati, come la musica, e che può essere utilizzata da qualsiasi computer senza digitare la passphrase;
2. una partizione criptata contenente dati riservati, da aprire solo su computer fidati.

19.1 Panoramica

19.1.1 Crittografia di un disco con LUKS e dm-crypt

Vi spiegheremo come criptare un disco utilizzando i metodi standard di GNU/.

Linux, chiamati *dm-crypt* e LUKS, che sono software open-source. Questo sistema è ben integrato con gli ambienti desktop, quindi la maggior parte delle operazioni sono possibili senza bisogno di strumenti speciali.

19.1.2 Altri software che non raccomandiamo

[pagina] Per crittografare un disco, si sconsiglia di utilizzare software proprietario di cui non
39 ci si può fidare, come FileVault, BitLocker, Stormshield Endpoint Security o Symantec
PGP Whole Disk Encryption. Esistono anche prodotti freeware, come
VeraCrypt [<https://www.veracrypt.fr/>], che possono essere eseguiti su sistemi
operativi proprietari. Tuttavia, se si utilizza un software, anche gratuito, su un
[pagina] sistema operativo proprietario, ci si fida implicitamente di quest'ultimo, poiché
22 ha inevitabilmente accesso ai dati decifrati.

19.1.3 Panoramica della fase

Se il disco è già stato utilizzato, può essere una buona idea iniziare a recuperare i dati (vedere pagina 141).

Se il disco da crittografare non ha spazio libero, iniziare a formattarlo (vedere questa pagina). Ciò può comportare la cancellazione di tutti i dati presenti sul disco.

Quindi, se si desidera crittografare solo una parte del disco, è necessario creare prima una partizione non crittografata (vedere la pagina a fianco).

Se si dispone già di spazio non partizionato sul disco, si può passare direttamente alla fase di crittografia (vedere pagina 148).

Non resta che inizializzarlo in modo che contenga dati criptati (vedere pagina 148). Ora è pronto per l'uso (vedere pagina 148).

19.2 Preparazione di un disco per la crittografia

Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

 *Durata: Circa dieci minuti.*

 Di seguito, si utilizzerà sempre il termine disco per indicare un'unità interna o esterna, nonché una chiavetta USB, una scheda SD o un disco SSD, a meno che non si specifichi diversamente.

La procedura qui descritta prevede l'eliminazione di tutti i dati presenti sul disco.¹ Se si dispone già di spazio non partizionato sul disco, è possibile passare direttamente alla fase di crittografia (vedere pagina 148).

19.2.1 Installare i pacchetti necessari

Per criptare un disco sono necessari i seguenti pacchetti: `secure-delete`, `dosfstools` e `cryptsetup`. Con Debian 11, è necessario installare il pacchetto `secure-delete` (vedere pagina 135), mentre gli altri due sono installati di default. Se si usa Tails, questi tre pacchetti sono già installati.

19.2.1 Formattare il disco con l'utilità Dischi

Formattare significa cancellare tutti i dati presenti sul disco.

Per aprire l'applicazione Dischi dalla panoramica delle attività: premere il tasto  ( su Mac), quindi digitare `dischi` e fare clic su *Dischi*.

Nella finestra dell'applicazione Dischi, la parte sinistra elenca i dischi noti al sistema; la parte destra consente di eseguire azioni.

1. Tuttavia, è possibile *ridimensionare* una partizione esistente mantenendo i file in essa contenuti.

Selezionare il dispositivo

A sinistra si trova l'elenco dei dischi. Se il computer in uso contiene un sistema crittografato, vengono mostrati anche i volumi crittografati del nostro sistema.

Le icone, le dimensioni indicate e i nomi dei dischi dovrebbero consentirci di identificare quello che stiamo cercando.

Una volta individuato il disco, selezionarlo dall'elenco. Le informazioni visualizzate sulla destra della finestra dovrebbero confermare la selezione del disco corretto.

Volumi di smantellamento

Se il volume è montato, l'icona quadrata ■ è visibile nella sezione di destra, sotto la rappresentazione grafica del disco nella sezione *Volumi*. Fare clic su questo pulsante per smontare il volume.

Se il disco contiene diversi volumi, smontateli uno alla volta: selezionateli nella rappresentazione grafica della sezione *Volumi*, quindi smontateli come spiegato in precedenza.

Riformattare il disco



Attenzione: formattare un disco significa cancellare tutti i file presenti.

Nella barra superiore del software, fare clic sull'icona , quindi su *Formato disco...* Si apre una finestra che offre la possibilità di scegliere se cancellare o meno i dati presenti sul supporto e se formattare il disco. A seconda del contesto e dei limiti discussi sopra, a pagina 42, scegliere se cancellare o meno i dati. Lasciare *Compatibile con tutti i sistemi e dispositivi* sul pulsante *Formatta*. Quindi fare clic sul pulsante *Formattazione*.

Dischi chiede se si vuole davvero formattare il dispositivo. È il momento di verificare se si è scelto il dispositivo giusto prima di commettere un errore. In caso affermativo, confermare facendo clic su *Formatta*.

La formattazione può richiedere un certo tempo e nell'applicazione Dischi viene visualizzata una barra di avanzamento. Attendere il completamento dell'operazione prima di smontare o scollegare l'unità.

19.3 Creare una partizione non crittografata

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Due minuti.*

Se lo desiderate, è il momento di creare una partizione non criptata in cui memorizzare dati non riservati e che potrete utilizzare da qualsiasi computer senza dover digitare una passphrase.

Se si desidera criptare l'intero disco, si può passare direttamente al passo successivo (vedere la pagina seguente).

Sempre nell'applicazione Dischi, selezionare il disco desiderato, quindi, sul lato destro, fare clic sull'area *Spazio disponibile* del diagramma *Volumi*. Sotto, fare clic sul simbolo .

Selezionare la dimensione desiderata per la partizione non crittografata nel campo dedicato. Lo spazio lasciato libero verrà utilizzato per la partizione crittografata. Fare clic su *Avanti*.

È possibile scegliere un nome per questa partizione. In *Tipo*, selezionare *Compatibile con tutti i sistemi e dispositivi (FAT)*. Una volta fatto questo, fare clic su *Crea*.

19.4 Creare una partizione crittografata

- 🔄 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*
- 🕒 *Durata: Dieci minuti + da pochi minuti a diverse ore per riempire lo spazio libero, a seconda delle dimensioni della partizione.*

19.4.1 Creare una partizione crittografata

Sempre in Dischi, con il disco di destinazione selezionato, fare clic con il pulsante destro del mouse sull'area *Spazio disponibile* del diagramma *Volumi*. Quindi fare clic sul simbolo **+** in basso.

Scegliete la dimensione della partizione: mantenete la dimensione massima, poiché vogliamo creare una singola partizione crittografata in questo spazio disponibile. Fare clic su *Avanti*.

È possibile assegnare un nome alla futura partizione crittografata. Non è necessario attivare l'opzione di *cancellazione*. La cancellazione avverrà nella fase successiva, tramite il riempimento casuale dei dati, che sarà più affidabile. Nella sezione *Tipo*, selezionare *Disco interno da utilizzare solo con sistemi Linux (Ext4)*, quindi selezionare *Volume protetto da password (LUKS)*. Fare clic su *Avanti*. Scegliere una passphrase adeguata (vedere pagina 103) per il volume crittografato e digitarla nei due campi appropriati. Infine, fare clic su *Crea*.

19.4.2 Riempire la partizione con dati casuali

Infine, riempiamo lo spazio vuoto del disco crittografato con dati casuali. In questo modo nascondiamo la posizione dei nostri dati, rendendo più difficile per chiunque decifrarli.

Nel diagramma *Volumi*, individuare la *partizione [...] LUKS* e selezionare il *File System* sotto di esso. Sotto il diagramma, fare clic **▶** su .

Nella parte inferiore della finestra, in *Contenuti*, appare un collegamento dopo *Montato su*. Fare clic su questo link per aprire la cartella, quindi seguire lo strumento per rendere irrecuperabili i dati precedentemente cancellati (vedere pagina 143).

Il processo richiede da pochi minuti a qualche ora, a seconda delle dimensioni e della velocità dell'unità (ad esempio, due ore per una chiave USB da 4 GB).

19.4.3 Scollegare il disco in modo pulito

Nel browser dei file, fare clic sul simbolo **▲**, quindi scollegare fisicamente il disco (se applicabile).

Il disco crittografato è ora utilizzabile.

19.5 Utilizzare un disco rigido crittografato

- 🔄 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*
- 🕒 *Durata: Due minuti, qualche ora... o mai, se la passphrase ci sfugge.*

Per consentire al sistema di accedere ai dati su un disco crittografato, è necessario specificare una passphrase (che è proprio quello che volevamo!). Ma questa operazione è più o meno semplice, a seconda dell'ambiente.

19.5.1 Con Debian (o altro GNU/Linux)

Su un sistema GNU/Linux con un ambiente desktop configurato per aprire automaticamente i supporti esterni, quando viene inserito un disco esterno contenente dati crittografati, appare una finestra che richiede la passphrase.

In caso contrario, questa finestra appare quando si chiede al sistema di aprire la partizione crittografata, ad esempio da *File* facendo clic sul nome del disco nella colonna di sinistra.

Per chiudere la partizione crittografata, è sufficiente smontare il disco come si farebbe normalmente.

19.5.2 Con altri sistemi

Non conosciamo un modo semplice per accedere alla partizione del disco crittografata in Windows o macOS. Anche se esistono soluzioni² è una buona idea che si tratta di sistemi operativi proprietari, nei quali non c'è motivo di fidarsi. pagina 39
nessun motivo di fidarsi.

Se si desidera inserire sul disco dati a cui si vuole accedere su computer di cui non ci si fida, la cosa migliore da fare è probabilmente fornire una seconda partizione non crittografata sul disco, come spiegato sopra.

[pagina
147

2. Per le versioni precedenti di Windows (fino a Vista), era possibile utilizzare FreeOTFE (<https://sourceforge.net/projects/freeotfe.mirror/>).

Salvataggio dei dati

In linea di principio, il backup è un'operazione relativamente semplice: fare una copia dei file che non si vogliono perdere, su un supporto di memoria diverso da quello in cui si trovano i dati.

Naturalmente, se ci prendiamo la briga di mettere i nostri dati di lavoro su dischi rigidi o chiavette USB criptate, anche queste copie devono essere criptate.

Altri due punti da tenere a mente quando si implementa una buona *politica di backup*:

- definire un metodo per i backup **regolari**,
- controllare di tanto in tanto se i backup sono ancora leggibili.

Quest'ultimo aspetto non va trascurato. Perdere i dati originali è spesso doloroso. E poi scoprire che i backup non sono in grado di *ripristinare* ciò che si è perso trasforma la situazione in una catastrofe.

È anche una buona idea archiviare i backup in un luogo diverso dai dati originali, per evitare che tutto venga distrutto nello stesso momento (incendio, danni da acqua...).

20.1 Caso speciale di archiviazione persistente Tails

Quando si usa Tails, esiste un metodo per eseguire il backup dell'intero volume persistente di una chiave Tails.

Per farlo, seguiremo la documentazione ufficiale di Tails, disponibile su qualsiasi chiavetta USB o DVD di Tails, anche senza una connessione a Internet.

Avviare Tails. Sul desktop, fare clic sull'icona *Tails Documentation*. Cercate la sezione *Come iniziare con Tails* e nella sezione *Archiviazione persistente crittografata* fate clic su *Crea un backup dell'archiviazione persistente* e seguite questa pagina di documentazione.

pagina

115

20.2 Con file manager e archiviazione crittografata

L'esecuzione di backup è soprattutto una questione di rigore e disciplina. Nei casi più semplici, si può fare a meno di un software specifico per la creazione di backup e limitarsi a eseguire copie su un supporto di memorizzazione crittografato utilizzando il proprio file manager.

20.2.1 Backup

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

 *Durata: per la prima volta, il tempo di criptare il supporto di memorizzazione e di decidere quali file sottoporre a backup; in seguito, dipende dalla quantità di dati da sottoporre a backup.*

pagina

145

La crittografia dei nostri backup è garantita dalla crittografia del supporto di archiviazione esterno, chiave USB o disco rigido.

Per fare copie regolarmente e senza perdere troppo tempo, si consiglia :

- avere da qualche parte un elenco di file e cartelle di cui eseguire il backup;
- fatevi un piccolo calendario dei giorni o delle settimane in cui farete i vostri risparmi, con le caselle da spuntare dopo averli fatti.

Una buona pratica è quella di creare una cartella (sul supporto di memorizzazione del backup) con la data del backup e di copiarvi i dati. In questo modo è facile mantenere diversi backup, se lo si desidera, e cancellare i backup precedenti con la stessa facilità.



PRECISIONE

Nella scelta dei file di cui eseguire il backup, tenere presente i dati di alcuni programmi (come quelli del programma di posta elettronica Thunderbird¹), che a volte si trovano in cartelle nascoste. In *File*, possono essere visualizzati facendo clic su *Afficher les fichiers cachés*.

20.2.2 Ripristino di un backup

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

 *Durata: dipende dalla quantità di dati da ripristinare.*

Durata: dipende dalla quantità di dati da ripristinare.

In caso di perdita dei dati originali, il ripristino è semplice come quello del backup: si effettuano copie in senso inverso.

20.2.3 Assicuratevi che i backup siano sempre leggibili

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

Tempo: circa cinque minuti, quindi attendere la verifica.

Se il backup dei dati è stato eseguito su un dispositivo di archiviazione esterno, è necessario prima **c o l l e g a r l o** al computer.

Forse il modo più ovvio per garantire che i backup siano sempre leggibili è quello di simulare un ripristino. Tuttavia, c'è un inconveniente: bisogna avere a disposizione abbastanza spazio libero per copiare tutti i dati di backup in una cartella temporanea, che poi si cancella.

pagina

97

Ecco un altro metodo, forse meno facile da implementare, ma che non presenta questo vincolo. Richiede l'uso di un terminale.

1. Vincent, Pippo e altri, 2021, *Profili - dove Thunderbird conserva i messaggi e altri dati dell'utente* [<https://support.mozilla.org/fr/kb/profils-thunderbird-conserve-donnees-utilisateur>].

Avviare il comando digitando (senza premere *Invio*,  o ):

```
tar -cPf / dev/ null
```

Quindi, aggiungere uno spazio e indicare la cartella contenente i backup, attraverso l'icona della cartella con il mouse e portandola nella finestra del terminale. Dopo aver rilasciato il pulsante, l'aspetto dell'applicazione dovrebbe essere il seguente:

```
tar -cPf / dev/ null '/ media/ external/ backups
```

La riproduzione ha inizio non appena si preme *Invio* (). La riga seguente deve rimanere vuota fino al termine dell'operazione.

Se nel frattempo compaiono messaggi di errore, come "*Errore di input/output*" o "*Erreur d'entrée/- sortie*", significa che il backup è corrotto. In questo caso, è necessario eseguire un nuovo backup su un nuovo supporto di memorizzazione (chiave USB o disco rigido), controllarlo e quindi eliminare il supporto di memorizzazione difettoso.

Dopo un po' di pazienza e il ritorno del prompt dei comandi \$, è possibile chiudere il terminale.

Nota: questi due metodi hanno in comune il difetto di non verificare l'integrità dei dati. pagina 53 La creazione di un meccanismo per farlo è difficile senza ricorrere a un sistema

software di backup.

20.3 Utilizzo di Déjà Dup

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Tempo: Cinque minuti per installare il software.*

In alternativa, è possibile utilizzare un software di backup specializzato. Uno di questi programmi, Déjà Dup, è facile da usare e produce backup criptati. Questi backup sono anche "in-crementali", cioè vengono salvati solo i nuovi file e le modifiche; i file invariati rispetto al backup precedente non vengono copiati di nuovo, per cui è possibile accedere ai file così com'erano a ogni backup.

Ciò che lo rende così semplice può essere un limite: quando si configura il software, si scelgono le cartelle di cui eseguire il backup e il supporto su cui memorizzarle. Ma non è possibile avere configurazioni multiple che permettano di salvare alcune cartelle su un disco rigido con una passphrase e altri dati su un server, ad esempio, con un'altra passphrase. Déjà Dup è quindi ideale per eseguire regolarmente il backup del contenuto della cartella personale, ma non molto di più.

Inoltre, non viene fornito con l'ambiente predefinito, quindi è necessario installare il software (vedere pagina 134) *Déjà Dup Backups* prima di poterlo utilizzare.

20.3.1 Esecuzione di un backup

🔄 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Tempo: circa 15 minuti per la configurazione, da pochi minuti a diverse ore per il backup, a seconda delle dimensioni del file da copiare.*

Aprire *Backup* dalla panoramica delle attività: premere  ( su Mac), quindi digitare *salva* e fare clic su *Backup*.

La prima volta che si avvia il programma, si viene accolti da due pulsanti: uno per *Creare il mio primo backup*, l'altro per *Ripristinare da un backup precedente*. Fare clic sul primo pulsante per definire ciò che si desidera eseguire il backup e dove. Viene visualizzata una finestra di *backup* che mostra diverse fasi:

1. Lasciare la *Cartella di cui eseguire il backup* impostata su *Cartella personale* con nome dell'account, che è sufficiente nella maggior parte dei casi. Aggiungete a *Cartelle da ignorare* le cartelle contenenti file spesso di grandi dimensioni ma più facili da trovare, come *Video* o *Musica*. Quindi selezionare *Avanti*.
2. In *Posizione di archiviazione*, selezionare la posizione del backup. Per archiviare il backup su un'unità esterna, collegare l'unità in questione al computer e selezionarla dall'elenco *Posizione di archiviazione*. Scegliere un nome per la cartella di backup in *Cartella*. Quindi selezionare *Avanti*.
3. L'opzione *Proteggi backup con password* è selezionata per impostazione predefinita: si inserisce quindi una passphrase (vedere pagina 103) in *Password di crittografia* per crittografare il nuovo backup.² il nostro nuovo backup. Si noti che la crittografia riguarda solo il contenuto effettivo dei file da sottoporre a backup: Dup non cripta i nomi dei file e delle directory di cui si esegue il backup. Inoltre, la passphrase non può essere modificata una volta definita. Fare clic su *Avanti* per avviare il backup.

Una volta completato il backup, la finestra *Backup* si chiude e lascia il posto alla *Panoramica backup*. Questa visualizza un messaggio di notifica sulla data dell'ultimo backup e sul prossimo backup pianificato.

L'automazione del backup può essere attivata tramite il pulsante *Salva automaticamente*, che diventa blu quando è abilitato.

Per impostazione predefinita, l'automazione è settimanale e il periodo di conservazione dei backup è permanente.

Tutti questi parametri possono essere modificati *tramite* le *Preferenze*, accessibili dal menu  :

- La posizione del backup può essere modificata nella scheda *Generale*.
- Il tempo di conservazione dei backup può essere limitato a tre mesi, sei mesi, un anno o a tempo indeterminato dalla scheda *Generale*.
- L'automazione del backup può essere attivata dalla scheda *Generale* e si può scegliere la *frequenza dei backup automatici* tra *Ogni giorno* e *Ogni settimana*.
- *Le cartelle da sottoporre a backup* sono elencate nella scheda *Cartelle*: il pulsante  aggiunge un'ulteriore cartella da sottoporre a backup; il pulsante  rimuove la cartella corrispondente dal backup.
- Anche le *cartelle da ignorare* sono elencate nella scheda *Cartelle* e vengono aggiunte ed eliminate allo stesso modo.

2. Se il supporto esterno è crittografato, si può decidere di non crittografare i file di backup.

Ciò significa una passphrase in meno da inventare e ricordare. Tuttavia, si perde la possibilità di compartimentare l'accesso, nel caso in cui il supporto esterno venga utilizzato per scopi diversi dal backup.

Quando vengono attivati i backup pianificati e il tempo indicato dal backup precedente è trascorso, Déjà Dup visualizza un messaggio di notifica per informarci che il backup pianificato è in ritardo e verrà avviato non appena il supporto esterno verrà ricollegato al computer. Non appena ciò avviene, si apre automaticamente una finestra che chiede di inserire la *passphrase* necessaria per aggiornare il backup.

20.3.2 Ripristino di un backup

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Cinque minuti per la configurazione, da pochi minuti a diverse ore per il ripristino, a seconda delle dimensioni del nostro backup.*

Aprire *Backup* dalla panoramica delle attività: premere  ( su Mac), quindi digitare *salvare* e fare clic su *Backup*.

Collegare il disco contenente i backup e aprirlo da *File* se è criptato.

L'operazione di ripristino viene avviata facendo clic sul pulsante *Ripristina*.

Se è la prima volta che si usa *Backup* (ad esempio per ripristinare la cartella personale dopo la perdita di un disco rigido), verrà chiesto di specificare la cartella in cui sono stati eseguiti i backup. In caso contrario, verranno utilizzati i parametri di backup già configurati.

Dopo un breve intervallo di tempo, *Backup* aff mostra l'elenco dei file e delle directory dell'ultimo backup, insieme alla sua data. È possibile scegliere un'altra data di backup dall'elenco a discesa *Data*. Il pulsante *Ripristina* può essere utilizzato non appena sono state selezionate tutte o alcune delle directory e dei file da ripristinare.

Successivamente, è necessario specificare la cartella in cui verranno scritti i file del backup. È possibile *ripristinare i file nelle loro posizioni originali* (il che potrebbe sostituire alcuni file con la vecchia versione del backup), oppure *ripristinare una cartella specifica*.

Dopo aver fatto clic su *Ripristina*, inizia la scrittura dei file dal backup, dopo aver richiesto la *passphrase* se il backup era criptato. Se tutto è andato bene, la finestra mostra che *i file sono stati ripristinati con successo*.

20.3.3 Assicuratevi che i backup siano sempre leggibili

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Da pochi minuti a diverse ore, a seconda delle dimensioni dei nostri backup.*

Il funzionamento incrementale di Déjà Dup assicura superficialmente la leggibilità dei salvataggi precedenti. Tuttavia, non si tratta di una garanzia.

Purtroppo, il metodo migliore attualmente disponibile con Déjà Dup per garantire il ripristino dei backup è... il ripristino in una cartella temporanea che verrà poi eliminata. Questo metodo è tutt'altro che pratico ed è necessario avere accesso a un disco rigido crittografato sufficientemente grande.

Tuttavia, è possibile garantire che i file contenenti i backup rimangano leggibili utilizzando gli stessi metodi descritti in precedenza.

Condividere un segreto

C Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

L Durata: Circa un'ora.

A volte si vuole che più persone condividano un segreto, senza che ciascuno abbia l'intero segreto.

A questo scopo sono state inventate diverse tecniche crittografiche. Utilizzando calcoli matematici leggermente diversi, tutte possono essere utilizzate per decodificare un segreto in diversi pezzi, che possono poi essere ricostruiti mettendo insieme alcuni di essi. ¹.

21.1 Condividere una passphrase

L'uso più pratico è quello di condividere la passphrase di un supporto crittografato come segreto.

Idealmente, questa fase dovrebbe essere eseguita su un sistema *in funzione*, in modo da non lasciare tracce del segreto che si sta per condividere.

pagina
145
pagina
113

21.1.1 Installare il pacchetto necessario

Per condividere il segreto, utilizzare il programma `ssss-split`. Questo programma è uno di quelli forniti con il sistema Tails *live*. Tuttavia, per usarlo su una Debian criptata, è necessario installare il pacchetto Debian `ssss`.

Gli strumenti contenuti nel pacchetto `ssss` devono essere utilizzati alla riga di comando. Tutte le operazioni dovranno quindi essere eseguite in un Terminale, senza poteri di amministrazione.

pagina
Tutte
135
pagina

21.1.2 Generare una passphrase casuale

Nel nostro caso, nessuno deve essere in grado di ricordare o indovinare la passphrase che verrà utilizzata per la crittografia. Quindi genereremo una passphrase completamente casuale digitando il comando :

```
➤ head -c 32 / dev/ random | base64
```

Il computer risponderà qualcosa come :

```
7 rZw00u+8 v1stea980uyU1efwNzHaKX9CuZ/ TK0bRWY=
```

1. Per maggiori dettagli, consultare l'articolo di Wikipedia sui [segreti distribuiti](https://fr.wikipedia.org/wiki/Secret_r%C3%A9parti) [https://fr.wikipedia.org/wiki/Secret_r%C3%A9parti].

Se si desidera variare la lunghezza della passphrase, sostituire 32 con il numero di caratteri desiderato. Selezionare questa riga con il mouse e copiarla negli appunti, facendo clic con il pulsante destro del mouse e poi su *Copia*.

21.1.3 Tagliare il segreto

Prima di tagliare il segreto, dobbiamo decidere in quanti pezzi verrà tagliato e quanti pezzi saranno necessari per ricostituirlo.

Quindi, sempre utilizzando il nostro terminale, dobbiamo usare `ssss-split` come segue:

```
> ssss-split -t NUMERO DI MORRORI-NECESSARIO -n
S NUMERO DI TOTALI
```

Il NUMERO DI PASSFRASI NECESSARIE è il numero di pezzi che devono essere assemblati per trovare la passphrase originale. Il NUMERO TOTALE DI PEZZI è il numero di pezzi in cui verrà tagliata la passphrase. Il messaggio AVVERTENZA: impossibile ottenere il blocco della memoria può essere facilmente ignorato se si utilizza un sistema *attivo*.

Quando viene richiesto il segreto, è possibile incollare il contenuto degli appunti facendo clic con il pulsante destro del mouse e poi facendo clic su *Incolla*.

Quindi premere *Invio* (`↵`) o `return`) per convalidare l'ordine.

Ciascuna persona che condivide il segreto dovrà mantenere una delle righe affisse successivamente. E questo nella loro **integrità**, facendo attenzione anche al primo numero seguito dal trattino.

Ecco un esempio con la chiave casuale generata in precedenza, condivisa tra sei persone e che richiede che tre di loro si riuniscano per trovarla:

```
$ ssss - split -t 3 -n 6
Generazione di azioni utilizzando uno schema (3 ,6) con sicurezza
dinamica Elnetver1.il segreto , al massimo 128 caratteri ASCII:
Utilizzando uno schema a 352 bit
s1 - b5e1c1e72576 a1a8091760 b18f125 e12bb6f2 b1f 2 dd9d93f 7072 ec
6b129b2e7a8b5bc87ef9675d3c6ee
7d4399a49 f83f 0af 05 fc 207 e3b 466 caef30ec4 d39c 060800371 feab93 594350
sb 769959a48dbf9c 71 ed9cd 2
b3 - 4f314b 718 c738 b 58873 dab 22d24e 526931 b 061 a6 ac331613 d8fe 79b
9f727539caa625473d ec0e6cf 77b6
c4bb -1 464 3 a1efcde 7f4f 5658415 a150 fcac 6da 04f 697 ebfeb9427 b59 dca
57b50 be0ce57755c51c0c
b5a6f c1a1eeb a12 504 0 b5 cbec 40 ab14964 d2cd 7463 af34 c389f81158
8f307 b6
b5e070897f783de985e7efb 726
s283677c f0402 f8d 68 bcce 722
ebba1f
```

21.1.4 Creare supporti crittografati

È quindi possibile creare il supporto crittografato. Quando si inserisce la passphrase, è possibile copiare il contenuto degli appunti, come prima, o trascriverlo con il supporto davanti a sé.

21.2 Ricostruire la passphrase

Per ricostituire la passphrase (il segreto), sono necessari almeno tanti pezzi quanti ne sono stati decisi al momento del taglio (tre nel nostro esempio).

Idealmente, anche questa fase dovrebbe essere eseguita su un sistema *in funzione*, in modo da non lasciare tracce del segreto condiviso.

21.2.1 Installare i pacchetti necessari

Come in precedenza, se il programma non è disponibile sul sistema, è necessario installare il file `ssss` e aprire un terminale.

pagina

135

21.2.2 Ricombinare il segreto

Per ricombinare il segreto, utilizzare il programma `ssss-combine`. È necessario dirgli quanti pezzi si hanno a disposizione:

```
ssss-combine -t NUMERO DI MORRORI-A-DISPOSIZIONE
```

Il programma richiede quindi di inserire i brani disponibili. È necessario digitare *Invio* (`↵`) dopo aver scritto ciascuno di essi. Se tutto va bene il programma aff visualizzerà la passphrase completa.

Per tornare all'esempio precedente, si ottiene :

```
$ ssss -combine -t 3
Immettere 3 azioni separate da linee nuove:
Condividi [1/3]: 4 -143 a1efcde7 f4f5658415 a150 fcac6 da04f697
sebf9a4527b750be59dcc755510 b0e57 ccc594
eS h a r e [ 26b1a1eeb04 ] 3 /: 2-af83f0 af05fc207 e3b 466caef30 ec4 d39
e060803714350 b7699a8db9594bfc71 ed9 cd2bf314
e060803714350 b7699a8db9594bfc71 ed9 cd2bf314
bS h a 738 r e [3/3]: 6- ebf7 a305 f14 bf3143 b801a222
e1e8574291215923774f9f335 d283677 f4c002f8
e1e8574291215923774f9f335 d283677 f4c002f8
Resulting passphrase: 7 rZw0U+8 v1stea00yU1efwzH-KXGz/
TK0bRWY=
```



Attenzione: se uno dei pezzi è stato digitato male, l'errore che si presenta non è necessariamente molto esplicito:

```
$ ssss -combine -t 3
Immettere 3 azioni separate da linee nuove:
Condividi [1/3]: 4 -143 a1efcde7 f4f5658415 a150 fcac6 da04f697
sebf9a4527b750be59dcc755510 b0e57 ccc594
eS h a r e [ 26b1a1eeb04 ] 3 /: 2-af83f0 af05fc207 e3b 466caef30 ec4 d39
e060803714350 b7699a8db9594bfc71 ed9 cd2bf31
e060803714350 b7699a8db9594bfc71 ed9 cd2bf31
aS h a b738 e r[3/3]: 6- ebf7 a305 f14 bf3143 b801a222
e1e8574291215923774f9f335 d283677
e1e8574291215923774f9f335 d283677
Resulting passphrase: ..... L.fm.....6 _.... v..
w.a....[...
modalità -x.
```

21.2.3 Aprire supporti criptati

Una volta ottenuta la passphrase, è possibile copiarla e incollarla per sbloccare il supporto crittografato o trascriverlo con la passphrase davanti a sé.

Utilizzo delle checksum

🔄 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: Da cinque a dieci minuti.*

Nella Parte I abbiamo parlato delle *checksum*: "numeri" a pagina 53 che possono essere usati per verificare l'integrità di un file (o di qualsiasi altro dato). Il principio è che è praticamente impossibile avere una somma di controllo identica per tutti i file.

due file diversi. Se, in una lettera, Ana dice a Bea che sul suo sito è possibile scaricare a programma che ha il checksum SHA256

171a0233a4112858db23621dd5ffa31d269cbdb4e75bc206ada58ddab444651f e che il file che Bea scarica ha lo stesso checksum, allora è quasi certo che nessuno ha manomesso il programma lungo il percorso. Quindi può eseguire il programma senza troppi timori.

Esistono diversi algoritmi - o *funzioni hash* - per la creazione di checksum. Questi includono :

- MD5 non è più sicuro e dovrebbe essere evitato;
- SHA-1 è stato ampiamente utilizzato fino al 2017, quando si è verificato un attacco effettivo a questo algoritmo. Da allora è stato utilizzato sempre meno. Dovrebbe essere abbandonato;
- Quelli della famiglia SHA-2 (SHA-224, SHA-256, SHA-384 e SHA-512) saranno ancora sicuri nel 2022. In questa sede utilizzeremo SHA-256, ma il metodo funziona anche con gli altri algoritmi di questa famiglia.

22.1 Ottenere il checksum di un file

Sia che si voglia verificare l'integrità di un file, sia che si voglia consentire ai destinatari di

A tale scopo, è necessario calcolare la somma di controllo di questo file. pagina 53 Per eseguire questi calcoli è possibile utilizzare sia uno strumento grafico che un terminale. Tuttavia, in questa sede non entreremo nei dettagli dell'uso di un terminale.

22.1.1 Installare il software necessario

Se non è già installato, installare il pacchetto `nautilus-gtkhash` (vedere pagina 135), quindi riavviare il computer. Questo pacchetto è installato di default in Tails.

22.1.2 Calcolo del checksum

Aprire i *file* dalla panoramica delle attività: premere  ( su Mac), quindi digitare e fare clic su *File*.

Selezionare il file per il quale si desidera ottenere le checksum, quindi fare clic con il tasto destro del mouse. Nel menu contestuale che appare, selezionare *Proprietà*, quindi la scheda *Stampe*.

Sono disponibili numerose *funzioni hash*, con tre selezioni predefinite: MD5, SHA1, SHA256. Se si desidera un checksum diverso da questi, selezionare la casella appropriata. Fare clic su *Hash*. Le somme di controllo appaiono ora nella colonna *Fingerprint*.

22.2 Controllare l'integrità dei file

Il checksum del file originale deve essere ottenuto con un mezzo sicuro diverso da quello utilizzato per ricevere il file. Ad esempio, se si scarica il file, si può ricevere il checksum in una lettera o per telefono; il modo migliore, ovviamente, è il passaparola.

Allo stesso modo, per consentire ad altre persone di verificare l'integrità di un file che inviamo loro, inviamo loro il checksum utilizzando gli stessi metodi.

Infine, utilizzando il metodo spiegato sopra, calcolate il checksum della nostra copia del file. Fate attenzione a usare la stessa funzione di hash utilizzata dalla nostra corrispondente. Se noi usiamo SHA1 e lei SHA256, ovviamente non otterremo lo stesso checksum. Se il nostro corrispondente ci propone diverse checksum, preferiamo l'algoritmo più difficile da decifrare (vedi pagina precedente), come indicato all'inizio di questo capitolo.

Verificare che le due checksum siano identiche: è un'operazione un po' lunga e noiosa. Spesso è più facile farlo a coppie o incollandoli uno sotto l'altro in un file di testo.

Installazione e funzionamento di un sistema virtualizzato

Lo scopo di queste ricette è quello di utilizzare un sistema operativo virtuale, cioè di eseguire diversi sistemi operativi su un unico computer, quasi come se fossero in esecuzione su macchine fisiche separate. Il sistema virtuale (chiamato *guest*) viene eseguito all'interno del nostro sistema GNU/Linux (chiamato *host*): si tratta della cosiddetta *virtualizzazione*. Questa tecnologia, insieme a una politica di sicurezza

Le modalità di utilizzo sono descritte nel caso d'uso a pagina 82, che spiega come lavorare su un documento sensibile di Windows.



PER SAPERNE DI PIÙ...

L'utilizzo di un sistema virtualizzato può avere altre ragioni. Ad esempio, è possibile avviare una chiave Tails (vedere pagina 113) in un sistema virtuale e utilizzarla senza dover riavviare il computer. È anche possibile installare Tails direttamente nel *Virtual Machine Manager*¹, allo stesso modo di altri sistemi operativi. È importante, tuttavia, considerare e analizzare attentamente le tracce che si possono lasciare nel sistema host, nel sistema guest o nei metadati dei documenti creati e condivisi.

23.1 Installare il gestore di macchine virtuali

🔄 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: Circa 15 minuti.*

23.1.1 Principio

Lo scopo di questa ricetta è quello di installare il *Virtual Machine Manager*² che ci permetterà di eseguire un sistema Windows virtuale (o qualsiasi altro sistema) all'interno del nostro sistema Debian GNU/Linux.

1. La documentazione in merito si trova [sul sito ufficiale di Tails \[https://tails.boum.org/install/vm/index.en.html\]](https://tails.boum.org/install/vm/index.en.html).

2. Le edizioni precedenti di questa *Guida* raccomandavano l'uso del software VirtualBox. Tuttavia, questa non è più disponibile in Debian. Se si utilizzava questo strumento in precedenza, è necessario reinstallare la macchina virtuale o migrarla da VirtualBox a Virtual Machine Manager. Questa procedura non è documentata in questa *Guida*, ma si può iniziare seguendo le istruzioni disponibili sul web: [Malte Gerken, 2017, Migrare una macchina virtuale da VirtualBox a libvirt \[https://maltegerken.de/blog/2017/01/migrate-a-vm-from-virtualbox-to-libvirt/\]](https://maltegerken.de/blog/2017/01/migrate-a-vm-from-virtualbox-to-libvirt/) (en Inglese).

23.1.2 Installare e lanciare Virtual Machine Manager

pagina

134

Il passo successivo è l'installazione del software *Virtual Machine Manager*.

Quindi, per avviare *Virtual Machine Manager*, aprire la panoramica delle attività premendo **[⌘]** (**[⌘]** su Mac), quindi digitare `virt` e fare clic su *Virtual Machine Manager*. Verrà richiesta la password di amministrazione, il che è normale.

23.2 Abilitazione della virtualizzazione hardware

 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Circa 15 minuti.*

23.2.1 Principio

La stragrande maggioranza dei processori odierni incorpora un supporto hardware speciale per la virtualizzazione, noto come *virtualizzazione hardware*, in modo che i sistemi virtualizzati funzionino senza problemi come se fossero in esecuzione su una macchina fisica reale. Tuttavia, questa funzione è talvolta disabilitata per impostazione predefinita su alcuni computer, rendendo le macchine virtuali estremamente lente.

23.2.2 Verificare se la virtualizzazione hardware è abilitata

Per verificare se la virtualizzazione hardware è abilitata sul nostro computer, possiamo utilizzare un piccolo programma fornito con Virtual Machine Manager.

pagina

97



A tale scopo, utilizzare un terminale e digitare il seguente comando:

```
virt - host - validare
```

Il comando `aff` visualizza quindi diverse righe di diagnostica. Cercate quella intitolata *QEMU: Verifica della virtualizzazione dell'hardware* (normalmente la prima):

- Se su questa riga compare la dicitura *PASS* (in verde), la virtualizzazione hardware è effettivamente abilitata. Possiamo quindi passare direttamente alla parte successiva di questo capitolo.
- Altrimenti, se su questa riga è presente la dicitura *FAIL* (in rosso), significa che la virtualizzazione hardware è disabilitata. Continueremo a leggere questa sezione per attivarla.

pagina

a fianco

23.2.3 Abilitazione della virtualizzazione hardware nel firmware

Per attivare questa funzione, è necessario modificare la configurazione del firmware del computer:

pagina

108

pagina

109

- Per prima cosa, riavviare il computer, quindi accedere all'interfaccia di configurazione del firmware.
- Se non si ha familiarità con l'interfaccia di configurazione del firmware, consultare la descrizione in un capitolo precedente.
- Una volta nel firmware, cercate qualcosa come *Virtualization Technology*, *VT-x* o *AMD-V* (che sono i nomi delle tecnologie di virtualizzazione hardware dei processori Intel e AMD, rispettivamente). Queste opzioni si trovano solitamente nei sottomenu *Advanced* o *System Configuration*. Questa opzione è probabilmente contrassegnata come *disabilitata*.

- Con i tasti freccia, selezionare l'opzione desiderata e impostarla su **Abilitato**, oppure premendo il tasto *Invio* () o quindi selezionando il valore corretto (se l'interfaccia del firmware indica qualcosa come *Invio: Seleziona* nel suo campo di aiuto), oppure utilizzando il tasto *ritorno* () e (se l'interfaccia indica +/-: Valore). e- (se l'interfaccia indica +/-: Valore).
- Una volta selezionato il valore corretto, salvare la modifica e uscire dall'interfaccia di configurazione del firmware.

pagina

111

23.2.4 Verificare che la virtualizzazione hardware sia abilitata

Il computer si riavvia: possiamo eseguire nuovamente il test con il comando `virt-host-validate` per verificare che la virtualizzazione hardware sia ora attivata.

23.3 Installazione di un Windows virtualizzato

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

 *Durata: Circa venti minuti, pi ù il tempo per installare Windows (da trenta minuti a oltre un'ora).*

Innanzitutto, scaricate un'immagine ISO della versione di Windows desiderata. Ad esempio, è possibile trovare immagini ISO ufficiali di versioni recenti di Windows sul sito web di Microsoft ³.

23.3.1 Creare una nuova macchina virtuale

Per lanciare Virtual Machine Manager, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `virt` e fare clic su *Virtual Machine Manager*.

Il programma si avvia ed è necessario inserire la password e autenticarsi. Fate clic sul menu *File*, quindi su *Nuova macchina virtuale* e seguite la procedura guidata in cinque fasi. Al termine di ogni fase, fare clic su *Avanti* per passare alla successiva.

- Passo 1: Selezionare il *supporto di installazione locale (immagine ISO o CD-ROM)*.
- Fase 2: Per *scegliere un supporto di installazione (ISO o CDR0M)*, fare clic su *Sfoglia...*, si apre una finestra. Fare clic su *Sfoglia localmente* in basso, quindi selezionare l'immagine ISO scaricata. Fare clic su *Apri*. Nel campo *Scegliere il sistema operativo che si sta installando*: se il sistema e la sua versione non sono ben riconosciuti, *deselezionare Rileva automaticamente dalla sorgente/supporto di installazione* per sceglierlo manualmente, ad esempio *Microsoft Windows 10*.
- Fase 3: specificare la *dimensione della memoria* e il numero di *CPU* dedicate alla macchina virtuale. Ecco i minimi consigliati per le ultime versioni di Windows :

Versione	Memoria (RAM)	CPU
Windows 7	1024 MiB	1
Windows 8	2048 MiB	1
Windows 10	2048 MiB	1
Windows 11	4096 MiB	2

3. <https://www.microsoft.com/fr-fr/software-download>

- Passo 4: scegliere la dimensione dell'immagine del disco allocata alla macchina virtuale. Dato che vogliamo ospitare un intero sistema Windows, deve essere consistente: 20 GB è un minimo.
- Fase 5: Inserire un *nome* per la macchina virtuale, quindi selezionare *Personalizza configurazione prima dell'installazione*.

Infine, fare clic su *Fine*.

Se viene visualizzato il messaggio *La rete virtuale non è attiva*, fare clic su *No*: non verrà comunque utilizzata per questa macchina virtuale.

Nella colonna di sinistra della finestra che si apre, selezionare l'hardware *NIC* (*Network Interface Card*), che rappresenta la scheda di rete della macchina virtuale, quindi fare clic su *Rimuovi* in basso. Nella finestra di conferma, selezionare *Sì*. La macchina virtuale è ora isolata dalla rete.

Quindi, aggiungere un canale necessario per la condivisione delle cartelle tra i sistemi host e guest. A tale scopo, fare clic sul pulsante in basso a sinistra *Aggiungi hardware*. Nella finestra che appare, fare clic su *Canale* nell'elenco a sinistra. Nell'elenco a discesa *Nome*, selezionare *org.spice-space.webdav.0*, quindi fare clic sul pulsante *Fine*.

Fare clic su *Avvia installazione* per avviare l'installazione di Windows.

23.3.2 Installazione di *Windows* nella macchina virtuale

Il sistema virtuale si avvia dal file ISO che gli abbiamo fornito e inizia l'installazione. Non entreremo nei dettagli del processo, che dipende dalla nostra versione di Windows, ma dobbiamo sottolineare che :

- Per visualizzare l'intero programma di installazione, scegliere il menu *Afficher* → *Scale affichage* * *Sempre*.
- Non inserire informazioni personali quando vengono richiesti *Nome* e *Organizzazione*. Mettere "utente", ad esempio.
- Allo stesso modo, se si desidera inserire un numero di serie di Windows, è possibile creare un collegamento se questo è stato assegnato ufficialmente.
- Durante la configurazione della rete, potrebbe apparire un messaggio di errore. Questo è un buon segno: abbiamo disabilitato la rete della macchina virtuale.

Una volta completata l'installazione, spegnere il Windows virtuale facendo clic sul menu *Macchina virtuale* → *Arresta* → *Arresta*. Se la macchina non si spegne, è possibile selezionare *Forza spegnimento* dallo stesso menu.

Dalla finestra della macchina virtuale, fare clic sul menu *Afficher* → *Dettagli*. Nell'elenco a sinistra, scegliere *SATA CDROM 1* o *IDE CD-ROM 1* (a seconda dell'ordinamento), quindi cancellare il contenuto del campo *Directory di origine* e fare clic su *Applica*.

23.3.3 Strumenti guest per *Virtual Machine Manager*

Alcuni driver specifici migliorano l'interazione tra *Virtual Machine Manager* e il sistema Windows guest, grazie a una tecnologia chiamata SPICE: si tratta di *Guest Tools* e *Folder Sharing Service*. Questi driver consentono, ad esempio, di copiare e incollare o trasferire file tra il sistema host e quello guest virtuale. A tal fine, si utilizzano due piccoli programmi di installazione.

Dal sistema host, scaricare il programma di installazione per Windows degli strumenti SPICEguest

4.

[pagina]

Per verificare l'autenticità del file scaricato, recuperarne la firma⁵ e importare

la chiave PGP ⁶ utilizzata per verificarla. L'impronta digitale della chiave ⁷ osservata da chi scrive queste righe, supponendo che abbia in mano una copia originale della guida, è :

```
94 A9 F756 61 F7 7 A61 6864 9 B23 A9D8 C214 29 AC 6 C82
```

pagina
343

Andare quindi alla pagina web del programma di installazione WebDAV per SPICE ⁸. Fare clic sul link per il download dell'ultima versione corrispondente all'architettura della nostra macchina virtuale. Il nome contiene *x86* per Windows a 32 bit o *-64* per Windows a 64 bit. Assicurarsi che sia presente anche un file di firma ⁹ per questa versione. Verificare l'autenticità del file. Se il file corrispondente al file scaricato è un *.sha256*, verificare l'autenticità utilizzando la somma di controllo. Scaricare la chiave PGP da questo link ¹⁰ con il browser web: nel menu a tendina in alto a destra , fare clic su *Salva con nome...* e salvarla, assegnandole un nome seguito dall'estensione *.asc*. Importare questa chiave per verificare l'autenticità del file. L'impronta digitale della chiave ¹¹ osservata da chi scrive queste righe, supponendo di avere tra le mani una copia originale della guida, è :

```
206 D 3 B35 2 F56 6 F3B 0 E65 72 E9 97 D9 123 D E37A 484 F
```

pagina
345

pagina
161
pagina
343

Seguire quindi le istruzioni per installare spice-guest-tools su un sistema virtualizzato.

Fate lo stesso con spice-webdavd. L'installazione di spice-webdavd può sembrare sorprendente: non c'è alcun messaggio che indichi il completamento dell'installazione. Non preoccupatevi.

Ora è possibile copiare e incollare il testo tra la macchina host e la macchina virtuale. È anche possibile copiare e incollare file, ma solo dalla macchina host alla macchina virtuale Windows. Se non funziona, provare a trascinare il documento da una finestra all'altra (il file trascinato arriva sul desktop della macchina virtuale Windows). Un'altra funzione è quella di modificare l'immagine della macchina virtuale in base alle dimensioni della finestra che ospita Windows. A tale scopo, fare clic sul menu *Afficher* → *Scale affichage* e selezionare *Automatically adjust virtual machine to window*.

pagina

169

pagina

169

23.3.4 Backup di Windows virtuale appena installato

L'installazione di Windows virtuale è stata completata, ma c'è ancora molto da fare! Prima di lavorare su documenti sensibili all'interno della macchina virtuale, è importante fare un'istantanea, cioè salvare lo stato di questo *Windows*, considerato "pulito" perché appena installato.

4. <https://www.spice-space.org/download/windows/spice-guest-tools/spice-guest-tools-latest.exe>

5. <https://www.spice-space.org/download/windows/spice-guest-tools/spice-guest-tools-latest.exe.sig>

6. <https://keys.openpgp.org/vks/v1/by-fingerprint/94A9F75661F77A6168649B23A9D8C21429AC6C82>

7. L'impronta digitale della chiave PGP importata può essere verificata utilizzando il software *Kleopatra* [pagina 345].

8. <https://www.spice-space.org/download/windows/spice-webdavd/>

9. In altre parole, un file con lo stesso nome e un'estensione *.sig*.

10. <https://keyserver.ubuntu.com/pks/lookup?op=get&search=0x206d3b352f566f3b0e6572e997d9123de37a484f>

11. L'impronta digitale della chiave PGP importata può essere verificata con il software *Kleopatra* [pagina 345].

23.4 Acquisizione di un'istantanea di una macchina virtuale

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

 Durata: Cinque minuti.

Per seguire il metodo di lavoro su un documento sensibile in Windows, potrebbe essere necessario salvare lo stato di una macchina virtuale che si considera "pulita". Per farlo, utilizzeremo la gestione delle istantanee delle macchine virtuali.

Per avviare Virtual Machine Manager, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `virt` e fare clic su *Virtual Machine Manager* e inserire la password. Selezionare la macchina virtuale desiderata e fare clic su *Apri*. Se è in esecuzione, spegnerla facendo clic su *Macchina virtuale* → *Disattiva*

* *Spegnere*.

Fare clic su *Afficher* → *Istantanee*. Nell'elenco a sinistra, fare clic sul pulsante  in basso. Nella finestra che appare, inserire il nome dell'istantanea, evitando l'uso di spazi e caratteri speciali, ad esempio "Windows_own". Aggiungere una descrizione se necessario, quindi fare clic su *Fine*.

23.5 Ripristino dello stato di una macchina virtuale da una snapshot

 Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

 Durata: a seconda delle dimensioni del disco.

Lo scopo di questa ricetta è ripristinare lo stato di una macchina virtuale da un'istantanea creata in precedenza. Ciò consentirà di utilizzarla per un nuovo progetto, come consigliato quando si lavora su un documento sensibile di Windows.

23.5.1 Istantanee di Afficher

A tale scopo, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `virt` e fare clic su *Virtual Machine Manager*, quindi inserire la password. Selezionare la macchina virtuale desiderata e fare clic su *Apri*. Nella nuova finestra, fare clic sul menu *Afficher* e selezionare *Snapshots*.

23.5.2 Selezione e ripristino di un'istantanea

Selezionare l'istantanea desiderata da cui ripristinare lo stato della macchina (ad esempio, "Windows_clean"). Fare clic sul pulsante , in basso a sinistra. Viene visualizzata una nuova finestra che chiede se si desidera eseguire l'istantanea selezionata. L'esecuzione di questa istantanea comporterà la perdita di tutte le modifiche apportate alla macchina virtuale dalla sua creazione. Se si è sicuri della propria scelta, fare clic su *Sì*; in caso contrario, fare clic su *No*.

Virtual Machine Manager ripristinerà lo stato della macchina virtuale così come era al momento dell'acquisizione dell'istantanea.

23.6 Installazione di nuovo software su un sistema virtualizzato

🔄 Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

🕒 **Durata:** Circa 20 minuti.

Per installare un software su un sistema Windows virtualizzato, è possibile utilizzare un'immagine ISO del disco del software, come spiegato qui. È anche possibile utilizzare un CD o un DVD.

È consigliabile partire da un "Windows pulito", e quindi ripristinare lo stato di una macchina virtuale considerata "pulita" da un'istantanea. Al termine dell'installazione, verrà creata una nuova istantanea contenente il software appena installato.

pagina
171
pagina
preceden
te.

23.6.1 Scaricare e controllare il software

Se non lo avete già, iniziate a trovare il software, ad esempio su Internet. Se possibile, controllate il file scaricato. Il programma scaricato è un programma di installazione, un programma che installa il software.

pagina
345

23.6.2 Creare un'immagine ISO dei programmi di installazione

Per trasferire un programma di installazione dal computer host al guest Windows, è necessario che sia in formato ISO. Se il programma di installazione è già in formato ISO, passare al paragrafo successivo. In caso contrario, si creerà un'immagine ISO del disco contenente il programma di installazione utilizzando il software Brasero.¹²

Per lanciare Brasero, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `bra` e fare clic su *Brasero*.

questa
pagina

Selezionare *Progetto dati* nella colonna di sinistra. Fare clic sull'icona  e aggiungere il file di installazione scaricato in precedenza.

Nell'elenco a discesa in fondo alla finestra, selezionare *File immagine*, quindi fare clic su *Brucia...* Scegliere un nome per il file e fare clic su *Crea immagine*. Una volta creata l'immagine, chiudere Brasero.

23.6.3 Importare l'immagine ISO nel sistema virtuale

Tornare a Virtual Machine Manager per condividere l'immagine del disco ISO.

A tale scopo, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `virt` e fare clic su *Virtual Machine Manager*. Infine, inserire la password richiesta.

Selezionare la macchina virtuale Windows su cui si desidera installare il software e fare clic su *Apri*. Nella nuova finestra, visualizzare la vista dettagliata della macchina virtuale facendo clic sul menu *Afficher* → *Dettagli*. Nell'elenco hardware a sinistra, selezionare *IDE CD-ROM 1* o *SATA CDR0M 1* a seconda delle caratteristiche del computer. Scegliere quindi la *posizione dell'immagine ISO* o la *directory di origine* e fare clic su *Naviga*. Nella finestra che appare, scegliere *Sfoggia locale* e selezionare l'immagine ISO, quindi fare clic su *Apri*. Fare quindi clic su *Applica* in basso a destra.

12. Potrebbe essere necessario installare *Brasero* [pagina 134].

23.6.4 Installare il software sulla macchina virtuale

Fare *Afficher* → *Console* per tornare a Windows. Se la finestra affiche *Guest è ferma*, avviare la macchina virtuale con *Virtual Machine* → *Start*. Windows dovrebbe rilevare l'immagine ISO come se fosse un CD/DVD. Se non lo fa, possiamo andare a cercarla in *Esplora file* (andare su *Questo PC* → *Unità CD (D:)*). Se non funziona la prima volta, ripetere l'operazione.

Per eseguire l'installazione vera e propria, fare doppio clic sul CD-ROM virtuale e fare doppio clic sul file per avviare l'installazione, il cui *tipo* è un'*applicazione*. A seconda del tipo di software installato, Windows potrebbe chiedere se autorizzare un programma sconosciuto (cioè non verificato da Microsoft). Se ci si fida del download di base, accettarlo. Accettare tutte le altre richieste del programma di installazione facendo clic su *Avanti*.

Una volta completata l'installazione, l'immagine ISO non è più necessaria. Tornare alla vista dei dettagli della macchina virtuale con *Afficher* → *Dettagli*, selezionare *IDE CD-ROM 1* o *SATA CDROM 1* ed eliminare il contenuto del campo *Posizione immagine ISO* o *Directory di origine*, quindi *Applicare*.

È quindi possibile eseguire un'istantanea di una macchina virtuale per mantenere una versione "pulita" del sistema virtuale con questo nuovo software.

pagina
168

23.7 Condivisione di una chiavetta USB con un sistema virtualizzato

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.*

 *Durata: Circa dieci minuti.*



Nota: non è sempre auspicabile che il sistema virtuale abbia accesso diretto alla chiavetta USB o al disco rigido esterno. Collegando una chiavetta USB al sistema Windows, i dati vengono scritti automaticamente su di essa. Per accedere ai dati chiave senza che il sistema virtuale abbia un accesso diretto, consultare il capitolo Condivisione di una cartella con un sistema virtualizzato.

successivo
pagina.

Per identificare la chiave e scoprire con quale nome viene riconosciuta, utilizzare Utility Disco. Iniziate aprendo la panoramica delle attività premendo  ( su Mac), quindi digitate *disco* e fate clic su *Dischi*. Nella finestra *Dischi*, sul lato sinistro sono elencati i dischi conosciuti dal sistema. Collegare la chiave USB al computer e questa apparirà nell'elenco. Selezionatela e annotate il nome del modello, che appare nella finestra di destra del software e di solito contiene il termine *USB* o *Flash*.

23.7.1 Collegare la chiave al sistema virtuale

Avviare Virtual Machine Manager aprendo la panoramica delle attività e premendo  ( su Mac), quindi digitare *virt* e fare clic su *Virtual Machine Manager*. Infine, inserire la password richiesta.

Selezionare la macchina virtuale a cui verrà collegata la chiave USB e fare clic su *Apri*. Nella nuova finestra, fare clic sul menu *Macchina virtuale* → *Avvio*. Per visualizzare il sistema Windows, fare clic sul menu *Afficher* → *Console*

Al termine dell'avvio del sistema, fare clic sul menu *Macchina virtuale* → *Reindirizza a dispositivo USB*. Nella finestra che si apre, selezionare la chiave USB riconosciuta dal nome del modello indicato in precedenza. Il sistema virtuale la riconosce immediatamente e si può chiudere la finestra.

23.7.2 Espellere la chiave e scollegarla dal sistema virtuale.

Iniziare con l'espulsione della chiave dal sistema Windows. È quindi importante rimuovere il reindirizzamento alla chiave USB, in modo che il percorso che collega la chiave USB a Windows sia attivo solo quando necessario. A tal fine, fare clic su *Macchina virtuale* → *Reindirizzamento al dispositivo USB*. Nella finestra che si apre, deselezionare la casella corrispondente alla chiave USB. È quindi possibile chiudere la finestra.

La chiave non è più accessibile da Windows, ma è ancora visibile dal sistema host. Se non è più necessaria, può essere rimossa e scollegata dal computer.

23.8 Condivisione di un CD o DVD con un sistema virtualizzato

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

 *Durata: Circa dieci minuti.*

23.8.1 Abilita la condivisione di CD/DVD

A tale scopo, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare *virt* e fare clic su *Virtual Machine Manager*. Infine, inserire la password richiesta.

Selezionare la macchina virtuale Windows con cui si desidera condividere un CD o un DVD e fare clic su *Apri*. Nella nuova finestra, visualizzare la vista dettagliata della macchina virtuale facendo clic sul menu *Afficher* → *Dettagli*. Nell'elenco hardware a sinistra, selezionare *IDE CD-ROM 1* o *SATA CDROM 1* a seconda delle caratteristiche del computer.

Inserire il CD o il DVD nell'unità e attendere qualche istante. Selezionare *CD-ROM* o *DVD* sulla destra, quindi fare clic su *Applica*. Il CD o DVD potrebbe avere un nome. Per trovarlo, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare *fic* e fare clic su *File*. Nella colonna di sinistra, cercate il nome del DVD.

Visualizzare la schermata della macchina virtuale con *Afficher* → *Console* e avviarla con *Virtual Machine* → *Start*. Windows dovrebbe rilevare il CD inserito. In caso contrario, provare a cercarlo in *Esplora file*. Se non funziona la prima volta, ripetere l'operazione.

23.8.2 Espulsione del CD/DVD

Una volta terminato l'utilizzo del CD in Windows, espellerlo da Windows, quindi tornare alla vista dei dettagli della macchina virtuale con *Afficher* → *Dettagli*, selezionare *IDE CD-ROM 1* o *SATA CDROM 1* e fare clic su *D*.

23.9 Condivisione di una cartella con un sistema virtualizzato

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

 *Durata: Circa 15 minuti.*

Poiché al *guest* di Windows non è consentito uscire dalla scatola per recuperare i file, potrebbe essere necessario inviare i file da "fuori". Vediamo come procedere.

 **Attenzione:** quando si impara a usare questo sistema di condivisione, si può essere tentati di configurarlo per dare accesso a tutti i dischi collegati al sistema host: questa è la **peggiore idea immaginabile** e distruggerebbe da sola l'intera politica di sicurezza.

23.9.1 Creare una cartella dedicata sul sistema host

Aprirete la panoramica delle attività premendo  ( su Mac), quindi digitate `fic` e fate clic su *File*. Scegliere quindi la posizione in cui si desidera collocare la cartella di scambio. Ad esempio: nella *Cartella personale*, fate clic sul pulsante , poi sull'icona  con un piccolo  in basso a destra (*Nuova cartella*) e datele un nome evocativo. ("*Cartella leggibile da Windows*" o "*Cartella in cui Windows può scrivere*", ad esempio). Questa è la cartella in cui verranno inseriti i file da trasferire a Windows.

23.9.2 Installare l'Afficheur remoto

Attualmente, Virtual Machine Manager non consente di attivare la condivisione delle cartelle. È necessario utilizzare il software *remoto Afficheur*. Il passo successivo consiste quindi nell'installare il software *Afficheur remoto*.

pagina

134

23.9.3 Abilitare la condivisione delle cartelle

Per attivare la condivisione delle cartelle, avviare prima la macchina virtuale Windows da Virtual Machine Manager.

Per accedere a Virtual Machine Manager, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `virt` e fare clic su *Virtual Machine Manager*. Inserire la password richiesta.

Nella finestra Virtual Machine Manager, fare clic con il tasto destro del mouse sulla macchina virtuale desiderata (ad esempio, *Windows_own*) e fare clic su *Start*.

La macchina virtuale si avvia, ma lo schermo non è visibile. Utilizzeremo l'Afficheur remoto per accedervi.

Aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `affi` e fare clic su *Afficheur distant*. La prima volta, inserire l'indirizzo della macchina virtuale nel campo *Indirizzo di connessione*. In genere, l'indirizzo è: `spice://localhost:5900`. Se è in esecuzione più di una macchina virtuale, la prima avviata avrà l'indirizzo `spice://localhost:5900`, la seconda `spice://localhost:5901` e così via. Dalla seconda volta, è possibile fare clic sull'indirizzo desiderato in *Connessioni recenti*. Fare clic sul pulsante *Connetti*.

Viene visualizzata la finestra *Consenti la neutralizzazione delle scorciatoie*. Essa chiede se si desidera neutralizzare le scorciatoie. Per avere lo stesso funzionamento tra l'Afficheur remoto e il *Virtual Machine Manager*, scegliere *Consenti*.



Attenzione: prima di selezionare la casella *Condividi cartella*, assicuratevi che Windows voglia leggere tutto il contenuto della cartella che avete chiesto di condividere.

Dalla finestra dell'Afficheur remoto contenente la macchina virtuale Windows, fare clic sul menu *File* → *Preferenze*. Nella finestra che appare, selezionare la cartella che si desidera condividere. A tale scopo, selezionare *Altro* dal menu a discesa sulla destra. Nella finestra di navigazione che si apre, selezionare la *cartella leggibile da Windows* creata, quindi fare clic su *Apri*. Selezionare le caselle *Condividi cartella* e *Sola lettura*.



Selezionate sempre la casella di *sola lettura*, a meno che non vogliate produrre file da Windows virtualizzato, nel qual caso dovrete assegnare alla cartella condivisa un nome esplicito come *Cartella in cui Windows può scrivere*.



Attenzione: al momento in cui scriviamo, un bug nell'Afficheur remoto fa sì che l'opzione di *sola lettura* non venga presa in considerazione. Di conseguenza, anche se questa casella è selezionata, il Windows virtualizzato sarà in grado di scrivere nella cartella condivisa. Se si desidera condividere i file con Windows, è preferibile inserirvi delle copie piuttosto che degli originali, per non correre il rischio che Windows li modifichi.

23.9.4 Copiare i file

Nella macchina virtuale Windows, aprire Esplora file. Dopo poco tempo, *Spice Client (Z:)* dovrebbe essere accessibile sotto *Questo PC*.

Spice Client (Z:) corrisponde alla cartella che abbiamo scelto di condividere sul nostro sistema host, ed è possibile leggere tutti i file e le cartelle che contiene e copiare ciò che ci interessa in un'altra cartella di Windows.

23.9.5 Smettere di condividere

Per un motivo o per l'altro, si potrebbe voler interrompere la condivisione della cartella con Windows.

Dopo aver avviato il sistema virtualizzato, aprire la panoramica delle attività premendo  (⌘ su Mac), quindi digitare `affi` e fare clic su Afficheur distant. In *Connessioni recenti*, fare clic sull'indirizzo desiderato, `spice://localhost:5900` per accedere alla prima macchina virtuale avviata. Fare clic sul pulsante *Connetti*.

Dalla finestra dell'Afficheur remoto contenente la macchina virtuale Windows, fare clic sul menu *File* → *Preferenze*. Nella finestra visualizzata, deselezionare la casella *Condividi cartella*.

La cartella selezionata non è più accessibile da Windows.

Mantenere il sistema aggiornato

Come abbiamo spiegato in precedenza, il malware si fa strada nei nostri computer, tra le altre cose, attraverso "falle di sicurezza".

Le correzioni di questi errori di programmazione (o di progettazione) vengono rese disponibili regolarmente, non appena vengono identificate. Una volta che queste correzioni sono disponibili, è particolarmente importante sostituire le vecchie versioni del software. Questo perché i problemi corretti, che in precedenza potevano essere identificati solo da pochi specialisti, ora sono pubblicamente conosciuti e referenziati... e quindi più facili da sfruttare.

24.1 Mantenere le code aggiornate

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Da trenta minuti a un'ora, più circa trenta minuti di download.*

Poiché un sistema *live* è una raccolta indivisibile di software, eseguita da un DVD o da una chiavetta USB, l'unica soluzione pratica per utilizzare le ultime versioni di questo software è assicurarsi di utilizzare l'ultima versione del sistema *live*.

pagina
113

Dopo aver collegato il sistema Tails *live* a Internet, viene visualizzata una finestra *Upgrade is proposed* o *New version is proposed* per notificare la disponibilità di una nuova versione che corregge le vulnerabilità di sicurezza.

Se si utilizza un DVD, distruggere quello contenente la vecchia versione e masterizzarne uno nuovo. A meno che non sia riscrivibile, nel qual caso dovrete cancellarlo e masterizzare l'ultima versione di Tails.

Se si dispone di una chiave USB e di una connessione a Internet, è possibile eseguire l'aggiornamento direttamente. Fate clic su *Aggiorna ora* e seguite la procedura guidata. Se si verifica un errore o se è necessario utilizzare un altro metodo di aggiornamento, la procedura guidata vi indirizzerà alla pagina di documentazione appropriata.

Questo si trova nella *documentazione di Tails* sul desktop. Nell'indice che si apre, cercate la sezione *Download, installazione e aggiornamento* e fate clic sulla pagina *Aggiornamento automatico*.

24.2 Mantenere aggiornato un sistema crittografato

pagina
119

Una volta installato, un sistema crittografato deve essere mantenuto aggiornato in modo da continuare ad essere affidabile. Le sezioni seguenti si concentrano sul sistema Debian, ma i concetti sono ampiamente applicabili a quasi tutti gli altri sistemi.

Ogni due anni circa, il progetto Debian rilascia una versione *stabile*. Questo rappresenta un enorme sforzo per coordinare la compatibilità delle diverse versioni del software, effettuare test approfonditi e garantire che non rimangano difetti importanti.

24.3 Aggiornamenti quotidiani per un sistema crittografato

☞ *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: Un minuto per avviare l'aggiornamento, più un tempo variabile per il download e l'installazione, durante il quale è possibile continuare a utilizzare il computer.*

Il senso di una release *stabile* di Debian è che, in seguito, il software che la compone non viene più modificato in profondità: gli aggiornamenti includono miglioramenti delle traduzioni, correzioni di problemi legati alla sicurezza o di problemi che impediscono il normale utilizzo di un programma, e così via.

In generale, queste nuove versioni vengono installate automaticamente dal sistema, purché abbia accesso a Internet, e non dovrebbero disturbare le piccole abitudini già acquisite.

24.3.1 Eseguire gli aggiornamenti

Una volta installato l'*ambiente desktop grafico*, il sistema controlla automaticamente la presenza di nuove versioni nei repository configurati quando è connesso a Internet.

pagina
136

In tal caso, viene visualizzata una notifica che indica la *disponibilità di aggiornamenti software*.

Fare clic su *Afficher* nella notifica, per aprire *Software*.

Viene visualizzato un elenco di aggiornamenti. Se *Logiciels* non li ha già scaricati tutti, viene visualizzato un messaggio

Viene visualizzato il pulsante *Download*, sul quale si fa clic per richiedere l'operazione.

Una volta scaricati gli aggiornamenti, appare il pulsante *Riavvia e aggiorna*. Fare clic su questo pulsante, quindi confermare facendo clic su *Riavvia e installa* di nuovo. Il computer si riavvia e chiede la passphrase per la crittografia del disco rigido, prima di installare gli aggiornamenti. Il computer si riavvia su un sistema aggiornato e richiede la passphrase.

24.3.2 Rimuovere i pacchetti obsoleti

Una volta riavviato il computer, dobbiamo ancora chiedere al sistema di rimuovere i componenti software non più necessari: poiché questa operazione non viene eseguita automaticamente dal sistema, è necessario eseguirla regolarmente, altrimenti il nostro disco - e in particolare la partizione */boot* - si riempirà gradualmente, fino al punto in cui non sarà più possibile eseguire nuovi aggiornamenti.

Non è ancora possibile eseguire questa operazione tramite l'interfaccia grafica, quindi è necessario aprire un Terminale.

Iniziate diventando un amministratore digitando il comando :

pagina
97

```
sudo su
```

Il computer dovrebbe chiedere la password di sessione. Se riceviamo

```
bash: sudo: comando non trovato, quindi digitare :
```

```
➤ su -
```

Il nostro terminale ha ora il potere amministrativo sul nostro sistema.

Il comando seguente, da digitare in questo terminale, rimuove i pacchetti obsoleti:

```
# apt autoremove
```

24.4 Aggiornamento a una nuova versione stabile

🕒 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.*

🕒 *Durata: Da mezza giornata a una giornata intera, compreso un lungo periodo di download durante il quale si può continuare a usare il computer e un lungo periodo di installazione durante il quale è meglio smettere di usarlo.*

Quando viene rilasciata una nuova versione *stabile* di Debian, il progetto mantiene aggiornata la *versione stabile* precedente, chiamata *oldstable*, **per almeno un anno**.¹ minimo. Questo periodo viene esteso da un team di *supporto a lungo termine*.² Ad esempio, la versione di Debian utilizzata nell'edizione 2017 di questa guida, Debian 9 Stretch, è stata supportata dal team di sicurezza Debian solo fino a luglio 2020 e il team di *supporto a lungo termine* si è occupato della manutenzione fino a giugno 2022.

È quindi necessario approfittare di questo periodo per aggiornare il sistema alla nuova versione stabile. Si tratta di un processo più delicato rispetto agli aggiornamenti quotidiani. Non necessariamente nell'implementazione vera e propria, ma nel fatto che è poi necessario adattarsi ai cambiamenti del software che usiamo abitualmente.

In ogni caso, prima di continuare, si consiglia vivamente di eseguire un backup dei dati.

pagina

151

Abbiamo due opzioni:

- Aggiornare il sistema alla nuova versione stabile. Il vantaggio di questa opzione è che consente di mantenere il software installato e le configurazioni effettuate nel tempo... il che può anche essere uno svantaggio se si è arremaggiato troppo. Se si sceglie questa opzione, continuare a usare questo strumento.
- Installare la nuova versione di Debian. Il vantaggio è che si fa tabula rasa. Lo svantaggio è che si perdono le configurazioni specifiche e si deve scaricare e controllare di nuovo il programma di installazione. Se si sceglie questa opzione, una volta effettuato il backup, si troverà il resto del processo nello strumento per fare una nuova installazione di Debian.

pagina

119

Il precedente aggiornamento della *Guida all'autodifesa digitale* utilizzava la versione 9 di Debian, chiamata Stretch, rilasciata nel giugno 2017. Al momento dell'aggiornamento di questa guida, Debian è alla versione 11, chiamata Bullseye, rilasciata nell'agosto 2021. È rischioso passare direttamente dalla versione 9 alla 11 senza passare per la versione 10, chiamata Buster, rilasciata a luglio 2019.

Per sapere quale versione di Debian si sta utilizzando, aprire la panoramica delle attività premendo  (⌘) su Mac), quindi digitare `param` e cliccare su

1. Debian, 2017, *DebianOldStable* [<https://wiki.debian.org/fr/DebianOldStable>].

2. Debian, 2021, *Debian Long Term Support* [<https://wiki.debian.org/fr/LTS>].

Impostazioni. Nella colonna di sinistra, scorrere fino in fondo e fare clic su *Informazioni*. La versione di Debian in uso appare sotto il *nome del sistema operativo*.

Se siete ancora alla versione 9 Stretch, vi proporremo un aggiornamento in due fasi, dalla versione 9 Stretch alla versione 10 Buster, quindi dalla versione 10 Buster alla versione 11 Bullseye. È possibile seguire solo la seconda fase se si è già alla versione 10 Buster.

24.4.1 Da Stretch a Buster

La procedura qui descritta riguarda l'aggiornamento dalla versione di Debian chiamata Stretch o 9, rilasciata a giugno 2017, a Buster o 10, rilasciata a luglio 2019.

Qui documenteremo una procedura di aggiornamento semplificata che è stata testata su installazioni Debian Stretch con un ambiente desktop grafico GNOME e software proveniente esclusivamente dai repository ufficiali di Debian.

Richiede una connessione a Internet per tutta la durata dell'aggiornamento.



Attenzione: questa procedura semplificata ha meno probabilità di funzionare se il sistema è stato modificato aggiungendo fonti di aggiornamento non ufficiali.

In questo caso, si faccia riferimento alle note di rilascio ufficiali di Debian off³ in particolare le sezioni Aggiornamenti da Debian 9 (Stretch)⁴ e Problemi da tenere presenti per Buster⁵.

Aggiornamento di Debian Stretch

Prima di tutto, è necessario avere una Debian Stretch aggiornata. Senza di essa, l'aggiornamento potrebbe non funzionare. Se non si è aggiornato quotidianamente, è il momento di mettersi in pari. Se viene richiesto di riavviare dopo numerosi aggiornamenti, farlo prima di procedere con i passi successivi.

pagina

176

Assicuratevi di avere abbastanza spazio libero sul disco rigido.

Per evitare spiacevoli sorprese, è necessario disporre di almeno 4 GB di spazio libero sul disco rigido contenente il sistema.

Aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `fic` e fare clic su *Fichiers*. Nella barra di sinistra, fare clic su *Altre posizioni*. A destra della riga *Computer*, viene indicato lo spazio disponibile, ad esempio *11,7 GB/17,1 GB disponibili* significa 11,7 GB disponibili.

Se non c'è abbastanza spazio sul disco rigido, una soluzione è eliminare i vecchi aggiornamenti diventati obsoleti. A tale scopo, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `package` e fate clic su *Package Manager*. Poiché il Package Manager consente di modificare il software installato sul computer, per aprirlo è necessaria una password.

Nel menu *Configurazione*, scegliete *Preferenze*, quindi selezionate la scheda *File* e fate clic sul pulsante *Elimina pacchetti nella cache*, quindi *OK* e chiudete *Synaptic Package Manager*.

Verificare nuovamente lo spazio disponibile su disco, come spiegato sopra. Se non è sufficiente, dovremo eliminare alcuni dei nostri file o rimuovere i loghi.

3. <https://www.debian.org/releases/buster/amd64/release-notes/index.fr.html>

4. <https://www.debian.org/releases/buster/amd64/release-notes/ch-upgrading.fr.html>

5. <https://www.debian.org/releases/buster/amd64/release-notes/ch-information.fr.html>

Disabilitare i repository non ufficiali

L'aggiornamento viene testato solo con i pacchetti forniti ufficialmente da Debian Stretch. Verranno quindi disabilitati tutti gli altri repository Debian, compresi i *backport*.

Per farlo, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `update` e fare clic su *Software e aggiornamenti*.

Nella scheda *Altro software*, deselezionare le caselle di controllo. Quando si effettua una modifica, inserire la password di amministrazione.

Fare clic su *Chiudi*. Se sono state apportate modifiche, viene visualizzata la finestra *Informazioni sul software disponibile non sono aggiornate*. Fare clic su *Aggiorna*.

Disattivare lo screensaver

Durante l'aggiornamento, il salvaschermo potrebbe bloccarsi, lasciando lo schermo mangiato dai vermi. È quindi consigliabile disattivarlo per tutta la durata dell'aggiornamento.

A tal fine, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare `param` e fare clic su *Impostazioni*. Nella colonna di sinistra, fare clic su *Privacy*.

Fare clic su *Blocco schermo*. Nella finestra visualizzata, disattivare *Blocco schermo automatico*. Chiudere questa finestra facendo clic su , quindi di nuovo su  nell'angolo in alto a destra, per chiudere la finestra *Impostazioni*.

Aprire un terminale

Poiché non è ancora possibile eseguire questa operazione tramite l'interfaccia grafica, è necessario aprire un Terminale.

97

pagina

Iniziate diventando un amministratore digitando il comando :

```
> sudo su
```

Il computer dovrebbe chiedere la password di sessione. Se riceviamo

`bash: sudo: comando non trovato`, quindi digitare :

```
> su -
```

Il nostro terminale ha ora il potere amministrativo sul nostro sistema.

Aggiornamento depositi

Iniziamo modificando i repository configurati per utilizzare quelli dedicati alla nuova versione. Apriamo nel terminale il file contenente l'elenco dei repository utilizzati da Debian.

```
# gedit / etc/ apt/ sorgenti. elenco
```

Si apre l'editor di testo. Scegliere  → *Trova e sostituisci*. Nella finestra che si apre, cercare "`stretch`" per sostituirlo con "`buster`". Fare quindi clic sul pulsante *Sostituisci tutto* e chiudere la finestra di ricerca con .

Se un'installazione o un aggiornamento sono stati eseguiti in precedenza utilizzando un CD o un DVD, è bene cercare le righe che iniziano con "`deb cdrom:`" e rimuoverle.

Si può quindi fare clic su *Salva* e chiudere l'editor.

Abbiamo modificato l'elenco dei repository, quindi ora dobbiamo scaricare l'elenco dei pacchetti disponibili in essi, prima di poterli installare; per farlo, sempre nel *Terminale*, che terremo aperto, digitiamo il comando :

```
#- aggiornamento apt
```

Se si verifica un errore relativo alla "cache di sistema di AppStream", è possibile ignorarlo senza preoccuparsi.

Avviare l'aggiornamento stesso

L'aggiornamento viene eseguito in diverse fasi, ognuna delle quali è controllata dal nostro terminale.

Il nostro primo comando dice al gestore di pacchetti, da un lato, che vorremmo che facesse meno domande possibili sui dettagli dell'aggiornamento; dall'altro, che non vogliamo vedere la cronologia delle modifiche:

```
#- esportare DEBIAN_PRIORITY=critical APT_LISTCHANGES_FRONTEND=none
```

Il nostro secondo comando esegue la prima parte dell'aggiornamento del

```
#- aggiornamento apt
```

sistema: presto il terminale affiche Vuoi continuare [S/n]? Dopo confermare premendo *Invio* () o) , a prima serie di finestre blu che ci chiedono come gestire alcune modifiche. Quando non si cerca di uscire dalle scelte di Debian, è sufficiente premere *Invio* ogni volta.

Può anche apparire una finestra che indica che un file di configurazione è stato modificato e chiede se si desidera sostituirlo con la nuova versione. *Mantenere o sostituire* è una scelta che dipende dall'entità delle modifiche apportate e dalle nuove funzionalità offerte. Non esiste quindi una risposta generica. Dovrete confrontare le versioni o tirare una monetina.

Dopo un po', alcuni pacchetti sono già stati aggiornati e il terminale dovrebbe tornare al prompt dei comandi.

Il comando seguente completerà l'aggiornamento del sistema:

```
#- apt full - upgrade
```

Poco dopo, il terminale si affaccia di nuovo Vuoi continuare?

[S/n] ? Dopo aver confermato premendo *Invio* () o) , si può vedere o

appare una seconda serie di finestre blu che chiedono come gestire alcune modifiche. Quando non si cerca di uscire dalle scelte di Debian, è sufficiente premere *Invio* ogni volta.

In questa fase dell'aggiornamento, può accadere che il desktop GNOME presenti dei messaggi di errore. Questo non è particolarmente preoccupante, poiché molti componenti del sistema vengono reinstallati. Questi problemi dovrebbero risolversi da soli una volta completato il processo.

Poche evoluzioni del sistema dopo, il terminale ci chiede ancora una volta dei comandi.

È quindi possibile immettere un comando finale per liberare spazio su disco: Poi :

```
#- apt autoremove
```

```
#- pulizia dell'appartamento
```

Primo riavvio

Ora è il momento di riavviare il sistema, utilizzando il menu  nell'angolo in alto a sinistra e scegliendo *Reboot*.

24.4.2 Da Buster a Bullseye

La procedura qui descritta riguarda l'aggiornamento dalla versione Debian Buster o 10, rilasciata a luglio 2019, a Bullseye o 11, rilasciata ad agosto 2021.

Qui documenteremo una procedura di aggiornamento semplificata che è stata testata su installazioni Debian Buster con un ambiente desktop grafico GNOME e software proveniente esclusivamente dai repository ufficiali Debian.

Richiede una connessione a Internet per tutta la durata dell'aggiornamento.



Attenzione: questa procedura semplificata ha meno probabilità di funzionare se il sistema è stato modificato aggiungendo fonti di aggiornamento non ufficiali.

In questo caso, fare riferimento alle note di rilascio ufficiali di Debian off⁶ in particolare le sezioni Aggiornamenti da Debian 10 (Buster)⁷ e Problemi da tenere presenti per Bullseye⁸.

Aggiornamento di Debian Buster

Prima di tutto, è necessario avere un Debian Buster aggiornato. Senza di esso, l'aggiornamento potrebbe non funzionare. Se non si è aggiornato quotidianamente, è il momento di mettersi in pari. Se viene richiesto di riavviare dopo numerosi aggiornamenti, farlo prima di procedere.

pagina

176

Assicuratevi di avere abbastanza spazio libero sul disco rigido.

Per evitare spiacevoli sorprese, è necessario disporre di almeno 4 GB di spazio libero sul disco rigido contenente il sistema.

Aprire la panoramica delle attività premendo  ( su Mac), quindi digitare *fic* e fare clic su *Fichiers*. Nella barra di sinistra, fare clic su *Altre posizioni*. A destra della riga *Computer*, viene indicato lo spazio disponibile, ad esempio *11,7 GB/17,1 GB disponibili* significa 11,7 GB disponibili.

Se non c'è molto spazio sul **disco** rigido, una soluzione è eliminare i vecchi aggiornamenti diventati obsoleti. A tale scopo, aprite la panoramica delle attività premendo  ( su Mac), quindi digitate *package* e fate clic su *Package Manager*. Poiché il Package Manager consente di modificare il software installato sul computer, per aprirlo è necessaria una password.

Nel menu *Configurazione*, scegliete *Preferenze*, quindi selezionate la scheda *File* e fate clic sul pulsante *Elimina pacchetti nella cache*, quindi *OK* e chiudete *Synaptic Package Manager*.

Se non c'è abbastanza spazio sul disco rigido, dovremo eliminare alcuni dei nostri file o rimuovere un software.

6. <https://www.debian.org/releases/bullseye/amd64/release-notes/index.fr.html>

7. <https://www.debian.org/releases/bullseye/amd64/release-notes/ch-upgrading.fr.html>

8. <https://www.debian.org/releases/bullseye/amd64/release-notes/ch-information.fr.html>

Disattivare lo screensaver

Durante l'aggiornamento, il salvaschermo potrebbe bloccarsi, lasciando lo schermo mangiato dai vermi. È quindi consigliabile disattivarlo per tutta la durata dell'aggiornamento.

Per farlo, aprire la panoramica delle attività premendo  (su Mac), quindi digitare  param e cliccare su *Impostazioni*. Nella colonna di sinistra, fare clic su *Privacy*.

Fare clic su *Blocco schermo*. Nella finestra visualizzata, disattivare *Blocco schermo automatico*. Chiudere questa finestra facendo clic su **X**, quindi di nuovo su **X** nell'angolo in alto a destra, per chiudere la finestra *Impostazioni*.

Aprire un terminale

Non è ancora possibile eseguire questa operazione tramite l'interfaccia grafica, quindi è necessario aprire un Terminale.

pagina

97

Iniziate diventando un amministratore digitando il comando :

```
sudo su
```



Il computer dovrebbe chiedere la password di sessione. Se riceviamo

```
bash: sudo: comando non trovato, quindi digitare :
```

```
su -
```



Il nostro terminale ha ora il potere amministrativo sul nostro sistema.

Aggiornamento depositi

Iniziamo modificando i repository configurati per utilizzare quelli dedicati alla nuova versione.

Attenzione: qui sta la differenza con l'aggiornamento precedente. Nel terminale, digitate :



```
sed -i 's, buster/ aggiornamenti , bullseye - sicurezza ,g' / etc/ apt/  
sorgenti. elenco  
sed -i 's, buster , bullseye ,g' / etc/ apt/ fonti. elenco
```



Si può quindi fare clic su *Salva* e chiudere l'editor.

Abbiamo modificato l'elenco dei repository, quindi ora dobbiamo scaricare l'elenco dei pacchetti disponibili in essi, prima di poterli installare; per farlo, sempre nel *Terminale*, che terremo aperto, digitiamo il comando :

```
aggiornamento apt
```

**Avviare l'aggiornamento stesso**

L'aggiornamento viene eseguito in diverse fasi, ognuna delle quali è controllata dal nostro terminale.

Il nostro primo comando dice al gestore di pacchetti, da un lato, che vorremmo che facesse meno domande possibili sui dettagli dell'aggiornamento; dall'altro, che non vogliamo vedere la cronologia delle modifiche:

```
esportare DEBIAN_PRIORITY=critical APT_LISTCHANGES_FRONTEND=none
```

Il secondo comando esegue la prima parte dell'aggiornamento del sistema:



```
aggiornamento apt
```

Ben presto, il terminale affiche **Desidera continuare [S/n]?** Dopo confermare premendo *Invio* ( o ), a prima serie di finestre blu che ci chiedono come gestire alcune modifiche. Quando non si cerca di uscire dalle scelte di Debian, è sufficiente premere *Invio* ogni volta.

Può anche apparire una finestra che indica che un file di configurazione è stato modificato e chiede se si desidera sostituirlo con la nuova versione. *Mantenere* o *sostituire* è una scelta che dipende dall'entità delle modifiche apportate e dalle nuove funzionalità offerte. Non esiste quindi una risposta generica. Dovrete confrontare le versioni o tirare una monetina.

Dopo un po', alcuni pacchetti sono già stati aggiornati e il terminale dovrebbe tornare al prompt dei comandi.

Il comando seguente completerà l'aggiornamento del sistema:

```
# apt full - upgrade
```

Poco dopo, il terminale si affaccia di nuovo **Vuoi continuare?**

[S/n] ? Dopo aver confermato premendo *Invio* ( ), si può vedere o

appare una seconda serie di finestre blu che ci chiedono come gestire alcune modifiche. Quando non si cerca di uscire dalle scelte di Debian, è sufficiente premere *Invio* ogni volta.

In questa fase dell'aggiornamento, può accadere che il desktop GNOME presenti dei messaggi di errore. Questo non è particolarmente preoccupante, poiché molti componenti del sistema vengono reinstallati. Questi problemi dovrebbero risolversi da soli una volta completato il processo.

Poche evoluzioni del sistema dopo, il terminale ci chiede ancora una volta dei comandi.

È quindi possibile immettere un comando finale per liberare spazio su disco: Poi :

```
# apt autoremove
```

```
# Primo riavvio  
pulizia dell'appartamento
```

Ora è il momento di riavviare il sistema, utilizzando il menu in alto a sinistra e scegliendo *Reboot*.

Riattivare altri repository Debian

Ora possiamo tirare un sospiro di sollievo. La maggior parte del lavoro è stata fatta. Ma ci sono ancora alcuni piccoli aggiustamenti da fare...

Se si sono disattivati i repository non ufficiali prima dell'aggiornamento, è il momento di verificare se sono ancora necessari con la nuova versione di Debian. In caso affermativo, riattivarli. È anche possibile riattivare lo screen saver se è stato precedentemente disattivato.

pagina
136

Riattivare il blocco dello schermo

A tale scopo, aprire la panoramica delle attività premendo  ( su Mac), quindi digitare *param* e fare clic su *Impostazioni*. Nella colonna di sinistra, fare clic su *Privacy*.

Fare clic su *Blocco schermo*. Nella finestra visualizzata, attivare *Blocco schermo automatico*. Chiudere questa finestra facendo clic su .

Assicurarsi che il nuovo sistema funzioni correttamente

Può essere utile assicurarsi che le azioni e i comandi più comuni siano funzionali. Se necessario, può essere necessario diagnosticare e risolvere eventuali problemi. È sicuramente meglio farlo non appena si inizia a usare il nuovo sistema, in modo da poter partire per altri due anni con un sistema funzionale. I problemi più comuni sono spesso descritti, insieme a suggerimenti su come risolverli, in varie documentazioni Debian e GNU/Linux.

[-----]
[pagina]
[-----]
129

Va inoltre sottolineato che esistono note di rilascio ufficiali del progetto Debian.⁹

9. <https://www.debian.org/releases/bullseye/amd64/release-notes/index.fr.html>

Pulire i metadati da un file documento

 Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

 Durata: pochi minuti.

Lo scopo dello strumento che stiamo per esaminare è quello di eliminare i metadati presenti in un documento prima della sua pubblicazione. Questi metadati non sono uguali in tutti i formati di documento: alcuni sono più difficili da pulire di altri, impossibile. Tuttavia, la maggior parte dei formati utilizzati per scambiare documenti finiti, siano essi testi, immagini, suoni o video, sono "pulibile".

Lo strumento da utilizzare a questo scopo è *MAT2* (per *Metadata Anonymization Toolkit 2*), che consente di ripulire facilmente un'ampia gamma di formati di file.

 **Attenzione:** la pulizia dei metadati non rende anonimo il contenuto dei file e non rimuove alcun contrassegno¹ inclusi nel contenuto stesso.

25.1 Installare il software necessario

Su un sistema in cui non è ancora presente, è necessario installare il pacchetto (vedere pagina 135). *mat2*. In Tails, *MAT2* è già installato.

25.2 Pulire uno o più file

Nel file manager, fare clic con il pulsante destro del mouse sul documento di cui si desidera rimuovere i metadati, quindi selezionare *Rimuovi metadati*. Viene creato un nuovo documento senza metadati. Esso riporta il nome del file originale, seguito da *.cleaned* e dall'estensione del file.

Suggerimento! Per elaborare più file, è possibile selezionare una serie di file e fare clic con il pulsante destro del mouse su *Rimuovi metadati*. Questa operazione può richiedere un certo tempo, a seconda del numero di file e delle loro dimensioni.

Alcuni formati non sono supportati da questo strumento. In questo caso, viene visualizzato il messaggio di avviso *Failed to clean some items*. Un pulsante *Mostra* visualizza un elenco di file che non sono stati elaborati. Se il formato non è supportato, è possibile esportare il file non elaborabile in un formato più comune. Ad esempio, per ripulire un file in formato XCF dal programma di manipolazione di immagini GIMP, è possibile esportarlo in formato JPEG o PNG.

1. Cfr. Wikipedia, 2014, *Tatuaggio digitale* [https://fr.wikipedia.org/wiki/Tatouage_num%C3%A9rique] e Wikipedia, 2014, *Steganografia* [<https://fr.wikipedia.org/wiki/St%C3%A9ganografia>].

25.2.1 Caso speciale dei file PDF

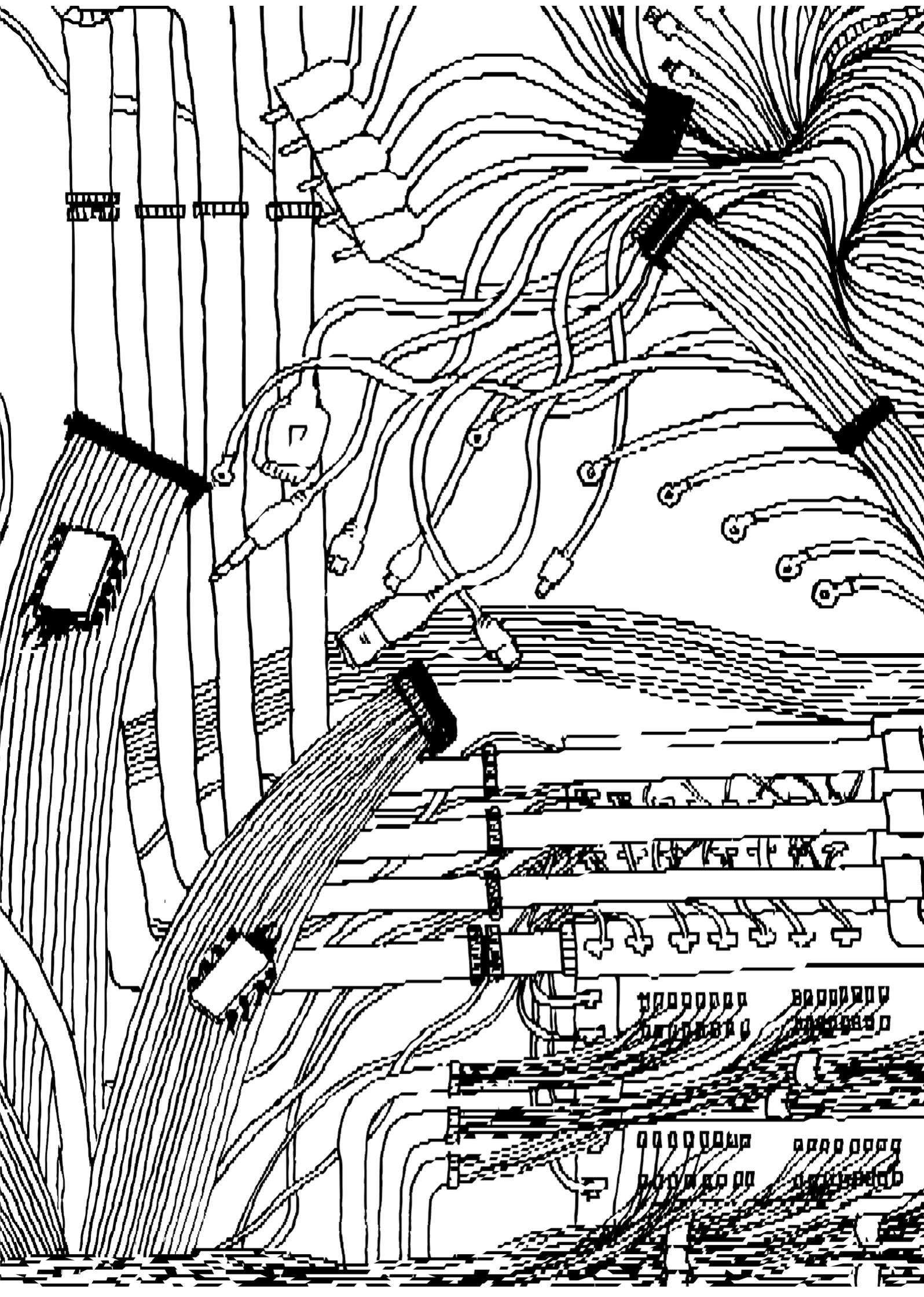
Per rimuovere correttamente i metadati da un file PDF, MAT2 lo "trasforma" in un'immagine. Ciò significa che un file PDF senza metadati perderà tutti i collegamenti ipertestuali e sarà più grande del file originale.

25.2.2 Caso speciale dei video

MAT2 rimuove i metadati da un file video, ma non è in grado di rimuovere altre tracce che a volte potrebbero aiutare a identificare la fonte del video: graffi o impronte digitali sull'obiettivo, ad esempio, o, come abbiamo visto sopra, segni invisibili e non rilevabili (noti come *filigrane digitali*) che potrebbero essere aggiunti direttamente alle immagini video dall'hardware o dal software di acquisizione utilizzato.

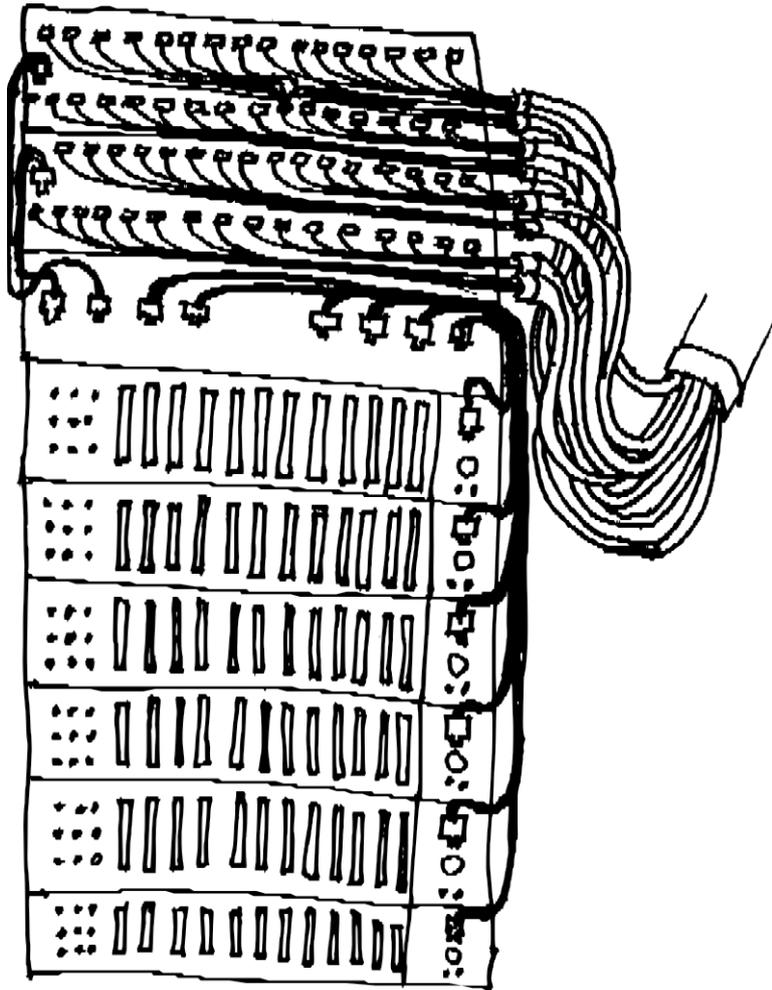
Quindi, per garantire che un video non contenga davvero informazioni rintracciabili, la cancellazione dei metadati di MAT2 non è sufficiente: occorre anche realizzare il video con materiale non legato ad alcuna identità (cioè che non sia mai stato usato per pubblicare immagini con un'altra identità contestuale), e usare solo Tails per montarlo.

Tuttavia, nella maggior parte dei casi e di fronte alla maggior parte degli avversari (e dei loro mezzi) che vorrebbero identificare l'autore di un video, l'eliminazione dei metadati del video con MAT2 è già una misura di protezione abbastanza buona.



VOLUME 2

In linea



QUARTA PARTE

Comprensione

Introduzione

Nel primo volume abbiamo spiegato che l'uso dei computer lascia tracce delle nostre attività e dei nostri dati. Addentrarsi nei misteri di queste macchine familiari si era già rivelato un po' complesso. Come sarà ora che proponiamo di collegarci a Internet? Cosa significa collegare il nostro computer ad altri computer sui quali abbiamo poco o nessun controllo? Un computer connesso è prima di tutto un computer, quindi è essenziale leggere il primo volume per poter affrontare questo *volume 2* sulla sicurezza *online*.

*

**

Partiamo dall'inizio. Internet è una rete. O meglio, un insieme di reti interconnesse che, partendo da un'oscura applicazione militare, si è espanso nel corso dei decenni fino a coprire il mondo intero. Una rete che ha visto una proliferazione di applicazioni, utenti, tecnologie e tecniche di controllo.

Molti hanno parlato all'infinito della "nuova era" che si stava aprendo, delle presunte possibilità di orizzontalità e trasparenza nella diffusione di informazioni e risorse, o nell'organizzazione collettiva, a cui questa nuova tecnologia poteva aprire - anche nel supporto che poteva offrire alle lotte politiche. Tuttavia, poiché sembra ovvio che ai poteri forti non piaccia ciò che può sfuggire loro, anche solo in parte, l'espansione degli usi è stata accompagnata da un'espansione delle tecniche di controllo, sorveglianza e repressione, le cui conseguenze stanno diventando sempre più evidenti.

Nel 2011, per la prima volta, i governi hanno organizzato la disconnessione di quasi tutta la loro popolazione dalla rete globale. I leader di Egitto e Iran, per esempio, hanno ritenuto che per meglio contenere le rivolte in atto sul loro territorio, avessero tutto l'interesse a limitare il più possibile le possibilità di comunicazione attraverso la rete - il che non ha impedito loro, nello stesso movimento, di cercare di organizzare la sorveglianza e il tracciamento su Internet. Il governo iraniano è stato così in grado di mettere in piedi un sistema di analisi del traffico che ha richiesto notevoli risorse per monitorare i ribelli, conosciuti o meno, mappare le loro relazioni per confonderli e condannare i ribelli che utilizzavano la rete per organizzarsi.

Un altro esempio: dall'introduzione di una versione cinese di Google¹ nel 2006, l'azienda ha accettato con vari gradi di docilità la politica del governo cinese di filtrare i risultati delle ricerche.

Metodi simili vengono utilizzati anche nei Paesi cosiddetti democratici. Per esempio, alla fine dell'estate 2011, dopo diversi giorni di disordini a Londra, due giovani uomini

1. Wikipedia, 2017, *Google China* [https://fr.wikipedia.org/wiki/Google_China].

sono stati condannati ² a 4 anni di carcere per aver indetto manifestazioni nei loro quartieri su Facebook, anche se le loro "chiamate" non hanno avuto seguito.

Allo stesso modo, le rivelazioni di Edward Snowden ³ sullo stato della sorveglianza elettronica effettuata dalla NSA ⁴ hanno dato credito ad alcune delle ipotesi più pessimistiche.

Per questo è fondamentale rendersi conto che l'uso di Internet, come quello del computer in generale, è tutt'altro che innocuo. Ci espone alla sorveglianza e alla repressione che ne può derivare: l'obiettivo principale di questo secondo volume è aiutare tutti a comprendere i rischi e i limiti associati all'uso di Internet. Ma si tratta anche di dare a noi stessi i mezzi per fare scelte consapevoli su come usare Internet. Scelte che possono complicare il compito dei gatekeeper, aggirare i sistemi di censura o addirittura permetterci di creare i nostri strumenti e le nostre infrastrutture. Un primo passo per riprendere il controllo di tecnologie che a volte sembrano destinate a sfuggirci, un'ambizione che va ben oltre lo scopo di questa guida.

*

* *

Ottobre 2010, Parigi

Ana arriva presto al lavoro questa mattina. Lavora a La Reboute, un'azienda di abbigliamento per corrispondenza che si trova all'ultimo piano di un edificio in Rue Jaurès: "Uff, 18 piani, non vedo l'ora di far riparare l'ascensore!". Si siede alla scrivania, si china e preme il pulsante di accensione del computer.

Sullo schermo appare una piccola finestra. "Connessione di rete stabilita". Prima di mettersi al lavoro, vuole controllare la posta elettronica. Ana fa clic sull'icona del browser web, aprendo una finestra che rimane vuota per qualche millisecondo, prima di far apparire la home page di Google. Mentre si gode mentalmente la pagina iniziale Sulla pagina "Speciale Halloween" di Google, Ana sposta il puntatore del mouse e fa clic sul link Accedi. Una volta caricata la pagina, inserisce il suo nome utente e il suo nome utente, quindi fa clic su Gmail. Alcuni Da qualche parte, in un'oscura stanza affollata di computer, un disco rigido gracchia. Pochi secondi dopo aver aperto il suo browser web, Ana inizia a sfogliare il suo i n b o x. Mentre consulta un'e-mail ricevuta dal leboncoin.fr, il suo sguardo è attratto dal link appena inserito nella colonna di destra: "Beh, qualcuno sta vendendo lo stesso modello di apparecchio foto di quella che sto cercando, proprio dietro l'angolo... forse dovrei farci un salto".

— "Ah beh, sei qui?"

La voce alle spalle di Ana la fa trasalire leggermente. È Bea, una collega.

— "Mi sono alzato un po' prima del solito, così ho preso la RER delle 7:27 invece che quella delle 7:43. Controllo rapidamente le mie e-mail

2. France Soir, 2011, *Émeutes à Londres : Deux jeunes condamnati a quattro anni di prigione* [<http://archive.francesoir.fr/actualite/international/emeutes-londres-deux-jeunes-condamnes-quatre-ans-prison-128302.html>].

3. Wikipedia, 2014, *Edward Snowden* [https://fr.wikipedia.org/wiki/Edward_Snowden].

4. *National Security Agency*, parte del Dipartimento della Difesa degli Stati Uniti, responsabile di la raccolta e l'analisi di dati stranieri e la protezione dei dati statunitensi.

prima di iniziare. Sto aspettando la conferma della prenotazione di un biglietto per le Baleari quest'inverno.

— *Vacanze al sole, conosco il tipo. E ci metterai molto?"*

Bea sembra avere fretta.

— *"Uh. no no, avevo quasi finito. Perché?"*

— *Beh, se non ti dispiace, vorrei prendere in prestito il tuo computer per un paio di minuti... Il mio è fermo da ieri, quindi sto aspettando che arrivi il nuovo responsabile informatico per risolverlo.*

Appena si siede, Bea clicca nervosamente sulla barra degli indirizzi del browser e inserisce direttamente l'indirizzo del blog su cui vengono regolarmente pubblicate informazioni sui personaggi politici del suo distretto. Non le piace usare Google per le sue ricerche, quindi lo ha memorizzato. Non si sa mai, potrebbe evitare di fare la spia. Apre una seconda scheda, inserisce anche l'indirizzo di no-log, la sua casella di posta elettronica, e si collega. Nickel, eccolo! Il documento relativo ai conti bancari svizzeri del sindaco del suo arrondissement, Mme Alavoine! Bea scarica immediatamente il documento e lo apre nell'editor di testo. Lo sfoglia rapidamente, cancellando alcuni dettagli che è meglio lasciare stare. Dopo aver inserito il suo nome utente e la sua password per accedere al blog, Bea copia e incolla il contenuto del documento dalla casella di posta elettronica e fare clic su Invia. "Speriamo che ispiri altre persone!"

Soddisfatta di poter finalmente inviare il suo documento, Bea si alza immediatamente e restituisce ad Ana il suo posto.

— *"Prendiamo un caffè?"*

Novembre 2010. Sede di La Reboute

Arrivata in ufficio, Sarah Ahmed, CEO di La Reboute, inizia a scorrere la posta ricevuta bevendo il suo caffè. Una convocazione alla stazione di polizia. Per una volta, c'è qualcosa di diverso dalle bollette! Non si tratta di un errore o di un'indagine di vicinato?

Sarah pensa di non avere nulla di cui vergognarsi, quindi non c'è da preoccuparsi. Così si reca alla stazione di polizia il giorno della convocazione.

— *"Signora Ahmed? Salve, vorremmo farle alcune domande su una denuncia per diffamazione. "*

Più tardi, lo stesso giorno. Ufficio di Ana

— *"Pronto, risorse umane di La Reboute, parla Ana.*

— *Pronto, parla la signora Ahmed. Senta, ho appena trascorso due ore in commissariato. Sono stata interrogata sui documenti bancari pubblicati su Internet riguardanti una certa Mme Alavoine, sindaco del 10^e, di cui non conoscevo l'esistenza fino a quel momento. Inoltre, durante l'interrogatorio, mi hanno consegnato un documento che li autorizzava a perquisire gli uffici di rue Jaurès.*

— *Che storia! Ma cosa ha a che fare con i nostri uffici?"*

— *È anche per questo che la sto chiamando. Affermano di avere tutte le prove che questi documenti sono stati pubblicati dai vostri uffici. Ho detto loro che non sono stato io, che non ho visto nulla.*

di cosa stavano parlando. Hanno fatto delle indagini, contattando non so chi. Ma dicono che è stata aperta un'indagine e che andrà fino in fondo. Che troveranno i responsabili. Potrei anche dirle che non sono esattamente rassicurato. Spero che lei non c'entri nulla e che si sia trattato di uno sfortunato errore.

— *Onestamente, sono il primo ad essere stupito: non vedo cosa c'entro io, o cosa c'entri tutto questo.*

— *Lo spero... Comunque, ora spetta alla polizia fare il suo lavoro.*

Vi richiamerò se avrò notizie da loro.

— *Ok, farò lo stesso se chiamano qui.*

— *Arrivederci".*

Ana rimette giù la cornetta, stordita. Si gratta la testa. Cos'è questa storia dei documenti bancari? Chi può essere stato?

Stazione di polizia centrale di Parigi, qualche settimana dopo

— *"Commissario Marta?*

— *Lo stesso.*

— *Parla l'ufficiale Neus. Chiamo per il caso Ala-voine. Abbiamo ricevuto un'e-mail dai colleghi tecnici e scientifici che lavorano sui computer sequestrati. E abbiamo una novità.*

— *Vai avanti, Neus. Continua.*

— *A quanto pare, i colleghi hanno trovato il documento sulla postazione di lavoro di una certa Ana. Era stato scaricato dal browser web e modificato. C'era una connessione a una casella di posta elettronica Gmail, nonché un altro indirizzo di posta elettronica, questa volta a no-log, poco prima della pubblicazione dei documenti incriminati.*

— *Ah, molto bene. Ora sappiamo chi convocare per l'interrogatorio! Ma come possiamo ottenere delle prove?*

— *Chiederemo a Gmail e no-log informazioni su questi indirizzi e-mail. Da lì, avremo senza dubbio qualcosa su cui basarci, o almeno abbastanza per fare le domande giuste!*

— *Bene, Neus. Molto bene, signore. Mi metterò in contatto con il procuratore. E mi faccia sapere non appena ci sono novità.*

— *Sì, commissario. Buona giornata".*

Alla faccia del contesto. Questa piccola storia fittizia potrebbe ricordarne altre, molto più reali. L'idea era semplicemente quella di mostrare quanto sia facile e veloce *esporsi* alla minima connessione a Internet, senza alcuna forma di sorveglianza mirata.

Uno degli obiettivi di questo secondo volume è quello di far luce sulle tracce digitali che possono ricondurre ad Ana e Bea. Poi, indicare alcuni modi per proteggersi dagli attacchi - mirati o meno.

Nozioni di base della rete

Internet non è uno spazio virtuale, una nuvola astratta di informazioni dove si può trovare di tutto e di più. O almeno, non è solo questo.

Internet è prima di tutto un insieme di reti¹. Milioni di reti, aggregate nel corso di diversi decenni e gestite in modo più o meno caotico da aziende, università, governi, associazioni e privati; milioni di computer e materiali di ogni tipo, collegati tra loro da un'ampia varietà di tecnologie, dal cavo di rame alla fibra ottica al wireless.

Ma per noi, dietro il nostro piccolo schermo, Internet è soprattutto ciò che ci permette di fare: visitare siti web, inviare e-mail, chattare con le persone o scaricare file. Nuove applicazioni appaiono in continuazione e solo l'immaginazione umana sembra limitare le possibilità.

Capire come funziona Internet e come proteggersi significa districarsi in questa complessità per capire come questi computer comunicano tra loro e come funzionano le varie applicazioni che utilizziamo.

26.1 Computer interconnessi

Molto presto nella storia dell'informatica si è capito che i computer dovevano essere in grado di condividere risorse e informazioni, soprattutto in ambito accademico e militare, e su distanze sempre maggiori. Così sono nate le reti di computer. Dapprima i computer venivano collegati tra loro in un'area ristretta - di solito un'università, un'azienda o un sito militare - e poi queste aree venivano collegate tra loro. Negli Stati Uniti, alla fine degli anni '60, fu creata ARPANET (*Advanced Research Projects Agency Network*), una rete che collegava le università di tutto il Paese. Molte delle tecniche utilizzate oggi su Internet sono state inventate per creare e migliorare la rete. La nascita di Internet è legata a quella del software libero e opera secondo principi simili di apertura e trasparenza.²Tuttavia, è stato originariamente sviluppato per soddisfare esigenze militari.

Le varie reti di computer sono state interconnesse, formando Internet, che si è espanso rapidamente a partire dagli anni Novanta.

1. Per una spiegazione di cinque minuti: Rémi spiega, 2015, *Internet! Come funziona?* [<https://www.youtube.com/watch?v=dCknqjcItU>]. Per una spiegazione dettagliata in quattro ore: Benjamin Bayart, 2012, *Qu'est-ce qu'Internet? - Ciclo di conferenze a Sciences Po* [<https://www.fdn.fr/actions/confs/qu-est-ce-qu-internet/>].

2. Secondo Benjamin Bayart, "non è possibile dissociare Internet e il software libero" perché sono apparsi nelle stesse date, hanno avuto gli stessi protagonisti e una crescita e un funzionamento simili. Benjamin Bayart, 2007, *Internet libre, ou Minitel 2.0? conferenza agli 8^{es} rencontres mondiales du logiciel libre, Amiens* [<https://www.fdn.fr/actions/confs/internet-libre-ou-minitel-2-0/>].

Sempre più oggetti, la cui funzione principale non è quella di essere un computer, sono connessi a Internet: telecamere di sorveglianza, autovelox, ecc.³ autovelox⁴ terminali PMU⁵ frigoriferi⁶ apparecchiature mediche⁷ giocattoli per bambini⁸ automobili⁹ ecc. Alcuni parlano addirittura di *Internet della Merda*¹¹ (per mostrare l'assurdità di molti degli oggetti che si stanno facendo strada su Internet).

26.1.1 Una rete di computer

"Una rete è un insieme di nodi [...] collegati da link".¹² In una rete di computer, i nodi sono i computer. È un insieme di computer collegati tra loro da cavi, onde, ecc. per formare una rete.

Non tutti i computer utilizzati nelle reti sono come i personal computer, fissi o portatili, che usiamo generalmente. Alcuni sono specializzati per svolgere funzioni particolari all'interno della rete. Per esempio, la "scatola" che permette alla maggior parte di noi di accedere a Internet è un piccolo computer; allo stesso modo, anche i server su cui sono memorizzati i siti web sono computer. A questo elenco si potrebbero aggiungere altri tipi di computer specializzati, alcuni dei quali sono descritti nelle pagine seguenti.

26.1.2 Scheda di rete

Nonostante le loro differenze, tutti i computer collegati in rete hanno necessariamente una cosa in comune: oltre all'hardware minimo che compone un computer, devono avere almeno una periferica utilizzata per collegarsi alla rete. Questa periferica è chiamata *-scheda di rete*. Essa stabilisce il collegamento con gli altri computer. Al giorno d'oggi, in ogni personal computer sono spesso integrate diverse schede di rete (una scheda di rete cablata e una scheda Wi-Fi, per esempio).

Ogni scheda di rete ha un indirizzo hardware che la identifica in modo più o meno univoco. Nella tecnologia domestica cablata, chiamata Ethernet, come nella tecnologia wireless *Wi-Fi*, questo indirizzo hardware è chiamato *indirizzo MAC*. L'indirizzo MAC fornito con la scheda è progettato per garantire che la probabilità che due schede di rete abbiano lo stesso indirizzo hardware sia molto bassa.¹³ Questo pone un problema in termini di anonimato, come vedremo più avanti.

3. Jérôme G., 2012, *Caméras IP : faille-securite-voyeur comblée*, Génération-NT [<https://www.generation-nt.com/actualites/camera-ip-trendnet-faille-securite-voyeur-1539071>].

4. Korben, 2013, *Les radars pédagogiques à la merci des pirates?* [<https://korben.info/les-radars-pedagogiques-a-la-merci-des-pirates.html>].

5. Ouest-France con AFP, 2020, *Parigi. Ha piratato i gratta e vinci di PMU e FDJ nei bar* [<https://www.ouest-france.fr/societe/faits-divers/paris-il-piratait-les-bornes-de-jeux-de-grattage-du-pmu-et-de-la-fdj-dans-les-bars-6949018>].

6. Fabien Soyez, 2013, *Vie privée : télé connectée, l'espion parfait*, CNET France [<https://www.cnetfrance.fr/news/vie-privee-tele-connectee-l-espion-parfait-39793195.html>].

7. Camille Kaelblen, 2016, *Is your connected fridge the ideal gateway for hackers?*, RTL [<https://www.rtl.fr/culture/futur/votre-frigo-connecte-est-il-la-porte-d-entree-ideale-pour-les-hackers-7785045780>].

8. Gilles Halais, 2012, *Un hacker a trouvé comment pirater à distance les pacemakers*, Franceinfo [https://www.franceinfo.fr/sciences/un-hacker-a-trouve-comment-pirater-a-distance-les-pacemakers_1631785.html].

9. Sandrine Cassini, 2015, *Les jouets VTech victimes d'un piratage*, Le Monde [https://www.lemonde.fr/economie/article/2015/12/01/les-jouets-vtech-victimes-d-un-cybercriminel_4821275_3234.html].

10. Paul Ackermann, 2015, *Une voiture piratée à distance par des hackers*, HuffPost [https://www.huffingtonpost.fr/2015/07/22/voiture-pirate-distance-hackers_n_7846132.html].

11. Guillaume Ledit, 2017, *On Twitter, "Internet of Shit" ridicolizza l'Internet degli oggetti... di merda*, Usbek & Rica [<https://usbeketrica.com/article/sur-twitter-internet-of-shit-ridicolise-l-internet-des-objets-merdiques>].

12. Wikipedia, 2014, *Computer rete* [https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique].

13. Un indirizzo MAC è una sequenza di 12 cifre esadecimali (da 0 a 9), poi a per 10, b per 11 e così via fino a f per 15) come 00:3a:1f:57:23:98.

26.1.3 Diversi tipi di link

I modi più comuni per collegare i PC a una rete sono il cavo, noto come Ethernet, o la radio, nota come *Wi-Fi*.



Un connettore Ethernet RJ-45 standard

Ma oltre alla presa telefonica, le nostre comunicazioni su Internet vengono trasmesse con molti altri mezzi. Esistono molti modi diversi di trasmettere informazioni: cavi di rame, fibre ottiche, onde radio *e così via*. Dalla trasmissione via modem ¹⁴ negli anni '90 alla fibra ottica ¹⁵ utilizzate per le connessioni intercontinentali, passando per l'ADSL negli anni ¹⁶ negli anni 2000, ognuno di essi presenta caratteristiche diverse, soprattutto in termini di velocità di trasmissione delle informazioni (nota anche come *larghezza di banda*) e di costi di installazione e manutenzione.

Queste diverse tecnologie non presentano gli stessi punti deboli per quanto riguarda la riservatezza delle comunicazioni affidate o le tracce che lasciano: ad esempio, sarà più facile intercettare un segnale radio ad ampio raggio da lontano che la luce che passa attraverso una fibra ottica.

26.2 Protocolli di comunicazione

Affinché le macchine possano parlare tra loro, non solo devono essere collegate, ma devono anche parlare un linguaggio comune. Questo linguaggio si chiama *protocollo di comunicazione*. La maggior parte dei "linguaggi" utilizzati dalle macchine su Internet sono definiti con precisione in documenti pubblici. ¹⁷ È questo che permette a reti, computer e software diversi di lavorare insieme, a patto che rispettino questi standard. Questo è il significato di *interoperabilità*.

Protocolli diversi rispondono a esigenze diverse: scaricare un file, inviare una e-mail, consultare un sito web *e così via*.

Per semplicità, di seguito illustreremo nel dettaglio questi diversi protocolli, classificandoli in tre categorie: protocolli fisici, di rete e applicativi. ¹⁸

14. "Modem" è la parola condensata per *modulatore-demodulatore*: consente di trasmettere dati digitali su un canale in grado di trasportare il suono, come una linea telefonica.

15. Una fibra ottica è un filo di materiale trasparente che trasmette dati sotto forma di impulsi di luce. In questo modo è possibile trasmettere grandi volumi di informazioni, anche su lunghe distanze.

16. ADSL (per *Asymmetric Digital Subscriber Line*) o VDSL (per *Very-high-bit-rate Digital Subscriber Line*) è una tecnologia che consente di trasmettere dati digitali su una linea telefonica indipendentemente dal servizio telefonico.

17. Questi documenti pubblici sono noti come *Request For Comments*. Il sito Commentcamarche spiega molto bene il concetto di RFC. Jean-François Pillou, 2011, *Les RFC*, CommentCaMarche [<https://web.archive.org/web/20210219111153/https://www.commentcamarche.net/contents/533-les-rfc>].

18. In realtà, è un po' più complicato. Per maggiori dettagli si veda: Wikipedia, 2017, *Internet Protocol Suite* [https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet].

E quale modo migliore di far capire il concetto se non con un'analogia?

Paragoniamo il viaggio delle nostre informazioni attraverso Internet all'instradamento di una cartolina, le cui tappe, dal centro di smistamento postale alla cassetta della posta, corrispondono ai diversi computer attraverso cui passa.

26.2.1 Protocolli fisici

Per portare la posta a destinazione, utilizziamo diversi mezzi di trasporto: aerei, navi, camion e persino biciclette.

Ciascuno di questi mezzi di trasporto è soggetto a una serie di norme: il codice della strada, il controllo del traffico aereo, il diritto marittimo *e così via*.

[pagina
preceden
te.] Allo stesso modo, su Internet, le varie tecnologie hardware descritte in precedenza implicano l'uso di diverse convenzioni. Queste sono note come *protocolli fisici*.

26.2.2 Protocolli di rete

Saper navigare non è sufficiente per far arrivare la cartolina al destinatario. Bisogna anche saper leggere un codice postale e avere qualche nozione di geografia per raggiungere il destinatario, o almeno il centro di smistamento più vicino.

È qui che entrano in gioco *i protocolli di rete*: il loro scopo è quello di consentire l'instradamento delle informazioni da una macchina a un'altra, a volte molto lontana, indipendentemente dalle connessioni fisiche tra queste macchine.

[pagina
202] Il protocollo di rete più conosciuto è l'IP. -----

26.2.3 Protocolli di applicazione

[pagina
209] Internet è spesso utilizzato per accedere al Web, cioè a un insieme di pagine accessibili su server, che possono essere consultate con un browser Web: <https://guide.boum.org> è un esempio di sito Web. Le applicazioni Web utilizzano un protocollo chiamato *HTTP*, la cui versione crittografata e autenticata è *HTTPS*. Il linguaggio comune spesso confonde il web con Internet, ad esempio con espressioni come "andare online". Ma il web è solo uno dei tanti usi di Internet.

In realtà, esiste un numero enorme di applicazioni che utilizzano Internet e che la maggior parte degli utenti di Internet non si rende nemmeno conto di utilizzare. Oltre al web, queste applicazioni includono la posta elettronica, la messaggistica istantanea, il trasferimento di file, le criptovalute *e altro ancora*.

È così che ci si imbatte in questi diversi protocolli che, pur utilizzando Internet, *non sono* protocolli web:

- *SMTP*, *POP* e *IMAP* sono protocolli utilizzati nella messaggistica elettronica.¹⁹ Esistono anche versioni crittate e autenticate (*SMTSPS*, *POPS*, *IMAPS*);
- *Skype*, *Signal*, *IRC* e *XMPP* sono tutti protocolli utilizzati per la messaggistica istantanea;
- *BitTorrent* è un protocollo di condivisione di file peer-to-peer.

In effetti, chiunque abbia una conoscenza sufficiente della programmazione può creare da solo un nuovo protocollo e quindi una nuova applicazione Internet.

[pagina
202
questa
pagina] Ogni applicazione Internet utilizza un linguaggio particolare, chiamato *protocollo applicativo*, e poi mette il risultato in "pacchetti" che vengono trasmessi dai protocolli di rete di Internet. Possiamo paragonare il protocollo applicativo al linguaggio in _____

¹⁹ Esiste una notevole differenza nei protocolli utilizzati, che ha conseguenze in termini di riservatezza e anonimato, a seconda che si utilizzi una casella di posta elettronica tramite il browser web (webmail) o tramite un client di posta. Maggiori informazioni più avanti [pagina 290].

per scrivere il testo di una cartolina: sia il mittente che il destinatario devono comprendere questa lingua. Tuttavia, l'Ufficio postale non ha bisogno di capire nulla, purché la lettera contenga un indirizzo valido.

In generale, le cartoline non vengono messe in busta: chiunque per strada può leggerle. Allo stesso modo, la sorgente e la destinazione scritte nell'intestazione del pacchetto possono essere lette da chiunque. Esistono anche molti protocolli applicativi che non sono criptati: in questo caso, il contenuto dei pacchetti può essere letto da chiunque.

pagina 47 chiunque.

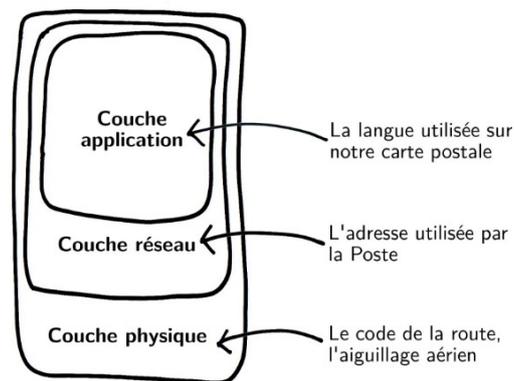
Non tutti i protocolli applicativi sono trasparenti. Sebbene molti di essi siano definiti da convenzioni aperte e accessibili (e quindi verificabili da parte del per-sonaio), non tutti i protocolli sono trasparenti.

sonnes qui le souhaitent), alcune applicazioni utilizzano protocolli proprietari con poca o nessuna documentazione. Questo rende difficile l'analisi delle informazioni sensibili contenute nei dati scambiati. Ad esempio, *Skype* funziona come una vera e propria scatola nera, che fa quello che si vuole (comunicare), ma forse anche molto di più: in particolare, si è scoperto che il contenuto dei messaggi viene analizzato ed eventualmente censurato²⁰ e che tutti gli indirizzi web inviati *tramite* e-mail vengono inoltrati a *Microsoft*²¹.

26.2.4 Incapsulamento

In realtà, durante una comunicazione vengono utilizzati contemporaneamente diversi protocolli, ciascuno con il proprio ruolo nell'instradamento delle informazioni.

È comune rappresentare questi diversi protocolli in strati sovrapposti.



Protocolli incapsulati

Infatti, quando comunichiamo per posta, la nostra comunicazione si basa sulla scrittura (in una certa lingua), poi sulla consegna da parte delle Poste, che a sua volta si basa su diversi mezzi di trasporto.

In modo analogo, un'applicazione Internet utilizzerà un *protocollo applicativo* prestabilito, sarà instradata tramite *protocolli di rete* e attraverserà le varie infrastrutture rispettando i *protocolli fisici* in vigore.

Questo è noto come incapsulamento: i protocolli applicativi sono incapsulati nei protocolli di rete, che a loro volta sono incapsulati nei protocolli fisici.

20. Ryan Gallagher, tradotto da Cécile Dehesdin, 2013, "Lanciare uova", "cinema cattivo"... L'elenco delle parole monitorate da Skype in Cina, Slate.fr [https://www.slate.fr/monde/69269/tom-skype-surveillance-chine-espionnage-liste-noire].

21. Jürgen Schmidt, 2013, *Skype's ominous link checking : Facts and speculation*, The H [http://www.h-online.com/security/features/Skype-s-ominous-link-checking-Facts-and-speculation-1865629.html] (in inglese).

26.2.5 Ulteriori informazioni sul protocollo IP

È interessante notare che, a differenza dei protocolli fisici e applicativi, i protocolli di rete sono relativamente universali. I protocolli fisici si evolvono con i progressi tecnologici, siano essi cablati o wireless. I protocolli applicativi si evolvono con lo sviluppo di nuove applicazioni: web, e-mail, chat, ecc. Tra questi due livelli, per sapere da che parte andare e come instradare i nostri pacchetti attraverso i milioni di reti Internet, dagli anni '80 tutto passa attraverso il protocollo *Internet* (IP).

Pacchetti

Nel protocollo IP, le informazioni da trasmettere vengono suddivise e confezionate in *pacchetti*, sui quali sono scritti gli indirizzi di invio e di destinazione. Questa "etichetta" è chiamata *intestazione* del pacchetto e contiene le informazioni necessarie per instradare i pacchetti da e verso la destinazione. I pacchetti di informazioni vengono poi trasmessi indipendentemente l'uno dall'altro, talvolta utilizzando percorsi diversi, e riassemblati una volta giunti a destinazione.

Oltre all'IP, esistono due protocolli: *TCP* (*Transmission Control Protocol*) e *UDP* (*User Datagram Protocol*). Il TCP è stato progettato per trasmettere i pacchetti senza perdere dati, prendendosi il tempo di controllare tutto. UDP garantisce la velocità degli scambi senza controllare che i pacchetti arrivino a destinazione; è utilizzato in particolare per le videoconferenze e le audioconferenze.

Indirizzo IP

Per funzionare, ogni computer collegato alla rete deve avere un indirizzo, che viene utilizzato per inviare i pacchetti: l'*indirizzo IP*. Questo indirizzo deve essere unico all'interno della rete. Infatti, se diversi computer della rete avessero lo stesso indirizzo, la rete non saprebbe a quale computer inviare i pacchetti.

Un indirizzo IP può essere paragonato a un numero di telefono: ogni telefono deve avere un numero di telefono per poter essere chiamato. Se più telefoni avessero lo stesso numero, ci sarebbe un problema.

Gli indirizzi utilizzati fin dai primi giorni di Internet hanno assunto la forma di quattro numeri da 0 a 255, separati da un punto: questi sono noti come indirizzi IPv4 (*Internet Protocol version 4*). Un indirizzo IPv4 ha il seguente aspetto 203.0.113.12.

Il protocollo IPv4 è stato definito all'inizio degli anni '80 e consente di assegnare un massimo di 4 miliardi di indirizzi. All'epoca non era immaginabile che Internet potesse essere accessibile al grande pubblico e si pensava che 4 miliardi fossero sufficienti.

Negli anni '90, in risposta all'incombente carenza di indirizzi, l'IETF ha iniziato a lavorare sull'IPv6 (*Internet Protocol version 6*).²² ha iniziato a lavorare sull'IPv6 (*Internet Protocol version 6*). Dal 2011 la carenza è una realtà e per i nuovi operatori è difficile ottenere indirizzi IPv4. Il protocollo IPv6 viene quindi gradualmente implementato dagli operatori (anche se ci sono alcuni recalcitranti). L'implementazione dell'IPv6 comporta una notevole posta in gioco politica²³ ma anche nuovi problemi di sicurezza²⁴. Nel 2022, i due protocolli (v4 e v6) opereranno in parallelo. Un indirizzo IPv6 ha il seguente aspetto 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

22. Wikipedia, 2016, *Internet Ingegneria Task Force* [https://fr.wikipedia.org/wiki/Internet_Engineering_Task_Force].

23. In questa lezione [<https://ldn-fai.net/intranet-ipv4-ou-internet-ipv6/>], LDN spiega le sfide del passaggio a IPv6.

24. Questo nuovo standard pone nuovi problemi per il nostro anonimato online. Florent Fourcot, 2011, *IPv6 et conséquences sur l'anonymat*, LinuxFr.org [<https://linuxfr.org/users/ffourcot/journaux/ipv6-et-cons%C3%A9quences-sur-lanonymat>]. Per continuare...

L'indirizzo IP è un'informazione estremamente utile per chiunque cerchi di monitorare ciò che accade in una rete, in quanto identifica in modo univoco un computer in rete in un determinato momento, senza essere una vera prova contro una persona (in quanto un computer può essere utilizzato da più persone).²⁵ contro un individuo (poiché un computer può essere utilizzato da più persone). Tuttavia, può indicare l'origine geografica di una connessione, fornire indizi e avviare o confermare i sospetti.

26.2.6 Porto

Molte applicazioni possono essere utilizzate contemporaneamente dallo stesso computer: leggere la posta elettronica in Thunderbird, guardare il sito web della SNCF, chattare con gli amici tramite la messaggistica istantanea, ascoltare musica online. Ogni applicazione deve ricevere solo i pacchetti ad essa destinati e contenenti messaggi in una lingua ad essa comprensibile. A volte, però, un computer collegato alla rete ha un solo indirizzo IP. A questo indirizzo si aggiunge un numero che consente al computer di inoltrare il pacchetto all'applicazione giusta. Questo numero viene scritto sul pacchetto, oltre all'indirizzo: è il numero di *porta*.

Per capire, paragoniamo il nostro computer a un edificio: l'edificio ha un solo indirizzo, ma ospita molti appartamenti e molte persone diverse. Il numero di appartamento su una busta viene utilizzato per inviare la posta al destinatario giusto. Lo stesso vale per i numeri di porta: servono per inviare i dati all'applicazione giusta.

Alcuni numeri di porta sono convenzionalmente assegnati a particolari applicazioni. Così, quando il nostro browser web vuole connettersi a un server web, sa che deve comporre la porta 80 (o 443 nel caso di una connessione crittografata). Allo stesso modo, per consegnare una e-mail, il nostro computer si connette generalmente alla porta 25 del server (o 465 se si tratta di una connessione crittografata).

Sul computer che stiamo utilizzando, ogni applicazione connessa a Internet apre almeno una porta, che si tratti di un browser Web, di un software di messaggistica istantanea, di un lettore musicale *e così via*. Pertanto, il numero di porte aperte nell'ambito di una connessione a Internet può essere molto elevato e la chiusura del browser Web spesso non è sufficiente a interrompere la connessione alla rete...

pagina

209



PRECISIONE

Più porte sono aperte, più sono i punti attraverso i quali persone malintenzionate o virus possono tentare di infiltrarsi in un computer collegato alla rete. *I firewall* di solito lasciano aperte solo alcune porte, come definito nella loro configurazione, e rifiutano le richieste ad altre porte.

26.3 Reti locali

È possibile creare reti senza Internet. In realtà, le reti di computer sono apparse molto prima di Internet. Negli anni '60, i protocolli di rete come l'HP-IB²⁶ che consentivano di collegare solo un numero limitato di computer, erano già in funzione reti *locali*.

25. Legalis, 2013, *L'adresse IP, preuve insuffisante de l'auteur d'une suppression de données sur Wikipedia* [<https://www.legalis.net/actualite/ladresse-ip-preuve-insuffisante-de-lauteur-dune-suppression-de-donnees-sur-wikipedia/>].

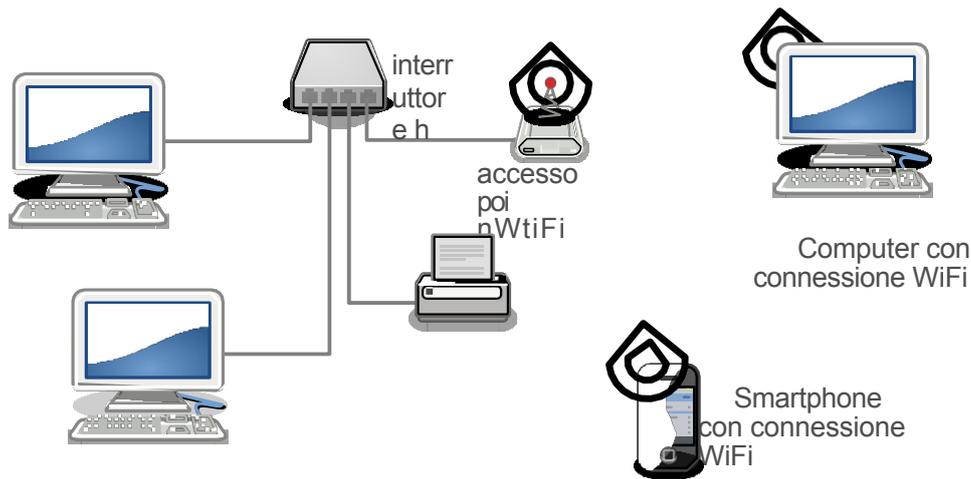
26. Wikipedia, 2014, *HP-IB* [<https://fr.wikipedia.org/wiki/HP-IB>].

26.3.1 La rete locale, la struttura di base di Internet

Quando si collegano diversi computer nella stessa casa, scuola, università, ufficio, edificio *e così via*, si parla di una *rete locale* (LAN). I computer possono quindi comunicare tra loro, ad esempio per scambiare file, condividere una stampante o giocare in rete.

Le reti locali possono essere paragonate alle reti telefoniche interne di alcune organizzazioni (aziende, università, *ecc.*).

Queste reti locali sono spesso costituite da diversi dispositivi che comunicano tra loro:



Schema della rete locale

26.3.2 Switch e punto di accesso Wi-Fi

Per collegare le macchine che compongono una rete locale, di solito ognuna di esse è collegata a una "ciabatta" di rete, tramite cavo o Wi-Fi. Spesso si usa uno "switch", che può essere paragonato a una ciabatta. Tuttavia, invece di inoltrare ogni pacchetto in arrivo a tutti i computer collegati, uno switch legge l'indirizzo del pacchetto e lo invia solo alla presa di destinazione giusta.

L'equivalente di uno switch nelle reti cablate è chiamato "access point" nel mondo wireless. Ogni punto di accesso ha un nome, che viene trasmesso all'area circostante (questo è l'elenco delle reti Wi-Fi che il nostro software di rete affigge).

Per continuare il nostro paragone, lo switch è un po' come il postino locale, che consegna la posta a ogni destinatario del quartiere. A tal fine, lo switch elabora le informazioni provenienti dalle schede di rete, identificate dal loro indirizzo hardware, collegate a ciascuna delle sue prese.

pagina

198

Così come l'accesso fisico a una macchina apre molte possibilità di recuperare informazioni, l'accesso fisico a una rete significa che, a meno di difese speciali, è possibile impersonare una delle altre macchine della rete. In questo modo è possibile raccogliere una grande quantità di informazioni sulle comunicazioni che circolano sulla rete, mettendo in atto un attacco "*monster-in-the-middle*". L'accesso fisico alla rete può essere ottenuto collegando un cavo a uno switch o *tramite* un punto di accesso Wi-Fi.

pagina

254

26.3.3 Indirizzamento

Per consentire alle macchine collegate alla rete di comunicare con il protocollo IP, è necessario che ciascuna di esse abbia un indirizzo IP. Sono stati sviluppati software e protocolli per automatizzare l'assegnazione degli indirizzi IP ai computer durante la fase di

pagina

202

connessione di rete, come i protocolli DHCP ²⁷ in IPv4 o NDP ²⁸ e i protocolli SLAAC in IPv6 ²⁹.

Per funzionare, il sistema deve ricordare l'associazione di una determinata scheda di rete, identificata dal suo indirizzo hardware, con un determinato indirizzo IP. La corrispondenza tra indirizzo IP e indirizzo hardware è utile solo all'interno della rete locale. Non c'è quindi alcun motivo tecnico per cui gli indirizzi hardware circolino su Internet, anche se ciò accade di tanto in tanto. ³⁰.

pagina
198

26.3.4 NAT e indirizzi riservati per le reti locali

Negli anni '90 gli organismi di standardizzazione di Internet si sono resi conto che il numero di indirizzi IPv4 disponibili non sarebbe stato sufficiente a far fronte alla rapida crescita della rete. In risposta a questo problema, alcuni intervalli di indirizzi sono stati riservati alle reti private e non sono utilizzati su Internet: si tratta degli *indirizzi privati*. ³¹.

pagina
202

Pertanto, la maggior parte delle "scatole" di Internet assegna ai computer che vi si collegano indirizzi che iniziano con 192.168 ³² in IPv4 e fe80: in IPv6. Diverse reti locali possono utilizzare gli stessi indirizzi IP privati, a differenza degli indirizzi IP su Internet, che devono essere unici in tutto il mondo.

I pacchetti che trasportano questi indirizzi non possono lasciare inalterata la rete privata. Questi indirizzi privati sono quindi utilizzati solo sulla rete locale. Così, ad esempio, una macchina può avere l'indirizzo IPv4 192.168.0.12 sulla rete locale, ma dal punto di vista delle altre macchine con cui comunica via Internet, sembrerà utilizzare l'indirizzo IPv4 della "scatola" (ad esempio, 203.0.113.48): questo sarà il suo *indirizzo pubblico*. È la "scatola" che si occupa di modificare i pacchetti di conseguenza, grazie alla *Network Address Translation (NAT)*.

26.4 Internet: reti interconnesse

Internet è l'acronimo di Reti Interconnesse.

Ciascuna di queste reti è chiamata *Autonomous System (AS)*.

26.4.1 Fornitori di servizi Internet

Un *Internet Service Provider (ISP)* è un'organizzazione che offre una connessione a Internet, tramite fibra ottica, onde elettromagnetiche o cavo coassiale. ³³ linea telefonica o cavo coassiale. In Francia, i principali ISP commerciali per uso domestico sono Bouygues, Orange, Free e SFR. Esistono anche diversi ISP associativi, come i membri della Fédération FDN. ³⁴.

Spesso un ISP gestisce la propria rete, alla quale sono collegate le "caselle" degli abbonati.

27. Utilizzato nelle reti IPv4, DHCP sta per *Dynamic Host Configuration Protocol* ().

28. Wikipedia, 2017, *Neighbor Discovery Protocol*

[https://fr.wikipedia.org/wiki/Neighbor_Discovery_Protocol].

29. Wikipedia, 2022, *IPv6*, sezione "Allocazione degli indirizzi IPv6" [https://fr.wikipedia.org/wiki/IPv6#Attribution_des_adresses_IPv6].

30. Uno dei modi in cui l'indirizzo fisico circola su Internet è l'uso di portali vincolati, di cui parleremo più avanti [pagina 216].

31. Nello stesso periodo, l'IETF stava lavorando alla versione 6 del protocollo IP [pagina 202], che risolveva il problema della carenza di .

32. Gli intervalli di indirizzi privati sono definiti per convenzione in un documento chiamato "RFC 1918". Oltre agli indirizzi che iniziano con 192.168, includono quelli che iniziano con 10 e da 172.16 a 172.31.

33. Wi-Fi, 4G o altro...

34. *L'elenco dei membri della Federazione FDN* [<https://www.ffdn.org/fr/membres>].

Per collegare una rete locale ad altre reti, è necessario un *router*. Si tratta di un computer che ha il compito di inoltrare i pacchetti tra due o più reti.

Una "scatola" utilizzata per collegare un'abitazione a Internet funge da router. Ha una scheda di rete collegata alla rete locale, ma anche un modem ADSL o una porta in fibra ottica collegata alla rete dell'ISP: si tratta di un router-modem. Non è solo parte della rete locale, ma anche di Internet: in IPv4, è l'indirizzo IP della "scatola" che è visibile da Internet su tutti i pacchetti che trasporta per i computer della rete locale. Con l'IPv6, invece, tutte le macchine collegate alla rete hanno indirizzi pubblici instradati e fanno quindi parte di Internet.

Il "box" è un piccolo computer che, nello stesso involucro del modem-router, integra un software per la gestione della rete locale (ad esempio un software DHCP), uno switch Ethernet e/o Wi-Fi per il collegamento di più computer e, talvolta, un decoder TV, un disco rigido, ecc. Il box può anche essere utilizzato per connettersi a Internet.

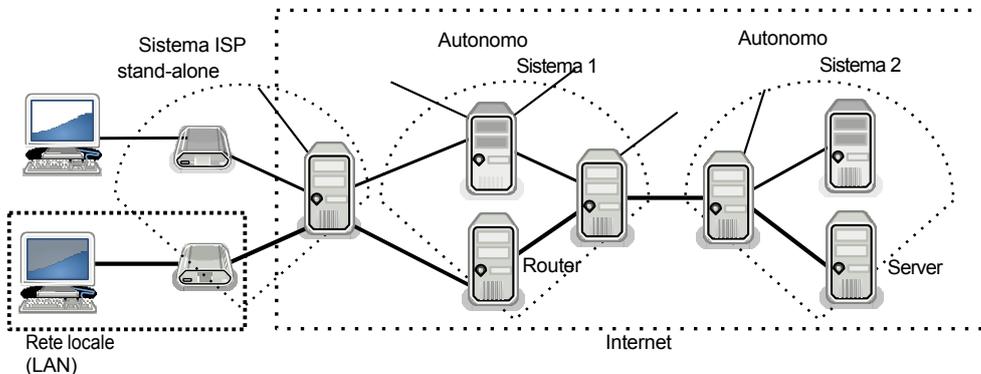
pagina
204

26.4.2 Sistemi autonomi

Un sistema autonomo è una rete coerente - solitamente sotto il controllo di una singola entità o organizzazione - in grado di operare indipendentemente da altre reti.

Nel 2022, l'interconnessione di oltre 72.000 SA in tutto il mondo ³⁵ formano Internet.

Un sistema autonomo può essere tipicamente la rete di un provider di servizi Internet (ad esempio Free, SFR o *tetaneutral.net*). In questo caso, ogni "box" utilizzato per collegare una rete domestica locale a Internet fa parte della rete del provider, che a sua volta è interconnessa con altri sistemi autonomi per formare Internet. Le organizzazioni che ospitano servizi Internet (ad esempio, Gitoyen ³⁶Google o Riseup) e quelle che gestiscono i "grandi tubi", come i cavi transatlantici attraverso i quali scorre gran parte dei dati di Internet, hanno anch'esse i loro sistemi autonomi.



Internet è un'interconnessione di reti autonome

Internet, quindi, non è una grande rete omogenea gestita centralmente. È piuttosto costituita da una moltitudine di reti interconnesse gestite da un'ampia varietà di organizzazioni e aziende, ognuna con il proprio modo di operare.

Tutte queste reti, infrastrutture e computer non funzionano da sole: sono gestite quotidianamente da persone chiamate *amministratori di sistemi e di rete*,

35. Sul [sito web del CIDR Report](http://www.cidr-report.org/as2.0/) [[http s://www.cidr-report.org/as2.0/](http://www.cidr-report.org/as2.0/)] si possono trovare statistiche interessanti sull'evoluzione degli AS.

36. Associazione che fornisce servizi a [Globenet](https://www.globenet.org/-Services-.html) [<https://www.globenet.org/-Services-.html>], diversi membri della Federazione FDN e diversi [Chaton](https://chatons.org/) [<https://chatons.org/>]. Ulteriori informazioni sono disponibili [sul sito web](https://gitoyen.org/) [<https://gitoyen.org/>].

"admins" o "adminsys"³⁷. Gli amministratori sono responsabili dell'installazione, della manutenzione e dell'aggiornamento di queste macchine, quindi hanno *necessariamente* accesso a molte informazioni.

In termini di monitoraggio, gli interessi commerciali e gli obblighi legali dei sistemi autonomi variano molto, a seconda del Paese e del tipo di organizzazione coinvolta (istituzioni, aziende, associazioni, *ecc.*). Nessuno ha un controllo completo su Internet e la sua natura globale complica qualsiasi tentativo di legislazione unificata. Di conseguenza, non c'è uniformità di pratiche.

Interconnessione di rete

Così come abbiamo collegato la nostra rete locale al sistema autonomo del nostro ISP, quest'ultimo stabilisce connessioni con altre reti. È quindi possibile passare informazioni da un sistema autonomo all'altro. È grazie a queste interconnessioni che possiamo comunicare con i vari computer che compongono Internet, indipendentemente dal sistema autonomo a cui appartengono.



Un router

Un router è un computer che collega diverse reti. Gli operatori hanno router sempre accesi, che assomigliano più a grandi scatole di pizza che a personal computer. Tuttavia, il loro principio di funzionamento è simile a quello degli altri computer e sono dotati di alcuni circuiti specializzati per passare molto rapidamente i pacchetti da una rete all'altra.

I sistemi autonomi si accordano per lo scambio di traffico reciproco, noto anche come accordo *di peering*. Nella maggior parte dei casi, il *peering* è gratuito e lo scambio è bilanciato. Per raggiungere i sistemi autonomi con cui non ha accordi *di peering*, un operatore può utilizzare un fornitore di transito. Un transit provider è un operatore che sa come raggiungere l'intera Internet e vende connettività ad altri operatori.³⁸



PRECISIONE

Esiste un principio che vieta qualsiasi discriminazione nel traffico, sia per quanto riguarda la fonte, la destinazione o il contenuto delle informazioni trasmesse in rete. Questo principio è noto come *neutralità della rete*. Questo principio garantisce che gli utenti di Internet non debbano affrontare una gestione del traffico Internet che abbia l'effetto di limitare il loro accesso alle applicazioni e ai servizi distribuiti in rete. Ad esempio, limitando la visione o il download di video online. La neutralità della rete garantisce che i flussi di informazioni non siano bloccati, degradati o favoriti dagli operatori di telecomunicazioni, garantendo il libero utilizzo della rete³⁹. In Francia, la Quadrature du Net⁴⁰ e la Fédération FDN⁴¹ difendono e promuovono la neutralità della rete.

⁴²

37. In seguito, utilizzeremo il termine "amministratori" per indicare gli amministratori di sistema e di rete.

38. Loïc Komol, 2013, *Le peering : petite cuisine entre géants du Net*, Clubic [<https://www.clubic.com/pro/it-business/article-558086-1-peering-petite-cuisine-geants-web.html>].

39. #DataGueule ha realizzato un video [<https://peertube.datagueule.tv/videos/watch/64077068-5d05-4815-9095-af63a33a91c4>] che spiega chiaramente la neutralità della rete e le questioni politiche associate.

40. La neutralità della rete vista da La Quadrature du Net [https://www.laquadrature.net/neutralite_du_net].

41. Principi fondanti della Fédération FDN [<https://www.ffdn.org/fr/principes-fondateurs>].

42. La neutralità della rete è definita nella legge francese all'articolo L33-1 del Code des postes et des communications électroniques [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043545209].

Punti di interconnessione...

Gli operatori di rete erano soliti far passare i cavi direttamente tra i loro router, il che significava molti cavi e molte spese. Ora utilizzano i *punti di interconnessione* (IX o IXP, per *Internet eXchange Point*), che sono luoghi in cui molti sistemi autonomi sono collegati tra loro. Gli operatori che desiderano connettersi a questi punti portano ciascuno una fibra e installano dei router. A causa dell'enorme volume di traffico che passa attraverso questi punti, essi sono di grande importanza strategica per i governi e le altre organizzazioni che desiderano monitorare ciò che passa attraverso la rete.⁴³

... interconnessi

I principali centri di interconnessione sono collegati da grandi fasci di fibre ottiche. Insieme, questi collegamenti formano *le dorsali* di Internet.⁴⁴

Per esempio, per collegare l'Europa all'America, diversi fasci di fibre ottiche corrono lungo il fondo dell'Oceano Atlantico. Questi fasci di fibre sono tutti punti deboli e di tanto in tanto un incidente, come l'ancora di una nave che taglia un cavo, può rallentare Internet su scala continentale.⁴⁵ Questo può sembrare strano, dato che storicamente l'idea di Internet era di ispirazione militare: una rete decentralizzata, che moltiplica i collegamenti in modo da essere resistente al taglio di uno qualsiasi di essi.

26.4.3 Instradamento

Abbiamo visto che i computer si scambiano informazioni inserendole in pacchetti.

pagina
202

Immaginate due computer collegati a Internet su reti diverse che vogliono comunicare. Ad esempio, il computer di Ana in Francia si collega al computer di Bea in Venezuela.

Il computer di Ana accede a Internet tramite la sua "casella", che fa parte della rete del suo ISP. Il computer di Bea, invece, fa parte della rete della sua università.

Il pacchetto destinato al computer di Bea arriverà prima sulla rete dell'ISP di Ana. Verrà inoltrato al router C del suo ISP, che funge da centro di smistamento. Il router legge l'indirizzo del computer di Bea sul pacchetto e deve decidere a chi inoltrare il pacchetto per avvicinarlo alla sua destinazione. Come viene effettuata questa scelta?

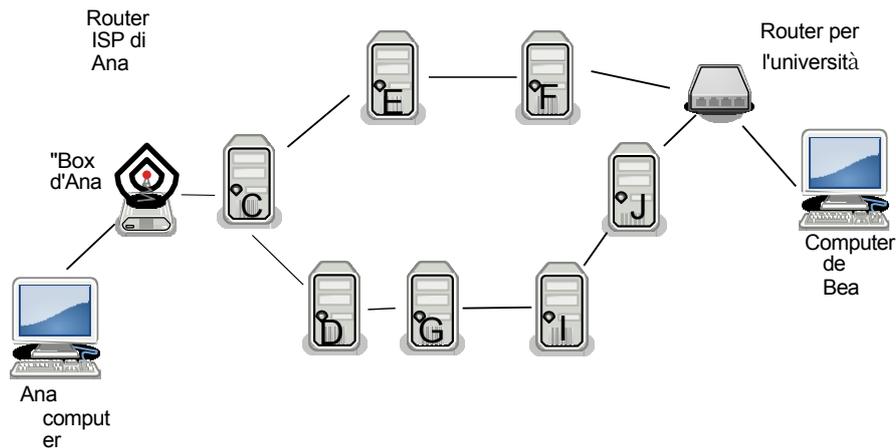
Ogni router mantiene un elenco delle reti a cui è connesso. Invia regolarmente aggiornamenti di questo elenco agli altri router a cui è collegato, i suoi vicini, che fanno lo stesso. Questi elenchi consentono al router di instradare i pacchetti in arrivo verso la loro destinazione.

Quindi il router dell'ISP di Ana sa che può raggiungere la rete universitaria di Bea attraverso quattro intermediari inviando il pacchetto al router D. Ma può anche

43. Guillaume Champeau, 2013, *How Germany also spies on our communications*, Numerama [<https://www.numerama.com/politique/26279-comment-l-allemande-aussi-espionne-nos-communications.html>].

44. TeleGeography, 2017, *Mappa dei cavi sottomarini* [<https://www.submarinecablemap.com/>] (en inglese).

45. Pierre Col, 2009, *Internet, ancore di barche e terremoti sottomarini*, ZDNet [<https://www.zdnet.fr/blogs/infra-net/internet-les-ancres-de-bateaux-et-les-seismes-sous-marins-39602117.htm>], Cécile Dehesdin, 2013, *Des coupures dans des câbles sous-marins ralentissent Internet dans plusieurs pays*, Slate.fr [<https://www.slate.fr/monde/70063/cable-internet-sous-marin-coupe-impact-afrique-egypte>].



Instradamento

Sceglierà di inviare il pacchetto a E, che ha un percorso più diretto.

Il pacchetto arriva quindi a E, il router di un operatore di transito, un'organizzazione pagata dall'ISP di Ana per instradare i pacchetti. E farà lo stesso tipo di calcolo e invierà il pacchetto a F. La rete di F comprende computer non solo in Europa, ma anche in America, collegati da un cavo transatlantico. F appartiene a una società, simile a quella che gestisce E, che è pagata dall'università di Bea. F invia infine il pacchetto al router dell'università, che lo spedisce al computer di Bea. Il nostro pacchetto è arrivato a destinazione.

Ciò significa che ogni pacchetto di informazioni che attraversa Internet passa attraverso diverse reti. Ogni volta, un router funge da centro di smistamento e lo inoltra a un altro router. Alla fine, ogni pacchetto passa attraverso molti computer diversi, appartenenti a molte organizzazioni diverse.

Inoltre, la topologia della rete, ovvero l'architettura, la disposizione e la gerarchia delle singole postazioni di lavoro, cambia nel tempo.

Quando Ana si connette nuovamente al computer di Bea il giorno successivo, i pacchetti inviati dal computer non seguiranno necessariamente lo stesso percorso del giorno precedente. Ad esempio, se il router E viene spento a causa di un'interruzione di corrente, il router dell'ISP di Ana instraderà i pacchetti attraverso D, che in precedenza aveva un percorso più lungo.

Il governo egiziano ha chiuso Internet durante la rivoluzione del 2011 agendo a livello di instradamento. I router dei principali ISP del Paese hanno smesso di dire agli altri router che erano loro a instradare i pacchetti verso i computer egiziani.⁴⁶ Di conseguenza, i pacchetti destinati all'Egitto non riuscivano più a passare, interrompendo di fatto l'accesso alla rete, senza tagliare alcun cavo.

26.5 Clienti e server

Storicamente, negli anni '80, ogni computer connesso a Internet forniva una parte di Internet. Non solo "andava a vedere le cose su Internet", ma offriva anche informazioni, dati e servizi ad altri utenti connessi a Internet: *creava* Internet tanto quanto *vi accedeva*.

46. Stéphane Bortzmeyer, 2011, *Interruzione di Internet in Egitto* [<https://www.bortzmeyer.org/egypte-coupure.html>].

Oggi il quadro generale è molto diverso. Come abbiamo visto, ci sono computer permanentemente accesi che hanno il compito di collegare tra loro i pezzi di Internet: i router. Allo stesso modo, esiste un'altra categoria di computer permanentemente accesi che contengono quasi tutti i dati e i servizi disponibili su Internet. Questi computer sono chiamati server, perché *servono* informazioni e servizi. Essi centralizzano la maggior parte dei contenuti, siano essi siti web, musica, e-mail e così via, su Internet. Questo crea una gerarchia verticale nella rete. Infatti, più informazioni si hanno, in senso lato, più potere si ha potenzialmente.

I server forniscono, al contrario dei client che si limitano ad accedere alle informazioni. Questa situazione corrisponde a un Internet in cui le nostre macchine agiscono principalmente come client, centralizzando Internet intorno ai fornitori di contenuti.⁴⁷

Prendiamo l'esempio di uno dei servizi disponibili su Internet, il [sito web della Digital Self-Defense Guide](https://guide.boum.org/) [https://guide.boum.org/]: quando Ana consulta una pagina di questo sito, il suo computer agisce come un *client*, collegandosi al *server* che ospita la Digital Self-Defense Guide.

Detto questo, qualsiasi computer può essere sia client che server, contemporaneamente o in successione. Ciò è particolarmente vero per il modello peer-to-peer, o *P2P*, ampiamente utilizzato per la condivisione di file. In questa situazione, ogni computer, altrimenti noto come *nodo*, è connesso alla rete e comunica sia come client che come server. Questi due ruoli non sono determinati dal tipo di macchina.

26.5.1 Server dei nomi

Quando Ana chiede al suo browser di andare al sito della Guida all'autodifesa digitale, il suo computer deve collegarsi al server che ospita il sito.

pagina
202

Per farlo, è necessario conoscere l'indirizzo IP del server. Tuttavia, un indirizzo IP è una serie di numeri piuttosto difficili da memorizzare, digitare o trasmettere, come 88.99.208.38 (per un indirizzo IPv4). Per risolvere questo problema, esistono dei server a cui si possono porre domande come: "Qual è l'indirizzo IP di guide.boum.org?", proprio come se si cercasse il numero di un corrispondente nell'elenco telefonico. Questo sistema si chiama DNS (*Domain Name System*). Quindi il computer di Ana inizia, tramite la sua "scatola", a interrogare il server DNS del suo provider di servizi Internet per ottenere l'indirizzo IP del server che ospita il nome di dominio guide.boum.org.

Il computer di Ana riceve l'indirizzo IP del server e può comunicare con esso.

26.5.2 Percorso della richiesta web

Il computer di Ana si collega quindi al server della guida (88.99.208.38) e gli invia una richiesta che significa: "Inviarmi la pagina iniziale del sito web guide.boum.org". I pacchetti che trasportano la richiesta lasciano il suo computer e passano attraverso la sua "scatola" per raggiungere il router del suo ISP. Attraversano poi diverse reti e router (non mostrati nel diagramma), prima di raggiungere finalmente il server di destinazione.

pagina
206
pagina
217

26.5.3 Software per server

Per inviare ad Ana la pagina web richiesta, il server la cerca nella sua memoria, sul disco rigido o la costruisce.

47. L'intervento di Benjamin Bayart *Internet libre, ou Minitel 2.0?* [https://www.fdn.fr/actions/confis/internet-libre-ou-minitel-2-0/], tenuto in occasione degli 8^{es} rencontres mondiales du logiciel libre di Amiens nel 2007, spiega molto bene questo cambiamento e le problematiche connesse.

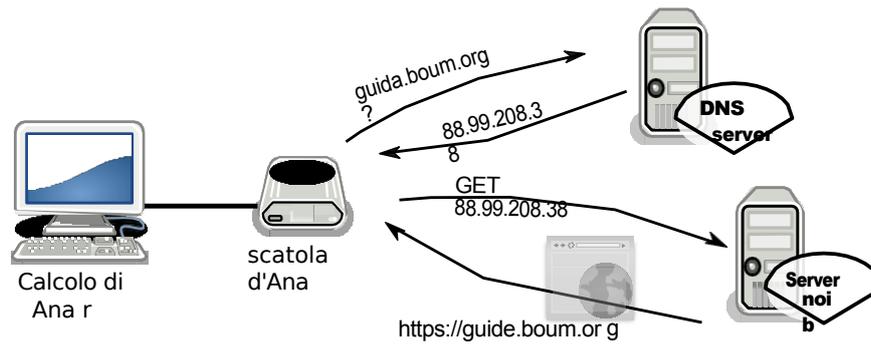


Diagramma di una richiesta web

Le pagine consultabili sul web non esistono necessariamente in una forma che possiamo vedere sul nostro computer *prima* di richiederne l'accesso. Spesso vengono generate automaticamente, su richiesta. Si tratta dei cosiddetti *siti web dinamici*, in contrapposizione ai siti web *statici*, le cui pagine sono scritte in anticipo.

Ad esempio, se si cerca "ouistiti moteur virtuose" in un motore di ricerca, non ha ancora la risposta in riserva. Il server esegue quindi il codice sorgente della pagina 39 del sito per calcolare la pagina contenente la risposta prima di inviarcela.

Sul server c'è un software che viene eseguito e risponde alle richieste. Il software del server è specifico per ogni applicazione: comprende il protocollo dell'applicazione. Nel presente esempio, questo software cerca e serve la pagina web del computer Ana: lo chiamiamo server *web*.

pagina

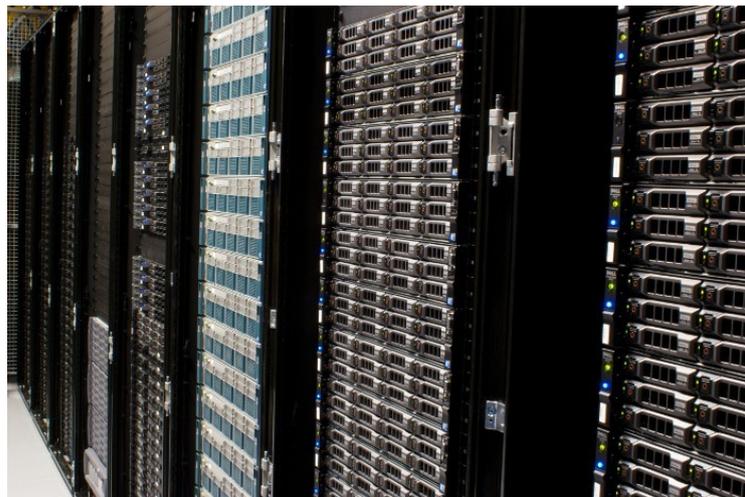
26.5.4 Hosting server

I server, ovvero i computer che eseguono il software per server di cui sopra, sono di solito ospitati in edifici con buone connessioni di rete e alimentazioni affidabili: i *data center*.

pagina

200

pagina
a fianco



Un corridoio di server in un centro dati

Oggi è di gran moda parlare di *cloud computing*. Questo concetto di "marketing" non mette in discussione la separazione tra i clienti e le aziende.

e server, al contrario. Significa semplicemente che i dati possono essere spostati da un server a un altro, per motivi legali, tecnici o economici. E questo senza che i proprietari siano necessariamente informati.



Non esiste una nuvola, ma solo i computer degli altri.



PRECISIONE

Google, ad esempio, ha almeno venti centri dati in tre continenti⁴⁸ per garantire che i suoi servizi siano operativi 24 ore su 24, 7 giorni su 7, anche quando alcune apparecchiature non sono disponibili.

I fornitori di hosting di questo tipo gestiscono centinaia di macchine fisiche in diversi centri dati in tutto il mondo, riunendo la loro capacità di archiviazione e di calcolo in una super-macchina astratta. Vendono poi "macchine virtuali", cioè quote della potenza di calcolo e di archiviazione di questa super-macchina. Amazon Elastic Compute Cloud (o EC2) è uno dei servizi più noti in questo campo.⁴⁹

Una macchina virtuale può essere spostata automaticamente in base all'utilizzo delle macchine fisiche, alla qualità della loro connessione di rete, ecc. Con un'infrastruttura di questo tipo, è impossibile sapere in anticipo quale macchina fisica - e quindi dove - si trova una determinata macchina virtuale.

In pratica, questo rende impossibile controllare i nostri dati.⁵⁰ Saranno davvero cancellati dalle macchine fisiche se li "cancelliamo"? Abbiamo visto nel primo volume che cancellare i dati da un computer è un'operazione complicata. Il problema diventa ancora più grave se non sappiamo di quale computer stiamo parlando. Inoltre, questo pone problemi legali: i dati che sono legali in un luogo possono finire per essere illegali perché la macchina che li contiene o li serve su Internet ha cambiato giurisdizione.

Si è quindi passati da un Internet in cui tutti consultavano e distribuivano i dati, a un modello in cui i dati erano centralizzati su macchine fisiche chiamate server, per arrivare oggi al *cloud*, in cui gli stessi dati possono essere memorizzati, a volte in modo sparso, su server indeterminati. Diventa estremamente complicato sapere dove i dati sono effettivamente conservati e l'utente ha ancora meno controllo su ciò che accade.

[pagina]

42

48. Google, 2017, *Ubicazione dei centri dati* [<https://www.google.com/about/datacenters/inside/locations/index.html>].

49. Wikipedia, 2014, *Amazon Elastic Compute Cloud* [https://fr.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud].

50. Jos Poortvliet, 2011, *openSUSE e ownCloud* [<https://news.opensuse.org/2011/12/20/opensuse-and-owncloud/>].

Tracce lungo tutta la linea

Il normale funzionamento della rete significa che molti computer possono vedere ciò che si fa su di essi. Non stiamo parlando di sorveglianza attiva. È solo che a volte è del tutto necessario. A volte, però, queste informazioni vengono raccolte perché "più convenienti", ad esempio per diagnosticare i problemi.

Il funzionamento di qualsiasi computer lascia un certo numero di tracce.

Questo è il tema del primo volume di questa guida.

pagina

27 Nel caso dell'uso online, non è solo il computer davanti ai vostri occhi che può tenere traccia di ciò che si sta facendo sulla rete, ma anche di ciascuno dei computer attraverso cui transitano le informazioni. Molti di questi

Le informazioni circolano *in chiaro*, non criptate.

pagina 47

27.1 Sul computer client

Il computer utilizzato per connettersi alla rete è chiamato client. Questo computer è a conoscenza di tutte le operazioni effettuate dall'utente e spesso ne tiene traccia.

pagina
209

Come ampiamente spiegato nel primo volume di questa guida, queste tracce, e la facilità con cui possono essere sfruttate, dipendono in larga misura dal computer e dal sistema operativo utilizzati.

pagina 27
dal

27.1.1 Memoria del browser web

Per renderli più facili da usare, i browser web registrano una grande quantità di informazioni sulle pagine visitate. Ecco alcuni esempi:

- La maggior parte dei browser web conserva una cronologia delle pagine web consultate.
- Spesso si offrono anche di registrare ciò che il navigatore inserisce nei moduli presenti in determinate pagine web, nonché le password di vari account online.
- In generale, salvano anche le pagine consultate di recente o di frequente per accelerare il caricamento: questa operazione è nota come "caching".¹

Tutti questi dati vengono memorizzati, consentendo alla polizia (e non solo) di risalire alle nostre abitudini di navigazione. Ricordiamo la nostra storia dall'inizio:

pagina
194

- A quanto pare, i colleghi hanno trovato il documento sulla postazione di lavoro di una certa Ana. È stato scaricato da

1. Per visualizzare il contenuto della cache del browser web Firefox o di Tor Browser, digitare `about:cache` nella barra degli indirizzi.

browser web e modificato. Ci sarebbe stata una connessione a una casella di posta elettronica Gmail, nonché un altro indirizzo di posta elettronica, questa volta a no-log, poco prima della pubblicazione dei documenti incriminati.

27.1.2 Biscotti

La parola "cookie" deriva dall'inglese "*fortune cookie*", che si riferisce ai dolci che nascondono un messaggio su un piccolo pezzo di carta. Un "cookie" è un piccolo pezzo di testo inviato da un sito web, che il browser dell'utente memorizza e poi invia al sito a ogni visita. Questo è ciò che consente alle applicazioni di webmail o ai siti commerciali, ad esempio, di ricordare che l'utente è stato autenticato con il suo indirizzo e la sua password durante la sessione, o di memorizzare la lingua che si desidera utilizzare.

I cookie consentono inoltre a un sito web di tenere traccia delle persone che lo visitano.

Le agenzie pubblicitarie su Internet inseriscono dei cookie "tracciati" negli annunci che pubblicano sui siti, consentendo loro di seguire i movimenti dell'utente Internet su tutti i siti che pubblicano annunci della stessa agenzia pubblicitaria. In questo modo, possono "raccolgere informazioni sempre più precise su di lei e di conseguenza offrirle pubblicità sempre più mirate".²

Inoltre, quando le pagine web vengono consultate, stabiliscono connessioni a siti pubblicitari, e spesso agli stessi siti, il che aumenta ulteriormente la possibilità di tracciamento da parte di questi siti.

Infine, alcuni cookie hanno una data di scadenza, mentre altri hanno una durata indefinita. - i siti che ce li trasmettono saranno in grado di identificare il nostro browser web per gli anni a venire!

I cookie tradizionali, tuttavia, sono limitati in termini di volume di dati e facili da cancellare da parte di un utente informato. Sono stati quindi "migliorati", ad esempio con la funzione "local web storage" inclusa nello standard HTML5, che consente di memorizzare diversi megabyte di dati nel browser web.³ inclusa nello standard HTML5, che consente di memorizzare diversi megabyte di dati nel browser web.

Altre tecniche di tracciamento prevedono la memorizzazione dello stesso cookie in punti diversi del browser web e la ricreazione di qualsiasi cookie cancellato a ogni visita (partendo dal presupposto che se ogni cookie può essere cancellato, non saranno cancellati tutti allo stesso tempo...⁴).

L'accettazione dell'uso dei cookie ha quindi conseguenze in termini di tracciamento e lascia tracce sul nostro computer e sui server.

27.1.3 Applicazioni lato client

Nell'evoluzione del web e dei suoi browser, è diventato subito chiaro che per avere un minimo di interattività era necessario che parte del codice sorgente del sito web fosse eseguito sul lato client, dal browser web, e non sul server web che ospita il sito.

Questo ha diversi aspetti pratici: dal lato del server web, significa meno lavoro e risparmio di hardware. Sul lato client, l'affichaggio e la funzionalità del sito web vengono accelerati. Inoltre, riduce al minimo il traffico di rete tra il browser e il sito web: non è necessario richiedere un'intera pagina del sito web ogni volta che si fa clic su un piccolo pulsante, ma deve essere trasmesso solo un piccolo frammento della pagina.

1. CNIL, *La publicité ciblée en ligne* [<https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enj-eux-pour-la-protection-des-donnees-personnelles>].

2. Wikipedia, 2020, *Archiviazione web locale* [https://fr.wikipedia.org/wiki/Stockage_web_local].

3. La libreria *evercookie* JavaScript [<https://samy.pl/evercookie/>] è un esempio di questo tipo di tecnologia.

Per abilitare queste funzioni sono state aggiunte delle tecnologie ai browser web: JavaScript e Java sono i principali rappresentanti.

Ma questi piccoli extra hanno anche un costo: come già accennato, ciò significa che la L'autore di un sito è in grado di eseguire il codice di sua scelta sui computer degli altri utenti.

utenti. (che pone una serie di problemi di sicurezza, come abbiamo visto a pagina 32 del primo volume di questa guida). I browser web hanno, naturalmente, hanno protezioni. browser, ma non coprono tutti i rischi, e non sostituiscono la vigilanza degli utenti di Internet.

Tanto più che queste tecnologie presentano talvolta funzionalità che, pur essendo utili, sollevano interrogativi: ad esempio, WebRTC ⁶una tecnologia progettata per integrare le comunicazioni in tempo reale nei browser web, consente l'accesso al microfono e alla telecamera del computer su cui viene utilizzata.

Come abbiamo visto, affidarsi a un software è una scelta complessa. E la pagina 39 dell'esecuzione di tali programmi solleva interrogativi sul potere concesso agli autori dei siti web o delle applicazioni di accedere alle risorse del nostro computer, e le informazioni in esso contenute.

Inoltre, prima di essere eseguiti dal browser web, questi frammenti di codice passano attraverso la rete, spesso senza alcuna autenticazione. Questo lascia possono essere modificati da malintenzionati ben posizionati, proprio come il resto di una pagina web.

pagina web.

Per introdurre malware, ad esempio. È anche possibile

are a pagina

con i dati che questi codici devono elaborare, nel tentativo di deviarne l'uso. Questo

Questo tipo di manipolazione delle pagine web è stata rilevata in passato quando un hotel di New York ha utilizzato un punto di accesso Wi-Fi dotato di un rete dedicata a questo compito⁷.

In definitiva, un browser web moderno ha così tante funzioni che i potenziali avversari hanno un numero considerevole di angoli di attacco.

27.1.4 Nei registri del software

I browser web non sono gli unici programmi che registrano tracce sul computer.

La maggior parte dei programmi software dispone di registri.

²⁹ Ad esempio, i software di messaggistica istantanea spesso registrano la cronologia delle conversazioni;

Anche il software di condivisione di file peer-to-peer (come BitTorrent), tende a ricordare Il software di posta elettronica tiene traccia delle e-mail scaricate di recente, e così via.

- A quanto pare, i colleghi hanno trovato il documento sulla postazione di lavoro di una certa Ana. È stato scaricato dal browser web e modificato.

Nella nostra storia, i poliziotti sono riusciti a rintracciare il documento di Bea nella cronologia del browser web e dell'elaboratore di testi del computer di Ana.

27.2 Sulla scatola: indirizzo hardware della scheda di rete

Abbiamo visto che la scheda di rete utilizzata da ogni computer per connettersi alla rete ha un indirizzo hardware, o indirizzo MAC. Questo indirizzo viene utilizzato da

5. Ciò comporta generalmente la possibilità di accedere al codice del sito web solo per funzioni limitate, eseguendolo in una "sandbox" (Wikipedia, 2014, *Sandbox (sicurezza informatica)* [[https://fr.wikipedia.org/wiki/Sandbox_\(s%C3%A9curit%C3%A9_informatique\)](https://fr.wikipedia.org/wiki/Sandbox_(s%C3%A9curit%C3%A9_informatique))]).
6. In Tor Browser, la funzionalità WebRTC è disattivata.
7. Justin Watt, 2012, *Hotel Wifi JavaScript Injection* [<https://justinsomnia.org/2012/04/hotel-wifi-javascript-injection/>].

per reindirizzare un pacchetto di dati alla scheda di rete giusta, ad esempio quando diversi computer sono collegati alla stessa "scatola".

Normalmente, questo indirizzo non esce dalla rete locale. Tuttavia, di solito ci si collega direttamente alla "scatola" di un provider di servizi Internet - se si utilizza la condivisione della connessione di un telefono, questo fungerà da "scatola". Ogni scheda di rete connessa al box gli assegna un proprio indirizzo hardware.

[pagina
na 29] La maggior parte delle "scatole" conserva un *registro* contenente questi indirizzi hardware, almeno per tutto il tempo in cui sono accese. È difficile conoscere il tipo e la quantità di informazioni contenute in questo registro, nonché la potenziale esistenza di backdoor o falle di sicurezza.⁸ o falle nella sicurezza. In effetti, questi "Le scatole funzionano con il software installato dall'ISP, che mantiene un accesso privilegiato, anche solo per aggiornare il software".

[pagina
22] Ad esempio, Orange ammette di aver raccolto, per 12 mesi, gli indirizzi fisici dei computer collegati ai suoi "box" e gli indirizzi IP associati per la "gestione della diagnostica".⁹ Per noi, il "box" è una vera e propria scatola nera, di cui non abbiamo le chiavi, e che può sapere (e fare) molto sulla rete locale.



PER SAPERNE DI PIÙ...

Se vi piace smanettare, potete sostituire il modem router del vostro ISP con un modem router con OpenWrt¹⁰ o, più semplicemente, aggiungere un router OpenWrt tra il box del vostro ISP e il vostro computer. Sono disponibili router preinstallati e alcune associazioni di ISP forniscono ai loro membri router con solo software libero.¹¹

Inoltre, quando la rete locale prevede l'uso del Wi-Fi, gli indirizzi hardware dei computer che si connettono alla rete sono

"In questo modo le Google Car, nello stesso momento in cui percorrevano migliaia di strade per creare la mappa di Google Street View, hanno approfittato dell'opportunità di registrare la loro "scatola" in Wi-Fi". In questo modo le Google Car, oltre a percorrere migliaia di strade per creare la mappa di Google Street View, hanno colto l'occasione per

"catturare gli indirizzi MAC dei computer circostanti"¹².

D'altra parte, è possibile cambiare temporaneamente l'indirizzo hardware di una scheda di rete, in modo da non essere rintracciati, ad esempio, dai nostri portatili¹³ nei nostri viaggi su .

Vanno citati anche i casi in cui, prima di potersi connettere a Internet, è necessario inserire un *login* e una password nel browser web: questo accade spesso sulle reti Wi-Fi pubbliche, siano esse quelle di una città, di un'istituzione o di un fornitore di servizi Internet (*FreeWifi*, *SFR WiFi pubblico* e altri *Wi-Fi di Bouygues Telecom*). Queste pagine sono note come *portali vincolati*. In questo caso, oltre all'indirizzo hardware della scheda Wi-Fi, l'organizzazione che gestisce il portale riceve l'identità dell'abbonato corrispondente a questi identificatori.

8. Un esempio di backdoor sui router di un produttore [<https://korben.info/backdoor-les-routeurs-d-link.html>].

9. Arancione, 2021, *Gestione della diagnostica* [https://web.archive.org/web/20210510112139/https://assistance.orange.fr/ordinateurs-peripheriques/installer-et-utiliser/la-securite/risques-et-prevention/les-donnees-personnelles/gestion-des-diagnostiques_195036-739979#onglet2].

10. OpenWrt è un sistema operativo gratuito per router. Ecco alcuni motivi per utilizzarlo ser [https://openwrt.org/fr/reasons_to_use_openwrt].

11. Un elenco di modem e router utilizzati dai membri della Federazione FDN: FDN Federation, 2017, *Modem e router* [<https://www.ffdn.org/wiki/doku.php?id=modems-routeurs>].

12. Europa 1 con AFP, 2011, *Street View : la Cnil épingle Google* [<https://www.europe1.fr/eco-nomie/Street-View-la-Cnil-epingle-Google-309338>].

13. Wikipedia, 2014, *Mac Spoofing* [https://fr.wikipedia.org/wiki/Filtrage_par_adresse_MAC#MAC_Spoofing].

27.3 Sui router: intestazioni dei pacchetti

Sul percorso tra un computer e il server a cui ci si vuole connettere, ci sono numerosi router, che rilanciano i pacchetti e li inviano al posto giusto.

pagina
206

Per sapere dove inviare un pacchetto, questi router leggono una sorta di busta su cui è scritta una certa quantità di informazioni; questa "busta" è chiamata *intestazione* del pacchetto.

pagina
202

L'intestazione di un pacchetto contiene molte informazioni necessarie per l'instradamento, tra cui l'indirizzo IP del computer di destinazione e l'IP pubblico del mittente (a cui inviare la risposta). Il router può quindi vedere quale computer vuole parlare con quale computer, così come il postino deve conoscere l'indirizzo del destinatario per inoltrare la posta, nonché l'indirizzo del mittente per un eventuale ritorno.

Le intestazioni contengono anche i numeri di porta di origine e di destinazione, che possono fornire informazioni sull'applicazione utilizzata.

pagina
203

Per svolgere il loro lavoro, i router *devono* leggere queste informazioni; *possono* anche tenerne traccia nei log.

Anche se non hanno alcun motivo per farlo, i router sono in grado di accedere all'interno della busta trasportata, ad esempio al contenuto della pagina web consultata dal navigatore o a quello di una e-mail inviata: si tratta della cosiddetta Deep Packet Inspection (DPI).¹⁴ Si tratta della cosiddetta *Deep Packet Inspection* (DPI).

Il fornitore francese di servizi Internet Orange, ad esempio, include nei suoi contratti di abbonamento una clausola relativa all'utilizzo dei "dati" di traffico.¹⁵

27.4 Sul server

Come i router, il server che ospita il sito visitato ha accesso alle intestazioni dei pacchetti IP e quindi a tutte le informazioni di cui abbiamo appena parlato. In particolare, esamina l'indirizzo IP della "casella" utilizzata dal computer che si collega, per sapere a chi inviare la risposta.

pagina
202

Oltre alle intestazioni IP, che corrispondono al livello di rete della comunicazione, il servizio legge le intestazioni del protocollo applicativo, che ~~capta~~ al livello di applicazione.

pagina
200
pagina
200

Ma il server legge anche il contenuto dei pacchetti stessi: infatti, è il server che deve aprire la busta e leggere la lettera per rispondere. Il software del server interpreta quindi la lettera ricevuta, che è scritta utilizzando il protocollo dell'applicazione, per fornire la risposta appropriata.

Tuttavia, molti protocolli applicativi contengono anche informazioni che identificano il computer collegato, come vedremo in dettaglio qui.

Come i computer client, anche i server dispongono di registri di sistema, di cui parleremo più diffusamente nella prossima sezione.

pagina
225

27.4.1 Intestazioni HTTP

Quando un browser web richiede una pagina web, include nella richiesta il nome del software, il suo numero di versione, il sistema operativo utilizzato e la lingua in cui è configurato.

14. Wikipedia, 2021, *Ispezione profonda dei pacchetti* [https://fr.wikipedia.org/wiki/Deep_packet_inspection].

15. Martin Untersinger, 2016, *Fin de l'Internet illimité : ça se précise chez Orange, qui dément* [<https://www.nouvelobs.com/rue89/rue89-internet/20121011.RUE3086/fin-de-l-internet-illimite-ca-se-precise-chez-orange-qui-dement.html>].

Ecco una richiesta inviata dal browser web Firefox:

```
GET / index. php HTTP/2
Host:
Uesxearmp-leA.geonrtg: Mozilla /5.0 ( X11 ; Linux x86_64 ; rv:91.5) Gecko
s/20100F1i0r1efox
/A c c91.5 ept: text/ html, application/ xhtml+xml, application/ xml;q=0.9,
simage/webp,*/*;
qA c c=0.8 ept - Lingua: fr- FR, en;q=0.5
Accept - Encoding: gzip, deflate, br
Referer: https:// duckduckgo. com/
```

Cookie: donazione - identificatore:
dd634367a6b4485ba288197bd92745b4

Per prima cosa vediamo un comando contenente il nome della pagina richiesta (/index.php), il nome del dominio corrispondente (example.org), seguito da un'intestazione contenente, tra le altre cose, il nome e la versione del browser web (Mozilla/5.0 (X11; Linux x86_64; rv:91.5) Gecko/20100101 Firefox/91.5) nonché il sistema operativo utilizzato (Linux x86_64), le lingue supportate (fr-FR per il francese dalla Francia, en per l'inglese), la pagina in cui si trovava il link che il navigatore ha seguito per arrivare alla pagina richiesta (https://duckduckgo.com/) e il cookie di sessione (donation-identifier: dd634367a6b4485ba288197bd92745b4).

pagina
214



PER SAPERNE DI PIÙ...

Nel browser web Firefox, possiamo affiggere in pochi clic le intestazioni delle nostre richieste :

- fare clic in  alto a destra ;
- selezionare *Strumenti aggiuntivi*, quindi *Strumenti di sviluppo web*, quindi selezionare la *rete* scheda.

Si apre un nuovo pannello. Quando una pagina viene caricata, per ogni richiesta viene visualizzata una riga. Selezionandone una - la prima, ad esempio, che corrisponde al caricamento della pagina stessa - se ne visualizzano le intestazioni nel pannello di destra, in una scheda denominata *Intestazioni*.

Queste informazioni vengono utilizzate dal server web, che adatta la sua risposta di conseguenza: è così che, ad esempio, un sito disponibile in diverse lingue viene visualizzato nella nostra lingua senza che noi lo specifichiamo.

Ma queste informazioni, come tutto ciò che passa attraverso il server, sono accessibili anche alle persone che si occupano della manutenzione del server: gli amministratori... e la loro gerarchia. In generale, i server conservano anche queste informazioni nei log, per periodi più o meno lunghi, in particolare a fini statistici e per facilitare la diagnostica in caso di guasto. Aggiungono alle intestazioni l'indirizzo IP di origine, la data e l'ora. Ecco una riga di log registrata per la nostra richiesta (l'indirizzo IP originale è all'inizio: 203.0.113.42):

```
203.0.113.42 - - [22/gen /2022:00:00:00 +0100] " GET / index. php
sHTTP /2" 200 2131 " https:// duckduckgo. com/" " Mozilla /5.0
X11 ; sLinux x86_64 ; rv:91.5) Gecko /20100101 Firefox /91.5)
Gseck /20100101 Firefox
```

o

/91.5"

pagina
225

27.4.2 **Intestazioni della posta**

Ogni e-mail contiene un'intestazione che, nonostante il nome, non ha nulla in comune con l'intestazione di una pagina web. Questa intestazione contiene informazioni sui dati contenuti nell'e-mail: un altro esempio di metadati, il "don-

sui dati". Raramente il nostro software di posta elettronica lo mostra nella sua interezza, ma è comunque presente. Spesso contiene molte informazioni sul mittente, molto più del semplice indirizzo e-mail.

Nell'esempio seguente, possiamo leggere l'indirizzo IP pubblico, cioè quello visibile su Internet, del computer utilizzato per inviare l'e-mail (203.0.113.98), che ci dice dove si trovava il mittente in quel momento, l'indirizzo IP del suo computer all'interno della sua rete locale (192.168.0.10), il software di posta elettronica utilizzato (Thunderbird/91.5.0) o anche il suo sistema operativo (Mac OS X 11).

pagina

205

```
Ritorno - Percorso: <bea@fai.net >
Consegnato - A: ana@example.org
Ricevuto: da smtp. fai. net ( smtp. fai. net [198.51.100.67]) da mail.
example.org ( Postfix) con ESMTTP id 0123456789 per
<ana@example.org >; Sat , 22 Jan 2022 20:00:00 +0100 ( CET)
Ricevuto: da [192.168.0.10] ( paris. abo. fai. net [203.0.113.98])
da smtp. fai. net ( Postfix) con ESMTTP id ABCDEF1234 ;
Sat , 22 Jan 2022 19:59:49 +0100 ( CET)
Messaggio - ID: <CB0ABB91 .17 B7F@fai.net
> Data: Sat , 22 Jan 2022 19:59:45 +0100
Da: Bea <bea@fai.net >
Utente - Agente: Mozilla /5.0 ( Macintosh; Intel Mac OS X 11;
rv:91.5) Gecko /20100101 Thunderbird /91.5.0
MIME - Versione: 1.0
A: Ana <ana@example.org > Oggetto:
Ci vediamo martedì
Contenuto - Tipo: text/ plain; charset=iso -8859 -1
Contenuto - Lunghezza: 22536
Linee: 543
```

A volte queste intestazioni contengono anche l'ID dell'abbonato presso il suo provider di servizi di posta o il nome della sua macchina.¹⁶

Come questi pochi esempi comuni, praticamente tutti gli en-

vedere non solo le informazioni sul contenuto, ma anche i metadati nella loro pagina [protocole](#).

27.5 Le tracce che lasciamo dietro di noi

Non si tratta solo delle tracce lasciate dal funzionamento delle reti: ci sono anche quelle che lasciamo noi stessi, più o meno volontariamente, ad esempio inserendo informazioni sui siti web o semplicemente collegandoci ai servizi.

Cercare di controllare le tracce che lasciamo sulle reti significa quindi anche riflettere sull'uso che facciamo dei servizi offerti da Internet e sui dati che affidiamo loro, argomenti che tratteremo in modo più approfondito nelle prossime sezioni.

¹⁶ Nella maggior parte dei casi, questo si trova nella linea `Received` della prima macchina o nella linea `Message-ID`. Ma altri software o servizi di messaggistica aggiungono altre righe più specifiche.

Monitoraggio e controllo di comunicazioni

Al di là delle tracce lasciate dal funzionamento stesso delle reti in generale e di Internet in particolare, è possibile "ascoltare" le nostre attività su Internet a diversi livelli.

Sempre più spesso, le organizzazioni che gestiscono parti della rete (cavi, server, ecc.) sono persino obbligate per legge a conservare una certa quantità di dati su ciò che accade sulle loro macchine, in base alle leggi sulla *conservazione dei dati*.

pagina
224

28.1 Chi riuole i dati?

Sono diverse le persone e le organizzazioni che possono avere occhi indiscreti sugli scambi in Internet. Genitori un po' troppo curiosi, siti web alla ricerca di clienti su cui puntare, multinazionali come Microsoft, la polizia di Saint-Tropez o la *National Security Agency* statunitense...

Come nel caso dei bug sui personal computer, le varie entità coinvolte non lavorano necessariamente insieme, né formano un insieme coerente. Se i curiosi sono troppo vari per pretendere di stilare un elenco esaustivo degli interessi in gioco, possiamo comunque descrivere alcune delle motivazioni più comuni.

28.1.1 Aziende alla ricerca di profili da rivendere

"Decidete di prenotare un biglietto aereo per New York su Internet. Due giorni dopo, mentre leggete il vostro giornale online, una pubblicità vi propone un'offerta interessante per il noleggio di un'auto a New York. Non si tratta di una semplice coincidenza: è un meccanismo pubblicitario mirato, come quello che si sta sviluppando sempre di più su Internet".¹

La pubblicità è una delle principali fonti di guadagno per le aziende che forniscono servizi "gratuiti" su Internet: caselle di posta elettronica, motori di ricerca, social media, ecc. Ma dal punto di vista dell'inserzionista, la qualità e quindi il prezzo degli spazi pubblicitari online dipende dall'interesse degli utenti di Internet. Tuttavia, dal punto di vista degli inserzionisti, la qualità e quindi il prezzo degli spazi pubblicitari online dipende dall'interesse che gli utenti di Internet mostreranno per gli annunci.

Ecco perché i dati personali valgono oro. Interessi, sesso, età, ecc. Questo è il tipo di informazioni che ci permette di presentare annunci ai quali gli utenti di Internet rispondono con maggiore probabilità. È in questo modo che Google incrocia i risultati dei suoi

1. CNIL, 2009, *Pubblicità online mirata* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf].

attività personali ² su tutti i suoi servizi, come il motore di ricerca, i video di YouTube guardati o le foto di Google Foto, per pubblicare annunci mirati su altre sue applicazioni, come Gmail³.

Inoltre, ogni sito visitato è un altro "centro di interesse". Quando si sommano tutte queste informazioni, emerge un intero profilo ⁴. Un piccolo software consente di vedere quali cookie vengono scaricati sul computer a ogni pagina visitata. Se si inizia visitando allocine.fr, quattro agenzie pubblicitarie registrano la visita. Se poi passa al sito *Le Monde*, ne saranno a conoscenza quattro agenzie pubblicitarie, due delle quali erano già presenti sul sito AlloCiné. Sanno quindi che l'utente ha visitato questi due siti e possono incrociare questi due centri di interesse. Visitando successivamente altri due siti (Gmail e Dailymotion), un totale di ventuno agenzie pubblicitarie è venuto a conoscenza della visita del navigatore. Ognuna di queste visite includeva XiTi e Google-Analytics. Di conseguenza, il più grande motore di ricerca del mondo è stato informato di tutti i siti visitati e può ora implementare una pubblicità mirata.

I social media sono particolarmente adatti a ottenere dati personali direttamente dagli utenti. Su Facebook, ad esempio, un'azienda può indirizzare un annuncio pubblicitario a ragazzi tra i 13 e i 15 anni che vivono a Birmingham, in Inghilterra, e che hanno come centro di interesse il "bere". Inoltre, Facebook indica che il target prescelto comprende circa un centinaio di persone ⁵. In questo modo, Facebook sfrutta i dati raccolti dai suoi iscritti per fornire pubblicità altamente mirate.

⁶. La pubblicità mirata è, infatti, "uno dei motivi per cui gli operatori di Internet hanno diversificato i loro servizi e le loro attività, al fine di raccogliere sempre più informazioni sul comportamento degli utenti su Internet". "Ad esempio, Google fornisce servizi di ricerca. Ha acquistato aziende pubblicitarie come DoubleClick. Ha [...] lanciato un servizio di Google Suggest, integrato nel suo browser Chrome, che invia a Google tutte le pagine web visitate dagli utenti di Internet, anche quando questi ultimi non vi hanno acceduto *tramite* il motore di ricerca, ecc."⁷

Per dare un'idea della posta in gioco, Google ha acquistato Doubleclick per 3,1 miliardi di dollari. ⁸

L'accumulo e l'elaborazione dei dati consente inoltre a Google di ordinare e adattare i risultati ai presunti interessi dell'utente di Internet. Così, per una ricerca identica, due persone con profili diversi non otterranno lo stesso risultato, con l'effetto di rafforzare gli interessi di ciascuno.

2. Julien Lausson, 2017, *Why Google won't stop targeted advertising and scanning your emails on Gmail*, Numerama [<https://www.numerama.com/tech/270293-pourquoi-google-ne-va-pas-arreter-la-publicite-ciblee-et-le-scan-de-vos-mails-sur-gmail.html>]

3. "Quando si apre Gmail, si vedono annunci selezionati in base alla loro utilità e pertinenza. Il processo di selezione e affissione di annunci personalizzati in Gmail è completamente automatizzato. Questi annunci vengono presentati all'utente in base alla sua attività online durante l'accesso a Google. Non analizziamo né leggiamo i vostri messaggi Gmail per scegliere quali annunci vi vengono mostrati". *Google, 2021, Come funzionano gli annunci in Gmail* [<https://support.google.com/mail/answer/6603?hl=fr>].

4. Data Gueule, 2014, *Big data: dati, dati, datemi!* - #DATAGUEULE 15 [<http://peertube.datagueule.tv/w/etMw3qxMsdZHcvhFzekvie>].

5. Un'interfaccia simile è disponibile pubblicamente e aiuta a rispondere ad alcune domande inquietanti: Tom Scott, 2014, *Actual Facebook Graph Searches* [<https://actualfacebookgraphsearches.tumblr.com/>].

6. CNIL, 2009, *Publicità online mirata* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf], pag. 13.

7. CNIL, 2009, *Publicità online mirata* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf], pag. 4.

8. *Le Monde*, 2007, *Google acquista DoubleClick per 3,1 miliardi di dollari* [https://www.lemonde.fr/technologies/article/2007/04/14/google-rachete-doubleclick-pour-3-1-milliards-de-dollars_896316_651865.html].

interessi e convinzioni. Questo è ciò che alcuni chiamano "l'individualizzazione di Internet".⁹

Oltre a essere tematicamente mirata, la pubblicità lo è anche geograficamente: grazie al GPS integrato nei terminali mobili come gli smartphone, ma anche grazie all'indirizzo IP e alle reti Wi-Fi "visibili" nel raggio d'azione del laptop o del telefono.¹⁰ In questo modo è possibile, ad esempio, visualizzare pubblicità di negozi situati nelle vicinanze dell'abbonato.

Gli interessi economici spingono i fornitori di servizi Internet a raccogliere profili il più possibile precisi degli utenti di Internet per poi vendere, direttamente o indirettamente, spazi pubblicitari mirati.

Una volta raccolte queste informazioni, le aziende saranno in grado di rispondere alle richieste della polizia. Tutti i grandi fornitori di contenuti hanno uffici dedicati alla risposta alle richieste, e quindi hanno moduli, procedure, ecc. scritti per i poliziotti, che spiegano il modo migliore per richiedere informazioni.¹¹

28.1.2 Aziende e governi che cercano di proteggere i propri interessi

Altre aziende si interessano a ciò che accade su Internet per proteggere i propri interessi. Si va dalla lotta dell'industria audiovisiva contro il download illegale, all'osservazione della tecnologia: le aziende osservano e analizzano centinaia di fonti (siti di notizie, database di registrazione di brevetti, blog di esperti, ecc.) in tempo reale e su base automatizzata, per tenersi al passo con gli ultimi progressi tecnologici e rimanere il più possibile competitive.

Le aziende non sono le uniche a controllare Internet. I governi, dal sistema giudiziario ai servizi segreti e alle forze di polizia, sono certamente i più curiosi.

Sempre più Paesi stanno introducendo leggi che consentono di identificare gli autori di qualsiasi informazione che circola su Internet.¹²

Ma si va anche oltre. Le agenzie di intelligence e gli altri servizi segreti non si accontentano più di spiare pochi gruppi o individui che considerano obiettivi. Ai margini della legalità, l'NSA, l'agenzia di intelligence statunitense, raccoglie "tutti i tipi di dati sulle persone - pensiamo che si tratti di milioni di persone".¹³ Tra i suoi obiettivi: "esaminare "virtualmente tutto ciò che un individuo fa su Internet""¹⁴ e stabilire un *grafo sociale*, cioè "la rete di connessioni e relazioni tra le persone".¹⁵ "In generale, analizzano reti situate a due gradi di separazione dall'obiettivo". Altrimenti

9. Xavier de la Porte, 2011, *Le risque de l'individualisation de l'Internet*, InternetActu.net, Fondazione. [\[https://web.archive.org/web/20210413221428/https://www.internetactu.net/2011/06/13/le-risque-de-lindividualisation-de-linternet/\]](https://web.archive.org/web/20210413221428/https://www.internetactu.net/2011/06/13/le-risque-de-lindividualisation-de-linternet/).

10. Audenard, 2013, *Bornes wifi et smartphones dans les magasins*, blogs/sécurité, Orange Business [\[https://www.orange-business.com/fr/blogs/securite/mobilite/souriez-vous-etes-pistes-merciaux-bornes-wifi-des-magasins\]](https://www.orange-business.com/fr/blogs/securite/mobilite/souriez-vous-etes-pistes-merciaux-bornes-wifi-des-magasins).

11. Negli ultimi anni sono trapelate diverse versioni della guida pubblicata da Facebook [\[https://publicintelligence.net/facebook-law-enforcement-subpoena-guides/\]](https://publicintelligence.net/facebook-law-enforcement-subpoena-guides/). Diverse altre guide simili (non tutte accurate) sono disponibili su [cryptome.org](https://cryptome.org/isp-spy/online-spying.htm) [\[https://cryptome.org/isp-spy/online-spying.htm\]](https://cryptome.org/isp-spy/online-spying.htm).

12. Begeek, 2013, *Facebook pubblica il suo primo rapporto internazionale sulle richieste governative* [\[https://www.begeek.fr/facebook-publie-premier-rapport-international-demandes-gouvernementales-102351\]](https://www.begeek.fr/facebook-publie-premier-rapport-international-demandes-gouvernementales-102351).

13. Bruce Schneier, citato in Guillaud, 2013, *Lutter contre la surveillance: armer les contre-pouvoirs*, Internet Act [\[https://web.archive.org/web/20220126013621/https://www.internetactu.net/2013/06/13/lutter-contre-la-surveillance-arter-les-contre-pouvoirs/\]](https://web.archive.org/web/20220126013621/https://www.internetactu.net/2013/06/13/lutter-contre-la-surveillance-arter-les-contre-pouvoirs/).

14. Maxime Vaudano, 2013, *Plongée dans la "pieuvre" de la cybersurveillance de la NSA*, Le Monde.fr [\[https://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html\]](https://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html).

15. Pisani, 2007, *Facebook/5: la ricetta* [\[https://www.francispisani.net/facebook5-la-recette/\]](https://www.francispisani.net/facebook5-la-recette/).

dice, la NSA spia anche coloro che comunicano con coloro che comunicano con coloro che vengono spiati".¹⁶.

I servizi segreti francesi dispongono oggi di un arsenale di leggi che consente loro di effettuare analisi su tutto il traffico Internet o su individui mirati in piena legalità, in Francia o all'estero.¹⁷ o all'estero.¹⁸.

28.2 Registri e conservazione dei dati

La maggior parte delle organizzazioni che forniscono servizi su Internet (connessione, hosting di siti, ecc.) conservano più o meno traccia di ciò che passa attraverso le loro macchine, sotto forma di registri di connessione: chi ha fatto cosa, quando. Chiamiamo questi *registri*.

Storicamente, questi registri hanno uno scopo tecnico: vengono utilizzati dai manutentori dei server per diagnosticare e risolvere i problemi. Tuttavia, possono anche essere molto utili per raccogliere dati sugli utenti di questi server.

28.2.1 Leggi sulla conservazione dei dati

Nella maggior parte dei Paesi occidentali, i fornitori di servizi Internet sono ora obbligati per legge a conservare i loro log per un certo periodo di tempo, per poter rispondere alle richieste.

Le leggi che regolano la conservazione dei dati definiscono più o meno chiaramente le informazioni che devono essere conservate in questi registri. Il concetto di fornitore di servizi Internet può quindi essere inteso in senso piuttosto ampio.¹⁹ Un cybercafé è un fornitore di servizi Internet che fornisce *anche* una macchina per accedere alla rete.

Al di là degli obblighi di legge, molti fornitori di servizi Internet conservano una quantità variabile di informazioni sugli utenti che utilizzano i loro servizi, in particolare per la pubblicità mirata. I GAFAM come Google, Amazon e Facebook sono particolarmente noti per questo. Poiché questo "modello di fornitura di servizi ad-supported" è praticamente diventato la norma.²⁰ È lecito pensare che molti altri stiano facendo lo stesso, in modo più discreto.

Nel Regno Unito, un Internet Service Provider (ISP) ha suscitato polemiche quando è emerso che stava tenendo traccia di tutte le pagine web visitate dai suoi abbonati per testare una tecnologia di profilazione progettata per "offrire" "pubblicità comportamentale".

²¹ ²².

Il server che ospita il contenuto utilizzato (pagina web, casella di posta elettronica, ecc.) e il provider di servizi Internet sono particolarmente adatti a disporre delle informazioni necessarie per identificare l'autore di una richiesta di connessione. In Francia, sono particolarmente colpiti dalle leggi sulla conservazione dei dati.

16. Manach, 2013, *Pourquoi la NSA espionne aussi votre papa (#oupas)*, Bug Brother [<https://bugbrother.blog.lemonde.fr/2013/06/30/pourquoi-la-nsa-espionne-aussi-votre-papa-oupas/>].

17. Légifrance, *Code de la sécurité intérieure*, articoli L851-2 e L851-3 [https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000030935576].

18. Légifrance, *Code de la sécurité intérieure*, articolo L854-1 [https://www.legifrance.gouv.fr/cod/es/article_lc/LEGIARTI000037200982/].

19. CNIL, 2010, *Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations?* [<https://www.cnil.fr/fr/conservation-des-donnees-de-trafic-hot-spots-wi-fi-cybercafes-employeurs-what-obligations>].

20. CNIL, 2009, *Publicité online mirata* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf], pag. 4.

21. CNIL, 2009, *Publicité online mirata* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf], pag. 17.

22. Arnaud Devillard, 2009, *Affaire Phorm : Bruxelles demande des comptes au Royaume-Uni* [<https://www.01net.com/actualites/affaire-phorm-bruxelles-demande-des-comptes-au-royaume-uni-501173.html>].

28.2.2 Registri tenuti dai provider di hosting

Abbiamo visto che il server che ospita un servizio (come un sito web, una casella di posta elettronica o una stanza di messaggistica istantanea) ha accesso a una grande quantità di dati.

pagina
217

In Francia, l'articolo 6 della Legge per la fiducia nell'economia digitale (LCEN)²³ (LCEN), che obbliga gli host di contenuti pubblici a conservare "i dati che possono consentire l'identificazione" di "qualsiasi persona che abbia contribuito alla creazione di contenuti pubblicati online"; ad esempio, scrivere su un sito di social media, un blog o un sito di media partecipativi, o postare su una mailing list pubblica.²⁴

Per i contenuti che costituiscono corrispondenza privata, l'articolo L34-1 del Codice delle Poste e delle Comunicazioni Elettroniche (CPCE) impone lo stesso obbligo per la scrittura di un'e-mail o l'invio di un messaggio istantaneo.²⁵ (CPCE) che impone lo stesso obbligo per la scrittura di un'e-mail o l'invio di un messaggio istantaneo, ad esempio. In concreto, ciò significa conservare per un anno tutti gli identificativi o pseudonimi forniti dall'autore, ma soprattutto l'indirizzo IP alla fonte della connessione ogni volta che il contenuto viene modificato.²⁶ Una richiesta all'Internet Service Provider (ISP) che fornisce questo indirizzo IP può quindi generalmente far risalire al proprietario della connessione utilizzata.

pagina
202

Inoltre, la legge sulla programmazione militare²⁷ promulgata a fine dicembre 2013, consente di richiedere queste stesse informazioni, in tempo reale, per motivi diversi: attacchi terroristici, attacchi informatici, attacchi al potenziale scientifico e tecnico, criminalità organizzata, ecc.

È questo obbligo di conservazione dei dati che consente alla polizia, nella nostra storia introduttiva, di ottenere informazioni dalle organizzazioni che ospitano gli indirizzi e-mail incriminati:

pagina
194

- *Chiederemo a Gmail e no-log informazioni su questi indirizzi e-mail. Allora probabilmente avremo qualcosa su cui basarci, o almeno qualcosa per fare le domande giuste!*

I provider di hosting possono essere più o meno collaborativi nel verificare la legalità delle citazioni inviate loro dalla polizia e nel rispondere ad esse.

23. Légifrance, 2022, Article 6 de la loi n° 2004575 du 21 juin 2004 pour la confiance dans l'économie numérique [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000045292730].

24. Légifrance, 2021, Decreto n. 2021-1362 del 20 ottobre 2021 sulla conservazione dei dati. consentire l'identificazione di qualsiasi persona che abbia contribuito alla creazione di contenuti pubblicati online [https://www.legifrance.gouv.fr/loda/id/JORFTEXT000044228912].

25. Légifrance, 2013, Articolo L34-1 - codice delle poste e delle comunicazioni elettroniche [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000028345210/].

26. "Le persone fisiche o giuridiche che forniscono, anche a titolo gratuito, per i dis- posizione del pubblico mediante servizi di comunicazione al pubblico on line, la memorizzazione di segnali, scritti, immagini, suoni o messaggi di qualsiasi natura forniti dai destinatari di questi servizi" (LCEN, op. cit., art. 6 comma 1.2 [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000045292730]), cioè le società di hosting, sono obbligate a conservare per un anno e per ogni operazione di creazione, modifica o cancellazione di contenuti: " a) l'identificatore del

connessione all'origine della comunicazione; b) i tipi di protocolli utilizzati per connettersi al servizio e trasferire contenuti" (articolo 5 del Decreto n. 2021-1362 del 20 ottobre 2021, op. cit. [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230063]).

Ma anche: " a) L'identificatore assegnato dal sistema informativo al contenuto, all'oggetto dell'opera, all'oggetto dell'operazione.

b) la natura dell'operazione; c) la data e l'ora dell'operazione; d) l'identificativo utilizzato dall'autore dell'operazione quando fornito dall'autore" (articolo 6 del decreto n. 2021-1362 del 20 ottobre 2021, op. cit. [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230065]), visto

l'articolo 1 del decreto n. 2021-1363 del 20 ottobre 2021, che ordina, in considerazione della minaccia grave e attuale alla sicurezza nazionale, la conservazione per un periodo di un anno di alcune categorie di dati di connessione [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230065]. dati di connessione

[https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044

231713].

27. Légifrance, 2014, Legge n. 2013-1168 del 18 dicembre 2013 sulla programmazione militare. per gli anni dal 2014 al 2019 e varie disposizioni riguardanti la difesa e la sicurezza nazionale [https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id].

alcuni rispondono ad una semplice e-mail della polizia, mentre altri aspettano una lettera firmata da un giudice²⁸ o addirittura non rispondono alle richieste²⁹.

Non solo le persone che hanno accesso al server possono collaborare volontariamente con i poliziotti, ma anche gli avversari possono, come nel caso di un computer personale, introdursi e spiare ciò che accade lì utilizzando scappatoie, senza passare per la fase di requisizione. Avranno quindi accesso a tutti i dati memorizzati sul server, compresi i log.

Ma non sempre il server conosce la vera identità degli utenti di Internet che si collegano ad esso: in genere, tutto ciò che può fornire è un indirizzo IP.

È qui che entra in gioco l'ISP.

28.2.3 Registri tenuti dai fornitori di servizi Internet

[pagina
205

Abbiamo visto che l'accesso a Internet avviene tramite un Internet Service Provider (ISP). Questo ISP è generalmente un'azienda che fornisce una "scatola" collegata a Internet. Ma può anche essere un'associazione o un'istituzione pubblica (un'università, ad esempio, quando si utilizzano le loro aule informatiche). Anche gli ISP sono soggetti alle leggi sulla conservazione dei dati.

All'interno dell'Unione Europea, una direttiva obbliga i fornitori di servizi Internet a tenere traccia di chi si è collegato, quando e da dove.³⁰ In pratica, ciò significa registrare quale indirizzo IP è stato assegnato a quale abbonato per quale periodo di tempo.³¹ Le istituzioni che forniscono accesso a Internet, come le biblioteche e le università, fanno lo stesso: in genere, si accede con un nome utente e una password. In questo modo è possibile sapere chi ha utilizzato quale postazione di lavoro in quale momento. La direttiva europea stabilisce che questi dati devono essere conservati per un periodo compreso tra 6 mesi e 2 anni. In Francia, il periodo legale è di un anno.³²

Controintuitivamente, questo obbligo si applica a tutti i luoghi che offrono accesso a Internet al pubblico, sia a pagamento che gratuitamente, anche se gli utenti non sono identificati. I gestori di bar che hanno ignorato questa disposizione hanno pagato il prezzo e si sono ritrovati in custodia di polizia per aver offerto il Wi-Fi ai loro clienti senza conservare i dati di connessione.³³

28. Globenet, 2014, *No-log, log e legge* [<https://www.globenet.org/No-log-les-logs-et-la-loi.html>].

29. "Va notato che i server che ospitano i siti del network Indymedia, domiciliati negli Stati Uniti a Seattle, rifiutano sistematicamente di rivelare alle autorità i log di connessione dei computer che consultano questi siti o che pubblicano un contributo, rendendo così non identificabili gli autori dei contributi" (fascicolo d'inchiesta giudiziaria citato da Anonymes, 2010, *Analyse d'un dossier antiterroriste* [https://infokiosques.net/spip.php?page=lire&id_article=789]).

30. Parlamento europeo e Consiglio, 2006, *Direttiva 2006/24/CE del Parlamento europeo e del Consiglio. Consiglio del 15 marzo 2006 sulla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche. e che modifica la direttiva 2002/58/CE* [<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>], nota come "Data Retention".

31. "Persone la cui attività consiste nel fornire accesso a servizi di comunicazione pubblici". en ligne" (LCEN, *op. cit.*), cioè gli ISP, sono tenuti a conservare per un anno: "a) l'identificativo della connessione; b) l'identificativo assegnato da questi soggetti all'abbonato; c) l'indirizzo IP assegnato alla fonte della connessione e la relativa porta" (articolo 5 del decreto n. 2021-1362 del 20 ottobre 2021, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230063]).

Ma anche: "a) La data e l'ora di inizio e fine della connessione; b) Le caratteristiche della connessione della linea dell'abbonato" (articolo 6 del decreto n. 2021-1362 del 20 ottobre 2021, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230065]), alla luce dell'articolo 1 del decreto n. 2021-1363 del 20 ottobre 2021, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEG IAR TI000044231713]).

32. Légifrance, 2021, Décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne [<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044228912>].

33. Sputnik France, 2020, *Les gérants de bars en garde-a-vue pour avoir-offert-du-wifi-a-leurs-clients-a-grenoble/* [https://fr.sputniknews.com/faits_divers/202009291044498557-des-gerants-de-bars-en-garde-a-vue-pour-avoir-offert-du-wifi-a-leurs-clients-a-grenoble/].

Inoltre, gli ISP e le società di hosting francesi sono tenuti a conservare "le informazioni relative all'identità civile dell'utente" per i cinque anni successivi alla scadenza del contratto dell'utente.³⁴ Devono inoltre conservare "altre informazioni fornite dall'utente al momento della sottoscrizione di un contratto o della creazione di un account".³⁵ e

"informazioni di pagamento [...] per ogni operazione di pagamento".³⁶ per un periodo di un anno dalla fine della validità del contratto o dalla chiusura del conto.

L'obiettivo delle leggi sulla conservazione dei dati è quindi quello di rendere facile per le autorità associare un nome a qualsiasi azione compiuta su Internet.

I poliziotti che indagano su un articolo pubblicato su un blog, ad esempio, possono chiedere al server che ospita il blog l'indirizzo IP della persona che ha pubblicato l'articolo, insieme alla data e all'ora corrispondenti. Una volta ottenute queste informazioni, possono chiedere all'ISP responsabile dell'indirizzo IP a chi era assegnato al momento dell'incidente.

- *Che storia! Ma cosa ha a che fare con i nostri uffici?*
- *È anche per questo che la sto chiamando. Affermano di avere tutte le prove che questi documenti sono stati pubblicati dai vostri uffici. Ho detto loro che non ero io, che non sapevo di cosa stessero parlando.*

È proprio di questo che stiamo parlando quando, nel nostro articolo all'inizio, la polizia sostiene, con prove a sostegno, che gli estratti conto sono stati spediti dagli uffici di Rue Jaurès. Per prima cosa hanno ottenuto dagli host del sito l'indirizzo IP della connessione responsabile della pubblicazione dei documenti incriminati. Questo primo passo permette di determinare da quale "casella" proviene la connessione. Una richiesta all'Internet Service Provider (ISP) rivela il nome dell'abbonato - un indirizzo bonus - attraverso il suo contratto, associato all'indirizzo IP.

pagina
194

28.2.4 VPN, una storia di fiducia

La VPN (*Virtual Private Network*) è un sistema inizialmente creato per condividere una rete privata tra diversi siti.³⁷ Crea un collegamento diretto tra il nostro computer e il server del provider VPN scelto. Una VPN consente di cambiare gli indirizzi IP della connessione a Internet: per i router e i server a cui ci si connette, la connessione non proviene più dalla "scatola" dell'ISP, ma dal server VPN. Questo può aiutare a bypassare alcuni tipi di censura.

34. "1° Il cognome e il nome, la data e il luogo di nascita o la ragione sociale, nonché il cognome e il nome, la data e il luogo di nascita della persona che agisce per suo conto quando il conto è aperto a nome di una persona giuridica; 2° L'indirizzo o gli indirizzi postali associati; 3° L'indirizzo o gli indirizzi di posta elettronica dell'utente e dell'eventuale conto o dei conti associati; 4° Il numero o i numeri di telefono." ([Articolo 2 del decreto n. 2021-1362 del 20 ottobre 2021 sulla conservazione dei dati personali](#)).

https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230081).

35. "1° L'identificatore utilizzato; 2° Lo pseudonimo o gli pseudonimi utilizzati; 3° I dati destinati a permettere all'utente di verificare o modificare la propria password, se necessario mediante un sistema di identificazione dell'utente doppio, nella loro ultima versione aggiornata." ([Articolo 3 del Decreto n. 2021-1362 del 20 ottobre, 2021 sulla conservazione dei dati](#), *op. cit.* [

https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230083]).

36. "1° Tipo di pagamento utilizzato; 2° Riferimento del pagamento; 3° Importo; 4° Data", il tempo e il luogo in caso di transazione fisica". ([Articolo 4 del Decreto n. 2021-1362 del 20 ottobre 2021 sulla conservazione dei dati](#), *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230085]).

37. Alcune aziende utilizzano l'archiviazione condivisa dei documenti sulla propria rete locale. Il La VPN consente una connessione crittografata e autenticata alla rete locale dell'azienda per l'accesso allo storage condiviso.

Alcuni servizi VPN trasmettono il traffico di molte persone con pochi indirizzi IP. In questo modo è possibile confondersi con la massa di persone che utilizzano il servizio VPN e complicare l'identificazione.

I dati possono essere crittografati per l'ISP, ma rimangono visibili al provider VPN. Gli amministratori della VPN hanno sempre accesso sia all'origine che alla destinazione delle comunicazioni. L'utilizzo di una VPN sposta semplicemente il problema dalla fiducia nell'ISP alla fiducia nella VPN.

Sebbene possa essere preso in considerazione in alcuni modelli di minaccia, l'uso delle VPN non viene sviluppato in questa guida. Se volete confondervi nella massa degli utenti di Internet ed essere facilmente identificabili, senza dipendere dalla fiducia in un singolo intermediario, è più sicuro usare Tor, come suggerito di seguito.

28.2.5 Richiesta

In Francia, quando la polizia vuole accedere ai registri previsti dalle leggi sulla conservazione dei dati, deve ricorrere a una *requisizione giudiziaria*: una richiesta ufficiale che obbliga le persone che amministrano un server a fornire le informazioni richieste... o a disobbedire. Queste requisizioni dovrebbero specificare le informazioni richieste ed essere legalmente fondate. Ma non sempre lo sono, e i fornitori di servizi Internet a volte forniscono informazioni che la legge non li obbliga a fornire.

Ecco un estratto di una richiesta ricevuta da un host di posta elettronica francese. L'indirizzo di posta elettronica dell'account in questione è stato anonimizzato sostituendo l'identificativo con l'*indirizzo*. L'ortografia non è stata modificata.



REQUISIZIONE GIUDIZIARIA

Tenente di polizia in servizio presso la B.R.D.P.

Preghiamo e, se necessario, chiediamo :

Monsieur le président de l'association GLOBENET 21ter, rue Voltaire 75011 Paris

allo scopo di :

Informazioni sull'indirizzo e-mail `adresse@no-log.org`

- Fornirci l'**identità completa** (cognome, nome, data di nascita, parentela) e le **coordinate** (postali, telefoniche, elettroniche e bancarie) del **titolare del conto**.
- Fornite gli ultimi TRE dati di connessione (indirizzo IP, data, ora e fuso orario) utilizzati per **consultare, leggere o inviare messaggi** con il suddetto indirizzo (Pop, Imap o Webmail).
- Indicare se è **attivo un reindirizzamento** su questa casella di posta e fornire l'e-mail di destinazione, se applicabile.
- Fornite il **numero di telefono dell'account no-log.org "adresse"** e gli **ultimi 30 dati di accesso**.
- Inviateci gli **ultimi TRENTA dati di connessione** (indirizzo IP, data, ora e fuso orario) alle **pagine di amministrazione** dell'account no-log "indirizzo".

Inoltre, è un dato di fatto che i poliziotti a volte chiedono tali informazioni con una semplice e-mail, ed è probabile che molti fornitori di servizi Internet rispondano direttamente a tali richieste ufficiose, il che comporta

che *chiunque* può ottenere tali informazioni spacciandosi per la polizia.

Le richieste sono all'ordine del giorno. I grandi ISP hanno ormai uffici legali dedicati per gestirle, e un tariffario codifica ogni tipo di richiesta.³⁸ Dall'ottobre 2013, in Francia, un tariffario approvato dal governo ha persino omogeneizzato questi diversi servizi.³⁹ Ad esempio, il costo dell'identificazione di un abbonato in base al suo indirizzo IP era di 4 euro (tariffe in vigore nell'ottobre 2013). Per più di 20 richieste, questa tariffa si riduce a 18 centesimi.

Nel primo semestre del 2020, ad esempio, Google ha ricevuto in media 1.349 richieste al mese dalla Francia di informazioni sulle sue utenti donne, per un totale di 10.864 account - cifre in costante aumento dal 2009. Dopo aver analizzato l'ammissibilità legale delle richieste, l'azienda ha risposto al 60% di esse.⁴⁰ L'altra metà delle richieste non rientrava nell'ambito di ciò che l'azienda riteneva di dover fornire per legge.

Oltre ai registri delle connessioni, dalla legge del 2016⁴¹ contro la criminalità organizzata del 2016, le autorità possono prendere visione del contenuto della corrispondenza memorizzata⁴² su semplice richiesta.

28.3 Ascolto di massa

Oltre ai registri e alle requisizioni previste dalle leggi sulla conservazione dei dati, le comunicazioni via Internet sono sistematicamente monitorate da vari servizi statali.

Un ex dipendente dell'operatore di telecomunicazioni statunitense AT&T ha testimoniato che la NSA (l'agenzia di intelligence elettronica degli Stati Uniti)⁴³ che l'NSA (l'agenzia di intelligence elettronica degli Stati Uniti) stava monitorando tutte le comunicazioni Internet e telefoniche che passavano attraverso un importante impianto di telecomunicazioni AT&T a San Francisco. Ciò avveniva utilizzando un supercomputer appositamente progettato per la sorveglianza di massa in tempo reale delle comunicazioni.⁴⁴ Ha anche affermato che probabilmente tali installazioni esistevano in infrastrutture simili in altre città statunitensi, come confermato dalle rivelazioni di un ex dipendente della NSA e della CIA.⁴⁵ Si dice che installazioni simili siano state installate dai servizi segreti britannici su oltre 200 fibre ottiche sottomarine.⁴⁶

38. Christopher Soghoian, 2010, *Il vostro ISP e il governo: Migliori amici per sempre* [<https://www.defcon.org/html/defcon-18/dc-18-speakers.html#Soghoian>].

39. Légifrance, 2013, *arrêté du 21 août 2013 pris en application des articles R. 213-1 et R. 213-2 del Codice di procedura penale francese che stabilisce le tariffe applicabili alle requisizioni emesse dagli operatori di comunicazione elettronica* [<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028051025>].

40. Google, 2021, *Francia - Google Information Transparency* [<https://www.google.com/transparencyreport/userdatarequests/EN/>].

41. Legge n. 2016-731 (*op. cit.*)

42. Légifrance, 2019, *Article n° 706-95-1 du code de procédure pénale* [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311668]; Questo articolo permette quindi di aggirare i vincoli di una perquisizione e di non avvertire l'interessato di questa invasione della sua privacy. privato.

43. Mark Klein, 2004, *L'implementazione da parte di AT&T dello spionaggio della NSA sui cittadini americani*. [<https://www-tc.pbs.org/wgbh/pages/frontline/homefront/etc/kleindoc.pdf>].

44. Reflets.info, 2011, *#OpSyria : BlueCoat maestro artigiano della censura siriana* [<https://web.archive.org/web/20160823002531/https://reflets.info/opsyria-bluecoat-maitre-artisan-de-la-censu-re-syrienne/>].

45. Craig Timberg e Barton Gellman, 2013, *NSA paying U.S. companies for access to communications networks* [https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html] (in inglese).

46. L'expansion.com, 2013, *"Operazione Tempora": come gli inglesi stanno superando le Americhe. Ricani per spiare Internet* [https://www.lexpress.fr/economie/high-tech/operation-tempora-comment-les-britanniques-depassent-les-americains-pour-espionner-internet_1434134.html].

I servizi di sicurezza francesi sono ora autorizzati a installare tali strumenti di analisi del traffico nelle reti degli ISP al fine di

per "individuare connessioni che potrebbero rivelare una minaccia terroristica".⁴⁷

Dalla legge finanziaria 2020⁴⁸ le autorità fiscali e doganali francesi sono state autorizzate a utilizzare automaticamente alcuni dati personali. Possono infatti raccogliere informazioni liberamente accessibili dai social media utilizzati per "mettere in contatto più parti al fine di vendere un bene, fornire un servizio o scambiare o condividere contenuti, un bene o un servizio", ovvero piattaforme come Le Bon Coin o BlaBlaCar.

La NSA ha anche ottenuto l'accesso diretto ai server di diversi "giganti" di Internet (Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL e Apple).⁴⁹, il che le consente di accedere ai dati che ospitano o che passano attraverso i loro server.⁵⁰ La DGSE, l'equivalente francese della NSA, ha accesso diretto alle reti di Orange.⁵¹

Allo stesso modo, le comunicazioni satellitari sono ascoltate dalla rete Echelon, un "sistema globale di intercettazione delle comunicazioni private e pubbliche" sviluppato dai paesi anglo-americani.⁵² sviluppato dai Paesi anglosassoni⁵³. Le informazioni a riguardo non sono chiare, ma sembra che anche la Francia abbia una rete di monitoraggio delle telecomunicazioni sul suo territorio.⁵⁴

L'NSA sta anche monitorando e incrociando gli scambi di e-mail per mappare le relazioni tra tutti i residenti negli Stati Uniti.⁵⁵ Sebbene tali pratiche non siano necessariamente documentate in altre parti del mondo, sono altrettanto possibili.

Inoltre, per qualsiasi organizzazione che abbia i mezzi per essere un nodo di rete significativo, ufficialmente o meno, si sta diffondendo l'uso della *Deep Packet Inspection* (o *DPI*). La sorveglianza *DPI* è particolarmente invasiva: non si limita più alle informazioni contenute nelle intestazioni dei pacchetti IP, ma tocca il contenuto stesso delle comunicazioni. Se queste non sono criptate, è possibile recuperare, ad esempio, il contenuto completo delle e-mail o la totalità delle nostre ricerche sul web.

L'uso di questa tecnica in Libia e in Siria, ad esempio, ha permesso di mettere sotto sorveglianza digitale l'intera popolazione del Paese, per poi attacchi mirati da portare a termine. Con l'aiuto e il sostegno della Francia governo, Amesys, un'azienda con sede in Francia⁵⁶ da

47. Légifrance, *Code de la sécurité intérieure*, articolo L851-3 [https://www.legifrance.gouv.fr/cod/es/article_lc/LEGIARTI000043887520/].

48. Légifrance, 2019, *LOI n° 2019-1479 du 28 décembre 2019 de finances pour 2020* [https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000039684091].

49. NSA, 2013, *Date Quando PRISM PRISM è iniziata Per Ogni Fornitore* [https://commons.wikimedia.org/wiki/File:Prism_slide_5.jpg].

50. Le Monde, 2013, *Le FBI aurait accès aux serveurs de Google, Facebook, Microsoft, Yahoo! et d'autres géants d'Internet* [https://www.lemonde.fr/ameriques/article/2013/06/07/le-fbi-a-acces-a-ux-serveurs-des-geants-d-internet_3425810_3222.html].

51. Jacques Follorou, 2015, *Espionnage : comment Orange et les services secrets coopèrent*, Le Monde [https://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-inc-es-tueuses_4386264_3210.html].

52. Wikipedia, 2021, *Echelon* [<https://fr.wikipedia.org/wiki/Echelon>].

53. Gerhard Schmid, 2001, *Relazione sull'esistenza di un sistema globale di intercettazione delle comunicazioni private ed economiche (sistema di intercettazione ECHELON)* [https://www.europarl.europa.eu/doceo/document/A-5-2001-0264_EN.html].

54. Wikipedia, 2021, *Frenchelon* [<https://fr.wikipedia.org/wiki/Frenchelon>].

55. Gorman, Siobhan, 2008, *NSA's Domestic Spying Grows As Agency Sweeps Up Data: Terrore Lotta Sfuma Linea Su Dominio; Tracciamento Email* [<https://www.wsj.com/articles/SB120511973377523845>].

56. kitetoa, 2011, *Amesys : le gouvernement (schizophrène) français a validé l'exportation vers la Libia di materiale d'esame massiccio di individui*, Reflets.info [<https://web.archive.org/web/20181121190456/https://reflets.info/articles/amesys-le-gouvernement-francais-a-valide-l-exportation-vers-la-libye-de-materiel-de-surveillance>].

[pagina

217

[pagina

217

[prossimo]
pagina.]

all'epoca, ha installato tali sistemi in Libia⁵⁷ Marocco, Qatar⁵⁸ e Francia⁵⁹.

28.4 Attacchi mirati

Quando un utente di Internet o una risorsa disponibile *via* Internet - come un sito web o una casella di posta elettronica - suscita la curiosità degli avversari, questi possono mettere in atto attacchi mirati. Questi attacchi mirati possono avvenire a vari livelli: le directory che consentono di trovare la risorsa, i server che la ospitano, i client che vi accedono *e così via*. In questa sezione esaminiamo queste diverse possibilità.

In Francia, i fornitori di servizi Internet sono tenuti per legge a bloccare l'accesso ai siti web che sono stati inseriti in una "lista di blocco" a seguito di una sentenza del tribunale⁶⁰ o considerati dall'*ufficio centrale di lotta contro la criminalità legata alle tecnologie dell'informazione e della comunicazione* come contenenti materiale pedopornografico, che provocano "direttamente atti di terrorismo" o che "glorificano" tali atti.⁶¹ Inoltre, un'ordinanza li obbliga a fare lo stesso per i siti web che violano il diritto d'autore o i diritti connessi.

⁶².

Nell'ottobre 2011, il Tribunal de Grande Instance de Paris ha ordinato a sette ISP francesi di bloccare "tramite IP o DNS" il sito web copwatchnord-idf.org⁶³ il sito era accusato di commenti ingiuriosi e diffamatori e di raccogliere dati personali sugli agenti di polizia. Nel febbraio 2012, il tribunale ha ordinato il blocco di uno dei 35 siti mirror⁶⁴ che il Ministero dell'Interno stava cercando di bloccare.⁶⁵

D'altra parte, il tribunale non ha ordinato il blocco degli altri 34 mirror citati dal Ministero dell'Interno, in quanto quest'ultimo "non ha indicato se ha cercato di identificare o meno i loro editori e host", né quello dei siti mirror che potrebbero apparire.

Più recentemente, nel 2019, il Tribunal de Grande Instance de Paris ha ordinato a Bouygues Télécom, Free, Orange e SFR di impedire l'accesso ai siti web di Sci-Hub e LibGen per violazione dei diritti d'autore o dei diritti di prossimità.⁶⁶ Questi siti forniscono accesso gratuito ad articoli scientifici che altrimenti sarebbero tenuti dietro un paywall dai loro editori accademici. Blocco

57. Fabrice Epelboin, 2011, *Kadhafi espionait sa population avec l'aide de la France* [<https://web.archive.org/web/2015062923215/https://reflets.info/kadhafi-espionait-sa-population-avec-%E2%80%99aide-de-la-france/>].

58. Reflets.info, 2011, *Qatar: il dito di Amesys tiene alto* [<https://web.archive.org/web/20200923032548/https://reflets.info/articles/qatar-le-finger-tendu-bien-haut-d-amesys>].

59. Jean Marc Manach, 2011, *Amesys monitora anche la Francia* [<https://web.archive.org/web/20171011205936/http://owni.fr/2011/10/18/amesys-surveillance-france-takieddine-libye-eagle-dga-dgse/>].

60. LCEN, *op. cit.* articolo 6-3 [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000043969099], creato dal Journal Officiel de la République Française, 2021, *loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République* [<https://www.legifrance.gouv.fr/jorf/id/JORFARTI000043964844>].

61. Légifrance, 2015, *décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant ad atti di terrorismo e siti che diffondono immagini pornografiche e rappresentazioni di minori* [<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030195477>].

62. Légifrance, 2020, *article L336-2 du code de la propriété intellectuelle modifié par Ordonnance n° 2019-738 du 17 juillet 2019* [<https://www.legifrance.gouv.fr/codes/id/LEGIARTI000033688218>].

63. Tribunale di grande istanza di Parigi, 2011, *Sentenza sommaria del 14 ottobre 2011* [https://data.over-blog-kiwi.com/1/13/34/21/20140707/ob_2fbf9e_jugement-tgi-paris-14-octobre-2011-gu-a.pdf].

64. Un sito mirror è una copia esatta di un altro sito web.

65. Legalis, 2012, *ordinanza di rifatto reso le 10 febbraio 2012* [<https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-10-fevrier-2012/>].

66. Numerama, 2019, *Sci-Hub e LibGen si battono per la libera diffusione del sapere scientifico: La Francia ordina il loro blocco* [<https://www.numerama.com/sciences/477218-sci-hub-et-libgen-lut-tent-pour-la-diffusion-gratuite-du-savoir-scientifique-la-france-ordonne-leur-blocage.html>].

che copre 57 domini è stato imposto per un anno. È da notare che gli ISP non hanno voluto opporsi a questa misura di censura. Nel 2021, una nuova sentenza ha esteso l'elenco a 278 domini.⁶⁷

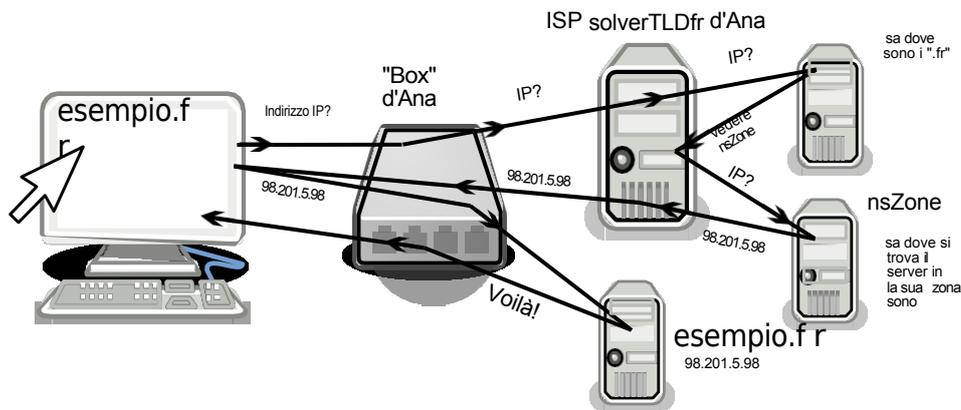
28.4.1 Bloccare l'accesso al fornitore di risorse

Vediamo i diversi modi per bloccare l'accesso a una risorsa su Internet.

Attacco ai nomi di dominio

È possibile deviare il traffico che doveva andare a un determinato server modificando la directory utilizzata per passare dal suo nome di dominio al suo indirizzo IP, ovvero il DNS.

Questo può essere fatto a diversi livelli.



Le fasi principali di una query DNS

Organizzazioni che gestiscono la directory dei nomi di dominio Per ragioni di efficienza e robustezza, il sistema di directory (DNS) è gestito da diverse organizzazioni, in un sistema informativo gerarchico e distribuito. Il database globale del DNS è quindi distribuito tra diversi server di nomi, ognuno dei quali gestisce solo una parte del database.

Alcune organizzazioni o società sono responsabili del DNS dei cosiddetti domini *di primo livello* (TLD), che corrispondono ai caratteri dopo l'ultimo punto del nome di dominio, come .com, .fr, .org, ecc. Tutti i domini che terminano in .fr sono sotto la responsabilità del server di nomi AFNIC. Tutti i domini che terminano in .fr sono sotto la responsabilità del server di nomi dell'AFNIC, un'associazione creata a questo scopo nel 1997. I domini che terminano in .com, invece, sono gestiti da Verisign, una società statunitense quotata in borsa.

L'elenco delle organizzazioni e delle società responsabili della gestione dei domini di primo livello è disponibile sul sito web della IANA⁶⁸ (Internet Assigned Numbers Authority), che gestisce i server radice del DNS, quello che ha autorità su tutti gli altri.

Mentre i gestori dei domini di primo livello hanno un ruolo puramente tecnico (mantenere un elenco aggiornato dei domini a loro affidati), quelli a cui delegano sono generalmente società commerciali (chiamate *registrar*) che vendono nomi di dominio.

Sta prendendo forma una mappa dei punti nevralgici in cui la censura può intervenire.

67. The Sound Of Science, 2021, [Esclusivo] Perché i principali ISP francesi stanno bloccando nuovamente Sci-hub e Libgen [https://web.archive.org/web/20221226013526/https://www.soundofscience.fr/2724].

68. IANA, 2014, *Root Zone Database* [https://www.iana.org/domains/root/db].



PER SAPERNE DI PIÙ...

Quindi, affittare un nome di dominio è un'operazione separata dall'averne un IP: ad esempio, per creare il proprio sito web, è necessario acquistare un nome di dominio da un lato, e trovare un hosting per il sito dall'altro, con un indirizzo IP collegato. E poi creare il collegamento tra i due. Alcune aziende offrono tutti questi servizi contemporaneamente, ma non è né sistematico né obbligatorio.

Sequestro di nomi di dominio Il sequestro di nomi di dominio più spettacolare fino ad oggi è stato sicuramente quello registrato in relazione alla chiusura del sito di file-hosting megaupload.com da parte del Dipartimento di Giustizia degli Stati Uniti. Per rendere inaccessibili i servizi del sito, l'FBI ha chiesto a Verisign, la società che gestisce i nomi di dominio .com, di modificare le sue tabelle di mappatura in modo che l'indirizzo non puntasse più ai server di Megaupload, ma a un server dell'FBI che indicava che il sito era stato sequestrato.⁶⁹

Tuttavia, una delle prime censure note di sospensione di un nome di dominio si è verificata nel 2007 presso un registrar: GoDaddy (il più grande al mondo). Nel contesto di una disputa tra uno dei suoi clienti, seclists.org, e un altro sito, mspace.com, GoDaddy si è schierato dalla parte di quest'ultimo e ha modificato il suo database, rendendo il sito irraggiungibile da un giorno all'altro e senza avvisare nessuno (tranne coloro che conoscono a memoria il suo indirizzo IP).⁷⁰ (ad eccezione di coloro che conoscono a memoria il suo indirizzo IP).

DNS bugiardi Infine, mentre la modifica degli elenchi globali è alla portata solo di pochi Stati e aziende, molti possono semplicemente falsificare la propria versione dell'elenco: questo è noto come "DNS bugiardi". Ad esempio, ogni ISP ha generalmente i propri server dei nomi di dominio (DNS), che vengono utilizzati per impostazione predefinita dai suoi abbonati.

Quando un server di nomi di dominio fornisce qualcosa di diverso da ciò che è stato registrato presso le autorità di registrazione, questo è noto anche come "DNS bugiardo".⁷¹ una violazione della neutralità della rete.

Questo è il livello a cui opera il blocco amministrativo dei siti in Francia: Gli ISP devono modificare i loro elenchi per reindirizzare gli indirizzi elencati dall'*Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* (Ufficio centrale per la lotta alla criminalità legata alle tecnologie dell'informazione e della comunicazione).

a una pagina del Ministero dell'Interno⁷².

Le persone che utilizzano l'ISP Orange hanno potuto sperimentare loro malgrado questo blocco il 17 ottobre 2016. A seguito di un "errore umano" "nell'aggiornamento dei siti bloccati"⁷³ per un'ora, il resolver di Orange ha dato una risposta "falsa" all'indirizzo fr.wikipedia.org, che non puntava ai server di Wikipedia, ma a una pagina che recitava: "Sei stato reindirizzato a questa pagina del sito web del Ministero degli Interni perché hai cercato di connetterti a una pagina la cui

pagina

207

69. Dopo questa chiusura, migliaia di utenti di Internet si sono trovati in un batter d'occhio privati dei loro contenuti (e non solo dei file piratati, viste le petizioni online e tutte le persone che hanno dichiarato che la loro vita professionale era rovinata perché non avevano più accesso a tutti i loro documenti).

70. Fyodor, 2007, *Seclists.org chiuso da Myspace e GoDaddy* [<https://seclists.org/nmap-a-n-nounce/2007/0/>].

71. Stephane Bortzmeyer *approfondisce il concetto* [<https://www.bortzmeyer.org/dns-menteur.html>].

72. Légifrance, 2015, *décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant ad atti di terrorismo o che li glorificano, e siti che diffondono immagini pornografiche e rappresentazioni di minori* [<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030195477>].

73. Marc Rees, 2016, *Blocage de Google, OVH et Wikipedia : "on ne cherche pas à vous cacher la vérité" assure Orange, Nextinact* [<https://www.nextinact.com/article/24123/101785-blocage-google-ovh-et-wikipedia-on-ne-ne-cherche-pas-a-vous-cacher-verite-assure-orange>].

il contenuto incita ad atti di terrorismo o condona pubblicamente atti di terrorismo".⁷⁴.

Dereferenziazione

Infine, un modo semplice ma efficace per impedire l'accesso a un sito web è quello di rimuoverlo dai motori di ricerca e dalle directory: si tratta del cosiddetto dereferenziamento. Il sito esiste ancora, ma non compare più sui motori di ricerca (come Google).

In Francia, il dereferenziamento è una delle tecniche utilizzate per bloccare i siti a livello amministrativo: l'*ufficio centrale di lotta contro la criminalità legata alle tecnologie dell'informazione e della comunicazione* invia ai motori di ricerca o agli elenchi un elenco di indirizzi che ritiene contengano materiale pedopornografico, "direttamente a favore di atti di terrorismo" o che "glorificano" tali atti.⁷⁵ I motori di ricerca hanno 48 ore di tempo per assicurarsi che questi indirizzi non compaiano più nei loro risultati. Nel 2020 sono state presentate 4.138 richieste di dereferenziazione, 4 delle quali sono state annullate dopo la revisione.⁷⁶

28.4.2 Phishing

Nella stessa ottica, il phishing⁷⁷ (noto anche come "*phishing*") consiste nell'indurre l'utente di Internet a connettersi a un sito che non è quello che pensa, ma ha un aspetto molto simile. Ad esempio, un sito che sembra esattamente quello di una banca, per ottenere le password dell'interfaccia di gestione del conto corrente. Per farlo, gli avversari acquistano un nome di dominio che a prima vista sembra quello giusto. Non resta che invogliare l'obiettivo a collegarsi al sito, di solito spaventandolo, ad esempio "Abbiamo rilevato un attacco al tuo conto" o "Abbiamo rilevato un attacco al tuo conto".

"Hai superato la tua quota", seguita da una proposta per regolarizzare la situazione. cliccando sul link trappola.

Per far sì che anche il nome di dominio affinché assomigli a quello del sito copiato, esistono numerose tecniche: l'avversario può, ad esempio, utilizzare caratteri speciali che hanno l'aspetto di caratteri dell'alfabeto latino. Ad esempio, sostituendo una "e" cirillica a una "e" latina in *example.org*, si ottiene un indirizzo che sembra (quasi) identico all'originale, ma che rappresenta un indirizzo diverso per il computer; si possono anche trovare dei trattini (*mabanque.fr* invece di *mabanque.fr*); a volte si tratta di un nome identico, con un dominio di primo livello (TLD):

.com,

.net, .org, .fr, ecc.) (*site.com* invece di *site.org*).

sottodomini (*paypal.phishing.com* si collega al sito di phishing, non a *paypal.com*), ecc.

I browser Web sono progettati per avvisare gli utenti del pericolo e chiedere conferma prima di accedere al sito sospetto.⁷⁸ Tuttavia, questo

74. Yannux, 2016, Screenshot della pagina del Ministero dell'Interno, twitter.com [https://pbs.twimg.com/media/Cu9JoGNWAAQAO9.jpg].

75. Légifrance, 2015, *décret n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites che provocano o condonano atti di terrorismo e siti che mostrano immagini pornografiche e rappresentazioni di minori* [https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030313562].

76. Alexandre Linden, 2021, *relazione sulle attività del 2020 della persona qualificata nominata in base all'articolo 6-1 de la loi n° 2004-575 du 21 juin 2004 créé par la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme*, CNIL [https://www.cnil.fr/sites/default/files/atoms/files/rapport_linden_2020.pdf], p. 9.

77. Si veda Wikipedia, 2014, *Phishing* [https://fr.wikipedia.org/wiki/Hameçonnage], che spiega alcune (parziali) contromisure a questo attacco.

78. Mozilla, 2022, *Come funziona la protezione da phishing e malware?* [https://support.mozilla.org/fr/kb/comment-fonctionne-protection-contre-hame%C3%A7onnage-e-malware]

La soluzione prevede che il browser web contatti un database centralizzato che elenca i siti considerati dannosi. Ciò può porre problemi di discrezione: il server che ospita questo elenco sarà necessariamente a conoscenza dei siti di phishing o malware visitati.

28.4.3 Attaccare il server

Un altro tipo di attacco consiste nell'attaccare il computer che ospita la risorsa di interesse. Questo può essere fatto sia fisicamente che da remoto.

Inserimento dei server

Si tratta semplicemente di un avversario che ha i mezzi - la polizia o la legge, ad esempio - per recarsi nel luogo in cui si trova il computer a cui è interessato. L'avversario può quindi sequestrare la macchina o copiare i dati in essa contenuti. Può poi studiare tutte le tracce lasciate su di esso dalle persone che vi si sono collegate... pagina 27 su almeno se

il suo disco rigido non è criptato.

Almeno quattordici server sono stati sequestrati dai tribunali in Europa tra il 1995 e il 2007.⁷⁹

47

Nel 2007, un server di Greenpeace Belgio è stato sequestrato dalla polizia belga a seguito di una denuncia per "associazione a delinquere" da parte di una società elettrica belga.

⁸⁰ contro che il ambientale organizzazione aveva chiesto per una unamanifestazione.

Più recentemente, nella primavera del 2017, sono stati sequestrati alcuni server appartenenti alla rete di anonimizzazione Tor⁸¹ in relazione, o almeno con il pretesto, di un'indagine su un cyberattacco che stava transitando attraverso questa rete⁸².

pagina 261

Violazione del server

Come qualsiasi computer, anche un server può essere *violato*: ciò comporta che l'aggressore "entri" nel computer. Nei programmi comunemente utilizzati sui server vengono regolarmente riscontrati errori di progettazione o di programmazione, che possono essere utilizzati per dirottare il funzionamento di un programma e ottenere l'accesso al computer su cui è in esecuzione. Sono possibili anche errori di configurazione del software da parte degli amministratori del server.

Nel 2014, ad esempio, sfruttando le vulnerabilità del software di pubblicazione utilizzato sul sito web di Gamma International, l'azienda dietro lo spyware FinFisher, un hacker ha potuto accedere al loro server.⁸³ Questo gli ha permesso di accedere a 40 gigabyte di documenti, tra cui un elenco dei loro clienti, documenti su

il funzionamento e l'efficacia del loro software spia, nonché parti del loro sito web.

il suo codice sorgente⁸⁴.

pagina 39

Le vulnerabilità che rendono possibile questo tipo di hacking non sono rare e qualsiasi server può essere colpito. Una volta entrati nel server, gli hacker possono potenzialmente ottenere l'accesso remoto a tutti i dati in esso memorizzati.

Anche senza entrare nel server, le vulnerabilità del software possono essere scoperte e sfruttate per esfiltrare informazioni accessibili a chiunque.

79. Globenet, 2007, *Sequestri di server in Europa: una storia* [https://www.globenet.org/Les-seizures-of-servers-in-Europe.html?start_aff=6].

80. Gérard De Selys, 2008, *Greenpeace, association de malfaiteurs*, *Articulations* n°33, CESEP [https://web.archive.org/web/20230129143208/https://www.cesep.be/PDF/ARTICULATIONS/ARTICULATIONS_33.pdf], pag. 7.

81. Guénaél Pépin, 2017, *WannaCrypt: Nodi Tor sequestrati dalle autorità francesi* [<https://www.nextinpact.com/article/26455/104302-wannacrypt-nuds-tor-saisis-par-autorites-francaises>].

82. Wikipedia, 2021, *WannaCry* [<https://fr.wikipedia.org/wiki/WannaCry>].

83. Phineas Fisher, 2014, *Hack Back - Guida fai da te per chi non ha la pazienza di aspettare gli informatori* [<https://gist.github.com/vlamer/2c2ec2ca80a84ab21a32#file-gistfile1-txt-L171>]. (in inglese).

84. Wikipedia, Phineas Fisher [https://en.wikipedia.org/wiki/Phineas_Fisher].

che non dovrebbero avere accesso. Questo è ciò che ha permesso la famosa fuga di dati personali da 500 milioni di account Facebook⁸⁵ da giugno 2020.

Attacco di negazione del servizio

Senza sequestrare o addirittura hackerare il server, è possibile impedirne il funzionamento saturandolo: l'avversario fa in modo che un gran numero di robot cerchi costantemente di connettersi al sito da attaccare. Oltre un certo numero di richieste, il software del server viene sopraffatto e non può più rispondere, rendendo il sito inaccessibile. Questo è noto come *attacco denial-of-service*.⁸⁶ I bot utilizzati per questo tipo di attacco sono spesso malware installati su computer personali all'insaputa del proprietario.

pagina

210

pagi

na

32

28.4.4 In viaggio

Infine, un avversario che controlla una parte della rete, come un ISP, può intercettare o dirottare i pacchetti in vari modi.

Filtraggio

Come già detto, un avversario che controlla uno dei router attraverso cui passa il traffico tra un utente di Internet e una risorsa può leggerne più o meno approfonditamente il contenuto dei pacchetti ed eventualmente modificarlo, tanto più facilmente se non è criptato.

pagina

217

pagina

206

Oggi praticamente tutti gli ISP utilizzano questo tipo di ispezione, il *DPI*, almeno a fini statistici. Inoltre, sono sempre di più quelli che la utilizzano, in modo più o meno discreto, più o meno deliberato, per anteporre alcuni pacchetti ad altri, a seconda della loro destinazione o dell'applicazione a cui corrispondono. Ad esempio, per rallentare il video-on-demand, che genera molto traffico (e quindi costa molto denaro), e dare priorità alla telefonia via Internet.⁸⁷ SFR, ad esempio, utilizza questo tipo di strumento per⁸⁸ per modificare le pagine web visitate dai suoi abbonati 3G.⁸⁹

pagina

229

La massiccia diffusione di apparecchiature che consentono questo esame approfondito dei pacchetti rende molto più facile la sorveglianza dei gateway delle reti ISP.

Analizzando questo tipo di dati, i governi possono identificare la posizione di un individuo, le sue relazioni e i membri di un gruppo, come gli "oppositori politici".

⁹⁰ Tali sistemi sono stati venduti da aziende occidentali a Tunisia, Egitto, Libia, Bahrein e Siria.⁹¹ e sono in uso anche in alcuni Paesi occidentali. Basati sulla sorveglianza di massa, questi sistemi consentono di prendere di mira gli utenti di Internet e di filtrare e censurare i contenuti.

pagina

229

L'uso di questa tecnica, ad esempio in Spagna, ha permesso ad alcuni ISP di monitorare il traffico dei propri utenti e di impedire loro di accedere al sito web dell'azienda.

⁹² dei suoi utenti per impedire loro l'accesso alla

85. Elise Viniacourt, 2021, *Facebook : les données de 533 millions d'utilisateurs en fuite sur-le-web*, Liberation.fr [https://www.liberation.fr/economie/economie-numerique/facebook-les-donnees-de-533-millions-dutilisateurs-en-fuite-sur-le-web-20210406_FNRIQR4PXB5BK6ALSEREIOPY/].

86. Wikipedia, 2021, *Attacco di negazione del servizio* [https://fr.wikipedia.org/wiki/Attaque_par_%C3%A9ni_de_service].

87. Wikipedia, 2021, *Deep packet inspection* [https://fr.wikipedia.org/wiki/Deep_packet_inspection].

88. bluetouff, 2013, *SFR cambia la fonte HTML delle pagine visitate su 3G* [https://web.archive.org/web/20150629235630/https://reflets.info/sfr-modifie-le-source-html-des-pages-que-vo-us-visit-en-3g/].

89. Wikipedia, 2021, *3G* [https://fr.wikipedia.org/wiki/3G].

90. Elaman, 2011, *Soluzioni per il monitoraggio delle comunicazioni* [https://wikileaks.org/spyfiles/docs/elaman/188_communications-monitoring-solutions.html].

91. Jean Marc Manach, 2011, *Internet massicciamente monitorato* [https://web.archive.org/web/20190411142441/http://owni.fr/2011/12/01/spy-files-interceptions-ecoutes-wikileaks-qosmos-amesys-libye-syrie/].

92. Sans Censure, 2020, *Sintesi del rapporto tecnico e dello stato attuale del sito Wome.nOnWeb* [https://sindominio.net/sincensura/fr/post/censura/].

l'ONG [Women on Web](https://www.womenonweb.org/fr/) [https://www.womenonweb.org/fr/], che fornisce informazioni e assistenza sull'aborto in tutto il mondo.

Ascolto

Proprio come le vecchie intercettazioni telefoniche, oggi è possibile registrare tutti o parte dei dati che passano attraverso un collegamento di rete: si tratta della cosiddetta "intercettazione IP". In questo modo è possibile, ad esempio, origliare tutto il traffico scambiato da un server o quello che passa attraverso una connessione ADSL domestica.

In Francia, tali intercettazioni sono autorizzate nell'ambito di un'indagine giudiziaria, ma anche per la "prevenzione del terrorismo" per raccogliere "informazioni o documenti [...] relativi a una persona [...] verosimilmente legata a una minaccia" ma anche relativi a "persone appartenenti all'entourage della persona interessata".⁹³

Se non si prendono particolari precauzioni, un'intercettazione IP rivela a un avversario gran parte della nostra attività su Internet: pagine web visitate, e-mail e relativo contenuto, conversazioni di messaggistica istantanea... tutto ciò che lascia il nostro computer "in chiaro". La crittografia delle comunicazioni rende molto più difficile l'analisi del contenuto risultante da tali intercettazioni: l'avversario ha comunque accesso ai dati scambiati, ma non può comprenderli e sfruttarli direttamente. Può quindi cercare di rompere la crittografia utilizzata... o tentare di eludere il modo in cui è stata implementata. Parleremo più avanti di questi aspetti legati alla crittografia. In ogni caso, l'avversario avrà sempre accesso a una certa quantità di informazioni preziose, come gli indirizzi IP dei vari interlocutori coinvolti in una comunicazione.

pagina

249

pagina

202

Analisi del traffico di rete

Quando il traffico è criptato, sono ancora possibili attacchi più sottili. Un avversario in grado di origliare il traffico di rete, anche senza avere accesso al contenuto dei dati, ha a disposizione altri indizi, come la quantità di informazioni trasmesse in un determinato momento.

Quindi, se Ana invia 2 MB di dati crittografati a un sito web di pubblicazione e pochi istanti dopo appare un nuovo documento di 2 MB su questo sito, l'avversario sarà in grado di dedurre che probabilmente è stata Ana a inviare questo documento.

Studiando la quantità di informazioni trasmesse per unità di tempo, gli avversari possono anche disegnare una "forma": la chiameremo "*pat-ta del traffico*".⁹⁴ Il contenuto di una pagina web criptata non avrà quindi lo stesso andamento di una conversazione di messaggistica istantanea criptata.

Inoltre, se lo stesso schema di traffico viene osservato in due punti della rete, gli avversari possono presumere che si tratti della stessa comunicazione.

Per fare un esempio specifico: consideriamo degli avversari che stanno origliando la connessione ADSL di Ana e che osservano del traffico criptato che non possono decifrare, ma che sospettano che Ana stia chattando con Bea tramite messaggistica istantanea criptata. Supponiamo che abbiano anche i mezzi per intercettare la connessione di Bea. Se osservano uno schema simile tra il traffico in uscita dalla casa di Ana e quello in entrata in quella di Bea pochi (milli-)secondi dopo, saranno avvantaggiati nella loro ipotesi - senza, tuttavia, avere una prova formale.

93. Légifrance, 2021, *Code de la sécurité intérieure*, article L851-2 [https://www.legi.france.gouv.fr/codes/article_lc/LEGIARTI000043887533/].

94. Yin Zhang, Vern Paxson, 2000, *Detecting Stepping Stones*, Proceedings of the 9th USENIX Security Symposium [https://www.usenix.org/legacy/events/sec2000/full_papers/zhangstepping/zhangstepping.pdf].

Questo tipo di attacco può essere utilizzato per confermare un'ipotesi preesistente, ma non per svilupparne una basata sulle sole informazioni raccolte, a meno che gli avversari non abbiano i mezzi per origliare l'intera rete in cui si trova il traffico tra Bea e Ana e non dispongano di una potenza di calcolo colossale. L'esistenza di tali avversari globali è tecnicamente possibile, ma non molto realistica. D'altra parte, agenzie come la NSA sono in grado di portare a termine questo tipo di attacco, almeno sulla scala del loro Paese: la NSA ha una potenza di calcolo che può essere sufficiente, e le fughe di notizie indicano che ascolterebbe il 75% del traffico Internet degli Stati Uniti.⁹⁵

28.4.5 Hackeraggio dei clienti

 [pagi]
 [na ---
 31
 Anche il computer dell'utente di Internet può essere un bersaglio. Così come gli aggressori possono introdursi in un server, possono anche introdursi in un personal computer. Errori di programmazione o altre falle nel sistema operativo o nelle applicazioni installate consentono talvolta agli avversari di effettuare la pirateria - legale o illegale - da Internet, senza avere accesso fisico alla macchina. Inoltre, l'intrusione può essere facilitata da pratiche scorrette da parte degli utenti, come l'apertura di allegati fraudolenti o l'installazione di programmi trovati a caso sul web.

Un famoso gruppo di hacker tedeschi, il Chaos Computer Club, ha scoperto un bug utilizzato dalla polizia tedesca per spiare e controllare un computer a distanza.⁹⁶ Tali cimici possono essere installate a distanza e sono consentite dalla legge francese.

 [pagi]
 [na ---
 31
 Ma lo "spionaggio a distanza" non è riservato solo alle pratiche di polizia. Negli Stati Uniti, una scuola superiore ha intrapreso una massiccia operazione di spionaggio. Con il pretesto di "recuperare i computer portatili rubati o smarriti", la scuola aveva installato una "funzione" che permetteva di accendere le webcam delle diverse migliaia di computer distribuiti agli studenti a discrezione della scuola. Il caso è venuto alla luce alla fine del 2009: uno degli studenti è stato accusato di "comportamento inappropriato", in questo caso di uso di droga. Il funzionario che accusava lo studente produsse come prova una foto che risultò essere stata scattata all'insaputa dello studente, dalla webcam del suo computer, mentre era a casa nella sua camera da letto.⁹⁷!

28.5 In conclusione

Identificare l'utente di Internet attraverso il suo indirizzo IP, leggere l'origine e la destinazione dei pacchetti attraverso le loro intestazioni, registrare varie informazioni in diverse fasi del viaggio, persino accedere al contenuto effettivo degli scambi... tutto questo è più o meno semplice a seconda dell'entità coinvolta.

I pirati, gli inserzionisti, la polizia di Saint-Tropez e la NSA non hanno le stesse possibilità tecniche e legali per accedere alle tracce descritte in questo capitolo.

Concludiamo osservando che il modo in cui Internet è stato concepito ed è più comunemente utilizzato è praticamente trasparente anche agli avversari più attenti... a meno che non utilizzino tutta una serie di parate adattate per rendere più difficili queste indiscrezioni; queste parate saranno discusse più avanti.

95. <https://www.la Tribune.fr/actualites/economie/international/20130821trib000781040/a-peine-25-du-traffic-web-americain-echappe-a-la-surveillance-du-nsa.html>.

96. Mark Rees, 2011, *CCC dissect a holey government Trojan horse*, PCInpact [<http://www.nextinpact.com/archive/66279-loppi-ccc-cheval-de-troie-faille-malware.htm>].

97. Io, me stesso e Internet, 2011, *Mais qui surveillera les surveillants?* [<https://web.archive.org/web/20180107033100/https://memyselfandinternet.wordpress.com/2011/02/14/%C2%AB-mais-qui-surveillera-les-surveillants-%C2%BB/>].

Web 2.0

Al giorno d'oggi, il termine web 2.0 è quasi di uso comune. Tuttavia, sembra difficile coglierne il vero significato, a causa del suo uso improprio o, al contrario, delle sue definizioni talvolta troppo tecniche.¹

È prima di tutto un termine di marketing, che definisce un'evoluzione del web in un momento in cui l'accesso di massa a Internet lo sta trasformando in un mercato succulento. Molte aziende, sia nel settore dei media, delle comunicazioni o della vendita al dettaglio, non possono più permettersi di ignorarlo. Hanno dovuto adattare i loro modelli di business a questo nuovo mercato.

L'arrivo di questi nuovi attori in un web che fino a quel momento era composto principalmente da università e appassionati ha trasformato il modo in cui i siti web vengono progettati e, di conseguenza, il modo in cui gli utenti del web li utilizzano.

Al di là di queste formulazioni di marketing, analizzeremo più da vicino come queste evoluzioni si manifestano agli utenti di Internet e i cambiamenti nel funzionamento della rete che esse comportano.

29.1 Applicazioni Internet ricche"...

Una di queste evoluzioni riguarda l'interattività dei siti web. Non si tratta più di semplici pagine statiche come quelle di un libro o di una rivista. Utilizzando tecnologie preesistenti del Web 2.0, come JavaScript, i siti web assomigliano sempre più ad applicazioni come quelle presenti sui nostri personal computer: siti dinamici che rispondono alle richieste dell'utente.

Inoltre, la maggior parte del software normalmente installato su un personal computer è stato trasposto in una versione web ed è ora accessibile tramite un browser.

Stiamo persino assistendo alla nascita di sistemi operativi, come Chrome OS, progettati interamente in questo senso. Questo movimento, questo passaggio dal software installato sul computer al web, è in particolare una risposta alle preoccupazioni relative a

incompatibilità di

software, licenze e aggiornamenti.

Non c'è bisogno di installare nulla: basta collegarsi a Internet e, tramite un browser web, si avrà accesso alla maggior parte delle applicazioni tradizionali: elaborazione testi, fogli di calcolo, e-mail, un diario collaborativo, un sistema di condivisione di file, un lettore musicale e così via.

Google Drive consente di scrivere documenti e di tenere la contabilità online, ad esempio. Ma il servizio consente anche di condividerlo con amici, colleghi e così via.

1. La presentazione di apertura della conferenza Web 2.0 di O'Reilly e Battelle, citata da Wikipedia, 2014, *Web 2.0* [https://fr.wikipedia.org/wiki/Web_2.0] è un ottimo esempio di definizione troppo tecnica.

Alcuni vedono addirittura nella possibilità di accedere a questi strumenti online da "qualsiasi computer, in qualsiasi paese, in qualsiasi momento" un modo per conciliare il lavoro con eventuali problemi medici, meteorologici o addirittura pandemici.² un modo per conciliare il lavoro con eventuali problemi medici, meteorologici o addirittura pandemici...

Non c'è bisogno di andare in ufficio, "basta un computer collegato a Internet per ricostituire immediatamente l'ambiente di lavoro".

29.2 ... e navigatori volontari

Quando queste aziende sono entrate nel mercato del web, hanno dovuto ripensare il loro modello di business. Con la crescita del pubblico di Internet, non era più possibile finanziare un sito web solo con la pubblicità, pagando un esercito di redattrici per fornire una quantità sempre maggiore di contenuti.

I fornitori di servizi hanno utilizzato una tecnica già presente da tempo sul web: affidarsi alla partecipazione degli utenti di Internet. D'ora in poi sono questi ultimi ad essere responsabili della scrittura dei contenuti che alimentano i siti. I fornitori di servizi si limitano a ospitare i dati e a fornire l'interfaccia per accedervi, ma anche e soprattutto ad aggiungere pubblicità intorno ad essi... e a incassare i soldi.

Per molti anni, la piattaforma di condivisione video YouTube ha permesso ai suoi utenti di caricare e visualizzare gratuitamente i video di loro scelta, senza alcuna contropartita visibile. Oggi, grazie al suo successo e al suo monopolio, la maggior parte delle persone che desiderano visualizzare e condividere video dipende da questa piattaforma, che consente a YouTube di imporre gradualmente la pubblicità. All'inizio la pubblicità veniva visualizzata su un banner accanto all'immagine, poi su un banner trasparente sopra l'immagine, e ora si tratta semplicemente di video incorporati all'inizio o nel mezzo di quello che si vuole guardare.

Un altro vantaggio di questa soluzione per i fornitori di servizi è che gli utenti di Internet forniscono più o meno consapevolmente tutta una serie di dati che possono essere monetizzati.³ che possono poi essere monetizzati, in particolare costruendo profili di consumatori e adattando gli affiché pubblicitari al pubblico.

pagina
221

Non è più vero, ad esempio, che i navigatori usano Internet solo per scaricare film o leggere i loro periodici preferiti. Sempre più spesso, ad esempio compilando la propria pagina Facebook, gli utenti di Internet producono contenuti e li offrono, per così dire, agli host o ad altre società che forniscono questi servizi. Di propria iniziativa, gli internauti mettono online un elenco della musica che ascoltano, le foto delle loro vacanze nella Mosa o le loro lezioni di storia contemporanea da condividere con i compagni di classe.

Naturalmente, fornendo contenuti, si forniscono anche informazioni su di sé, informazioni che gli occhi indiscreti degli inserzionisti e di altri avversari sono destinati a utilizzare.

pagina
221
pagina
223

29.3 Centralizzazione dei dati

L'uso dello spazio di archiviazione su Internet va generalmente di pari passo con la centralizzazione dei dati degli utenti di Internet. Gli spazi di archiviazione online più utilizzati sono infatti nelle mani dei giganti del web.

2. Lionel Damm e Jean-Luc Synave, 2009, *Entrepreneur 2.0, la boîte à outils de la compétitivité... à petit frais* [<https://web.archive.org/web/20220125225053/https://www.confederationconstruction.be/Portals/28/UserFiles/Files/WP2guideentrepreneurweb20.pdf>].

3. Fanny Georges, Antoine Seilles, Jean Sallantin, 2010, *Des illusions de l'anonymat - Les stratégies de préservation des données personnelles à l'épreuve du Web 2.0*, Terminal numéro 105, Technologies et usages de l'anonymat à l'heure d'Internet [<https://www.revue-terminal.org/article/s/105/introDossierAnonymat105.pdf>].

L'utilizzo di applicazioni online significa, tra l'altro, che i documenti non vengono più archiviati su un computer personale, un disco rigido o una chiavetta USB. Vengono invece archiviati su server remoti, come quelli gestiti dai server di Google, in centri di elaborazione dati lontani dall'utente di Internet, sia geograficamente che tecnicamente. ⁴in centri di elaborazione dati lontani dall'utente di Internet, sia geograficamente che tecnicamente. In altre parole, gli utenti di Internet perdono il controllo sui propri dati.

La semplice mancanza di connessione a Internet rende impossibile l'accesso ai propri documenti, a meno che non si sia effettuato un backup. Questo cambiamento nell'archiviazione

Inoltre, non è possibile cancellare in modo sicuro i documenti della pagina 42 memorizzati su di essa.

Questa tendenza a migrare dati e applicazioni dal personal computer a Internet crea anche una "dipendenza da connessione". Quando tutta la musica, la rubrica e le mappe della città esistono solo su Internet, diventa difficile immaginare di usare un computer *offline*. Tuttavia, qualsiasi connessione a Internet apre delle porte. E più un computer è esposto, più è difficile garantirne la sicurezza, dall'anonimato dell'utente alla riservatezza dei dati che gli vengono affidati.

Non c'è nemmeno la garanzia che i nostri dati online siano sicuri. Anche se un'organizzazione ci dà tutte le garanzie di sicurezza oggi (eppure, che prove abbiamo di questo?), non è comunque al sicuro domani dalla scoperta di una falla o di un errore di configurazione del programma che permetterebbe a chiunque di accedere a questi dati, come nel caso del servizio di archiviazione dati online criptato Dropbox. ⁵

Le aziende a cui affidiamo i nostri dati possono anche, di propria iniziativa, cancellare i contenuti ⁶cancellare il nostro account ⁷o addirittura chiudere i loro servizi senza alcuna colpa, o semplicemente fallire. E quando gli Stati entrano in gioco, una decisione del tribunale può chiudere un servizio, come nel caso di Megaupload, o una semplice segnalazione da parte di un'autorità di un altro Stato può ora costringere un fornitore di servizi online a rimuovere contenuti qualificati come terroristici in meno di un'ora. ⁸

29.4 Controllo del programma

La maggior parte delle volte, queste applicazioni online sono sviluppate in modo più chiuso rispetto a le applicazioni gratuite che si possono installare sul proprio computer. Quando Google o Facebook decidono di modificare l'interfaccia o di cambiare il modo in cui funzionano le cose servizio, per "riordinare", l'utente web non ha voce in capitolo.

Inoltre, l'interattività di queste applicazioni web implica che parte del loro programma debba essere eseguito sul computer client (il nostro), utilizzando tecnologie come JavaScript o Java. Queste tecnologie sono ora attivate di default nei nostri browser web, per tutti i siti. È bello, pratico e moderno. Ma

4. Il paragrafo *Elementi creati o forniti dall'utente* nelle *Norme sulla privacy* [<https://policies.google.com/privacy?hl=fr#infocollect>] per i servizi forniti da Google dimostra chiaramente la mancanza di potere concreto che un utente di Internet ha sui contenuti che ha memorizzato online. "Ciò che è tuo, rimane tuo", ma Google è libero di farne ciò che vuole, come finché lasci i tuoi contenuti sui suoi server.

5. Vincent Hermann, 2011, *Dropbox ammette di possedere chiavi di accesso ai dati duplicate* [<https://www.nextinpact.com/archive/64460-dropbox-conditions-utilisation-chiffrement-securite.htm>].

6. Marie Claire, 2018, *Cancro al seno: Facebook censura le pubblicazioni sulla mastectomia (di nuovo)* [<https://www.marieclaire.fr/cancer-du-sein-facebook-censure-publications-mastectomie,1249169.asp>].

7. Owni, 2011, *Dopo 7 anni di utilizzo, ha fatto cancellare il suo account Google, comprese le e-mail, i calendari, i documenti, ecc.* [<https://web.archive.org/web/20200224160152/http://owni.fr/2011/08/29/google-cancellazione-account-dati-personali-vita-privata-dio/>].

8. Articolo 17 del *Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, sulla lotta alla diffusione di contenuti terroristici online* [<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32021R0784>].

Queste tecnologie pongono una serie di problemi per la sicurezza dei nostri computer e quindi per la riservatezza dei nostri dati.⁹... Tuttavia, è possibile¹⁰ il loro utilizzo su base individuale, a seconda del livello di fiducia che si ripone in esse.

29.5 Dalla centralizzazione al self-hosting decentralizzato

Di fronte alla crescente centralizzazione dei dati e delle applicazioni, possiamo godere dei vantaggi di una rete partecipativa e interattiva senza perdere il controllo sui nostri dati? La sfida sembra scoraggiante. Ma si sta lavorando per sviluppare applicazioni Internet che operino in modo decentrato sul computer di ciascun navigatore, anziché essere centralizzate su pochi server. Progetti come i social media peer-to-peer, Mastodon¹¹ Nextcloud¹² la distribuzione YunoHost¹³ o BriqueInter.net.¹⁴ stanno lavorando in questa direzione.

Finché non saranno facili da usare come le soluzioni offerte dai giganti del Web 2.0, è già possibile ospitare da soli la maggior parte dei servizi che si desidera offrire o utilizzare.

9. Non abbiamo alcun controllo sui programmi JavaScript o Java inviati dall'applicazione web. È quindi del tutto possibile che bug o altre funzionalità dannose [pagina 32] siano incluse in questi programmi e quindi eseguite dal nostro a vigateur.

10. A seconda del browser web utilizzato, esistono *estensioni* come **noscript** [<https://noscript.net>], che consentono di gestire questi parametri.

11. **Mastodon** [<https://joinmastodon.org/>].

12. **Nextcloud** [<https://nextcloud.com/fr/>].

13. **Pagina del progetto YunoHost** [https://yunohost.org/#/index_fr].

14. **La BriqueInter.net** [<https://labriqueinter.net/>].

Identità contestuali

Uno dei presupposti di questa *guida* è il desiderio che le nostre azioni, i nostri gesti e i nostri pensieri non siano automaticamente, se non del tutto, legati alla nostra identità civile.

Tuttavia, può essere necessario o semplicemente preferibile sapere con chi stiamo parlando: per esempio, per avviare una discussione su un forum o inviare e-mail. In questi casi, avere un'*identità*, cioè essere identificabili dal nostro corrispondente, semplifica la comunicazione.

30.1 Definizioni

Innanzitutto, due definizioni:

- *anonimato* significa non rivelare il proprio nome;
- *Pseudonimo* significa scegliere e utilizzare un nome diverso dalla propria identità civile.

Per il modo in cui funziona, è molto difficile essere *anonimi* o rimanere uno *pseudonimo* su Internet.

30.1.1 Soprannomi

Uno *pseudonimo* è un'identità che non è quella assegnata a una persona dallo stato civile. Possiamo scegliere di chiamarci "Falaise", "Amazone enragée", "Zigouigoui" o anche "Jeanne Dupont". Mantenendo lo stesso pseudonimo per diversi scambi, i nostri interlocutori avranno buone probabilità di pensare che i vari messaggi scritti con questo *pseudonimo* provengano dalla stessa persona: potranno quindi risponderci, ma non potranno venire a picchiarci se non sono d'accordo.

Quando si sceglie uno pseudonimo, tuttavia, bisogna essere consapevoli che esso può essere di per sé un indizio della persona che lo utilizza, almeno per le persone che già conoscono lo pseudonimo.

30.1.2 Identità contestuale

Bea scarica immediatamente il documento e lo apre nell'editor di testo. Lo sfoglia velocemente, cancellando alcuni dettagli che è meglio lasciare stare. Dopo aver inserito il suo login e la sua password per Collegandosi al blog, Bea copia e incolla il contenuto del documento dalla sua casella di posta elettronica e clicca su Invia. "Speriamo che ispiri altri!"

Continuando il filo della nostra storia introduttiva, l'identità contestuale corrisponderebbe a "una o più persone che pubblicano informazioni sul sindaco", e la persona fisica a Bea.

Sia che parliamo con persone con cui condividiamo la passione per l'arrampicata, sia che parliamo del nostro progetto professionale con un consulente del Pôle emploi o con il nostro banchiere, il tenore di ciò che diciamo, il modo in cui ne parliamo, non è lo stesso. Da un lato saremo piuttosto esaltati e avventurosi, dall'altro più sobri e seri. Possiamo quindi parlare di identità contestuale.

È lo stesso quando si usa il computer: quando si posta un messaggio su un forum di incontri, si annuncia una grande festa sul proprio account Facebook o si risponde a un'e-mail di papà, si utilizzano diverse identità contestuali. Queste possono, ovviamente, essere mescolate tra loro per formare un'unica identità composta dalle tre identità contestuali sopra menzionate: la donna single, la festaiola e la figlia di.

Un'identità contestuale è quindi un frammento di una "identità" globale che si suppone corrisponda a una persona fisica o a un gruppo. Come una fotografia è un'istantanea di una persona o di un gruppo, da una certa angolazione, a una certa età e così via, così un'identità contestuale è un frammento di una "identità" globale.

pagina
213

Non è facile essere assolutamente anonimi su Internet: come abbiamo visto, molte tracce vengono registrate quando si utilizza la rete. Questo fenomeno è ancora più vero con i social media, per i quali la generazione di un'identità unica e tracciabile è un core business.¹ È impossibile non lasciare tracce, ma può essere possibile lasciare tracce che non portano da nessuna parte.

Difficoltà simili si incontrano quando si sceglie lo pseudonimo: più si usa uno pseudonimo, più tracce si lasciano dietro di sé. Piccoli indizi che, se incrociati, possono rivelare l'identità civile che corrisponde a uno pseudonimo.

30.2 Dall'identità contestuale all'identità civile

Esistono vari modi, più o meno offensivi, per minare uno pseudonimo o rivelare il legame tra un'identità contestuale e la persona o le persone fisiche che la utilizzano.

30.2.1 Controllo incrociato

pagina
precedente.

Partendo dall'esempio di tre identità contestuali, è legittimo chiedersi cosa comporti destreggiarsi tra queste diverse identità in termini di anonimato. Supponendo che si utilizzi uno pseudonimo piuttosto che la propria identità civile, potrebbe essere più appropriato avere un'identità, cioè uno pseudonimo, in ogni contesto: uno per i siti di incontri, un altro per i social media e uno per le relazioni familiari, ecc. Se le informazioni provenienti da queste identità non sono compartimentate, cioè se si usa lo stesso pseudonimo, il loro incrocio può ridurre il numero di persone a cui possono corrispondere. In questo modo è più facile collegare una presenza digitale a una persona fisica, e quindi dare un nome all'identità contestuale corrispondente.

Consideriamo, ad esempio, una persona che usa lo pseudonimo *bruise76* su un blog in cui dice di essere vegetariana e di amare i film d'azione. Ci sono solo tante persone che corrispondono a questi criteri. A ciò si aggiunge il fatto che questo stesso pseudonimo viene utilizzato per organizzare una festa in una tale e tale città tramite i social media e per comunicare via e-mail con la signora Unetelle. Probabilmente non ci sono molti vegetariani che amano i film d'azione, organizzano una festa nella stessa città e comunicano via e-mail con la signora Unetelle.

1. Ippolita, 2012, *Non mi piace Facebook* [<http://inventin.lautre.net/livres/Ippolita-J-aime-pas-Facebook.pdf>].

Più numerosi e variegati sono gli usi di uno pseudonimo da parte di una stessa persona, più ristretto è il numero di persone che possono corrispondere a quello pseudonimo. In questo modo, attraverso un controllo incrociato degli usi dello stesso pseudonimo, è possibile indebolire o addirittura rompere lo pseudonimo.

Ecco un esempio della debolezza dello pseudonimo: AOL ha pubblicato i risultati di 3 mesi di query inviate al suo motore di ricerca. Le query della stessa persona erano associate allo stesso pseudonimo. Con un controllo incrociato, è stato possibile rompere lo pseudonimo associato alle query.²

Allo stesso modo, anche il governatore dello Stato del Massachusetts è stato vittima di questo incrocio di dati quando la sua cartella clinica, presumibilmente anonimizzata, è stata identificata tra quelle di tutte le cittadine dello Stato. Il ricercatore che ha effettuato questa dimostrazione di de-anonimizzazione dei dati è arrivato persino a inviargli la sua cartella clinica per posta.³

30.2.2 Correlazione temporale

Un po' più tecnica questa volta, la correlazione temporale permette anche di rompere o indebolire un po' di più l'anonimato o lo pseudonimo. Se, in un breve lasso di tempo, si verifica una connessione alla casella di posta `amazon@exemple.org` e a `jeanne.dupont@courriel.fr`, la probabilità che questi due indirizzi di posta siano nelle mani della stessa persona aumenta, a maggior ragione se questa osservazione si ripete. Di seguito verranno illustrate varie contromisure, per soddisfare esigenze diverse.

30.2.3 Stilometria

L'analisi statistica può essere applicata alla forma di qualsiasi tipo di dato, compreso il testo. Analizzando le⁴ caratteristiche di un testo, come la frequenza delle parole⁵ la lunghezza di parole, frasi e paragrafi e la frequenza dei segni di punteggiatura, possiamo mettere in relazione testi anonimi con altri testi ed estrarre indizi sui loro autori.

Questo tipo di analisi è stata utilizzata, ad esempio, durante il processo a Theodore Kaczynski⁶ per dimostrare che era l'autore del manifesto "La società industriale e il suo futuro".⁷

Gli autori di un recente studio⁸ hanno cercato di "simulare un tentativo di identificazione dell'autore di un blog pubblicato in forma anonima. Se l'autore è sufficiente a evitare di rivelare il suo indirizzo IP o qualsiasi altro identificatore esplicito, il suo avversario (ad esempio un censore governativo) può passare ad analizzare il suo stile di scrittura". I risultati dimostrano che la stilometria può ridurre notevolmente il numero di possibili autori di un determinato blog.

2. Nate Anderson, 2006, *AOL rilascia i dati di ricerca di 500.000 utenti* [<https://arstechnica.com/uncategorized/2006/08/7433/>].

3. Paul Ohn, 2009, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* [<http://www.uclalawreview.org/pdf/57-6-3.pdf>].

4. Ad esempio, grazie a software come *The Signature Stylometric System* [<https://www.philocomp.net/texts/signature.htm>] o *Java Graphical Authorship Attribution Program* [https://evl1abs.com/?page_id=42].

5. Le parole-strumento sono parole il cui ruolo sintattico è più importante del loro significato. In genere sono *parole di collegamento* [<https://fr.wikipedia.org/wiki/Mot-outil>].

6. Kathy Bailey, 2008, *Forensic Linguistics in Criminal Cases, Language in Social Contexts* [https://archive.org/download/bailey-forensic-linguistics-paper/Bailey_-_Forensic_Linguistics_Paper.doc] (in inglese).

7. Theodore Kaczynski, 1998, *La società industriale e il suo futuro* [<https://www.fichier-pdf.fr/2012/12/20/kaczynski/kaczynski.pdf>].

8. Hristo Paskov, Neil Gong, John Bethencourt, Emil Stefanov, Richard Shin, Dawn Song, 2012, *On the Feasibility of Internet-Scale Author Identification* [<https://www.cs.princeton.edu/~arvindn/publications/author-identification-draft.pdf>].

testo anonimo - la precisione aumenta ovviamente con il numero di campioni "firmati", cioè con un autore noto, forniti al software di analisi.

Il più delle volte, ciò consente di ridurre la dimensione dell'insieme di possibili autori da 100 a 200 su 100.000 iniziali. "[...] aggiunto a un'altra fonte di informazioni, questo può essere sufficiente a fare la differenza tra l'anonimato e l'identificazione di un autore". Al momento in cui scriviamo, nel 20% dei casi è addirittura possibile identificare direttamente l'autore anonimo.

La particolarità di questo lavoro è che supera l'ambito dei piccoli campioni (circa un centinaio di possibilità) a cui si limitavano gli studi precedenti, per concentrarsi sull'identificazione dell'autore tra un numero molto elevato di possibilità; in altre parole, dimostra che la stilometria può essere utilizzata per confermare l'origine di un testo sulla base di un numero molto elevato di campioni.

Tuttavia, scrivere nel tentativo di mascherare il proprio stile, senza alcuna particolare competenza, sembra rendere inefficaci le analisi stilometriche. Imitare lo stile altrui inganna addirittura in più della metà dei casi.⁹

Altri ricercatori stanno sviluppando un software che suggerisce le modifiche necessarie per anonimizzare un testo.¹⁰

30.3 Compartimentazione

Come abbiamo appena visto, ci sono diversi modi in cui un'identità civile può essere abbinata a un'identità contestuale. L'uso dello stesso nome per attività diverse è senza dubbio la pratica che più rischia di confonderci.

È quindi importante riflettere attentamente sul modo in cui si utilizzano gli pseudonimi. Spesso è pericoloso mescolare diverse identità contestuali sotto lo stesso pseudonimo. Il modo migliore per evitarlo è tenerle chiaramente separate fin dall'inizio, in modo da limitare eventuali problemi successivi. Dopo tutto, una pratica o un'identità che può essere utilizzata in un determinato momento può improvvisamente trasformarsi in una fonte di problemi a causa di condizioni esterne che non possono necessariamente essere previste o controllate.

Tuttavia, queste pratiche non sono sempre facili da implementare. Infatti, oltre alle tecniche descritte sopra, la separazione tra queste diverse identità contestuali dipende da molti altri parametri. In particolare, le relazioni che si stabiliscono con altre persone, siano esse digitali o meno. Non è necessariamente facile avere un'identità contestuale diversa per ogni aspetto della propria personalità o per ogni attività, o evitare che alcune di esse si sovrappongano. Queste identità si evolvono con le attività che le assegniamo e nel tempo. Più a lungo vengono utilizzate, più la loro separazione tende a diminuire. È quindi spesso difficile bilanciare e misurare gli sforzi necessari per creare più identità contestuali rispetto ai benefici attesi. Tanto più che in genere è complicato fare marcia indietro in questo campo.

Alcuni strumenti, come i social media, li rendono addirittura praticamente impraticabili, imponendo una trasparenza assoluta.

9. M. Brennan, R. Greenstadt, 2009, *Practical attacks against authorship recognition techniques*, in *Proceedings of the Twenty-First Innovative Applications of Artificial Intelligence Conference (Atti della ventesima conferenza sulle applicazioni innovative dell'intelligenza artificiale)*. [h

t
[tps://www.aaai.org/ocs/index.php/IAAI/IAAI09/paper/viewFile/257/1017](https://www.aaai.org/ocs/index.php/IAAI/IAAI09/paper/viewFile/257/1017)].

10. Andrew W.E. McDonald, Sadia Afroz, Aylin Caliskan, Ariel Stoleran, Rachel Greenstadt, 2012, *Usare meno istanze della lettera "i": Toward Writing Style Anonymization*, The 12th Privacy Enhancing Technologies Symposium [https://www1.icsi.berkeley.edu/~sadia/papers/anonymouth.pdf].

30.4 Social media: funzioni centralizzate e identità unica

In effetti, i social media tendono a centralizzare funzioni che in precedenza erano svolte da strumenti diversi, dallo scambio di messaggi alla pubblicazione di notizie ai newsgroup. Tendono a sostituire la posta elettronica, la messaggistica istantanea, i blog e i forum.

Allo stesso tempo, si stanno sviluppando nuove funzioni, come una certa vita digitale relazionale in cui l'esistenza di una comunicazione prevale sul suo contenuto, spinta al parossismo dai "pokes", quei messaggi senza contenuto.

¹¹. Il web

2.0 incoraggia l'espressione su temi precedentemente considerati intimi¹².

In definitiva, non c'è molto di nuovo, a parte la centralizzazione di numerose funzioni e pratiche diverse in un unico strumento. In effetti, questo è il

design "all-in-one" e la facilità d'uso di queste piattaforme ne hanno decretato il successo. Ma questa centralizzazione solleva domande sulle conseguenze dell'uso di questi strumenti sulla nostra intimità.

La pressione sociale per l'uso dei social media è molto forte in alcuni luoghi: quando i gruppi li usano per la maggior parte delle loro comunicazioni, dai messaggi interpersonali agli inviti alla pubblicazione di informazioni, non partecipare ai social media significa essere emarginati. Il successo di questi siti si basa sull'"effetto rete": più persone li usano, più è importante essere presenti.

Ma allo stesso tempo, questi social media ci permettono anche di sfuggire a queste pressioni di gruppo e di assumere o sperimentare più facilmente alcune parti della nostra personalità che non sono necessariamente tollerate da questi gruppi.

La centralizzazione di tutte le attività su un'unica piattaforma rende estremamente difficile l'utilizzo di pseudonimi diversi per identità contestuali diverse. Infatti, mettendo tutte le informazioni in un unico luogo, si massimizza il rischio di sovrapposizione delle diverse identità contestuali. Molti social media richiedono un'unica identità, corrispondente all'identità civile di una persona fisica. Questa è una differenza fondamentale rispetto a un modello in cui un individuo può avere diversi blog con toni e contenuti diversi, ciascuno con uno pseudonimo diverso. Inoltre, proprio come nei siti di incontri, dove più si è onesti e migliori sono i risultati, qui più contenuti si forniscono, più si usa questa piattaforma, migliori sono le interazioni.

Ciò è tanto più vero se si considera che l'utilizzo della propria identità civile fa parte delle regole di reti come Facebook, che predispone vari meccanismi per tracciare gli pseudonimi¹³. Queste aziende spingono al limite il *modello di business* della pubblicità mirata e della vendita di profili: "mettono in atto diversi processi tecnici per catturare le identità degli utenti, dalle identità basate sulle loro dichiarazioni, alle identità attive¹⁴ e identità calcolate in base all'analisi

11. Fanny Georges, 2008, *Les composantes de l'identité dans le web 2.0, une étude sémiotique et statistique*, Communication au 76^{ème} congrès de l'ACFAS : Web participatif : mutation de la communication?, Québec, Canada [<https://hal.archives-ouvertes.fr/hal-00332770/>].

12. Alain Rallet e Fabrice Rochelandet, 2010, *La regolamentazione dei dati personali sul web* Réseaux numero 167, Données personnelles et vie privée [<https://www.cairn.info/revue-reseaux-2011-3-page-17.htm>].

13. Nikopik, 2012, *Facebook e le sfuriate* [<https://geeko.lesoir.be/2012/09/24/facebook-demand-e-a-ses-membres-de-denoncer-les-pseudonymes/>].

14. Per "identità attiva" si intendono i messaggi che appaiono automaticamente sulla che dettaglino l'attività di una persona sulla piattaforma. Questi messaggi non rispecchiano ciò che la persona sta che si trovano sul sito, ma quello che stanno facendo lì. Per esempio, "Ana ha cambiato la foto del suo profilo" o "Ana è ora amica di Betty". Fanny Georges, Antoine Seilles, Jean Sallantin, 2010, *Des illusions de l'anonymat - Les stratégies de préservation des données personnelles à l'épreuve du Web 2.0*, Terminal numéro 105, Technologies et usages de l'anonymat à l'heure d'Internet [<https://journals.openedition.org/terminal/1876>].

del loro comportamento (siti visitati, numero di messaggi, ecc.). Sembra che l'anonimato totale stia diventando impossibile in un universo virtuale in cui gli utenti sono prima di tutto consumatori che devono essere osservati".¹⁵

Nel luglio 2011, Max Schrems è riuscito a ottenere tutti i dati che Facebook deteneva su di lui, appellandosi a una direttiva europea. Il file che ha ricevuto è composto da 1.222 pagine ¹⁶che comprendono non solo tutte le informazioni disponibili sul suo profilo, ma anche tutti gli eventi a cui è stato invitato (compresi gli inviti rifiutati), tutti i messaggi inviati o ricevuti (compresi i messaggi cancellati), tutte le foto caricate su Facebook accompagnate da metadati che includono la geolocalizzazione, tutti i "pokes" inviati o ricevuti, tutti gli "amici" (compresi gli "amici" cancellati), i log delle connessioni a Facebook (compresi l'indirizzo IP e la geolocalizzazione), tutte le "macchine" (identificate da un cookie) utilizzate da un profilo, nonché altri profili che utilizzano gli stessi "pokes".

"o la posizione dell'ultima connessione nota a Facebook".

(longitudine, latitudine, altitudine).

Infine, nonostante la dichiarazione del fondatore di Facebook secondo cui l'era della privacy è finita ¹⁷restano da sviluppare e rielaborare diverse strategie, per giocare con i vari margini ancora rilevanti. E questo con l'obiettivo di mettere mano a queste domande fondamentali: "Che cosa vogliamo mostrare?", "Che cosa vogliamo rendere visibile?" e "Che cosa vogliamo nascondere, e a quale costo?"

15. Chantal Enguehard, Robert Panico, 2010, *Approches sociologiques*, Terminal numéro 105, Technologies et usages de l'anonymat à l'heure d'Internet [https://journals.openedition.org/terminal/1868].

16. Damien Leloup, 2012, *Max Schrems: "L'importante è che Facebook rispetti la legge"*, Le Monde [https://www.lemonde.fr/technologies/article/2011/11/23/max-schrems-l-important-c-est-que-facebook-respecte-la-loi-1607705_651865.html].

17. Bobbie Johnson, 2010, *La privacy non è più una norma sociale, dice il fondatore di Facebook*. [https://www.theguardian.com/technology/2010/jan/11/facebook-privacy].

Nascondere il contenuto delle comunicazioni: la crittografia asimmetrica

Nel primo volume di questa guida abbiamo visto che la strada più seria per proteggere i dati da occhi indiscreti è la crittografia.

47 illeggibile da chiunque non sia in possesso della *chiave segreta*.

pagina

31.1 Limiti della crittografia simmetrica

Con la crittografia simmetrica, la stessa chiave segreta viene utilizzata sia per la crittografia che per la decrittografia.

La crittografia simmetrica è ideale per la crittografia di chiavette USB e altri supporti di memorizzazione.

50 supporti di memorizzazione.

Quando si vuole criptare una comunicazione, la cosa è più complicata: la persona che deve decrittare i dati non è la stessa che li ha criptati.

Se la chiave segreta fosse la stessa per tutte le persone con cui si comunica, ognuna di esse sarebbe in grado di decifrare messaggi non destinati a loro. Abbiamo quindi bisogno di tante chiavi segrete quante sono le persone con cui comunichiamo e dobbiamo trovare un modo per scambiare queste chiavi segrete in modo riservato.

31.2 Una soluzione: la crittografia asimmetrica

Negli anni '70 i crittografi hanno trovato una soluzione ai problemi posti dalla crittografia.

crittografia simmetrica creando una crittografia asimmetrica.

47 Con la crittografia asimmetrica, ogni persona che comunica dispone di una coppia di

chiavi: una

chiave *pubblica*, in modo che i messaggi criptati possano essere scritti su di essi, e una *chiave privata* in modo

che

che possono decifrarli e leggerli.

Per ogni scambio, immaginate che le comunicazioni viaggino in una scatola dotata di una speciale serratura.

La chiave pubblica blocca la casella quando viene inviato il messaggio. Tuttavia, non può essere utilizzata per sbloccare la casella.

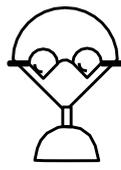
L'altra chiave, quella privata, viene utilizzata solo per sbloccare la scatola e quindi accedere al suo contenuto.

La chiave pubblica può essere distribuita a chiunque. Può anche essere messa online, poiché serve solo a bloccare la casella. La chiave privata, invece, non viene mai condivisa.

pagina

pagina

Nel nostro esempio, la crittografia avviene sul computer di Bea e la decrittografia sul computer di Ana.



Ana

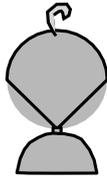


Chiave pubblica di Ana



Chiave privata di Ana

Ana ha un paio di chiavi.



Bea

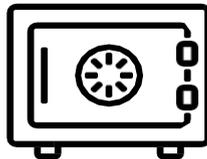


Chiave pubblica di Bea



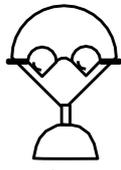
Chiave privata di Bea

Bea ha anche un paio di chiavi.



La scatola di Ana

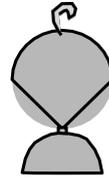
I messaggi destinati ad Ana saranno inseriti in una scatola che sarà chiusa con la sua chiave pubblica.



Ana

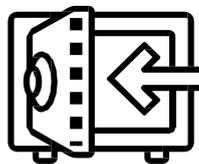


La chiave pubblica di Ana



Bea

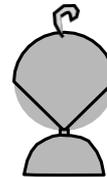
Bea ottiene la chiave pubblica di Ana.



La casella di Ana

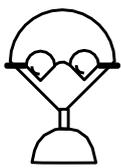


Chiave pubblica di Ana



Bea

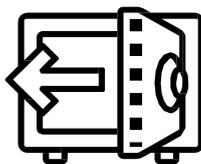
Bea deposita un messaggio nella cassetta di Ana, poi la chiude con la chiave pubblica di Ana.



Ana



La chiave privata di Ana



La scatola di Ana

Ana usa la sua chiave privata per sbloccare la scatola e recuperare il messaggio. Solo la sua chiave privata può sbloccare la scatola.

31.3 Crittografia end-to-end

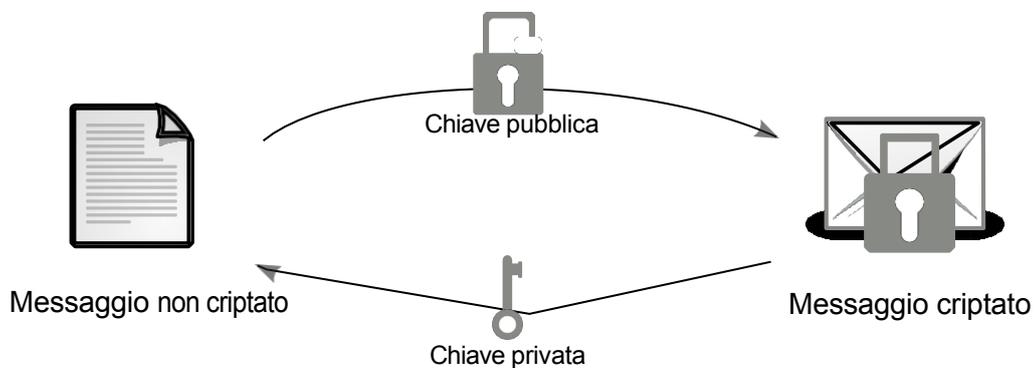
Quando solo chi comunica può leggere i messaggi scambiati, si parla di *crittografia end-to-end*. In linea di principio, ciò impedisce le intercettazioni, anche da parte dei fornitori di telecomunicazioni, dei fornitori di servizi Internet e persino del fornitore di servizi di comunicazione. Con la crittografia end-to-end, nessuno è in grado di intercettare le chiavi crittografiche necessarie per decifrare la conversazione.

I sistemi di crittografia end-to-end sono progettati per resistere a qualsiasi tentativo di sorveglianza o falsificazione, in quanto nessun terzo può decifrare i dati comunicati o memorizzati. In particolare, i servizi che offrono la crittografia end-to-end non sono in grado di consegnare alle autorità una versione decifrata dei messaggi dei loro utenti.

!

31.3.1 Una questione di numeri primi...

In realtà, le chiavi pubbliche e private sono numeri. Ciò che una chiave può criptare, l'altra può decriptare:



La chiave pubblica viene utilizzata per la crittografia e la chiave privata per la decrittografia.

Ma come è possibile che la chiave pubblica possa criptare un messaggio senza permetterne la decriptazione? La crittografia asimmetrica si basa infatti su problemi matematici estremamente difficili da risolvere. L'algoritmo di crittografia RSA, ad esempio, si basa sulla "fattorizzazione dei numeri interi". In altre parole, la scomposizione di un numero intero in numeri primi.

Dato il numero 12, è semplice decomporlo in $2 \times 2 \times 3$. Allo stesso modo, 111 è uguale a 3×37 . Ma come si fa a decomporre il numero seguente, che ha 232 cifre. Ma come si scompone il seguente numero, che ha 232 cifre?

1230186684530117755130494958384962720772853569595334792197322452151726400
 5072636575187452021997864693899564749427740638459251925573263034537315482
 6850791702612214291346167042921431160222124047927473779408066535141959745
 9856902143413

Il risultato è il prodotto di due numeri primi, ciascuno con 116 cifre.

Il problema della fattorizzazione dei numeri interi è stato studiato dai matematici per oltre 2000 anni, ma non è ancora stata trovata una soluzione pratica: la soluzione più conosciuta è quella di provare con tutti i primi possibili.

Con i computer di oggi, questo calcolo richiederebbe molto più tempo di una vita umana.² I numeri più difficili da fattorizzare sono i prodotti di due

1. Questa sezione è tratta da [Wikipedia, 2022, Crittografia end-to-end \[https://fr.wikipedia.org/wiki/Chiffrement_de_bout_en_bout\]](https://fr.wikipedia.org/wiki/Chiffrement_de_bout_en_bout).

2. La fattorizzazione di questo numero di 768 bit nel 2010 ha richiesto 10 operazioni²⁰. I ricercatori che l'hanno effettuato, stimano che il calcolo avrebbe richiesto circa 2.000 anni su un singolo core di un AMD

grandi numeri primi. Sceglieremo quindi numeri sufficientemente grandi che, anche con computer estremamente potenti, non possono essere fattorizzati in un tempo realistico.

Affidarsi a questo metodo significa scommettere che l'avversario ha una potenza di calcolo relativamente limitata. La dimensione della chiave, misurata in bit, è di fondamentale importanza. Se consideriamo che una chiave asimmetrica a 2048 bit è sicura fino al 2030³ una chiave a 512 bit può essere violata in pochi mesi sui personal computer di fascia alta di oggi.⁴ Si tenga presente che ciò che può essere violato da un computer in dieci anni potrebbe essere violato in un anno da dieci computer identici al primo.

Inoltre, se un giorno qualcuno risolverà questo problema matematico, sarà possibile decifrare senza troppe difficoltà gli scambi criptati che sono stati registrati. Questo tipo di raccolta e archiviazione dei dati fa parte delle attività dell'NSA, l'agenzia di intelligence statunitense.⁵ Molti segreti militari e commerciali verrebbero quindi rivelati a coloro che hanno accesso a queste registrazioni. In altre parole, possiamo immaginare un bel pasticcio tra aziende concorrenti e agenzie di intelligence nemiche...

Nel frattempo, gli attacchi ai crittosistemi asimmetrici sono attualmente rivolti al modo in cui sono implementati in un particolare software, o a un errore nel codice sorgente, piuttosto che al principio matematico del sistema.

31.4 Firma digitale

Le coppie di chiavi utilizzate per la crittografia asimmetrica possono essere usate anche per dimostrare l'autenticità di un messaggio. Come funziona? Riprendiamo l'esempio di Bea che invia un messaggio ad Ana. Questa volta Bea vuole firmare digitalmente il suo messaggio in modo che Ana possa essere sicura che sia lei l'autrice.

Nel primo volume di questa guida abbiamo parlato di *checksum*, o *impronta digitale*: un numero utilizzato per verificare l'integrità di un messaggio. Questa impronta digitale viene utilizzata anche per firmare i dati digitali. Per prima cosa, il computer di Bea calcola l'*impronta digitale* del messaggio che invierà ad Ana.

Successivamente, l'impronta digitale viene crittografata con la chiave privata di Bea: questa è la *firma digitale*. Esatto: l'impronta digitale viene crittografata con la chiave privata di Bea, che solo lei possiede, e non con la chiave pubblica di Ana. Questa firma viene utilizzata per autenticare il mittente, non il destinatario. Come abbiamo appena visto, le chiavi pubbliche e private sono in realtà due numeri scelti in modo tale che uno possa decifrare ciò che l'altro ha criptato. Quindi nulla vieta di criptare qualcosa con la chiave privata. La chiave pubblica viene poi utilizzata per decifrarlo.

Bea invia poi il messaggio con la sua firma ad Ana.

Per verificare la firma, il computer di Ana calcola anche l'impronta digitale del messaggio e decifra la firma in parallelo.

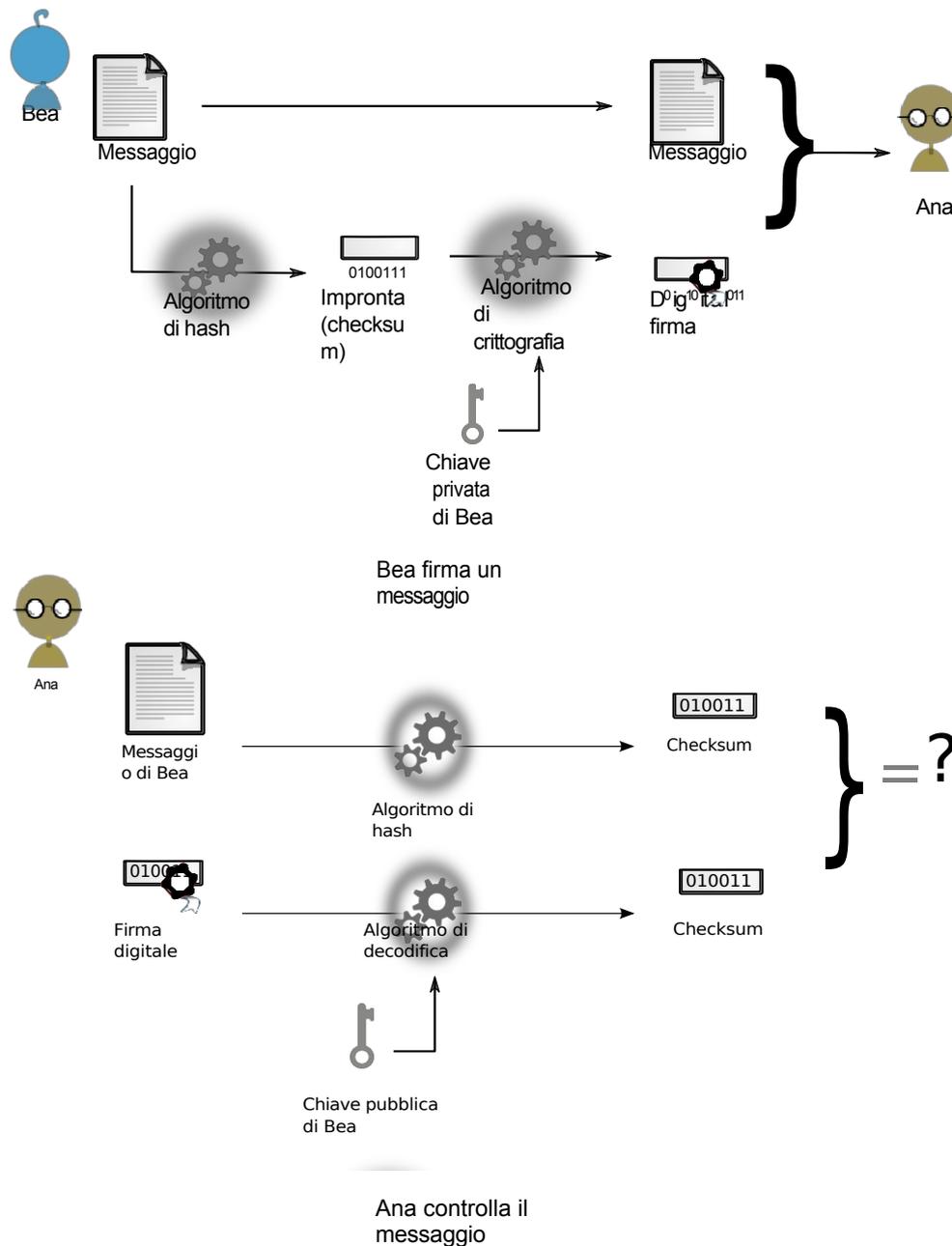
Poiché è cifrata con la chiave privata di Bea, per decifrare questa firma è sufficiente la chiave pubblica di Bea. Se l'impronta digitale del messaggio ricevuto corrisponde alla firma

Opteron a 2,2 GHz, che corrisponde a diverse centinaia di anni su un processore attuale (Klein-jung et al., 2010, *Factorization of a 768-bit RSA modulus* [https://eprint.iacr.org/2010/006.pdf] -in inglese).

3. Agence nationale de la sécurité des systèmes d'information, 2014, *Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes crypto graphiques* [https://www.ssi.gouv.fr/uploads/2014/11/RGS_v- 2-0_B1.pdf].

4. S. A. Danilov, I. A. Popovyan, 2010, *Fattorizzazione di RSA-180* [https://eprint.iacr.org/2010/270.pdf] (in inglese).

5. Nicole Perlroth, Jeff Larson e Scott Shane, 2013, *N.S.A. Able to foil Basic Safeguards of Privacy on Web*, The New York Times [https://archive.org/details/n.-s.-a.-able- to-foil-basic-safe-guards-of-privacy-on-web].



decifrato (che non è altro che l'impronta digitale del messaggio calcolata dal computer di Bea), Ana è sicura dell'autenticità del messaggio ricevuto. Bea conserva la sua chiave privata in un luogo sicuro. È quindi l'unica che ha potuto criptare l'impronta digitale che Ana ha decriptato con la chiave pubblica di Bea.

Lo svantaggio di questa certezza è che per Bea, in possesso della chiave privata, sarà più difficile negare di essere l'autore del messaggio.

31.5 Verifica dell'autenticità della chiave pubblica

La crittografia asimmetrica consente di crittografare e firmare i messaggi senza dover prima scambiare un segreto condiviso.

Tuttavia, non risolve una questione importante: come posso essere sicuro di avere davvero la vera chiave pubblica del mio destinatario e che non si tratti di qualcuno che ha usurpato la sua chiave pubblica per poter intercettare i miei messaggi, dandomi una falsa impressione di sicurezza?

31.5.1 L'attacco del mostro al centro

Prendiamo l'esempio di Ana, che desidera ricevere un messaggio criptato da Bea, in presenza di un avversario, Carol, che potrebbe avere accesso ai messaggi scambiati:

- Ana inizia inviando a Bea la sua chiave pubblica. Carole può leggerla.
- Bea cripta il suo messaggio con la chiave pubblica ricevuta e lo invia ad Ana.
- Carol, che non possiede la chiave privata di Ana, ma solo la sua chiave pubblica, non può decifrare il messaggio.
- Ana può decifrare il messaggio utilizzando la chiave privata che tiene in un luogo sicuro.

Tuttavia, se Carole riesce a modificare gli scambi tra Ana e Bea, le cose si complicano:

- Quando Ana invia la sua chiave pubblica a Bea, Carole la intercetta e invia a Bea, al posto di quella di Ana, una chiave pubblica di cui detiene la corrispondente chiave privata.
- Bea cripta il suo messaggio con la chiave pubblica ricevuta e lo invia ad Ana. Ma la chiave ricevuta apparteneva a Carole: l'ha sostituita a quella di Ana.
- Carole intercetta nuovamente il messaggio. Questa volta, però, è criptato con la sua chiave pubblica, di cui possiede la chiave privata. Può quindi decifrare il messaggio per leggerlo e modificarlo, se necessario. Quindi cripta nuovamente il messaggio con la vera chiave pubblica di Ana, prima di inviarlo ad Ana.
- Ana può quindi decifrare il messaggio con la sua chiave privata, senza rendersi conto di nulla.

Ad esempio, Bea è convinta di utilizzare la chiave di Ana, mentre in realtà sta usando la chiave di Carole. Allo stesso modo, Carole può usurpare la chiave pubblica di Bea e falsificare la firma sul messaggio inviato da Bea ad Ana. Ana riceverà un messaggio criptato debitamente firmato... da Carole.

Questo attacco è noto come *attacco monster-in-the-middle (MitM)*.⁶ Nel nostro esempio, Carole era il *mostro nel mezzo*, in grado di leggere e modificare la comunicazione crittografata fingendo di essere l'altra parte della comunicazione.

Un avversario può posizionarsi come un *mostro nel mezzo* con vari mezzi.

Il provider di servizi Internet (ISP), ad esempio, si trova in una posizione particolarmente favorevole, poiché tutto il traffico passa inevitabilmente attraverso di lui. Allo stesso modo, un nodo di rete *di grandi dimensioni* attraverso il quale passa una quantità significativa di traffico si troverà in una posizione favorevole per effettuare questo attacco.⁷ Infine, un avversario con accesso alla rete locale in uso può sempre instradare il traffico di rete attraverso il suo computer, utilizzando tecniche più specifiche.⁸

Per difendersi da questo attacco, Bea deve avere un modo per verificare che la chiave pubblica che sta utilizzando sia effettivamente quella di Ana. Anche se la chiave pubblica non è un'informazione riservata, è importante assicurarsi della sua *autenticità* prima di utilizzarla.

A volte, il modo più semplice per Bea è incontrare Ana per verificare che la chiave pubblica in suo possesso sia davvero la sua. Non importa se Carole è presente

6. L'uso comune è parlare di *attacco man-in-the-middle* [https://fr.wikipedia.org/wiki/Attaque_del%27homme_du_milieu]. La comunità hacktivista mette in discussione l'inclusività di questo concetto, utilizzando espressioni alternative: *man-in-the-middle*, *person-in-the-middle*, *machine-in-the-middle*, *mostro nel mezzo* [<https://sindominio.net/sincensura/fr/post/informe/#inspection-profonde-des-paquets>], ecc.

7. Pixellibre.net, 2011, *#OpSyria: le prove parlano da sole*. [<https://pixellibre.net/2011/10/opsyria-bluecoat-censure-leaks-censorship-syrie/>], o più precisamente, in inglese Jakub Dalek e Adam Senft, 2011, *Behind Blue Coat, Investigations of commercial filtering in Syria and Birmania*, The Citizen Lab [<https://citizenlab.ca/2011/11/behind-blue-coat/>].

8. Wikipedia, 2014, *ARP poisoning* [https://fr.wikipedia.org/wiki/ARP_poisoning].

al momento di questo incontro: avverrà solo una verifica della chiave *pubblica* e non verranno scambiati segreti (tranne il fatto che Bea e Ana desiderano comunicare, ma data la sua posizione, Carole potrebbe saperlo in altri modi). Una volta completata la verifica, è possibile impostare la crittografia end-to-end tra Ana e Bea.

Tra i due, circolerà un messaggio il cui contenuto sarà criptato; solo l'intestazione della comunicazione, sia essa una richiesta HTTP o un'e-mail, circolerà *in chiaro*.

pagina
217

Tuttavia, spesso accade che Bea non possa incontrare Ana, soprattutto se non la conosce: se incontra qualcuno che si presenta come Ana, Bea non può essere sicura che sia davvero Ana. Questo è di solito il caso in cui si vogliono criptare le connessioni a un sito web: non si conoscono le persone che ci sono dietro.

31.5.2 Infrastruttura a chiave pubblica gerarchica

La prima soluzione comunemente utilizzata è quella di far certificare le chiavi pubbliche da autorità fidate, firmandole digitalmente: si tratta dei cosiddetti *certificati*. Ana chiede all'autorità di certificare la sua chiave pubblica. L'autorità verifica l'identità di Ana, ad esempio chiedendo la sua carta d'identità, e poi firma digitalmente la sua chiave. Prima di utilizzare la chiave di Ana, Bea (o il suo computer) controlla che sia stata firmata da un'autorità che ritiene affidabile. Questa procedura è nota come *infrastruttura a chiave pubblica gerarchica* (o *PKI gerarchica*).

pagina
252

Il protocollo TLS

È il principio comunemente utilizzato per autenticare i siti web o i server di posta elettronica con cui il computer stabilisce una connessione crittografata. Le ragioni più comuni per stabilire una connessione crittografata a un sito web sono la protezione delle password, ad esempio quando si accede a un account di posta elettronica, o la protezione dei dati bancari, quando si fanno acquisti online. Il protocollo utilizzato per questo tipo di crittografia si chiama TLS (ex SSL).⁹

pagina
208

Questo standard incapsula il normale protocollo applicativo in un livello di crittografia. Ad esempio, il protocollo web HTTP, quando è incapsulato in TLS e quindi criptato, è chiamato HTTPS. Lo stesso vale per i protocolli di posta elettronica POPS, IMAPS e SMTPS.

pagina
199

Il protocollo TLS può essere spiegato come un saluto molto cordiale tra il computer di origine e il server di destinazione. Essi cifrano la comunicazione scambiandosi le chiavi di cifratura.

pagina
201

Il problema delle autorità di certificazione

Le autorità di certificazione (CA) garantiranno che le chiavi di crittografia siano quelle corrette e produrranno un *certificato elettronico* a tale scopo. Tuttavia, questa soluzione sposta solo il problema: bisogna fidarsi dell'autorità di certificazione. In genere si tratta di società commerciali e, più raramente, di autorità pubbliche.

Microsoft, Apple e Mozilla includono le autorità di certificazione governative tra le autorità di certificazione riconosciute dai loro browser web.¹⁰ Mozilla Firefox include¹¹ autorità di certificazione governative

9. SSL per Secure Sockets Layer è il predecessore di TLS per Transport Layer Security.

10. Christopher Soghoian, Sid Stamm, 2011, *Bugie certificate: Detecting and Defeating Government Interception Attacks Against SSL*, Financial Cryptography and Data Security [https://s3.amazonaws.com/files.cloudprivacy.net/ssl-mitm.pdf].

11. Common CA Database, 2017, *Certificati CA in Firefox* [https://ccadb-public.secure.force.com/mozilla/CACertificatesInFirefoxReport].

(cinese, catalano, spagnolo, olandese, turco), società di certificazione (Entrust, GoDaddy, Verisign) e società di telecomunicazioni (Amazon, Deutsche Telekom, Google).

Firefox include anche l'autorità dell'Internet Security Research Group

¹²). Questo gruppo ha creato Let's Encrypt ¹³ un'autorità di certificazione gratuita, aperta e automatizzata lanciata nel 2016 che semplifica l'accesso a certificati elettronici validi per i piccoli server.

pagina
254

Ma i governi, che spesso possono posizionarsi come *mostri nel mezzo*, hanno il potere di designare qualsiasi certificato come valido per un sito web firmandolo con la loro autorità di certificazione: i browser web che lo includono non se ne accorgerebbero.

Nel caso delle aziende, il loro obiettivo primario non è certificare le identità, ma guadagnare vendendo la certificazione dell'identità come servizio. Ma verificare un'identità è costoso. Che prova abbiamo che lo stiano facendo correttamente? Che le chiavi private che usano per firmare siano conservate in un luogo sicuro? Ancora una volta, è una questione di fiducia. Possiamo solo sperare che, anche solo per mantenere la loro attività, queste autorità di certificazione facciano il loro lavoro correttamente...

pagina
235

Solo che... gli esempi dimostrano che a volte lo fanno molto male. Nel 2008, ad esempio, i ricercatori sono riusciti a creare certificati "validi" contraffatti, in quanto sei autorità di certificazione utilizzavano ancora algoritmi crittografici di cui era nota la rottura dal 2004. ¹⁴ I certificati creati in questo modo sono certificati "veri-falsi": il browser web li riconosce come reali, perché nonostante la loro origine fraudolenta, tutto fa pensare che siano stati emessi da un'autorità riconosciuta.

Nel 2011 sono stati creati nove certificati falsi firmati da Comodo, un'autorità di certificazione. Almeno uno di questi certificati è stato utilizzato sul Web. ¹⁵ L'azienda ha impiegato più di una settimana per riconoscere pubblicamente questa compromissione - e probabilmente molte aziende non lo fanno in queste situazioni, per evitare la cattiva pubblicità e le perdite finanziarie che ne derivano. ¹⁶ e le perdite finanziarie che ne derivano.

Inoltre, sembra che, su ordine della polizia o dei tribunali del loro paese, alcune autorità di certificazione forniscano ai poliziotti certificati falsi, emessi a nome delle entità che desiderano controllare. ¹⁷ Detto questo, questi certificati falsi devono essere collocati nel posto giusto su Internet e combinati con attacchi da parte del *mostro di mezzo*, per poter essere sfruttati al meglio. Infine, poiché le nostre connessioni attraversano generalmente diversi Paesi, questo attacco può essere messo in atto da un Paese diverso da quello da cui ci stiamo connettendo.

pagina
254
pagina
208

In un opuscolo di vendita, Packet Forensics, un'azienda statunitense che vende apparecchiature per la sorveglianza di rete, scrive che "per utilizzare il nostro prodotto in questo scenario, gli utenti governativi hanno la possibilità di importare una copia di una chiave legittima che possono ottenere (potenzialmente attraverso una requisizione del tribunale)". ¹⁸ L'amministratore delegato di Packet Forensics avrebbe confermato verbalmente all'autore di

12. <https://www.abetterinternet.org/about/>

13. <https://letsencrypt.org/fr/about/>

14. Alexander Sotirov et al., 2008, *MD5 considered harmful today - Creating a rogue CA certificate* [<https://www.win.tue.nl/hashclash/rogue-ca/>].

15. Comodo, 2011, *Comodo Fraud Incident* [<https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html>].

16. Jacob Appelbaum, 2011, *Rilevare le compromissioni dell'autorità di certificazione e i browser Web collusione* [<https://blog.torproject.org/detecting-certificate-authority-compromises-and-web-browser-collusione>].

17. Christopher Soghoian, Sid Stamm, 2011, *Bugie certificate: Detecting and Defeating Government Interception Attacks Against SSL*, Financial Cryptography and Data Security [<https://s3.amazonaws.com/files.cloudprivacy.net/ssl-mitm.pdf>].

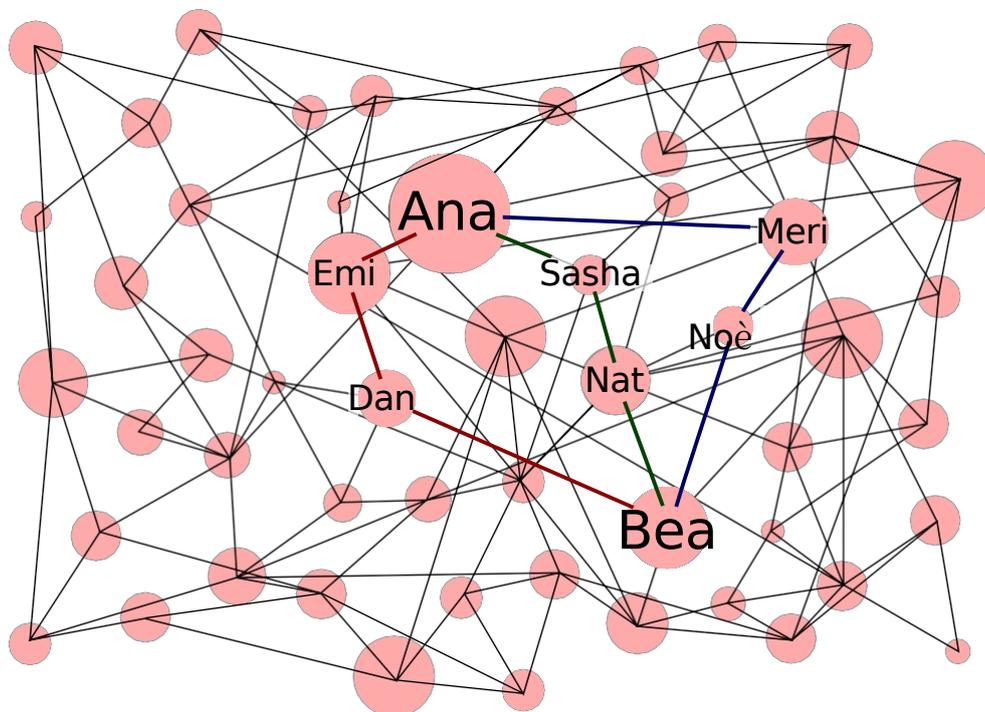
18. "Per utilizzare il nostro prodotto in questo scenario, gli utenti governativi hanno la possibilità di importare una copia di qualsiasi chiave legittima ottenuta (potenzialmente per ordine del tribunale)". Citazione dal documento di Christopher Soghoian e Sid Stamm citato sopra.

lo studio di clienti governativi che collaborano con le autorità di certificazione per ottenere certificati falsi da utilizzare nelle operazioni di sorveglianza ¹⁹.

31.5.3 Rete di fiducia

Un'altra soluzione alla questione dell'autenticità delle chiavi pubbliche è la *rete di fiducia*.

Piuttosto che fidarsi di qualche autorità centralizzata, si tratta di stabilire un legame di fiducia da persona a persona. Bea non conosce Ana, ma conosce Dan, che conosce Emi, che conosce Ana. Quindi *c'è un percorso di fiducia* tra Bea e Ana. Se ci fosse solo questo percorso di fiducia, significherebbe che Bea ripone un alto livello di fiducia in Emi, che non conosce direttamente. Ma Bea conosce anche Nat, che conosce Sasha, che conosce anche Ana. Conosce anche Noah, che conosce Meri, che conosce Ana. Ci sono quindi tre percorsi di fiducia tra Ana e Bea, che non ha bisogno di avere una fiducia totale in tutte le parti coinvolte nella certificazione.



Una rete di fiducia che lega Ana e Bea

Queste reti di fiducia sono comunemente utilizzate per autenticare software e comunicazioni personali, come le e-mail, utilizzando lo standard OpenPGP. Purtroppo, non sono comunemente utilizzate per autenticare i siti web, sebbene ciò sia tecnicamente possibile. ²⁰.

Le reti di fiducia permettono quindi di difendersi dagli attacchi del mostro di mezzo, senza doversi affidare ad autorità centralizzate. Tuttavia, partecipare a una rete di fiducia richiede la rivelazione dei legami tra persone, reti di amici o attivisti. Vogliamo davvero pubblicare l'elenco dei nostri amici o compagni?

pagina
254

19. Questa citazione si trova in una versione in bozza, datata aprile 2010, dell'articolo di Christopher Soghoian e Sid Stamm citato sopra; questa versione è disponibile su [cryptome.org \[https://cryptome.org/ssl-mitm.pdf\]](https://cryptome.org/ssl-mitm.pdf) (in inglese).

20. Per esempio, la [Monkeysphere \[https://manpages.debian.org/bullseye/monkeysphere/monkeysphere.1.en.html\]](https://manpages.debian.org/bullseye/monkeysphere/monkeysphere.1.en.html) estende l'uso delle reti di fiducia OpenPGP all'autenticazione dei siti web.

31.6 Riservatezza persistente

[pagina
249]

Come abbiamo visto, chiunque sia in possesso di una chiave segreta può usarla per decifrare un testo che è stato criptato utilizzando la chiave pubblica $\bar{a}d\ \bar{e}ss\bar{a}$ associata. Si tratta di una proprietà molto utile, ma in alcuni casi può rivelarsi imbarazzante.

Supponiamo che un malintenzionato registri una conversazione online crittografata tra due persone. Naturalmente, non sarà in grado di leggere immediatamente il contenuto della conversazione. Tuttavia, potrebbe avere l'idea di introdursi nelle case o nei computer di queste persone e impossessarsi delle loro chiavi private. In questo caso, sarà in grado di leggere, *a posteriori*, tutte le conversazioni passate che ha memorizzato.

Questo è stato il caso di qualche anno fa, quando gli amministratori del server di *autistici.org* si sono accorti durante un processo che la polizia era entrata in possesso delle chiavi segrete installate sul loro server, perché stavano producendo scambi di e-mail per il verbale che normalmente non avrebbero potuto leggere.²¹

Per evitare che un segreto comprometta molti altri segreti che dipendono da esso (come il contenuto delle conversazioni criptate di messaggistica istantanea, gli scambi di e-mail *e così via*), alcuni pacchetti software includono le cosiddette funzioni di riservatezza persistente²² (o *Perfect Forward Secrecy*).

Garantiscono che anche se un giorno un segreto a lungo termine, tipicamente una chiave privata, viene scoperto da un avversario, gli scambi saranno protetti dall'analisi a posteriori.

Infatti, invece di utilizzare direttamente la chiave pubblica per criptare le comunicazioni, questo tipo di crittografia utilizza un protocollo di scambio segreto progettato per funzionare anche su un canale di comunicazione insicuro, negoziando una chiave temporanea a ogni sessione di comunicazione. In questo caso, la chiave segreta di una coppia di chiavi serve solo a garantire che la persona giusta sia contattata, firmando lo scambio segreto.

] Questo segreto temporaneo viene poi utilizzato per criptare simmetricamente le comunicazioni.

[pagi --
na 55]

Una volta terminata la comunicazione, il software coinvolto è sufficiente per dimenticare questo segreto temporaneo. Anche se qualcuno dovesse mettere le mani sulle chiavi segrete di entrambe le parti, la riservatezza della comunicazione non sarebbe compromessa: i partecipanti allo scambio non hanno più accesso ad esse.

Per proteggere la privacy degli utenti di Internet, il protocollo TLS implementa la riservatezza persistente.

31.7 Sintesi e limiti

La crittografia asimmetrica è quindi un buon complemento alla crittografia simmetrica ogni volta che dobbiamo proteggere non solo i nostri dati, ma anche il contenuto delle nostre comunicazioni: scambi di e-mail, navigazione sul Web, conversazioni di messaggistica istantanea *e così via*. Non è così complicata da usare come si potrebbe pensare, e rendere la crittografia una routine significa evitare che informazioni particolarmente sensibili vadano perse nella confusione.

Per concludere questo piccolo tour delle tecniche crittografiche, vale la pena ricordare che la crittografia, per quanto difficile da violare, ha dei limiti, che abbiamo toccato nel primo volume di questa guida. Questi limiti riguardano in particolare la fiducia che riponiamo in

[pagi
na
50]

21. Austitci, 2005, *CRACKDOWN*, violato autistici.org - alcune note legali [https://www.autistici.org/ai/crackdown/legal_en.html].

22. Wikipedia, 2014, *Privacy persistente* [https://fr.wikipedia.org/wiki/Confidentialit%C3%A9_persistente].

nel computer e nel software a cui la crittografia e la decrittografia (e quindi la *testo in chiaro*) è affidato. Inoltre, influiscono sugli obblighi legali di fornire autorità i mezzi per decriptare le comunicazioni quando richiesto. Infine, a pagina 50 si parla dell'evoluzione della crittografia: ciò che è sicuro oggi potrebbe non esserlo domani. Infine, mentre la crittografia nasconde il contenuto della comunicazione, le parti coinvolte (chi sta comunicando con chi) rimangono visibili.

Routing Tor o onion

Abbiamo visto che è possibile nascondere il contenuto delle comunicazioni attraverso la crittografia. Tuttavia, è sempre possibile per gli avversari determinare la fonte e la destinazione delle comunicazioni. Tor risolve questo problema.

32.1 Il problema: nascondere origine e destinazione

Le lettere cartacee riportano l'indirizzo del destinatario e quello del mittente. Allo stesso modo, su Internet, ogni pacchetto contiene un indirizzo IP di origine (mittente) e un indirizzo IP di destinazione (destinatario). I server a cui ci si connette possono quindi capire da dove proviene il pacchetto. Anche quando i dati sono criptati, gli indirizzi rimangono visibili.

Il percorso tra il mittente e il destinatario coinvolge più router. Ognuno di questi router ispeziona l'indirizzo IP di destinazione e inoltra il pacchetto al router vicino più vicino. In questo modo, possono vedere che il mittente sta comunicando con il destinatario, proprio come i postini possono vedere da dove viene e dove va un pacco.

In particolare, il fornitore di servizi Internet è in grado di fare un profilo esaustivo dell'uso di Internet da parte dei suoi abbonati. Allo stesso modo, tutti i router di Internet che vedono passare i nostri pacchetti possono profilare il nostro comportamento.¹

32.2 Una soluzione: Tor

Tor è l'acronimo di *The Onion Router*. È un software gratuito di pagina 39. In generale, Tor cerca di risolvere tre problemi di privacy²:

In primo luogo, Tor impedisce ai siti web e ad altri servizi di conoscere la posizione degli utenti di Internet, che possono utilizzare per creare database sulle loro abitudini e interessi. Con Tor, le connessioni a Internet non rivelano i dati personali per impostazione predefinita.

In secondo luogo, Tor impedisce di spiare il traffico a livello locale (come gli ISP o un avversario che abbia accesso al Wi-Fi di casa) e di vedere quali informazioni vengono consultate su quali server. Inoltre, impedisce loro di limitare ciò che può essere visualizzato e pubblicato.

1. La maggior parte di questa sezione è stata adattata dal sito web di Tor: *Quale protezione fornisce Tor?* [https://support.torproject.org/fr/about/protections/].

2. Questa sezione è tratta dal sito web del Progetto Tor: *Quale protezione offre Tor?* [https://support.torproject.org/fr/#protections].

In terzo luogo, Tor instrada le connessioni attraverso diversi relay Tor, in modo che nessun singolo relay Tor possa sapere cosa viene fatto. Poiché questi relay sono gestiti da organizzazioni o individui diversi, la distribuzione della fiducia garantisce una maggiore sicurezza rispetto a una semplice VPN.

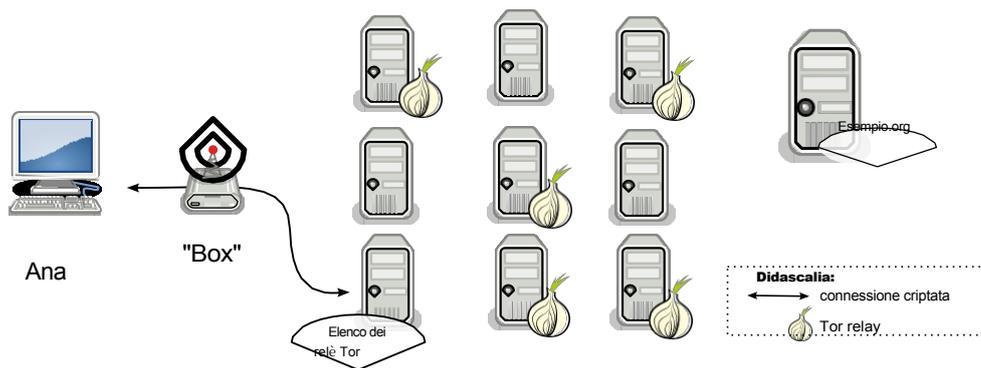
pagina

227

32.2.1 Creare un circuito

Invece di seguire un percorso diretto dalla sorgente alla destinazione, i pacchetti di dati seguono un percorso attraverso una serie di relè, scelti in parte a caso.³ Questo rende impossibile per gli avversari associare la sorgente e la destinazione osservando un singolo punto.

Ad esempio, quando Ana vuole collegarsi a *example.org* usando Tor, il suo computer stabilisce prima un circuito Tor.



Connessione a una directory di relay Tor

Per farlo:

1. Tor recupera un elenco di nodi Tor disponibili da una directory;
2. Tor sceglie un primo relay da questo elenco e stabilisce con esso una connessione criptata;
3. Tor sceglie un secondo relay dalla lista e stabilisce una connessione criptata a questo secondo relay attraverso il primo relay;
4. Infine, Tor sceglie un terzo relay dall'elenco, chiamato nodo di uscita, e stabilisce una connessione cifrata a questo terzo relay attraverso il primo e il secondo relay.

Questo insieme di tre relè forma il cosiddetto *circuito Tor*.

32.2.2 Funzionamento del circuito

I dati passano quindi attraverso questi tre relay prima di raggiungere il server di destinazione (in questo caso *example.org*). La risposta del server seguirà lo stesso percorso, al contrario.

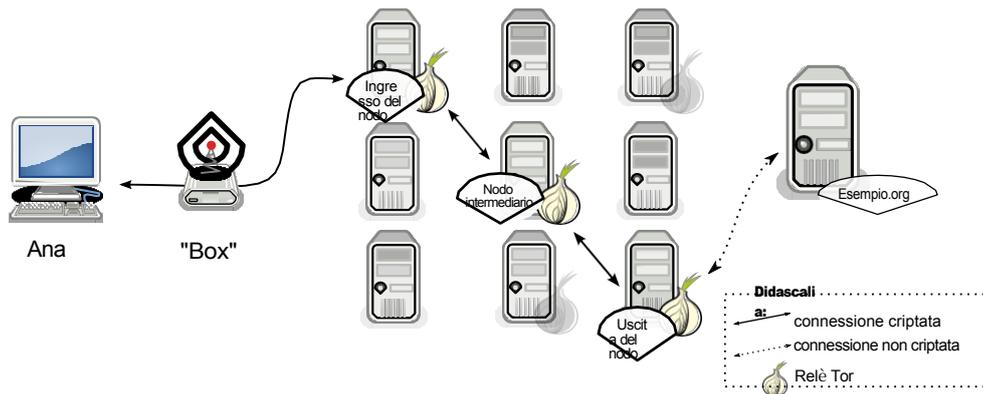
Il circuito viene percorso passo dopo passo e ogni relè lungo il percorso conosce solo quello che gli ha trasmesso i dati e quello a cui li ritrasmetterà. Nessun singolo relay conosce il percorso completo di un pacchetto di dati. Un eventuale intermediario o un relay compromesso non può analizzare facilmente il traffico di rete per stabilire una relazione tra la fonte e la destinazione di una connessione. Quindi nessuno dei computer sa che il computer di Ana si sta collegando a *example.org*.

Si noti che un circuito Tor è composto da tre intermediari. Se il circuito fosse costituito da un singolo relè, comprometterlo significherebbe mettere a repentaglio la nostra

pagina

235

3. La scelta dei relè avviene rispettando vari vincoli elencati nelle specifiche di Tor: **Roger Dingledine, Nick Mathewson, 2021, Tor Path Specification** [<https://gitweb.torproject.org/torspec.git/tree/path-spec.txt>], sezione "2.2. Selezione del percorso e vincoli".



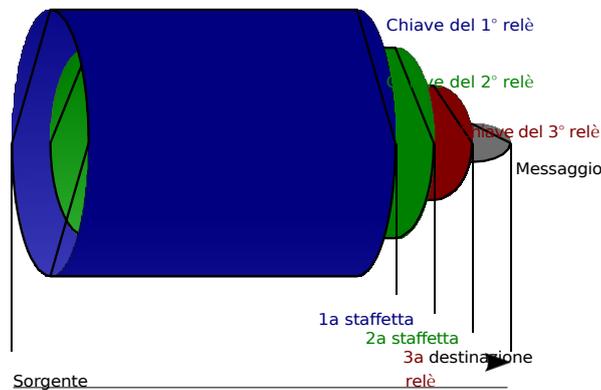
Utilizzo di un circuito Tor

riservatezza, in quanto questo intermediario sarebbe a conoscenza sia dell'origine di una comunicazione che della sua destinazione. L'uso di tre relay evita questa sovrapposizione senza rallentare troppo la connessione. A parte i nodi di uscita, nessun relay può conoscere il contenuto delle comunicazioni che trasporta.

I "nodi di uscita" si distinguono dagli altri relay Tor per due aspetti: sono gli unici che possono potenzialmente vedere il traffico in chiaro (se gli utenti Tor non usano HTTPS, ad esempio) e sono gli unici esposti su Internet. In altre parole, il traffico di chi usa Tor sembra provenire da questi nodi di uscita. Inoltre, le persone che gestiscono i nodi di uscita sono talvolta considerate responsabili del traffico che passa attraverso quel nodo e devono spiegare perché.⁴

Come ulteriore precauzione, il circuito Tor utilizzato viene automaticamente sostituito ogni dieci minuti senza attività.⁵

32.2.3 Crittografia a cipolla



Principio di instradamento a cipolla

Abbiamo visto che il computer di Ana negozia una connessione criptata con ogni relè del circuito utilizzato. Di conseguenza, i dati che desidera trasmettere a *example.org* hanno diversi livelli di crittografia all'uscita del suo computer:

- crittografia della connessione al primo relè ;

4. Nos oignons, 2020, *Rapport Moral* [https://nos-oignons.net/Association/Rapport_moral_2019-2020.pdf] p. 5, sezione Abusi.

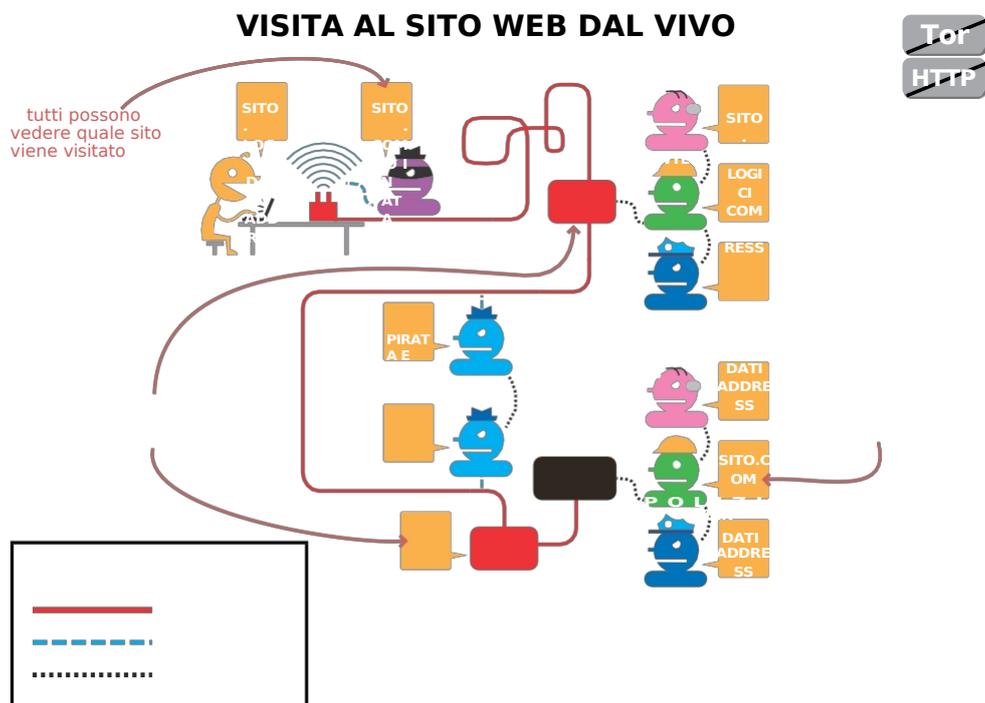
5. Progetto Tor, 2021, *Quanto spesso Tor cambia i suoi percorsi?* [https://support.torproject.org/en/about/change-paths/].

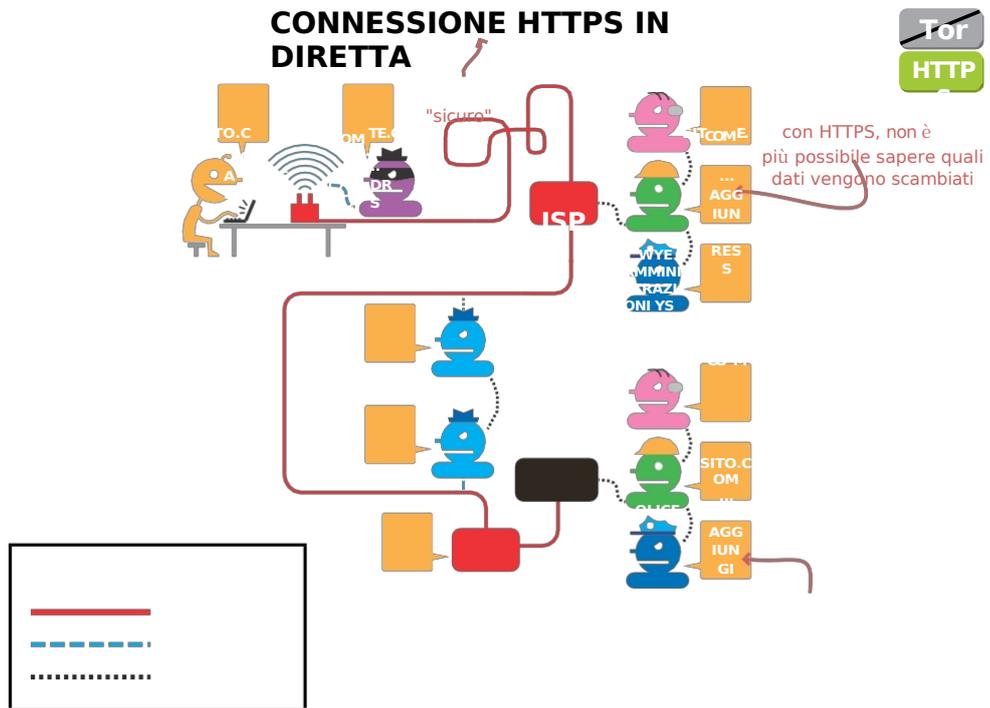
- crittografia della connessione al secondo relè ;
- crittografia della connessione al terzo relè.

Come una cipolla con diverse pelli, i dati di Ana saranno *avvolti* da diversi strati di crittografia. Per questo motivo si può parlare di "*cipolla*". Ogni volta che passano attraverso un relay, viene *rimosso* uno strato di crittografia. Ogni strato è crittografato in modo da poter essere letto solo dal relay che deve rimuoverlo. Ciò significa che nessuno dei relè può decifrare le informazioni che non sono destinate a loro.

32.2.4 Tor illustrato

Ecco quattro diagrammi che illustrano cosa possono vedere o spiare i terzi, a seconda che si utilizzi o meno l'HTTPS e che si utilizzi o meno Tor quando si visita un sito web.





LEGGENDA

- Connessione a Internet
- Ascoltare
- Condivisione dei dati

il sito può ancora localizzarci

Connessione live HTTPS



il nodo di ingresso
conosce il nostro
indirizzo

b
u
t

h
e

c
a
n

s
e
e

c
h
e

w
e

u
s
e

T
o
r

ma è
l'unico nodo
che lo
conosce

il sito non sa
più da dove
proviene la
nostra
connessione

il nodo di uscita può
osservare
dati scambiati

LEGGENDA

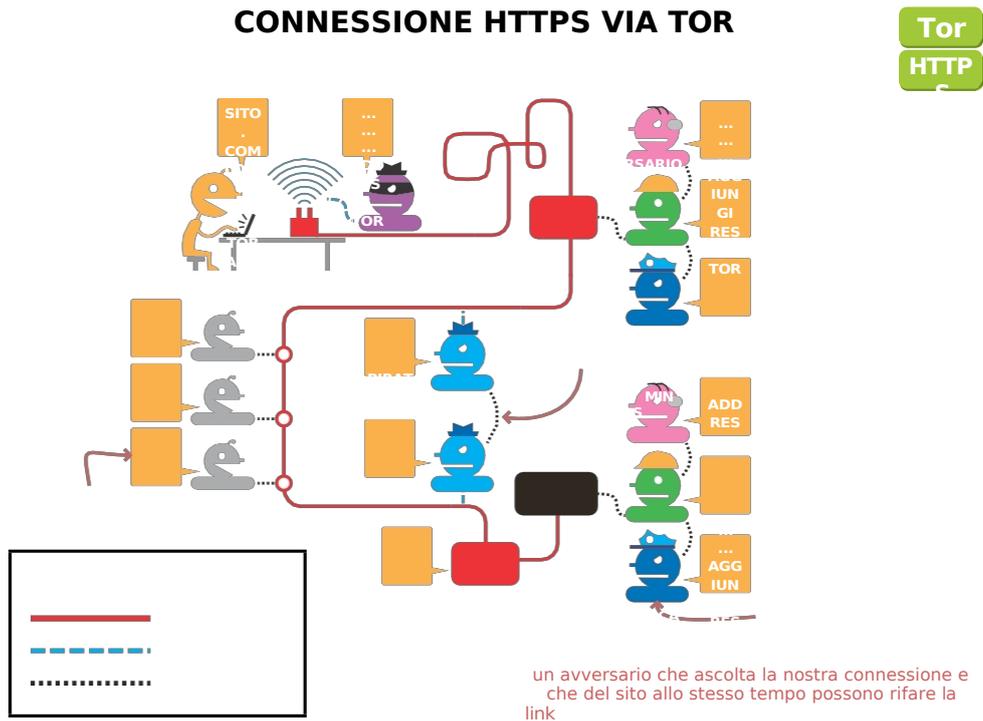
**Connessione a
Internet**

Ascoltare

Condivisione dei dati

d'altra parte, sa che
Tor è stato utilizzato

Visitare un sito web tramite Tor



con HTTPS, il nodo di uscita conosce solo la destinazione

LEGGENDA

Connessione a Internet

Ascoltare

Condivisione dei dati

la polizia può anche sequestrare il server invece di chiedere admins

Connessione HTTPS tramite Tor

32.3 servizi di cipolla

Se si desidera fornire servizi (come un sito web o un server di posta istantaneo) senza rivelare l'indirizzo del server (IP), è possibile utilizzare un servizio onion.⁶ Come per ogni utente Tor, l'indirizzo IP del server impostato non viene rivelato. Chiunque voglia connettersi ad esso dovrà utilizzare la rete Tor. In questo modo, i servizi onion proteggono la riservatezza sia del server che delle persone che lo utilizzano.

Per connettersi, gli utenti di Internet utilizzeranno il sistema di "rendezvous point" di Tor. Il "punto di incontro" è il terzo relè per ciascuno dei due protagonisti dello scambio: il cliente e il servizio a cipolla. Il cliente costruisce un circuito Tor

con questo "punto di incontro" come terzo relè. Il servizio onion fa lo stesso. Il cliente e il servizio onion si "incontrano" e possono scambiarsi informazioni.

Questi servizi a cipolla possono essere utilizzati, ad esempio, per creare un sito web senza temere la censura. L'identificazione della posizione fisica del server (o delle persone che pubblicano o visitano il sito web), infatti, è resa molto più difficile che con un sito web convenzionale: richiede la creazione di un attacco alla rete Tor.

pagina

268

32.4 Partecipare alla rete Tor

La rete Tor è volontaria. È aperta a tutti, poiché nessun relay può sapere da dove provengono o dove vanno le comunicazioni. Chiunque può quindi gestire un relay Tor sul computer di sua scelta. Questo relè si unisce alla rete pubblica e trasmette il traffico delle persone che utilizzano questa rete.

6. *The Tor Project, 2013, Come funzionano i servizi onionici?*
[<https://community.torproject.org/oni-on-services/overview/>]. Questi servizi a cipolla hanno indirizzi *.onion*.

32.4.1 Impostazione di un relè Tor

Il fatto che chiunque possa creare un relay introduce la diversità, rafforzando così l'efficienza della rete Tor nel suo complesso.

I relay Tor sono legalmente considerati router⁷ e non sono quindi

Pagina 29 Questa è una buona cosa, perché se gli avversari avessero accesso ai log di più relay Tor, sarebbero in grado di scoprire i circuiti a posteriori.

Come abbiamo visto in precedenza, le persone che gestiscono gli exit node sono talvolta considerate responsabili del traffico che passa attraverso quel nodo e devono dare spiegazioni alle autorità. Per questo motivo, per evitare di esporsi individualmente, è meglio configurare Tor in modo che il proprio relay non possa essere un exit node, e contribuire a un'associazione dedicata alla gestione degli exitnode.⁸

32.4.2 Costruire un ponte Tor

È anche molto utile impostare i "ponti" o i "bridge" Tor⁹. Si tratta di relè speciali che non sono elencati negli elenchi pubblici della rete Tor.¹⁰ della rete Tor. Possono consentire alle persone i cui ISP filtrano le connessioni a Tor di connettersi comunque alla rete.

32.5 Alcune limitazioni di Tor

Tor può facilmente dare una falsa impressione di sicurezza. In effetti soddisfa l'esigenza di nascondere il proprio indirizzo IP e di nascondere i server con cui si comunica. Ma Tor non risolve tutti i problemi¹¹:

1. Tor non vi proteggerà se non lo usate correttamente;
2. Anche se si configura e si utilizza Tor in modo corretto, esistono comunque potenziali attacchi che possono compromettere la protezione offerta da Tor;
3. Nessun sistema di anonimizzazione è ancora perfetto e Tor non fa eccezione: non sarebbe saggio affidarsi esclusivamente alla rete Tor se si ha bisogno di assoluta riservatezza.

Vediamo più da vicino alcune di queste limitazioni.

32.5.1 La persona disinformata o noncurante

Quando non si è informati, è molto probabile che si commetta un errore. Quando si usa uno strumento, è fondamentale capire non solo a cosa serve, ma anche a cosa non serve e quali sono i suoi limiti.

Ad esempio, se utilizziamo il Tor Browser per compilare moduli web con informazioni personali, il sito web non conoscerà la nostra posizione originale, ma avrà tutte le informazioni contenute nel modulo. Quindi non saremo totalmente anonimi.

7. *Le nostre cipolle, 2013, Che cos'è?* [https://nos-oignons.net/%C3%80_propos/index.fr.html].

8. *Le nostre cipolle, 2013, Che cos'è?* [https://nos-oignons.net/%C3%80_propos/index.fr.html].

9. Per comprendere e utilizzare i ponti Tor, consultare la [documentazione di Tails, Connettersi alla rete Tor](https://tails.boum.org/doc/anonymous_internet/tor/index.fr.html#index1) [https://tails.boum.org/doc/anonymous_internet/tor/index.fr.html#index1] e la [pagina dedicata ai ponti Tor del progetto Tor](https://bridges.torproject.org/?lang=fr) [<https://bridges.torproject.org/?lang=fr>].

10. Gli indirizzi dei ponti Tor possono essere ottenuti visitando [BridgeDB](https://bridges.torproject.org/?lang=en) [<https://bridges.torproject.org/?lang=en>].

11. Per ulteriori informazioni, consultare il sito web di Tor: [Progetto Tor, 2021, Sono completamente anonimo se uso Tor?](https://support.torproject.org/fr/faq/staying-anonymous/) [<https://support.torproject.org/fr/faq/staying-anonymous/>].

Attenzione ai documenti scaricati. Possono contenere "risorse Internet" (immagini, video, ecc.) che potrebbero rivelare il nostro indirizzo IP se li apriamo con un'applicazione non configurata per connettersi con Tor (ad esempio, un visualizzatore di PDF). Per evitare l'esposizione, è possibile aprire i documenti scaricati con Tails, che si connette a Internet solo *tramite* Tor, oppure con un computer disconnesso da Internet.

32.5.2 Gli avversari vedono che usiamo Tor

L'ISP o l'amministratore della LAN di Ana può facilmente capire che si sta connettendo a un relay Tor e non a un normale server web.¹² Infatti, l'elenco degli IP dei nodi di ingresso Tor è pubblicamente disponibile su Internet. L'uso dei *ponti* Tor consente una maggiore discrezione nei confronti dell'ISP o dell'amministratore della LAN.

Allo stesso modo, l'elenco dei nodi di uscita della rete Tor è pubblico. Gli amministratori dei siti web, che possono vedere l'origine delle visite in entrata, saranno quindi in grado di identificare quelle provenienti da un relay Tor.

Tor non protegge facendo assomigliare gli utenti Tor a qualsiasi persona a caso su Internet, ma facendo assomigliare tutti gli utenti Tor. Diventa impossibile capire chi è chi tra loro. Più persone usano Tor e più varie sono le loro attività, meno incriminante sarà l'uso di Tor. La forza della rete risiede in questo insieme indistinguibile di utenti - *l'insieme dell'anonimato*.

32.5.3 I nodi di uscita di Tor possono spiare le comunicazioni che trasmettono.

Tor non cripta le comunicazioni al di fuori della propria rete. Quindi Tor non può criptare ciò che passa tra il nodo di uscita e il server di destinazione. Qualsiasi nodo di uscita può quindi catturare il traffico che trasmette a Internet.¹³

Nel 2007, ad esempio, un ricercatore di sicurezza informatica ha intercettato migliaia di e-mail private inviate da ambasciate e ONG di tutto il mondo origliando il traffico dal nodo di uscita che amministrava¹⁴ con un attacco "monster in the middle".

Per proteggersi da tali attacchi, è necessario utilizzare la crittografia end-to-end, come descritto nella sezione sulla crittografia asimmetrica.

32.5.4 Attacco con schema temporale

Il design di Tor non protegge da alcuni tipi di attacchi, in particolare da quelli di analisi del traffico.¹⁵ Uno di questi è l'attacco "temporal pattern". L'idea alla base di questo attacco è quella di osservare la velocità di invio dei dati in due punti del percorso, ad esempio al primo relay e al terzo relay (nodo di uscita). Ad esempio, inviamo un flusso come il codice Morse: tre pacchetti inviati a raffica, poi cinque secondi di silenzio, poi tre pacchetti *e così via*.

12. Questa e le sezioni seguenti sono fortemente ispirate al sito web di Tails [[https:// tails.boum.org/doc/about/warnings/index.en.html#doc-about-warnings.fr.tor](https://tails.boum.org/doc/about/warnings/index.en.html#doc-about-warnings.fr.tor)].

13. Progetto Tor, 2021, *Quando uso Tor, le intercettazioni elettroniche possono ancora vedermi? informazioni che condivido con i siti web, come ad esempio le informazioni di tipo l o g i n a l e , e q u a l i che digito nei moduli?* [<https://support.torproject.org/fr/https/https-1/>].

14. Kim Zetter, 2007, *Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise (I nodi incostanti trasformano l'anonimizzatore Tor nel paradiso degli intercettatori)* [[https:// www.wired.com/politics/security/news/2007/09/embassy_hacks](https://www.wired.com/politics/security/news/2007/09/embassy_hacks)].

15. Wikipedia, 2014, *Attacco all'analisi del traffico* [[https://fr.wikipedia.org/wiki/Attaque_par traffic_analysis](https://fr.wikipedia.org/wiki/Attaque_par_trafic_analysis)].

Gli avversari che vedono che il computer di Ana sta inviando un flusso con un determinato schema temporale sul primo relè e che osservano un flusso con lo stesso schema sul nodo di uscita che va a *example.org*, possono dedurre che probabilmente è il computer di Ana a essere connesso a *example.org*.¹⁶

La forza, ma anche la debolezza, di Tor è che chiunque può non solo usarlo, ma anche amministrare un relay Tor: Ana, Bea, un'università, la CIA e così via. Se gli avversari hanno accesso alle informazioni solo da uno dei relè attraverso cui passano i dati, non c'è problema. Se, sfortunatamente, gli avversari cooperanti hanno accesso a più relè, possono effettuare un attacco "a schema temporale".

Anche i provider di servizi Internet (ISP) e i grandi fornitori di contenuti o risorse utilizzati in molti siti web - inserti pubblicitari, funzionalità di ricerca e social media - sono in una buona posizione per osservare il traffico e quindi collaborare a questo tipo di attacco.

32.5.5 Tor non protegge dagli attacchi di conferma

Abbiamo appena visto che il progetto di Tor non protegge dagli avversari che possono misurare il traffico in entrata e in uscita dalla rete Tor. Infatti, se gli avversari possono confrontare i due flussi, è possibile correlarli tramite statistiche di base.

Consideriamo ora alcuni avversari che hanno ragione di credere che sia Ana a postare su questo blog anonimo. Per confermare la loro ipotesi, possono osservare il traffico in uscita dalla connessione in fibra di Ana e quello in entrata nel server che ospita il blog. Se osservano gli stessi modelli di dati quando confrontano questi due tipi di traffico, saranno in grado di confermare la loro ipotesi.

Tor protegge Ana dagli avversari che cercano di determinare chi pubblica sul blog anonimo. Ma non protegge da avversari con maggiori risorse che cercano di confermare un'ipotesi monitorando i punti giusti della rete e poi facendo la correlazione.

Questo tipo di attacco può essere effettuato anche con ipotesi più ampie.

Consideriamo degli avversari che sospettano che un gruppo di connessioni ADSL si connetta a un blog anonimo sul quale gli autori postano solo via Tor. Immaginiamo che questi avversari abbiano accesso sia al traffico del gruppo di connessioni ADSL in questione, sia a quello del server - grazie a una requisizione o a una scatola nera, per esempio.¹⁷ Questi avversari possono quindi utilizzare un attacco "temporal pattern" per scoprire quale connessione del gruppo sospetto è responsabile di quale connessione al server. In questo modo, la pubblicazione di un post su un blog può essere correlata a una connessione tra un gruppo di persone sospettate di partecipare a questo blog anonimo.

pagina

228

32.5.6 Tor non protegge da un'organizzazione globale

Un'organizzazione globale avversa è un'entità in grado di analizzare il traffico tra tutti i computer di una rete. Ad esempio, studiando il volume di informazioni che fluiscono attraverso la rete in ogni momento, sarebbe statisticamente possibile identificare un circuito Tor, poiché lo stesso flusso di informazioni appare ogni pochi millisecondi in ogni nodo del circuito. L'avversario potrebbe così stabilire il collegamento tra un utente Tor e il suo server di destinazione.

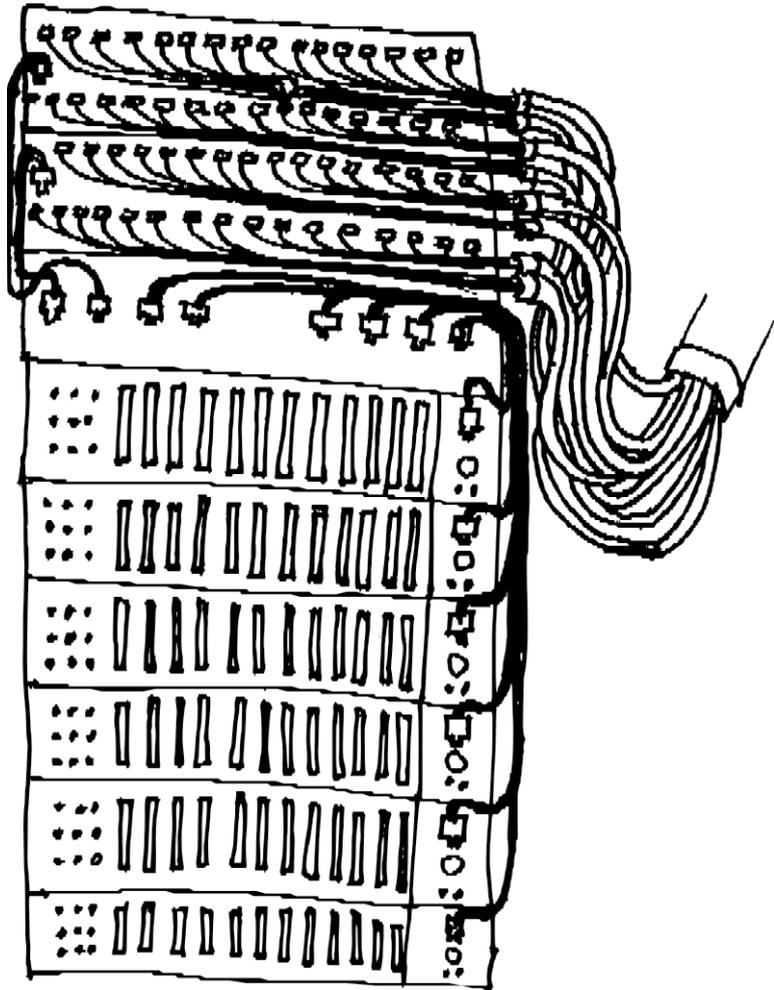
16. Vedi Wikipedia, 2014, *Tor (rete)* [[https://fr.wikipedia.org/wiki/Tor_\(r%C3%A9seau\)](https://fr.wikipedia.org/wiki/Tor_(r%C3%A9seau))].

17. In questo caso, ci riferiamo al sistema che consente ai servizi di intelligence di analizzare automaticamente i metadati delle comunicazioni Internet in Francia (*Le Monde*, 2017, *Une première "scatola nera" della legge sull'intelligence ora attiva* [https://www.lemonde.fr/pixels/article/2017/11/14/les-boites-noires-de-la-loi-sur-le-renseignement-sont-desormais-actives_5214596_4408996.html]).

Un'organizzazione globale avversaria con risorse paragonabili a quelle dell'NSA, ad esempio, potrebbe anche mettere a punto altri attacchi volti a rompere la riservatezza fornita dalla rete Tor. Si tratta di una compromissione di Tor, che consente tempi di navigazione ragionevoli (per il web o la messaggistica istantanea, ad esempio).¹⁸.

Tuttavia, i rischi derivanti da queste limitazioni non sono paragonabili a quelli che si corrono navigando senza Tor. Tor è uno degli strumenti per la privacy più efficienti di Internet. Sebbene questi rischi debbano essere tenuti presenti, non devono dissuaderci dall'usarlo con saggezza.

18. Roger Dingledine, Nick Mathewson, Paul Syverson, 2004, *Tor Project: The Second-Generation Onion Router* [<https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf>], sezione "3. Obiettivi e presupposti del progetto".



QUINTA PARTE

Scegliere le risposte giuste

Introduzione

Niente panico! Proteggersi non è né impossibile né troppo complicato. Possiamo procedere lentamente, concetto per concetto, per progettare la nostra strategia di autodifesa digitale.

Prima di Internet, incontravamo i nostri amici ogni sera all'angolo della strada. Soluzioni ancora possibili, ma da non dimenticare. Oggi possiamo utilizzare strumenti per criptare il nostro messaggio e inviarlo dall'altra parte del mondo in pochi millisecondi.

In questa sezione descriveremo esempi concreti, noti come *casi d'uso*, per proporre soluzioni ad alcune situazioni tipiche.

Caso d'uso: siti web di consulenza

33.1 Contesto

L'attenzione si concentra sulla consultazione delle informazioni disponibili sul web: leggere un periodico, seguire un blog, *ecc.* Sono tutte attività ordinarie quando si è *online*.

Tuttavia, vogliamo svolgere queste attività in modo discreto, per varie ragioni, tra cui possiamo citare:

- sventare la sorveglianza o aggirare la censura, sia da parte di un leader, di un amico intimo o di uno Stato;
- evitare la raccolta e la collazione di informazioni personali per scopi commerciali;
- generalizzare l'uso di pratiche discrezionali, proteggendo così coloro che ne hanno veramente bisogno, "annegandoli".

33.2 Valutazione dei rischi

33.2.1 Cosa vogliamo proteggere?

In questo caso, ciò che ci interessa è innanzitutto l'anonimato, o almeno lo pseudonimato: ciò che cerchiamo di nascondere non è il contenuto di ciò che viene consultato, ma *da chi* viene consultato.

Abbiamo visto in precedenza che l'uso di Internet, e del Web in particolare, lascia molte tracce di vario tipo, in luoghi diversi. Molte di esse, come piccoli sassolini, tracciano un percorso dalla risorsa consultata a una casa, a un computer o addirittura alla persona che vi sta dietro. È quindi di queste tracce sulla rete che vogliamo sbarazzarci, in primo luogo dell'indirizzo IP. Tuttavia, poiché l'IP è necessario per il corretto funzionamento della rete, la strategia sarà quella di **garantire che** chiunque segua questa traccia finisca in un vicolo cieco.

Si può anche desiderare di non lasciare traccia della navigazione sul computer, in particolare sul disco rigido.

[pagina]

202

33.2.2 Da chi vogliamo proteggerci?

Questa è una domanda importante: a seconda della risposta, la politica di sicurezza appropriata può variare notevolmente.

Fornitore di servizi Internet

Ana lavora per una grande azienda e accede a Internet tramite la rete aziendale. Durante l'orario di lavoro consulta i suoi blog preferiti, ma non vuole che il suo datore di lavoro lo sappia.

In questo caso, Ana vuole proteggersi dagli occhi indiscreti dei responsabili della rete, in questo caso la sua azienda. In questo caso, l'avversario ha accesso a tutto il traffico di rete che passa attraverso la sua connessione, poiché l'azienda funge da fatturatore. Tuttavia, non ha occhi su altre parti di Internet.

Fornitori di contenuti

Bea è iscritta a un forum nazionale di polizia e trascorre - non senza un piacere maligno - una certa quantità di tempo a creare problemi nelle discussioni tra poliziotti.

In questo caso, Bea non vuole che il sito che ospita il forum sappia che è lei a creare problemi. Come abbiamo già visto, il suo indirizzo IP viene conservato per un periodo di tempo variabile dal sito visitato. L'avversario avrà quindi accesso alle intestazioni IP e a quelle HTTP.

Un'ampia varietà di avversari

Agathe visita regolarmente il sito di pubblicazione di documenti riservati su cui Bea ha pubblicato gli estratti conto bancari. Poiché l'argomento è delicato, sa che il blog in questione potrebbe essere monitorato. Quindi non vuole che nessuno sappia che ci va.

L'avversario non ha un posto fisso nella rete: può trovarsi nel computer di Agathe, nella sua "scatola", nel blog o in qualsiasi punto del percorso tra il suo computer e il blog. L'avversario può anche trovarsi in più luoghi contemporaneamente.

33.3 Definizione di una politica di sicurezza

Poniamo ora le domande previste dalla nostra metodologia:

1. Quale insieme di pratiche e strumenti ci proteggerebbe a sufficienza dai nostri avversari?
2. Di fronte a una simile politica di sicurezza, quali sono gli angoli di attacco più pratici?
3. Quali risorse sono necessarie per sfruttarle?
4. Pensiamo che i nostri avversari possano utilizzare questi mezzi?

33.3.1 Primo passo: accedere a uno dei nostri server

L'angolo di attacco più pratico per l'avversario: analizzare i dati registrati dai server che forniscono la connessione o che ospitano le risorse consultate.

Risorse necessarie :

- connettersi al server che fornisce la connessione, se l'avversario è l'ISP o collabora con l'ISP;
- connettersi al server che ospita la risorsa consultata se l'avversario è il fornitore di contenuti o collabora con esso.

Se l'avversario è l'ISP o il fornitore di contenuti, sarà sufficiente consultare i suoi log di connessione. Ma è anche possibile che altri avversari accedano a queste informazioni, attraverso requisizioni, contratti commerciali, collaborazioni volontarie o addirittura hacking.¹ o anche attraverso l'hacking.

Credibilità di un attacco di questo tipo: probabile se la nostra connessione o il sito che visitiamo attirano l'attenzione dell'avversario.

Contro questo tipo di attacco, una soluzione efficiente è l'utilizzo del routing a cipolla.²

1. Jacques Follorou, *Le Monde*, 2014, *Espionnage : comment Orange et les services secrets coopèrent* [https://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-inc estueuses_4386264_3210.html].

attraverso la rete Tor, come descritto di seguito. Per mantenere separate le nostre identità contestuali, faremo attenzione a non mescolare le nostre attività quotidiane con quelle che vogliamo mantenere più discrete.

pagina
243

33.3.2 Secondo passo: osservare il computer che si sta utilizzando

Se utilizziamo l'onion routing, l'avversario che osserva i dati che circolano sulla rete non può sapere da dove provengono e dove vanno. Deve quindi trovare un altro modo per arrivarci.

L'angolo di attacco più pratico: l'accesso alle tracce lasciate sul computer dalla pagina 27 dei siti visitati.

Mezzi necessari: accesso al computer utilizzato.

Credibilità dell'attacco: nel caso in cui Ana utilizzi il suo computer di lavoro, è molto facile per l'avversario. In altri casi, e a seconda dell'avversario, è necessario un furto con scasso (chiamato anche perquisizione, quando è legale), oppure corrompere il computer oggetto dell'attacco, ad esempio installando un software di 31 dannoso.

pagina
31

Per difendersi da questo attacco, è necessario proteggere il disco rigido per rendere difficilmente accessibili le tracce lasciate. Meglio ancora, evitare di lasciare tracce in primo luogo utilizzando un sistema *live* amnesico, che non registra nulla sul computer in uso.

pagina
119
pagina
113

33.3.3 Passo 3: Attaccare Tor

Angolo di attacco: sfruttare i limiti dell'anonimato fornito da Tor, ad esempio effettuando un attacco di conferma.

pagina
267
pagina
269

Risorse necessarie: essere in grado di monitorare diversi punti della rete, ad esempio la connessione utilizzata e il sito visitato.

Credibilità di un attacco di questo tipo: è improbabile che un avversario come un'azienda che cerca di monitorare le proprie dipendenti donne metta in atto un attacco di questo tipo. Idem per i gendarmi di Saint-Tropez. Potrebbe invece essere alla portata di un fornitore di servizi di rete nazionale o globale, o addirittura di poliziotti specializzati. Ancora una volta, non dimentichiamo che c'è una differenza significativa tra "avere la capacità tecnica di compiere un attacco" e "compiere effettivamente un attacco". Questa differenza è dovuta principalmente al costo economico e al ritorno sugli investimenti di un attacco mirato.

Ricordate che molti altri attacchi contro Tor sono possibili o previsti. Soprattutto, è importante comprendere gli obiettivi e i limiti del routing a cipolla, per non darsi la zappa sui piedi.

pagina
261
pagina
267

33.4 Scegliere tra gli strumenti disponibili

A seconda delle vostre esigenze e della vostra politica di sicurezza, dovrete scegliere tra diversi strumenti.

33.4.1 Browser Tor sul nostro sistema o in Tails

Browser Tor sul nostro sistema operativo

Il Tor Browser è un *pacchetto* software: fornisce un browser web preconfigurato per navigare in modo riservato, utilizzando la rete Tor, dal nostro sistema.

2. Contro alcuni degli avversari qui elencati, possono essere sufficienti altre soluzioni tecniche, come ad esempio l'impiego di a VPN l'uso di di [https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel], ad esempio. Tuttavia, il routing a cipolla protegge da molti più attacchi possibili rispetto a una VPN, che inserisce solo un intermediario tra noi e la risorsa consultata.

pagina
313

funzionamento abituale ³. Una volta installato il Tor Browser, si può scegliere di utilizzare questo browser web abilitato a Tor o il proprio browser web abituale. ⁴.

Vantaggi Il Tor Browser consente di navigare sul web con Tor dal proprio sistema operativo abituale. Ad esempio, è possibile lavorare su un documento con i nostri strumenti abituali, mentre si cercano informazioni sul web in modo anonimo.

Svantaggi Poiché il Tor Browser funziona sul sistema operativo abituale, ciò significa che una vulnerabilità in quest'ultimo permetterebbe agli avversari di aggirare la protezione offerta dall'uso della rete Tor. Soprattutto, se utilizzato al di fuori di un sistema amnesico, il Tor Browser rischia di lasciare tracce sul disco rigido del computer in uso.

Il Tor Browser è basato su Firefox e potrebbe verificarsi un ritardo prima che gli aggiornamenti di quest'ultimo diventino effettivi. Durante questo periodo, il Tor Browser presenta vulnerabilità di sicurezza note e pubblicate.

Se il Tor Browser si blocca, si possono perdere definitivamente tutte le letture e le ricerche in corso. ⁵.

Il Tor Browser non impedisce ad altri programmi di connettersi a Internet senza passare per Tor, anche se vengono aperti dal Tor Browser (software P2P, lettori PDF, lettori multimediali, ecc.).

Coda

pagina
113

Coda ⁶ è un sistema *live* progettato per proteggere la privacy e l'anonimato dei suoi utenti. Consente di accedere a Internet in modo anonimo praticamente da qualsiasi luogo e da qualsiasi computer. Inoltre, non lascia traccia delle attività svolte sul computer, a meno che non sia esplicitamente richiesto.

Vantaggi Quando si usa Tails, non solo non si lascia traccia sul computer che si sta utilizzando, ma il software che deve accedere a Internet viene configurato per utilizzare la rete Tor e le connessioni dirette (che non consentono l'anonimato) vengono bloccate.

Inoltre, trattandosi di un sistema *live*, Tails può essere avviato da un DVD o da una chiavetta USB, senza modificare il sistema operativo installato sul computer. Quindi è possibile utilizzarlo a casa, sul computer di qualcun altro o persino nella biblioteca locale.

Per ulteriori informazioni, consultare la [pagina "Come funziona Tails"](https://tails.boum.org/about/index.en.html) [https://tails.boum.org/about/index.en.html].

Svantaggi Innanzitutto, poiché Tails è un sistema operativo a sé stante, è necessario riavviare il computer per utilizzarlo. ⁷. È anche più complesso da installare

3. Nel nostro caso si tratta di Debian, ma il Tor Browser funziona anche con qualsiasi altra distribuzione GNU/Linux, proprio come con Windows o macOS.

4. È possibile configurare un browser web per utilizzare Tor, ma non è consigliabile, poiché anche con una buona conoscenza tecnica è difficile garantire che tutte le richieste del browser passino attraverso Tor. Il Tor Browser esiste proprio per superare questa difficoltà.

5. È possibile cambiare questo comportamento modificando le impostazioni predefinite di Tor, impostazioni che mirano a rendere la navigazione quasi amnesica.

6. Si veda il sito web di Tails [https://tails.boum.org/index.fr.html].

7. Tails può anche essere utilizzato in una macchina virtuale [pagina 163] nel sistema abituale. In questo caso, la memoria della macchina virtuale e tutti i dati saranno visibili all'utente. Inoltre, se il sistema operativo utilizza la memoria virtuale (swap), è possibile che i dati della macchina virtuale vengano scritti sul disco rigido. Inoltre, se il sistema operativo utilizza la memoria virtuale (swap) [pagina 25], è possibile che i dati della macchina virtuale finiscano per essere scritti sul disco rigido. È quindi praticamente impossibile garantire l'amnesia di un sistema Tails utilizzato in questo modo.

pagina
22

Browser Tor. Infine, avrete bisogno di una chiavetta USB (con una capacità di almeno 8 GB) o di un DVD contenente Tails.

Poi, a causa dell'amnesia del sistema, se il browser web si blocca, perdiamo tutte le pagine che stavamo visualizzando, proprio come con Tor Browser.

Per evitare di mischiare le normali attività quotidiane con quelle che si vogliono rendere più discrete quando si usa Tails, è necessario riavviare il computer quando si passa da un'identità contestuale all'altra.

Un altro svantaggio di Tails è il ritardo tra gli aggiornamenti di sicurezza per i programmi altrimenti inclusi in Tails e gli aggiornamenti dello stesso software in Tails. Questo svantaggio è simile a quello del Browser Tor, in quanto c'è un ritardo tra gli aggiornamenti di Firefox e la loro inclusione nel Browser Tor.

Per ulteriori informazioni, consultare la [pagina "Avvertenze" di Tails \[https:// tails.boum.org/doc/about/warnings/index.en.html\]](https://tails.boum.org/doc/about/warnings/index.en.html).

33.4.2 Fare la propria scelta

Alla fine della giornata, si deve scegliere tra :

- utilizzare il sistema operativo abituale;
- utilizzare un sistema amnesico *dal vivo*.

In altre parole, quali tracce (eventualmente criptate) siete disposti a lasciare sul computer o sulla chiavetta USB che state utilizzando? Avete bisogno del resto del vostro ambiente per la navigazione anonima?

Ancora una volta, non c'è una risposta giusta o sbagliata: si tratta di scegliere la soluzione più adatta a voi. Inoltre, è perfettamente possibile testare una soluzione e poi passare a un'altra, se necessario.

Alla fine, ci sono due possibilità:

- utilizzare il Tor Browser da una Debian criptata. Ciò consente di navigare in modo quasi anonimo mentre si utilizza il sistema abituale. D'altra parte, le tracce (criptate) saranno probabilmente lasciate sul disco rigido del computer.
- utilizzare il browser web Tails. Non viene lasciata alcuna traccia sul disco rigido del computer utilizzato, o addirittura nessuna se non si utilizza la persistenza.

pagina
119

pagina
116

Una volta effettuata la scelta, vedere il paragrafo corrispondente qui sotto.

33.5 Navigare sui siti web con Tor Browser

Se, dopo aver valutato i pro e i contro, decidete di usare *Tor Browser*, ci sono alcune precauzioni da prendere.

33.5.1 Preparazione della macchina e installazione del browser Tor

Innanzitutto, dato che non utilizziamo un sistema *live*, le tracce della navigazione (segnalibri, file scaricati, a volte anche cookie o cronologia) verranno registrate.

Applicare la stessa politica di un nuovo avvio è una buona idea. Successivamente, è necessario scaricare e installare il Browser Tor. Il capitolo

del Tor Browser descrive questa procedura.

Installazione
pagina
313

33.5.2 Utilizzo del browser Tor

pagina
313

Il capitolo sull'installazione del Tor Browser spiega anche come avviarlo. Questo strumento è stato appositamente progettato per essere il più semplice possibile da usare. Quando viene lanciato, tutti i software necessari (Tor e il Tor Browser) vengono avviati e configurati. Non resta che attendere l'apertura della finestra del Tor Browser e siamo pronti per iniziare a navigare nella rete Tor.

pagina
261

Attenzione: solo la navigazione di *siti web attraverso* la finestra del Browser Tor garantisce una connessione riservata. Tutte le altre applicazioni (client di posta elettronica, messaggistica istantanea, Torrent, *ecc.*) riveleranno il vostro vero indirizzo IP.



pagina
202

Inoltre, una volta chiusa questa finestra, dovrete rilanciare Tor Browser e attendere l'apertura di una nuova finestra per riprendere la navigazione attraverso la rete Tor.

33.5.3 Si vedono presto i limiti

Il Tor Browser è un ottimo strumento perché è così facile da usare, ma presto ci si rende conto dei suoi limiti. Solo le connessioni avviate dal Tor Browser passano attraverso la rete Tor. Se si desidera utilizzare un altro browser web, la connessione non passerà più attraverso questa rete, il che può essere fastidioso. Se non si fa attenzione, si può rapidamente trovare il browser sbagliato e pensare che la navigazione passi attraverso la rete Tor, mentre non è così. Inoltre, consente di utilizzare Tor solo per navigare sul web che, anche se è molto utilizzato, è solo una parte di Internet, come abbiamo spiegato in precedenza.

pagina
200

E la privacy online non riguarda solo la falsificazione degli indirizzi IP. Tutte le altre tracce che lasciamo sul web e sul nostro computer possono tradirci prima o poi, e il Tor Browser non protegge da questo.

33.6 Navigazione nei siti web con Tails

33.6.1 Ottenere e installare Tails

Tails è un software libero e può quindi essere scaricato, utilizzato e condiviso senza restrizioni. Viene eseguito su un computer indipendentemente dal sistema già installato. Infatti, Tails può essere lanciato da un supporto esterno, come un DVD o una chiavetta USB, senza utilizzare il disco rigido.

pagi
na
39

Per prima cosa è necessario scaricare Tails (vedere pagina 114). Per assicurarsi che il download sia andato a buon fine, è necessario controllare l'immagine ISO del file (vedere pagina 114).

Una volta verificata, è possibile procedere all'installazione su chiave USB o DVD (vedere pagina 115).

33.6.2 Avviare le code

Ora che Tails è stato installato e riavviato (vedere pagina 115), è possibile iniziare a usarlo senza modificare il sistema operativo del computer.

33.6.3 Connessione a Internet

Una volta che Tails ha terminato l'avvio, cioè una volta che il desktop ha terminato l'affichering, non resta che connettersi a Internet: si veda la [documentazione di Tails su come "Connettersi a una rete locale" \[https://tails.boum.org/doc/anonymous_internet/networkmanager/index.en.html\]](https://tails.boum.org/doc/anonymous_internet/networkmanager/index.en.html). È quindi possibile navigare in rete.

33.6.4 Limiti

Una soluzione di questo tipo si basa sull'uso di Tor e Tails e quindi eredita i limiti di entrambi gli strumenti:

I limiti di Tor sono già stati discussi nel paragrafo "Terzo passo: attaccare Tor".

Per i limiti di Tails, troverete un ampio elenco di avvertenze [sul sito web del progetto](https://tails.boum.org/doc/about/warnings/index.fr.html) [https://tails.boum.org/doc/about/warnings/index.fr.html].

Vi invitiamo a leggere attentamente entrambi i documenti.

Caso d'uso: pubblicazione di un documento

34.1 Contesto

Una volta terminata la stesura di un documento sensibile, vorremmo pubblicarlo alla pagina 79 di Internet, preservando il nostro anonimato (il fatto che non possa essere associato a nessun nome) o il nostro pseudonimato (il fatto che possa essere associato solo a un nome scelto).

diversa dalla nostra identità civile).

Come bonus, vorremmo poter includere un indirizzo di contatto pubblico corrispondente a questo pseudonimo.

34.2 Valutazione dei rischi

34.2.1 Cosa vogliamo proteggere?

Il contenuto del documento è pubblico. Non ci interessa la sua riservatezza. D'altra parte, cerchiamo di nascondere i legami tra il documento e le persone che lo hanno scritto. È l'**anonimato** o lo **pseudonimo** che ci interessa.

Inoltre, se rendiamo pubblico un documento sensibile la cui semplice consultazione potrebbe essere ritenuta incriminante, dobbiamo anche cercare di limitare la possibilità di identificare le persone che vi accedono.

34.2.2 Da chi vogliamo proteggerci?

Come nel caso precedente, il nostro obiettivo è quello di proteggerci da occhi indiscreti che cercano di vedere chi fa cosa sul web.

pagina
277

Saremo ancora più attenti alle tracce lasciate, dato che si tratta di pubblicare un documento che si presume possa dispiacere a una o più persone con un certo potere di causare problemi. È quindi probabile che venga avviata una ricerca di indizi nel tentativo di trovare la persona o le persone che hanno prodotto il documento (o che lo hanno consultato), ad esempio inviando richieste all'host.

pagina
278
pagina

34.3 Definizione di una politica di sicurezza

In primo luogo, vedremo la pubblicazione e la consultazione dei documenti, quindi l'utilizzo di un contatto pubblico ad essi collegato.

209

34.3.1 Pubblicazione

Tecnicamente, pubblicare un documento significa "salvarlo" su un server collegato a Internet, detto *host*. Questa operazione viene spesso eseguita tramite un sito web. Tuttavia, non utilizzeremo gli stessi siti se vogliamo pubblicare testi, suoni o video.

pagina
209
pagina
211

Dobbiamo quindi scegliere con cura il nostro host, tenendo conto dei numerosi criteri in gioco: tipo di documento, disponibilità, condizioni di hosting, resistenza dell'host alle pressioni legali, rischi per l'host posti dal nostro documento, possibilità di consultare il documento senza rischi di identificazione, ecc. *Un elenco più esaustivo di questi criteri è disponibile nella sezione "Strumenti"*. Un elenco più esaustivo di questi criteri è disponibile nella sezione "Strumenti".

pagina

319

Una volta fatta la nostra scelta, dobbiamo essere sicuri che il nostro documento rimanga disponibile per la consultazione: se il nostro ospite non gradisce la nostra pubblicazione, riceve pressioni o addirittura una richiesta di rimozione, il nostro lavoro potrebbe diventare non disponibile.

Per evitare questo tipo di inconveniente, è possibile ospitare più volte lo stesso file, se possibile su server situati in Paesi diversi. Poiché la messa online di un file è molto più rapida di un'azione legale, questa sembra essere una buona soluzione per evitare la censura.

Quali sono gli angoli di attacco a disposizione di un potenziale avversario?

Primo passo: leggere il documento

A prima vista, l'avversario dispone di un grande volume di dati di cui cercare le tracce: il contenuto del documento.

Pertanto, una possibile firma, come uno pseudonimo o una città, una data, la lingua in cui è scritto il documento o anche semplicemente il tema del documento sono tutti indizi che possono condurre ai suoi autori. Un testo che descrive le pratiche abusive dell'azienda Machinex nel novembre 2012 è stato probabilmente scritto da dipendenti di questa azienda o da persone che hanno condiviso la loro lotta in quella data.

pagina

245

L'avversario può anche tentare un'analisi stilometrica per confrontarlo con altri testi, anonimi o meno, e cercare di dedurre informazioni sugli autori. Per quanto ne sappiamo, questo tipo di attacco è davvero efficace solo quando ci sono già forti sospetti su un sottoinsieme di potenziali autori, ma questo è un campo di ricerca recente. Poiché vogliamo distribuire questo documento su larga scala, non saremo in grado di nascondere il contenuto. Tuttavia, se ritenete che sia necessario fare questo sforzo, potreste prestare particolare attenzione a modificare il vostro stile di scrittura.

pigi

na

30

Infine, se pubblichiamo il nostro documento senza prendere ulteriori precauzioni, l'editore può cercare qualsiasi metadato che possa fornire informazioni.

Questi diversi metodi non richiedono grandi abilità tecniche e sono quindi alla portata di molti avversari.

Per proteggersi, seguire queste ricette:

- se possibile, lavoreremo sul nostro documento utilizzando metodi che limitano la quantità di metadati che possono essere registrati;
- In tutti i casi, è buona norma rimuovere i metadati prima della pubblicazione.

page 185

79

Secondo passo: chiedere a chi vede

In assenza di tracce facilmente sfruttabili all'interno del documento, uno degli angoli di attacco più pratici è quello di cercare tracce della pubblicazione in rete.

pagina

228

pagina

225

226

A seconda dei suoi poteri, il nostro avversario può requisire il contenuto dall'host o trovare un altro modo per ottenere i log della connessione e quindi ottenere l'indirizzo IP utilizzato. Può quindi rivolgersi all'ISP corrispondente a questo indirizzo IP per ottenere il nome dell'abbonato.

Anche in questo caso, per far fronte alla situazione, utilizzeremo Tor per connetterci a Internet, strappando questa traccia prima di pubblicare il nostro documento.

Per quanto riguarda la scelta dell'hosting, valgono ancora i problemi discussi in precedenza. Inoltre, è probabile che alcune delle piattaforme su cui vorremmo depositare il nostro documento non funzionino se si usa Tor o, come Facebook, impongano controlli di identità difficili da aggirare e incompatibili con la nostra esigenza di anonimato: questo limiterà gli host utilizzabili.

Per pubblicare il nostro documento su un server web *convenzionale*, inizieremo in pratica seguendo la ricetta per trovare un hosting web.

Nella maggior parte dei casi, la pubblicazione avverrà tramite un browser web. Seguiremo quindi il percorso "browser web" del caso d'uso precedente.

È anche possibile ospitare il nostro documento da soli, grazie ai *servizi onion* di Tor: rendono disponibile un server web o un altro tipo di server senza doverne rivelare l'indirizzo IP. Non utilizzano un indirizzo pubblico, quindi possono operare facilmente anche dietro un firewall o un altro box di traduzione degli indirizzi

di rete (NAT).

Se preferite ospitare il vostro documento su un servizio Onion, dovrete seguire la ricetta per utilizzare OnionShare.

Terzo passo: osservare il computer che si sta utilizzando

Questo angolo di attacco è simile a quello descritto nella sezione "guardare il computer in uso" del caso d'uso precedente. Torniamo quindi a leggere (o rileggere) quel capitolo per rivedere il tutto.

Passo 4: Attaccare Tor

Nella disperazione, l'avversario può anche tentare di attaccare Tor (si veda la sezione (si veda "Attacco a Tor" nel caso d'uso precedente).

34.3.2 Visualizzazione dei documenti

Un altro criterio da tenere in considerazione nella scelta di un provider di hosting è il rischio che rappresentiamo per coloro che vengono a consultare il nostro documento. Preferiamo hosting provider che limitino la possibilità che un potenziale avversario possa identificare queste persone.

Gli strumenti di attacco a disposizione dell'avversario sono quelli già trattati nel caso d'uso precedente. Li ripeteremo brevemente qui, adattandoli al caso della consultazione dei documenti.

Primo passo: chiedere a chi vede

Come visto nel caso d'uso precedente, una persona che viene a consultare il nostro documento può essere identificata dal suo ISP o host, in quanto l'accesso al documento apparirà nei suoi log di connessione.

Per ridurre questo rischio, consigliamo a chiunque voglia accedere al documento di utilizzare la rete Tor. Dovremo anche assicurarci che l'host scelto sia accessibile tramite Tor o che offra l'accesso tramite un servizio onion.

È anche importante scegliere un host che non sia una piattaforma su cui le persone potrebbero già essere autenticate e quindi essere "ri-conosciute" dall'host quando accedono al documento, anche se stanno usando Tor. Quindi, ad esempio, si dovrebbero evitare i social media o le piattaforme di hosting di contenuti dei giganti del Web 2.0.

pagina

319

pagina

281

pagina

266

pagina

203

pagina

205

pagina

359

pagina

279

pagina

279

pagina

278

pagina

226

pagina

261

pagina

266

pagina

239

Infine, possiamo anche optare per gli host che non tengono i log delle connessioni o che si rifiutano di consegnarli alla polizia in caso di requisizione.

pagina

228

Secondo passo: osservare il computer che si sta utilizzando

Abbiamo poco controllo su questa situazione. Possiamo tuttavia consigliare a chiunque voglia consultare il nostro documento di seguire le raccomandazioni del caso d'uso precedente di questa guida, in modo da lasciare meno tracce possibili sul proprio computer.

pagina

278

Passo 3: Attaccare Tor

Come per la pubblicazione del documento, l'avversario può anche tentare di attaccare Tor per cercare di identificare chi lo visualizzerebbe (si veda la sezione

pagina

279

(vedere "Attack Tor" nel caso d'uso precedente).

34.3.3 Contatto con il pubblico

Quando pubblichiamo un documento, possiamo volere che le persone che lo leggeranno siano in grado di contattarci. Questo contatto apre nuove possibilità di attacco al nostro avversario in cerca di scappatoie da sfruttare.

Se abbiamo preso tutte le precauzioni per essere il più possibile anonimi quando abbiamo pubblicato il documento, ma il nostro indirizzo di contatto è `nom.prenom@exemple.org`, queste precauzioni saranno inutili: l'indirizzo di contatto fornisce il nostro nome direttamente all'avversario.

pagina

243

Per evitare questo errore, ci assicureremo di avere uno pseudonimo che sarà usato solo per questo documento - o per un gruppo di documenti - a seconda dell'identità contestuale che vogliamo adottare.

pagina

244

L'avversario vorrà quindi sapere chi si nasconde dietro questo pseudonimo. Per cercare di nascondere "chi sta usando questo indirizzo e-mail", può essere utile il caso d'uso "Scambio di e-mail nascondendo la propria identità".

pagina

293

Infine, si potrebbe desiderare di nascondere il contenuto delle e-mail scambiate, ma questo può essere molto complesso: nella misura in cui si desidera avere un indirizzo di contatto pubblico, l'accessibilità può entrare in conflitto con la discrezione. Tuttavia, oltre all'indirizzo e-mail di contatto, è sempre possibile specificare una chiave pubblica OpenPGP associata, in modo che chiunque desideri inviarci messaggi criptati possa farlo. Le ricette per la creazione di una coppia di chiavi OpenPGP e per l'esportazione della chiave pubblica mostrano come fare.

pagina

333

Possiamo quindi prendere tutta una serie di precauzioni per aumentare l'anonimato del nostro contatto, ma possiamo difficilmente agire dall'altro "capo del tubo". Le persone che ci contatteranno potranno quindi correre dei rischi dialogando con noi, senza pensare al loro anonimato. Ricordare loro le condizioni di riservatezza e anonimato è essenziale. Inoltre, non sappiamo mai veramente chi ci sta contattando, quindi dobbiamo stare attenti a ciò che diciamo se non vogliamo comprometterci.

pagina

339

Caso d'uso: scambio di messaggi

35.1 Contesto

Ora vogliamo scambiare messaggi con altre persone, siano esse per augurare buon anno alla nonna o per lavorare su un documento delicato. pagina 79 Non ci preoccupiamo della sincronia dello scambio, a differenza di una conversazione telefonica o di un dialogo di messaggistica istantanea.

o di messaggistica istantanea: in questo caso si parla di comunicazione *asincrona*.

Un altro caso d'uso sarà dedicato al dialogo sincrono. Per ora, concentriamoci sulla posta elettronica.

pagina
299

35.2 Valutazione dei rischi

35.2.1 Cosa vogliamo proteggere?

Quando si invia un'e-mail, una serie di informazioni viene potenzialmente rivelata ai nostri avversari. Quali informazioni?

Quando ci poniamo questa domanda, spesso la prima cosa che ci viene in mente è il *contenuto del* messaggio. Anche se non tutti i messaggi che ci scambiamo sono necessariamente top-secret, alcuni meritano più discrezione di altri: per evitare che i dettagli delle nostre relazioni intime vengano divulgati, o perché il contenuto di un messaggio potrebbe metterci nei guai, dalla perdita del lavoro alla prigione. Più in generale, non ci entusiasma l'idea che la postina legga oggi tutte le lettere che abbiamo ricevuto negli ultimi anni, per stuzzicare il nostro appetito prima di attendere con ansia quelle che arriveranno domani. Eppure, quando ci scambiamo e-mail senza prendere particolari precauzioni, gli intermediari possono leggere le nostre comunicazioni in modo totalmente trasparente, come se fossero cartoline.

Al di là del contenuto di queste cartoline, può essere interessante nascondere informazioni contestuali, come la data dello scambio, l'identità dei protagonisti, la loro posizione, *ecc.*

Il fatto che una persona scriva a un'altra può essere di per sé una formazione sensibile. In effetti, le relazioni tra le persone sono talvolta prese di mira da alcune forme di sorveglianza, ad esempio per ricostituire una rete di oppositori politici. ¹ per esempio. Queste tracce sono generalmente presenti nelle intestazioni dei messaggi di posta elettronica e nei log delle connessioni.

pagina
217
pagina
218
pagina
218
pagina
224

1. Jean-Marc Manach, 2011, *Réfugiés sur écoute* [<https://web.archive.org/web/20221019100157/http://owni.fr/2011/12/01/amesys-bull-eagle-surveillance-dpi-libye-wikileaks-spyfiles-kadhafi/index.html>].

35.2.2 Da chi vogliamo proteggerci?

Potreste voler nascondere alcune o tutte queste informazioni alle varie macchine che possono accedervi e alle persone che hanno accesso a queste macchine.

pagina
217

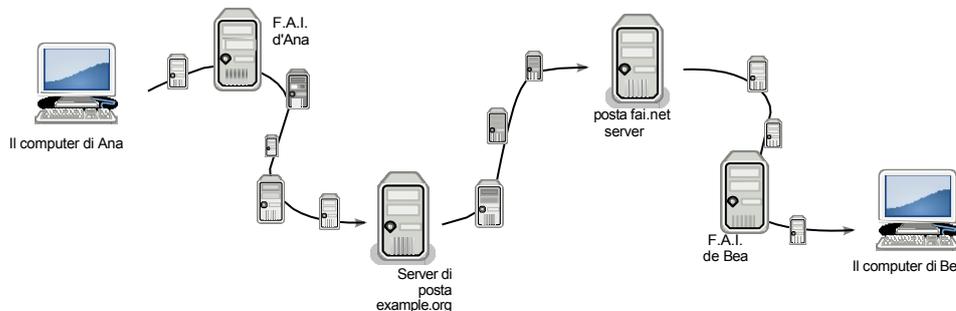
Tra queste macchine ci sono i server coinvolti. Come minimo, per un messaggio inviato da Ana (ana@example.org) a Bea (bea@fai.net), queste saranno :

- del server che Ana usa per inviare il messaggio: in genere, questo sarà *example.org* ;
- del server responsabile della ricezione dei messaggi e della loro archiviazione nella casella di posta elettronica di Bea: *fai.net*.

pagina
205
pagina
217

Ma non è tutto. Lungo il percorso si trovano numerosi altri computer (*router*) che hanno accesso alle informazioni che trasportano:

- tra il computer di Ana e il suo ISP;
- tra l'ISP di Ana e il suo server di posta *example.org* ;
- tra *example.org* e il server di posta Bea *fai.net*;
- quando Bea controlla la sua casella di posta elettronica, il messaggio viaggia tra il server di posta *fai.net* e il suo ISP,
- tra l'ISP di Bea e il suo computer.



Un'e-mail passa attraverso molti intermediari

Le persone che amministrano queste macchine sono le prime ad avere accesso alle informazioni che elaborano, ma non ne hanno necessariamente i diritti esclusivi. Queste informazioni possono finire nelle mani di hacker più o meno governativi, con o senza requisizioni.

pagina
235
pagina

Infine, ogni volta che si consulta la casella di posta elettronica, ogni volta che si invia un messaggio, è probabile che si lascino tracce sul computer che si sta utilizzando. Può essere una buona idea nascondere queste tracce a chi potrebbe dare un'occhiata al contenuto dei nostri dischi rigidi.

228
pagi
na

35.3 Due questioni

Possiamo voler proteggere sia la nostra identità - e anche quella dei nostri destinatari - sia il contenuto dei nostri scambi. Si tratta delle informazioni contenute nelle due parti della nostra cartolina digitale: il testo a sinistra e le intestazioni a destra. Queste informazioni compaiono nel corso dei nostri messaggi e possono essere oggetto di attacchi. La politica di sicurezza che definiremo dipenderà in particolare dal modo in cui consultiamo le nostre e-mail. Infatti, il suo utilizzo può comportare diversi protocolli che non hanno le stesse conseguenze in termini di tracce.

pagina
200

35.4 Webmail o client di posta?

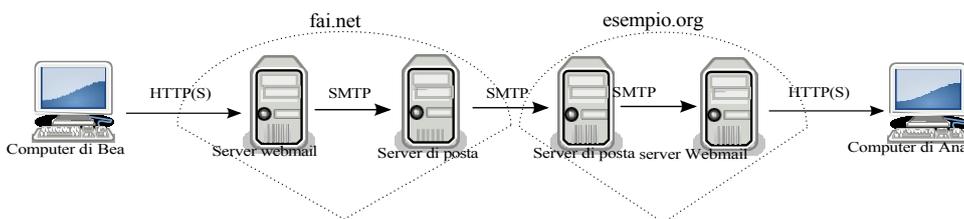
Esistono due modi di utilizzare la posta elettronica, che consentono entrambi le stesse azioni: utilizzare la webmail o un client di posta. La scelta si basa su diversi criteri, tenendo presente che

Entrambi possono essere utilizzati per lo stesso indirizzo e-mail e la scelta di uno o dell'altro non è irreversibile.

35.5 Webmail

La **webmail** è un sito web che consente di controllare la posta elettronica *tramite* un browser. Il suo utilizzo si è diffuso a macchia d'olio a partire dai primi anni 2000, a tal punto che abbiamo quasi dimenticato altri modi di utilizzare la posta elettronica. Hotmail e Gmail sono due esempi molto popolari di provider di hosting che ne promuovono l'uso (anche se possono essere utilizzati solo come webmail). Anche in questo caso si tratta di una tendenza del Web 2.0: non è più necessario avere un proprio sistema operativo per accedere alla casella di posta elettronica (sia sul computer che sulla chiavetta USB contenente un sistema *live*): È sufficiente l'accesso a Internet.

pagina
239



Bea invia un'e-mail ad Ana, entrambe utilizzano la webmail.

La webmail è fondamentalmente un'interfaccia web che ci permette di agire sui server di posta. Schematizziamo uno scambio di e-mail tra Ana e Bea, che utilizzano entrambe la webmail:

- il "percorso di rete" tra il computer di Bea e la sua casella di posta elettronica ospitata da *fai.net* verrà navigato utilizzando un protocollo web (HTTP o HTTPS)
- ha seguito un breve periodo presso *fai.net*, che ha garantito il passaggio dalla webmail alla posta elettronica.
- seguito da un viaggio con protocollo di posta elettronica (SMTP) tra *fai.net* e *example.org*
- ancora una volta, su *example.org*, tra i protocolli mail e web
- poi dal Web (HTTP o HTTPS) al computer di Ana.

35.5.1 Vantaggi

Uno dei vantaggi della webmail, come di tutte le applicazioni web, è che non è necessario installare, aggiornare o configurare il software di posta. La webmail è anche una caratteristica chiave del Web 2.0: è possibile accedere alla propria casella di posta elettronica da qualsiasi computer connesso a Internet, in qualsiasi momento e ovunque.

Se si utilizza un sistema *live* e non si cripta la posta elettronica, questo ha il vantaggio di non lasciare tracce sul disco.

35.5.2 Svantaggi

Il lato negativo è che se non si è connessi, tutta la corrispondenza è inaccessibile (a meno che non si sia salvata tutta o parte di essa su un supporto pratico: chiavetta USB, disco rigido, ecc.).

pagina
151

Il fatto che sia possibile utilizzare qualsiasi browser web per accedere alla nostra casella di posta elettronica può rapidamente incoraggiarci a utilizzare *qualsiasi* browser web, e con esso i computer di cui non abbiamo motivo di fidarci.

Poi, a seconda del livello di fiducia che riponete nel vostro host di posta, dovete chiedervi quanto siano centralizzati i vostri dati. L'uso massiccio della webmail ha portato a una situazione in cui migliaia di caselle di posta elettronica, con tutto il loro contenuto, finiscono nelle mani dei maggiori provider di servizi di posta, affidando loro la custodia di una montagna di dati personali. Questi provider possono utilizzarli per scopi commerciali, consegnarli alle varie autorità o semplicemente perderli. Inoltre, se consideriamo la nostra corrispondenza sensibile in un modo o nell'altro, forse preferiremmo non farla ricadere sulle spalle di persone - perché c'è ancora qualcuno dietro le macchine - che non vogliono assumersene la responsabilità. Questo è stato probabilmente il caso, nell'agosto 2013, di Lavabit ² che ospitava un account di posta elettronica di Edward Snowden e che ha deciso di cessare l'attività. La chiusura ha fatto seguito a richieste e persino a pressioni da parte di agenzie governative come la NSA e l'FBI.

Infine, ma non per questo meno importante, l'uso della webmail può consentirci di trarre il massimo vantaggio da una serie di funzionalità che vengono visualizzate nel nostro browser quando consultiamo la nostra casella di posta elettronica. Annunci pubblicitari che possono essere selezionati in base al contenuto delle nostre e-mail.

pagina
221

35.6 Client di posta elettronica

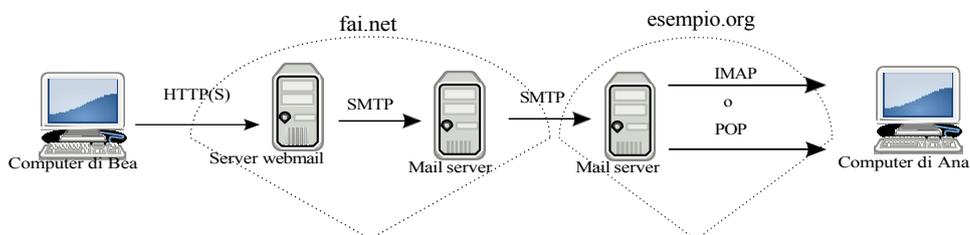
Un client di posta elettronica è un'applicazione software utilizzata per gestire la posta elettronica: ricevere, leggere, inviare, *ecc.* I client di posta elettronica più noti sono Outlook di Microsoft e Thunderbird di Mozilla. Ne esistono molti altri che, nonostante le differenze, hanno un'interfaccia sostanzialmente simile a quella delle webmail.

A differenza della webmail, in cui si utilizza il browser web per consultare i messaggi di posta elettronica memorizzati sul server dell'host, qui si leggono le e-mail utilizzando un software installato sul computer. Per memorizzare le e-mail si utilizza un dispositivo di archiviazione locale (il disco rigido del computer, una chiavetta USB, *ecc.*).

Per tornare al nostro piccolo diagramma precedente, dobbiamo sostituire i protocolli web con i protocolli di posta. Esistono due diversi protocolli per la ricezione della posta: *IMAP (Internet Message Access Protocol)* e *POP (Post Office Protocol)*.

Il primo, IMAP, è utilizzato per gestire le e-mail memorizzate sui server di posta del nostro host. A ogni connessione alla casella di posta, avviene una sincronizzazione per garantire lo stesso stato (numero di e-mail, bozze, cartelle, *ecc.*) sul server di posta e sul nostro client di posta, e viceversa. Questo avviene senza scaricare alcun contenuto dal server di posta. Solo l'elenco delle e-mail e le loro intestazioni possono essere scaricate sul nostro client di posta, ad esempio.

Il secondo protocollo, POP, scarica i vari contenuti della casella di posta elettronica direttamente sul nostro client di posta, senza necessariamente lasciarne una copia sul server remoto.



Bea invia un'e-mail ad Ana, Bea usa una webmail, Ana usa un client di posta.

2. Wikipedia, 2014, *Lavabit* [<https://fr.wikipedia.org/wiki/Lavabit>].

35.6.1 Vantaggi

I vantaggi e gli svantaggi possono essere specifici del protocollo utilizzato per ricevere la posta, ma alcuni sono comuni a tutti.

Con un client di posta elettronica, è possibile recuperare la casella di posta nello stesso stato in cui è stata controllata l'ultima volta, anche senza una connessione a Internet. Ciò significa che è possibile leggere, scrivere o eliminare le e-mail offline. E di inviarle o riceverle di nuovo quando viene ripristinata la connessione. Inoltre, l'uso di un client di posta elettronica ci evita di dover sopportare la miriade di pubblicità che popolano il web.

Utilizzando il protocollo POP, potrete beneficiare di altri vantaggi, come la decentralizzazione della posta elettronica. Invece di lasciare tutta la nostra corrispondenza su server remoti, la posta elettronica viene rimpatriata sul computer. Ciò significa che non dobbiamo lasciare tutte le nostre e-mail presso i principali host di posta elettronica e che gli host di posta elettronica più piccoli non occupano troppo spazio su disco. Il fatto che le e-mail finiscano sul sistema del destinatario ci permette anche di avere un maggiore controllo sulla loro gestione, ad esempio per quanto riguarda l'eliminazione effettiva di e-mail che potrebbero rivelarsi critiche. Infine, ma non meno importante, meno dati vengono lasciati alle aziende che non si preoccupano della riservatezza della corrispondenza. Un'avvertenza: l'host può comunque fare una copia dell'e-mail prima che venga rispedita al client di posta.

35.6.2 Svantaggi

Per utilizzare un client di posta, è necessario configurarlo in modo che sappia quale casella di posta leggere, a quale server connettersi e quale protocollo utilizzare.

È più complicato controllare la posta elettronica da un computer diverso dal proprio (a casa di un amico o al lavoro, per esempio), a meno che non si utilizzi il client di posta di un sistema *live* persistente (come Tails), installato su una chiavetta USB.

Inoltre, se il vostro client di posta è configurato in modo da non lasciare la posta sul server, questa verrà memorizzata solo sul supporto di memoria del vostro client di posta. Se questo viene perso (sul disco rigido del computer o sulla chiavetta USB su cui avete installato un sistema Live Tails persistente), potete dire addio ai vostri preziosi messaggi... a meno che non abbiate fatto un backup.

pagina

151

35.7 Scambiare e-mail nascondendo la propria identità

L'obiettivo è quello di nascondere a un avversario il fatto che siamo uno dei corrispondenti di uno scambio di e-mail. Potrebbe trattarsi di uno scambio di e-mail con un ricercato politico o con un amico perso da tempo.

35.7.1 Definizione di una politica di sicurezza

La nostra preoccupazione principale sarà quella di nascondere i nomi delle persone che si scambiano e-mail, o almeno di rendere la loro identificazione il più difficile possibile. Cosa farebbe un avversario per trovarli?

Primo passo: chiedere alle postine

Il nostro provider di posta è un nodo di rete attraverso il quale è destinata a passare la nostra corrispondenza digitale. Un avversario interessato a questo settore avrebbe quindi buone ragioni per darvi un'occhiata, tanto più che può essere molto facile farlo.

Allo stesso modo, gli intermediari tra Bea e Ana (compresi i rispettivi ISP) vedono le intestazioni delle e-mail, che possono fornire una grande quantità di informazioni (tra cui, per alcuni host, gli indirizzi IP dei corrispondenti). Un attacco di questo tipo è

pagina

218

più che probabile se il contenuto delle e-mail o i protagonisti degli scambi attirano l'attenzione di autorità dotate di poteri sufficienti. È giusto dire che, in primo luogo, non avere un indirizzo e-mail come *nom.prenom@exemple.org* è già un buon riflesso. Prima di tutto, dovrete pensare di usare un pseudonimo, per crearvi un'identità contestuale.

pagina

243

Detto questo, se "Kiwi Poilu" scrive regolarmente a Caroline Carot, Sofiane Carot e Francine Carot, un avversario *potrebbe* dire che appartiene alla famiglia Carot, o che fa parte della cerchia ristretta: anche l'identità delle persone a cui scriviamo è rivelatrice.

Inoltre, se utilizzate un pseudonimo, ma un avversario osserva che le e-mail che state monitorando provengono da una casa o da un appartamento particolare, può stabilire il collegamento. Per questo motivo, come per la navigazione sul Web, è possibile utilizzare il routing a cipolla o l'uso di un sistema di live amnesia appositamente progettato per coprire le tracce fino al nostro computer.

pagina

261

pagina

113

Infine, il contenuto degli scambi può rivelare abbastanza sui loro autori da attribuire loro un nome. Nascondere un'identità richiede quindi attenzione non solo alle intestazioni, ma anche al contenuto dell'e-mail.

Per proteggere il contenuto delle e-mail da occhi indiscreti, sia per se stesso che per ciò che può rivelare sugli autori delle e-mail, utilizziamo la crittografia delle e-mail.

pagina

a fianco

Secondo passo: osservare il computer che si sta utilizzando

Se si utilizza la rete Tor e un pseudonimo per proteggere la propria identità, un potenziale aggressore può cercare di accedere alle tracce lasciate sul computer per dimostrare che la persona sospettata è effettivamente in possesso dell'account e-mail in questione.

pagi

na

27

pagina

119

pagina

113

Per proteggersi da questo attacco, criptare il disco rigido o utilizzare un sistema live amnesico.

Ciò è ancora più importante se si utilizza un client di posta elettronica, poiché non sono solo le tracce a essere lasciate sul sistema, ma anche le e-mail stesse.

Passo 3: Attaccare Tor

Un aggressore in grado di monitorare diversi punti della rete, come la connessione utilizzata e l'host di posta, potrebbe essere in grado di annullare l'anonimato fornito dalla rete Tor.

Non dimentichiamo che ci sono molti altri possibili attacchi alla rete Tor e che è essenziale capire da cosa protegge e da cosa non protegge.

pagina

261

pagina

267

35.7.2 Scegliere tra gli strumenti disponibili

Esistono diversi strumenti per comunicare via e-mail, per cui la scelta dipende dai vari criteri menzionati in precedenza. Ad esempio, si può preferire di non lasciare le e-mail sul server dell'host, ma di leggerle e rispondere offline, oppure di non scaricare una copia delle e-mail, ma di accedervi online.

35.7.3 Webmail

Poiché la webmail è un uso specifico del web, per le domande relative a Tor Browser o Tails - i loro vantaggi, svantaggi e utilizzo - si prega di fare riferimento al caso d'uso relativo alla navigazione web (vedere pagina 277). Certificati o autorità di certificazione utilizzati per la crittografia della connessione

al server di posta devono essere autentici, poiché un aggressore che abbia i mezzi per ingannare l'utente a questo punto sarà in grado di recuperare in chiaro tutti gli scambi con il server di posta, compresi il login e la password della mailbox. È quindi necessario verificarle con cura (vedere pagina 323).

Inoltre, se si utilizza la webmail di Tails su un computer di dubbia provenienza, per esempio

In caso di attacco da parte di un keylogger, è consigliabile utilizzare una tastiera visiva (nota anche come "tastiera virtuale") quando si inserisce la password dell'account di posta elettronica.

pagina
327

35.7.4 Client di posta elettronica

Se preferite utilizzare un client di posta piuttosto che la webmail, potete scegliere tra :

- Utilizzare Tails (vedere pagina 113) e seguire lo strumento Configurare e utilizzare Thunderbird (vedere pagina 329). Eventuali tracce lasciate localmente verranno cancellate allo spegnimento del sistema.
- Utilizzare Tails e Thunderbird configurando la persistenza (vedere pagina 116), quindi seguire lo strumento Configurare e utilizzare Thunderbird (vedere pagina 329). Il contenuto della casella di posta elettronica sarà memorizzato su una chiave USB, che conterrà quindi tracce criptate.
- Installare un client di posta sul sistema criptato (vedere pagina 119). A tale scopo, installare il pacchetto `thunderbird-110n-en`³ seguendo la ricetta per l'installazione del software (vedere pagina 135), quindi seguire lo strumento di configurazione e utilizzo di Thunderbird (vedere pagina 329). Le tracce saranno lasciate sul disco rigido criptato del computer.

Tuttavia, come per la webmail, è necessario verificare quali certificati o autorità di certificazione offrono la crittografia della connessione al server di posta.

pagina
323

35.8 Scambio di e-mail riservate

L'obiettivo è quello di nascondere il contenuto delle nostre e-mail in modo che nessuno, oltre al destinatario, possa leggerle; ciò può essere utile quando il contenuto dei nostri messaggi è *delicato* o dice molto sulla persona che li ha scritti.

Per definire la nostra politica di sicurezza, dobbiamo considerare l'uso dei cifrari in diversi modi. Prendiamo il punto di vista dell'avversario e vediamo come possiamo proteggerci.

35.8.1 Primo passo: chiedere alle postine

Senza particolari misure di protezione, i servizi di hosting di posta elettronica sono in grado di leggere il contenuto delle e-mail che ci vengono inviate. Questo perché è sui loro server che le nostre e-mail vengono instradate e memorizzate. Non c'è una grande differenza tra l'utilizzo di un particolare protocollo, di un client di posta o di una webmail.

I nostri messaggi possono essere conservati per anni fino a quando non li rimpatriamo o li cancelliamo, o anche più a lungo se uno dei server ne fa una copia, ad esempio come parte di un backup. Da qui l'importanza di chiudere le caselle di posta elettronica una volta esaurita la loro utilità. Questo ha anche il vantaggio di non occupare spazio su disco e di non consumare risorse a vuoto presso l'host di posta.

3. Il protocollo OpenPGP, utilizzato per la crittografia delle e-mail [questa pagina], è stato integrato e attivato di default dalla versione 78.2.1 di Thunderbird. Ciò significa che non è più necessario installare il componente aggiuntivo Enigmail, che era richiesto nelle versioni precedenti.



PER SAPERNE DI PIÙ...

Se vi piace smanettare, potete creare e ospitare da soli il vostro server di posta su un servizio onion (vedere pagina 266).

Leggere i nostri messaggi è una violazione della riservatezza della corrispondenza.

- come leggere una lettera non indirizzata, non richiede alcuno sforzo tecnico, nemmeno quello di aprire una busta. È così semplice, infatti, che è stato automatizzato da Gmail, che fa leggere ai "robot" il contenuto delle e-mail dei suoi utenti per individuare lo *spam*, ma anche per "semplificare la loro vita", ad esempio individuando l'aereo che stanno per prendere e avvisandoli se è in ritardo. ⁴.



PRECISIONE

Questi "robot" non sono né automi né androidi, ma piccoli programmi che scansionano "automaticamente" i contenuti per identificare qualcosa: ad esempio, i "robot" di Google scansionano le pagine web per indicizzare le parole chiave rilevanti che potrebbero essere ricercate. Tali robot sono utilizzati anche dai poliziotti per segnalare se qualcuno utilizza determinate parole della loro presunta "Dizionario dei terroristi".

Per quanto riguarda gli intermediari tra i computer dei protagonisti dello scambio di e-mail e i server dei rispettivi host di posta elettronica, esistono due possibili situazioni. La prima, ormai piuttosto rara, è quando la connessione tra il computer e il server di posta non è crittografata.

In questo caso, i vari intermediari riceveranno l'equivalente delle cartoline. Si troveranno in una situazione simile a quella degli host postali, con la differenza che le cartoline saranno semplicemente in transito... a meno che non siano predisposti per ispezionare in modo più approfondito la posta che trasportano, sia a fini statistici per migliorare la qualità del loro servizio, sia per tenerci d'occhio.



Connessione non crittata ai server di posta

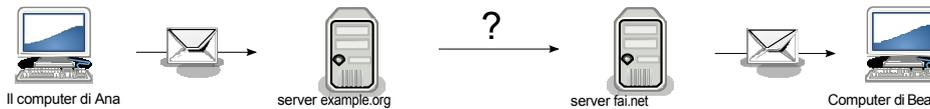
pagina
249

La seconda situazione è quella in cui la connessione tra il computer e il server di posta è crittografata con il protocollo *TLS*. ⁵ Ciò è possibile indipendentemente dal protocollo utilizzato. In questo caso, gli intermediari tra le due macchine vedranno le cartoline infilate nelle buste. L'host di posta non sarà interessato dalla crittografia e avrà comunque accesso all'e-mail nella sua interezza.

4. Janko Roettgers, 2017, *Google continuerà a leggere le vostre e-mail, ma non per gli annunci*. [<https://va.riety.com/2017/digital/news/google-gmail-ads-emails-1202477321/>] (in inglese).

5. Quando vogliamo criptare una connessione con un server web o di posta elettronica, utilizziamo il protocollo TLS. Si tratta di uno standard che incapsula [pagina 201] il protocollo normalmente utilizzato. Ad esempio, il protocollo web HTTP, se incapsulato in TLS e quindi criptato, si chiama HTTPS. Lo stesso vale per i protocolli di posta POPS, IMAPS e SMTPS.

Infine, non è garantito che la connessione tra il server di posta di Ana e quello di Bea sia criptata, nel qual caso l'e-mail viaggerà in parte come una lettera, in parte come una cartolina.



Connessione criptata ai server di posta

Crittografate le vostre e-mail

Per garantire che il contenuto dei nostri messaggi non possa essere letto da nessun intermediario, compreso l'ufficio postale, possiamo crittografarli direttamente sul nostro computer, ancora prima di inviarli. Per farlo, utilizzeremo lo standard di crittografia asimmetrica OpenPGP. Sarebbe anche possibile utilizzare la crittografia simmetrica, ma i suoi limiti ce la sconsigliano vivamente.

Con la crittografia asimmetrica, solo il destinatario, per il quale è stata eseguita la crittografia, sarà in grado di decifrare il messaggio. Non dimentichiamo, però, che anche la crittografia asimmetrica ha i suoi limiti, che possono consentire a un avversario di rivelare il contenuto criptato.

In pratica, se non l'avete già fatto, inizierete importando la chiave pubblica del vostro destinatario. Poi dovremo verificarne l'autenticità. Inoltre, se intendiamo stabilire una corrispondenza e quindi ricevere e-mail in cambio, avremo bisogno anche di una coppia di chiavi: una sarà utilizzata dai nostri corrispondenti per crittografare le e-mail per noi, l'altra ci permetterà di decifrarle. Se non disponete già di una coppia di chiavi di crittografia, seguite la ricetta per crearne e gestirne una.

Si noti, tuttavia, che questo metodo cripta solo il contenuto dell'e-mail. Non modifica in alcun modo le intestazioni delle e-mail.

A seconda che si scelga di utilizzare un client di posta o una webmail, il metodo utilizzato per crittografare le e-mail sarà diverso.

Crittografia delle e-mail in Thunderbird

Seguite la ricetta per crittografare le e-mail in Thunderbird (vedere pagina 333).

Crittografia delle e-mail per la webmail con Tails

Se preferite criptare le vostre e-mail utilizzando la webmail, evitate di scrivere il vostro messaggio nella finestra del browser web e poi crittografarlo. Questo perché alcuni attacchi, in particolare tramite JavaScript, potrebbero accedere al nostro testo dallo stesso browser web. Inoltre, il testo scritto all'interno della webmail potrebbe essere automaticamente salvato in bozze non crittografate. Sarebbe molto spiacevole offrire in chiaro un testo che si vuole crittografare.

Non spiegheremo come criptare le e-mail per la webmail con Debian criptata, ma solo con Tails.

Il metodo attualmente consigliato per la crittografia della posta elettronica e per la crittografia del testo è descritto nella documentazione di Tails.

Una volta avviato Tails (vedere pagina 115), affiggere il desktop e fare doppio clic sull'icona *Tails Documentation*. Nell'indice che si apre, cercate la sezione *Crittografia e privacy* e fate clic sulla pagina *Crittografia di testi e file con GnuPG e Kleopatra*. Al momento della stampa, questa pagina non era ancora stata tradotta in francese. Seguire la sezione *Lavorare con il testo crittografato*.

pagina
249

pagina
258

pagina
337

pagina
338

pagina
333

pagina
218

pagina
214

testo crittografato) in questa pagina di documentazione, in particolare nella sezione *Per crittografare il testo*.

La persona che riceve l'e-mail dovrà seguire la procedura *Per decriptare il testo* nella stessa pagina di documentazione.

50

[
[
pagi
na
31

[
[
pagi
na
50

[
[
pagi
na

35.8.2 Secondo passo: osse rvar e il com pute r che si sta utili zzan do

abbia accesso ai dati del nostro host e non possa origliare la rete, ma possa venire a utilizzare i nostri dati: quali tracce dei nostri scambi troverà sul nostro computer?

Se questa persona riesce a mettere le mani sul nostro computer o su quello del nostro destinatario, impadronendosi o riuscendo a installarvi un software dannoso, potrà accedere a tutte le e-mail memorizzate e alle tracce lasciate; sia che queste tracce siano dovute al funzionamento della macchina sia che siano state lasciate dai protagonisti.

Per proteggerci da un avversario che potrebbe impossessarsi del nostro computer, ci preoccupiamo di crittografare il nostro disco rigido per rendergli più difficile l'accesso ai dati memorizzati. Questo non ci proteggerà dal software maligno che vuole esfiltrare questi dati, da qui l'importanza di installare solo software affidabile. Possiamo anche utilizzare un sistema *live* amnesico.

Si noti che se le e-mail memorizzate fanno parte di uno scambio crittografato con crittografia asimmetrica, anche se ha accesso al computer e ai dati in esso memorizzati, l'avversario non sarà in grado di leggerle, a meno che non abbia accesso anche alla chiave segreta. Se usiamo Thunderbird per inviare le nostre e-mail crittografate, questa chiave segreta è protetta dalla password principale di Thunderbird, sempre che ne abbiamo impostata una; nel portachiavi OpenPGP del desktop, la chiave segreta è protetta da una passphrase. Senza la master password o la passphrase, l'avversario non sarà in grado di trovare la chiave segreta e quindi non potrà leggere le e-mail crittografate.

35.8.3 Terzo passo: attacco alla crittografia dei media

Se si controlla la posta elettronica su una Debian crittografata, le tracce sul disco rigido del computer saranno crittografate, sia che si utilizzi una webmail o un client di posta. In quanto tali, non saranno utili a un avversario. Tuttavia, alcuni avversari possono avere modi per attaccare questa crittografia. Inoltre, se la persona con cui si conversa via e-mail non fa lo stesso, il livello complessivo di protezione dei contenuti sarà pari a quello della protezione più debole. In effetti, dopo aver preso grandi precauzioni e aver scambiato e-mail con qualcuno che ha, ad esempio, un Debian non criptato, o che è permanentemente acceso ⁶ può essere più pericoloso, perché potrebbe dare una falsa impressione di sicurezza. A maggior ragione se è facile individuare o dare un nome ai protagonisti dello scambio.

Se si usa un programma di posta su un sistema *live* amnesico, non ci saranno tracce sul computer usato dopo lo spegnimento, ma ce ne saranno sulla partizione persistente se è stata configurata. Queste saranno criptate, il che riporta al caso precedente di una Debian criptata.

Se non volete lasciare tracce sul computer che state utilizzando, crittografato o meno, potete utilizzare il sistema Tails live senza persistenza, sfruttando la sua amnesia.

35.8.4 Quarta fase: crittografia del messaggio di attacco

Un avversario che abbia accesso alle e-mail crittografate può cercare di sfruttare i limiti della crittografia per decifrare i messaggi.

6. All'accensione, una macchina con un disco rigido criptato contiene una grande quantità di informazioni decriptate nella sua RAM [pagina 18].

S
u
p
p
o
n
i
a
m
o

c
h
e

u
n

a
g
g
r
e
s
s
o
r
e

n
o
n

pagina
18
che
si
sta
utili
zzan
do
pagina
330

Caso d'uso: dialogo

36.1 Contesto

Nel caso precedente, i messaggi sono stati scambiati in modo asincrono, proprio come in uno scambio epistolare. Tuttavia, è possibile che si desideri una comunicazione sincrona, come in una telefonata, sia per una riunione per lavorare su un documento delicato o per chiacchierare con un amico. La soluzione più semplice potrebbe essere quella di incontrarsi o di telefonarsi, ma non sempre è possibile o auspicabile. A volte la messaggistica istantanea è una buona alternativa.

Molti conoscono e utilizzano regolarmente la messaggistica di Skype (il sostituto di MSN o Windows Live Messenger di Microsoft) o la messaggistica interna di Facebook, solo per citare gli esempi più noti. È comodo, certo, ma è possibile avere qualcosa di pratico senza sacrificare la discrezione!

36.2 Valutazione dei rischi

36.2.1 Cosa vogliamo proteggere?

Le risposte possibili a questa domanda sono le stesse dello scambio di messaggi. Si potrebbe voler proteggere il contenuto dello scambio, la posizione dei protagonisti, le loro identità, i loro collegamenti e così via.

36.2.2 Da chi vogliamo proteggerci?

Anche in questo caso, le risposte sono simili a quelle date nel caso dello scambio di messaggi: si potrebbe voler nascondere tutte o parte di queste informazioni alle varie macchine attraverso le quali passano, così come alle persone che potrebbero avervi accesso.

Tra queste macchine ci sono innanzitutto i server di messaggistica istantanea utilizzati dai vari corrispondenti.

Seguono i router, situati sul percorso tra i protagonisti dello scambio, in particolare quelli dei rispettivi ISP (Internet Service Provider).

Infine, vengono lasciate tracce sui computer utilizzati.

36.3 Definizione di una politica di sicurezza

Passiamo ora ad esaminare le questioni esposte nella nostra metodologia, adottando il punto di vista del nostro avversario a pag. 65.

36.3.1 Primo passo: tutte le informazioni necessarie per i più curiosi

I sistemi di messaggistica interna di Facebook, Skype, *ecc.* consentono a molte persone di accedere a informazioni che non le riguardano: Facebook o Micro-soft vedono tutte le nostre conversazioni sulle loro macchine e possono archivarle per accedervi in seguito. La polizia deve solo chiedere le informazioni, e una falla nella sicurezza del server può dare accesso a molte altre persone. Per non parlare del fatto che Facebook cambia regolarmente le impostazioni sulla privacy senza preavviso, e potrebbe decidere domani di rendere pubblico ciò che oggi è "privato".

Inoltre, Skype registra la cronologia delle conversazioni sul computer utilizzato, quindi chiunque abbia accesso al computer potrebbe accedere a questa cronologia (amico, ladro, amante geloso...).

Ma Microsoft e Facebook non hanno inventato la messaggistica istantanea e ci sono molte alternative disponibili. Esistono numerosi programmi che si possono installare sul computer per comunicare utilizzando una serie di protocolli: Skype, IRC, XMPP e altri ancora.

Utilizzando un software affidabile, possiamo disattivare l'archiviazione delle conversazioni e limitare così le tracce lasciate sul nostro computer.

Ci sono anche server che forniscono indirizzi di messaggistica istantanea e non sono in grado di fare controlli incrociati come Google, Microsoft o Facebook.

Per seguire questo percorso su un sistema Debian precedentemente installato (criptato) (vedere pagina 119), fare riferimento allo strumento di installazione del software (vedere pagina 131) per installare pidgin. Se si usa Tails, questo software è già installato¹.

36.3.2 Fase 2: Chiedere ai padroni di casa

Utilizzando un client di messaggistica istantanea e vari server, non si centralizzano tutti i collegamenti e i dialoghi nelle stesse mani. Tuttavia, sia il contenuto delle conversazioni che le parti che comunicano rimangono accessibili dai computer attraverso i quali passano.

Sebbene sia spesso possibile impostare il nostro software per criptare la connessione al server di posta, i dialoghi rimangono accessibili al server. Inoltre, di solito non è garantito che anche il collegamento tra il server e l'altro corrispondente sia criptato.

[pagina 228]
[pagina 235] Un avversario con i mezzi per farlo potrebbe contattare gli amministratori del server utilizzato, o anche le organizzazioni che forniscono la rete, per ottenere informazioni sulle conversazioni. Potrebbe anche cercare di "hackerare" le loro macchine. La riservatezza dei dialoghi è quindi strettamente legata alla fiducia che riponiamo nei server di messaggistica che utilizziamo e anche nelle infrastrutture di rete, in particolare nel nostro fornitore di accesso.

[pagina 249] Per rendere ancora più difficile per un avversario leggere il contenuto dei nostri dialoghi, possiamo utilizzare la crittografia end-to-end per garantire la riservatezza.

Per seguire questo metodo su un sistema Debian precedentemente installato (criptato) (vedere pagina 119), seguire gli strumenti di installazione del software (vedere pagina 131) per installare il pacchetto pidgin-otr, quindi utilizzare la messaggistica istantanea con OTR (vedere pagina 351).

1. Tails sta discutendo la sostituzione di Pidgin con un altro programma di messaggistica istantanea. Questa proposta di cambiamento è tracciata sul gitlab di Tails [<https://gitlab.tails.boum.org/tails/tails/-/problemi/8573>].



PER SAPERNE DI PIÙ...

Attualmente si stanno sviluppando e integrando in Debian soluzioni tecniche per consentire la crittografia end-to-end nelle conversazioni di gruppo. Un esempio è Dino², che ha annunciato l'integrazione del protocollo di cifratura OMEMO.³

36.3.3 Terzo passo: Mantenere i link visibili

Se utilizziamo la crittografia end-to-end in un dialogo di messaggistica istantanea, un avversario non può più accedere al contenuto della conversazione, a meno che non rompa la crittografia, acceda al nostro computer o si introduca in esso.

Tuttavia, un avversario che abbia accesso alla rete o al server di posta utilizzato può sempre vedere con chi stiamo parlando. Per nascondere i collegamenti, dobbiamo utilizzare identità contestuali e connetterci in modo anonimo, ad esempio utilizzando Tor. Questo non solo garantisce la riservatezza grazie alla crittografia, ma anche *lo pseudonimato*.

Utilizzando un sistema *live* amnesico come Tails, ci si occupa anche di tutte le tracce che potrebbero essere lasciate sul computer in uso. A meno che non si utilizzi la persistenza, nel qual caso le tracce crittografate saranno conservate nella partizione persistente della chiave USB di Tails.

Se non ne avete già uno, dovrete iniziare a creare una chiave USB o un DVD Tails (vedere pagina 113).

Quindi, dopo aver effettuato il boot nel supporto contenente Tails (vedere pagina 107), dovremo definire un'identità contestuale da utilizzare e impostare la persistenza di Tails (vedere pagina 116) per questa identità attivando l'opzione "Pidgin".

Infine, potremo seguire l'uso dello strumento di messaggistica istantanea con OTR (vedere pagina 351).

In questo caso si combinano due criteri: la riservatezza e l'anonimato. Nel passo precedente abbiamo visto come ottenere la *riservatezza* utilizzando la crittografia OTR. Qui abbiamo appena visto come ottenere *l'anonimato e la riservatezza* usando la crittografia OTR sotto Tails, oltre a un'identità contestuale. Tuttavia, si può desiderare *l'anonimato o lo pseudonimato da soli*, cioè senza la riservatezza. Infatti, potremmo voler nascondere la nostra identità senza nascondere il contenuto delle nostre conversazioni, ad esempio quando chattiamo in "Per seguire questa traccia, avviare Tails e poi usare Pidgin. Per seguire questa traccia, avviare Tails (vedere pagina 115), quindi utilizzare Pidgin (vedere pagina 351) senza utilizzare la crittografia OTR, con un account creato per l'occasione.

36.4 I limiti

Innanzitutto, questo metodo rimane vulnerabile agli attacchi di crittografia di cui abbiamo appena parlato e agli attacchi a Tor.

Ma ci sono anche alcune limitazioni specifiche alle conversazioni in tempo reale. Ad esempio, lo stato "online" o "offline" di un'identità è solitamente accessibile pubblicamente. Un avversario può quindi vedere quando un'identità è online, ed eventualmente correlare più identità: perché sono sempre online nello stesso momento; oppure, al contrario, perché non sono mai online nello stesso momento, ma spesso in successione, e così via.

2. **Dino** [<https://prism-break.org/fr/projects/dino/>].

3. **Protocollo OMEMO** [<https://prism-break.org/fr/protocols/omemo/>].

pagina
358
pagina
238
pagina
243
pagina
261

pagina
279



PRECISIONE

Per fare in modo che le identità sembrino "sempre attive", è possibile utilizzare un computer "fantasma" o proxy⁴ su un computer fidato che sia sempre attivo e connesso al server di messaggistica istantanea. In questo modo, è questo computer, e non il server, a "vedere" quando si è connessi o meno, e questo stato non è più pubblico. La creazione di un'infrastruttura di questo tipo, tuttavia, esula dagli scopi di questa guida.

Poi, nel caso particolare in cui l'anonimato (o lo pseudonimato) prevalga su altri vincoli, ad esempio se si vuole chattare in una stanza pubblica, si aggiungono altri limiti a quelli già citati. Un'identità contestuale corre sempre il rischio di finire legata a un'identità civile, come abbiamo visto nella sezione sugli pseudonimi. Infatti, anche con uno pseudonimo, il contenuto e la forma delle nostre conversazioni possono rivelare molto della persona che sta dietro la tastiera.

pagina

244

È bene tenere presente che quando si cerca di definire una politica di sicurezza per una relazione tra più persone, che si tratti di una telefonata, di uno scambio di e-mail o di una messaggistica istantanea, il livello complessivo di sicurezza sarà livellato dal livello di sicurezza del protagonista meno prudente. Se, ad esempio, ci preoccupiamo di utilizzare Tails per non lasciare tracce della nostra conversazione sul computer, mentre il nostro interlocutore utilizza il suo sistema operativo abituale senza alcuna protezione particolare, allora quest'ultimo sarà senza dubbio il punto più debole della nostra politica di sicurezza della comunicazione.

pagina

289

Infine, come già detto, la crittografia OTR non consente attualmente a più di due persone di conversare contemporaneamente. Tuttavia, la ricerca si sta muovendo in questa direzione⁵.



PER SAPERNE DI PIÙ...

Nel frattempo, se vi piace armeggiare, è già possibile configurare il proprio server di messaggistica istantanea (ad esempio XMPP) su un servizio onion (vedere pagina 266).

4. Wikipedia, 2014, *Proxy* [<https://fr.wikipedia.org/wiki/Proxy>].

5. Ian Goldberg *et al*, 2009 *Multi-party Off-the-Record Messaging*, CACR Tech Report 2009- 27 [<http://www.cacr.math.uwaterloo.ca/techreports/2009/cacr2009-27.pdf>]; Jacob Appelbaum *et al*, 2013, mpOTR [<https://libraries.io/github/ioerror/mpOTR>].

Caso d'uso: condivisione di documenti sensibile

37.1 Contesto

Abbiamo visto come pubblicare i documenti che si desidera rendere pubblici. Ma a volte è anche necessario condividere le informazioni con un gruppo ristretto di persone. documenti sensibili come documenti di lavoro confidenziali, foto di vacanze o i dettagli di contatto di una fonte disposta a divulgare documenti aziendali interni

In questo caso, ci concentreremo sulla condivisione di documenti sensibili via Internet, che è l'argomento di questo secondo volume della *guida*. A seconda della situazione, potrebbe essere possibile scambiare anche chiavette USB criptate, documenti cartacei *e così via*.

37.2 Valutazione dei rischi

37.2.1 Cosa vogliamo proteggere?

Contenuto del documento

Il contenuto dei file condivisi è riservato. Solo i destinatari devono potervi accedere, come avviene per l'invio di un messaggio di posta elettronica. Ad esempio, se si vogliono condividere le foto delle vacanze con la propria famiglia, è necessario nascondere le foto stesse. Il fatto che i destinatari siano membri della famiglia non è, *a priori*, un'informazione sensibile. Si tratta di *proteggere ciò che si condivide*.

Sorgente e destinazione

Anche l'identità della fonte e del destinatario può far parte delle informazioni da proteggere. Nel caso di documenti aziendali trapelati, chi ha inviato i documenti e a chi sono due informazioni particolarmente sensibili (la protezione delle fonti di informazione dei giornalisti è, infatti, alla base dell'etica giornalistica). Si tratta di *proteggere chi condivide con chi*.

Possiamo quindi dividere la questione in tre parti: la prima riguarda la protezione della fonte, la seconda la protezione del destinatario e la terza riguarda specificamente la riservatezza dei documenti da condividere.

37.2.2 Da chi vogliamo proteggerci?

Lo scopo è quello di proteggere l'utente da occhi indiscreti che cercano di vedere *chi fa cosa* sul web, come nel caso della navigazione dei siti web. Ma anche da occhi indiscreti che potrebbero *imbattersi* in questi file.

37.3.3 Terzo passo: guardare il computer di origine

I documenti riservati o le loro tracce possono rimanere sul vostro computer, intenzionalmente o meno.

Le soluzioni sono o la crittografia del disco rigido o l'evitare di lasciare tracce fin dall'inizio utilizzando un sistema *live* amnesico.

pagina
119
pagina
113

37.4 Protezione dei destinatari

Dopo aver preso le precauzioni necessarie per proteggere noi stessi, dobbiamo pensare anche ai destinatari dei nostri file. Anche se non possiamo sempre conoscere l'elenco completo delle persone che avranno accesso a questi documenti, o proteggerli per loro, possiamo sempre fare in modo che sia necessario un minimo di protezione perché possano accedervi.

Il modo più semplice, efficiente e realizzabile è quello di utilizzare un servizio onion, che costringerà i destinatari a utilizzare anche la rete Tor. Per farlo, dovrete seguire lo strumento OnionShare.

pagina
266
pagina
359

37.5 Proteggere i file riservati

Dopo aver pensato alla protezione delle persone che condividono i vostri documenti, è il momento di pensare alla protezione dei file stessi.

La procedura è simile a quella dello scambio di e-mail riservate. Ma non utilizzeremo la posta elettronica, sia perché i nostri file sono troppo voluminosi, sia perché non disponiamo di un elenco preciso di destinatari e quindi di un elenco di indirizzi e-mail a cui inviare i file. Preferiamo condividere i nostri file online su un server, come nel caso di una pubblicazione privata.

pagina
295

Le soluzioni che utilizziamo parlano di crittografia in modi diversi, a pagina 47, a seconda della nostra politica di sicurezza e del nostro approccio alla condivisione.

pagina
385

37.5.1 Scegliere tra gli strumenti disponibili

Esistono diversi strumenti per crittografare i nostri file prima di condividerli. La scelta dipende dal livello di condivisione e dalla qualità della crittografia richiesta.

37.5.2 Crittografia fornita dall'host

Innanzitutto, la soluzione che sembra richiedere il minimo sforzo è quella di mettere i nostri documenti su un servizio di file hosting che offre la possibilità di crittografarli direttamente sul server che li ospita.

pagina
319

In genere, questi servizi criptano i file nel browser dell'utente prima di inviarli al server. Il sito crea quindi un link di download con la chiave di decodifica inclusa nel link.² Uno dei vantaggi è che questa chiave non è in possesso dell'host del servizio, che quindi non ha accesso ai file dell'utente e, anche in caso di pressioni o richieste da parte dei poliziotti, non è in grado di fornirli in chiaro. Lo svantaggio principale di questo metodo è che la chiave di decrittazione è contenuta nel link di download. In altre parole, chiunque abbia accesso a questo link ha anche accesso ai file.

pagina
228

2. I server che ospitano questi servizi possono utilizzare diversi pacchetti software. Lufi e Up1 sono due esempi. Possiamo fidarci di loro *a priori* e chi scrive queste righe non conosce altri software di questo tipo.

L'utilizzo di questi servizi per condividere file riservati dipende quindi dal livello di fiducia che si può riporre nel software che fornisce il servizio e nell'host che lo ha configurato, nonché dalla riservatezza del link di download.

Per limitare i rischi, tuttavia, è possibile selezionare l'opzione che attiva la cancellazione dei file subito dopo il primo download. In questo modo si garantisce che i file vengano scaricati una sola volta e si può scoprire se i file sono già stati scaricati e se il metodo di comunicazione utilizzato per trasmettere il link non era riservato.

Se, tuttavia, si desidera crittografare utilizzando il servizio di file hosting, sarà necessario

:

- utilizzare il Browser Tor (vedere pagina 315) per accedere al web ;
- consultare la sezione Condividere un file (vedere pagina 321) della sezione *Trovare un web hosting* strumento ;
- disporre di un modo per trasmettere il link per il download in modo riservato, ad esempio inviandolo in un messaggio di posta elettronica criptato (vedere pagina 333).

37.5.3 Crittografia prima della condivisione

Un'altra opzione è quella di criptare i file prima di metterli online. Questa soluzione è un po' più complessa da implementare, ma ha il vantaggio di non richiedere la fiducia dell'host. Siete voi a scegliere come criptare i vostri file e anche chi può decriptarli.

Anche in questo caso sono disponibili diverse opzioni: a seconda del numero di destinatari, possiamo crittografare i nostri file con una passphrase o con una o più chiavi pubbliche.

[pagina
103:
pagina
249

In entrambi i casi, prestate molta attenzione al nome del file contenente i documenti criptati: se questo nome è esplicito, potrebbe rivelare informazioni sul contenuto dei documenti. Rinominare i file con un nome neutro, come "documento" o "archivio".

Crittografia con una passphrase

[pagina
103

Crittografare i nostri file da condividere con una passphrase significa che chiunque ne sia in possesso può decifrare e accedere ai nostri documenti. Tuttavia, è necessario conoscere la loro posizione, cioè l'indirizzo web da cui è possibile scaricarli o avere accesso a uno dei computer su cui sono memorizzati.

Un dettaglio importante è che chiunque abbia accesso ai file deve conoscere la passphrase utilizzata per crittografarli, in modo da renderli leggibili. È quindi necessario utilizzare un mezzo di comunicazione riservato per condividere questo segreto tra tutti i destinatari, cosa che a volte può risultare complicata.

[pagina
249

Infine, incontreremo le stesse limitazioni discusse nel capitolo sulla crittografia simmetrica.

Crittografare con una o più chiavi pubbliche

Se abbiamo un elenco definito di persone con cui condividere i nostri documenti e ognuna di esse possiede una coppia di chiavi OpenPGP, possiamo crittografare i file con le loro chiavi, in modo che solo loro possano decifrarli alla fine.

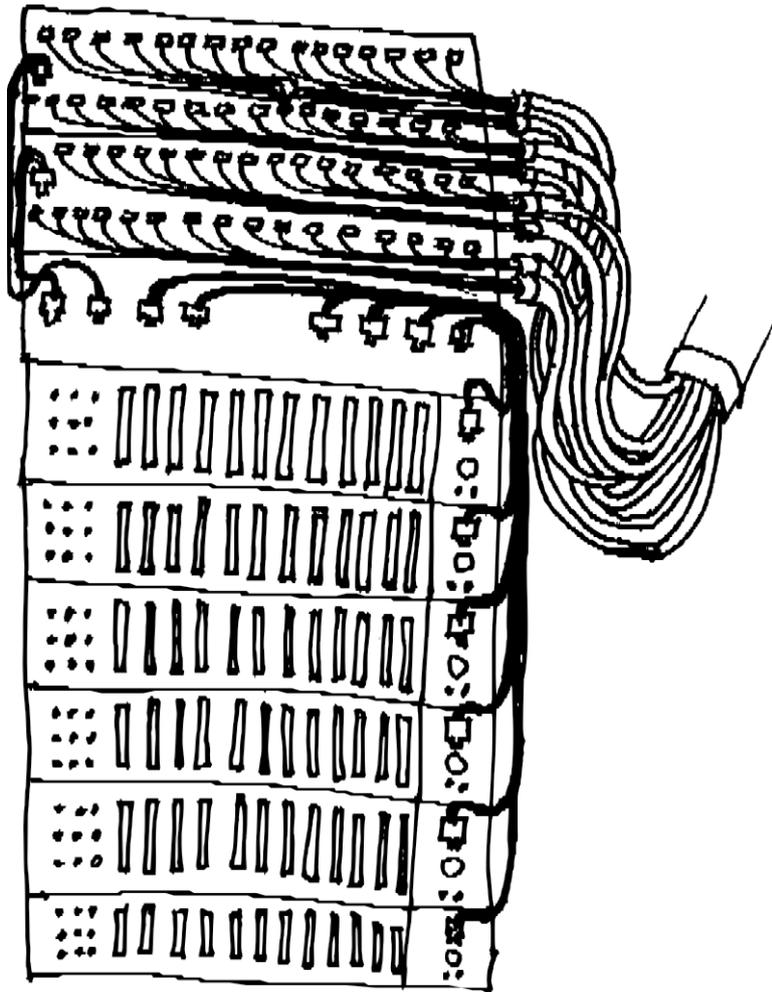
Andiamo

Per prima cosa è necessario seguire lo strumento di crittografia dei dati (vedere pagina 347), quindi scegliere una delle due soluzioni sopra menzionate per ospitare questi file:

- utilizzare un servizio di web hosting (vedere pagina 319)
- o ospitarli voi stessi con OnionShare (vedere pagina 359).

Decriptazione dei file

I destinatari dei documenti dovranno decifrarli seguendo l'apposita ricetta (vedi pagina 348).



SESTA PARTE

Strumenti

Introduzione

In questa terza sezione spiegheremo come applicare in pratica alcune delle idee sopra esposte.

Questa sezione è un'appendice tecnica alle precedenti. Una volta comprese le problematiche legate alla privacy nel mondo digitale e scelte le risposte adeguate, resta da chiedersi "Come si fa?", a cui questa appendice fornisce alcune risposte.

pagina
275

Per la maggior parte delle ricette presentate in questa guida, si presuppone che si utilizzi GNU/Linux con il desktop GNOME; queste ricette sono state scritte e testate sotto Debian GNU/Linux versione 11 (soprannominata Bullseye) ¹ e Tails versione 5 ² (*The Amnesic Incognito Live System*).

Tuttavia, questi sono generalmente adattabili ad altre distribuzioni basate su Debian, come Ubuntu³ o LinuxMint⁴.

Se non state ancora usando GNU/Linux, date un'occhiata ai casi d'uso nella prima sezione.

Le procedure sono presentate passo per passo e, laddove possibile, viene spiegato il significato delle azioni proposte.

pagina
71
pagina
113

L'ordine in cui ogni ricetta viene descritta è importante. A meno che non sia indicato diversamente, si raccomanda di non saltare un passaggio e poi tornare indietro. Il risultato potrebbe essere molto diverso da quello atteso.

Infine, è importante utilizzare la versione più aggiornata di questa guida, poiché il software si evolve. È possibile trovarla sul sito web <https://guide.boum.org/>.

-
1. <https://www.debian.org/releases/bullseye/index.fr.html>
 2. <https://tails.boum.org/index.fr.html>
 3. <https://www.ubuntu-fr.org/>
 4. <https://linuxmint.com/>

Installazione e configurazione del browser Tor

 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: 15 minuti.*

Come abbiamo visto, quando navighiamo in rete, i siti che visitiamo possono registrare il nostro indirizzo IP, rendendo più facile per gli avversari rintracciarci. Per questo motivo, a volte è necessario nascondere il nostro indirizzo IP. Tor è un software che consente di instradare la propria connessione attraverso una rete di

pagina
202

"Questo nasconde il nostro vero indirizzo IP. Si tratta del cosiddetto onion routing.

pagina
261

Per utilizzare la *rete di anonimizzazione Tor*, è necessario configurare non solo il software Tor stesso, ma anche il software che lo utilizzerà, come il browser web. Queste impostazioni sono spesso complesse, tanto che è difficile essere sicuri dell'anonimato che ne deriva.

Per questo motivo è meglio utilizzare Tor su un sistema *live* dedicato, oppure con un "kit pronto all'uso": il Tor Browser. Si tratta di uno strumento che rende molto semplice l'installazione e l'utilizzo di Tor su un sistema "classico". Non è necessaria alcuna configurazione e tutto il software necessario per la *navigazione su Tor* è incluso.

pagina
113

Il Tor Browser riunisce :

- Browser web Firefox, impostato per utilizzare Tor ;
- Software Tor ;
- un launcher, per avviare tutto con un semplice doppio clic.



Si noti che il Tor Browser non fornisce l'anonimato per l'intero computer: solo le connessioni ai siti web avviate in questo browser passano attraverso Tor. **Tutte le altre connessioni (client**

mail, aggregatori RSS, Torrent, altri browser web e così via) non vengono anonimizzati. Inoltre, anche quando il Tor Browser cerca di ridurre al minimo le tracce lasciate, i dati di navigazione come i cookie o la cronologia possono comunque essere salvati sul disco rigido, così come i file scaricati o i segnalibri del browser. Nel corso della navigazione, potremmo anche cliccare su un link che apre un altro programma (ad esempio un lettore musicale), che non passa attraverso Tor. Questi avvisi non sono

Non possiamo prenderla alla leggera, perché potrebbero trapelare indizi sulla natura della nostra navigazione.

Ecco come installare il Tor Browser su una Debian criptata. Tuttavia, per poter utilizzare un sistema che si connette a Internet solo *tramite*

pagina
119

Tor e la possibilità di utilizzare Tor con un software diverso da un browser web, il modo più semplice è rivolgersi a un sistema *live* come Tails.

pagina
113

38.1 Installare il browser Tor

Per installare il browser Tor in Debian :

- Aggiungere il deposito contributivo (vedere pagina 136).
- Installare il software *Tor Browser Launcher* (vedere pagina 134) cercando *torbrowser* nell'elenco dei software.
- Avviare *Tor Browser Launcher* premendo  ( su Mac), digitare *torb* e fare clic su *Tor Browser Launcher*.

Si apre una finestra di configurazione di *Tor Browser Launcher*. È possibile lasciare le opzioni predefinite e fare clic su *Installa Tor Browser*.

Al primo avvio, *Tor Browser Launcher* scarica il Tor Browser dal [sito ufficiale di Tor](https://www.torproject.org/fr/) [https://www.torproject.org/fr/] e controlla automaticamente la firma dell'archivio, estraendolo ed eseguendolo.

Al momento in cui scriviamo, il nome del browser non è stato tradotto e si chiama *Tor Browser* in inglese. Dopo l'installazione, sul computer appare un collegamento, per trovarlo afficher la panoramica delle attività premendo il tasto  (su Mac), quindi digitare *tor*.

Se Tor è bloccato (dal nostro ISP, per esempio), o se l'uso di Tor potrebbe sembrare sospetto a qualcuno che controlla la nostra connessione a Internet, possiamo configurare il Tor Browser in modo da usare i ponti Tor per nascondere il nostro uso di Tor.

La documentazione di Tor Browser può essere consultata facendo clic su 

* Guida → *Tor Browser User's Guide* e poi andare alla pagina *Bridges*.

38.2 Aggiornamento del browser Tor

Il Tor Browser scarica automaticamente gli aggiornamenti necessari e si offre di applicarli. Per farlo, fare clic sul menu , quindi su *Riavvia per aggiornare il Tor Browser*.

Navigare sul web con Tor

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Da cinque a dieci minuti.*

Lo scopo di questo strumento è quello di navigare sul web in modo riservato utilizzando il Tor Browser. Non c'è molta differenza rispetto all'uso di un browser web "classico", che considereremo un prerequisito.

pagina
261

Se non si utilizza il sistema Tails live (vedere pagina 113), è necessario installare il Tor Browser (vedere pagina 313).

Una volta avviato Tor Browser, è possibile utilizzarlo quasi come un normale browser web. Tuttavia, ci sono alcuni dettagli da notare.

Prima di tutto, è necessario capire da cosa protegge Tor, ma soprattutto da cosa non protegge, in modo da non fare qualsiasi cosa nella convinzione di essere protetti.

pagina
267



Nota bene: a meno che non si utilizzi Tails, solo la navigazione con Tor Browser beneficia della riservatezza fornita da Tor.

Oltre a queste limitazioni, dovete sapere che i siti web che visitate potrebbero sapere che vi state connettendo *tramite* la rete Tor. Alcuni, come Wikipedia, lo usano per bloccare le modifiche anonime. Altri, come Google, vi chiederanno di risolvere sfide chiamate "captcha" per dimostrare che siete effettivamente una persona. ¹ per dimostrare di essere una persona (e non un robot) prima di accedere ai loro servizi. Risolvere queste sfide significa produrre lavoro non retribuito, di solito per i GAFAM. ²...

Alcune funzioni sono disattivate per evitare di lasciare tracce, come la memorizzazione dei cookie sul disco o il salvataggio delle password.

39.1 Andare alla cartella di download di Tor Browser

Tutti i file scaricati dal Tor Browser vengono salvati in una cartella specifica, ben nascosta. ³ Il modo più semplice per trovare questa cartella di download è scaricare un documento dal Tor Browser e *aprire la cartella contenente il file*.

Ad esempio, in una pagina web con immagini, è possibile fare clic con il tasto destro del mouse per *salvare l'immagine come*

..... Una volta completato il download, viene visualizzato un nuovo simbolo 

1. Wikipedia, 2017, *CAPTCHA* [<https://fr.wikipedia.org/wiki/CAPTCHA>].

2. Xavier de La Porte, 2016, *Le "captcha" ou l'art de faire travailler sans rémunérer*, L'Obs [<https://www.nouvelobs.com/rue89/rue89-ce-qui-nous-arrive-sur-la-toile/20140217.RUE2129/le-captcha-ou-l-art-de-faire-travailler-sans-remunerer.html>].

3. Se il Tor Browser è installato dal Tor Browser Launcher e la lingua del programma è la stessa di Tor Browser. Se il sistema operativo è francese, la cartella di download si trova nella cartella personale:

.local/share/torbrowser/tbb/x86_64/tor-browser_fr/Browser/Téléchargements.

() appare accanto alla barra degli indirizzi. Questa freccia affianca l'elenco dei download e il simbolo  ci invita ad *aprire la cartella contenente il file*. Si apre una nuova finestra, che è la cartella dei download di Tor, e il percorso per raggiungerla è indicato nella barra dei menu. Ora possiamo spostare i file scaricati dove vogliamo.

Se si desidera accedere più facilmente a questa cartella, è possibile creare un collegamento alla cartella Tor *Downloads*:

- Nel browser Tor, dopo il download, a destra della barra degli indirizzi, fare clic su  ()
- Nel menu a discesa, fare clic sull'icona  per aprire la cartella contenente il file scaricato.
- Nella parte superiore della finestra che si apre, nella barra degli indirizzi, fare clic su *Download* .
- Dal menu a discesa, selezionare *Aggiungi ai segnalibri*.
- Il segnalibro appare nella colonna di sinistra.
- Fare clic con il tasto destro del mouse su di esso e selezionare *Rinomina....*
- Dategli un nome chiaro, come *Tor Browser Downloads*.

39.2 Limiti di geolocalizzazione

Quando si utilizza Tor, per il sito web che stiamo visitando, la nostra connessione sembra provenire dalla posizione del nodo di uscita utilizzato. Alcuni siti utilizzano l'indirizzo IP dei visitatori per scegliere la lingua di affichage. Questi siti possono quindi presentare affichage in lingue inaspettate.

Inoltre, alcune agenzie governative localizzano i loro utenti in base ai loro indirizzi IP, quindi l'uso di Tor può creare problemi quando si ha a che fare con le agenzie governative.⁴



PER SAPERNE DI PIÙ...

Sembra che le autorità francesi che monitorano gli indirizzi IP degli utenti controllino solo il Paese di origine della connessione e non (ancora?) gli indirizzi dei nodi di uscita di Tor.

È possibile configurare temporaneamente il Tor Browser in modo da utilizzare solo i nodi di uscita in Francia, che forniranno sempre un IP francese durante la navigazione.

Attenzione: l'uso di questa opzione riduce la riservatezza.

Per fare ciò, quando si utilizza un browser Tor installato con torbrowser-launcher :

1. Chiudere il browser Tor.
2. Dalla home directory, trovare il file di configurazione di Tor chiamato *torrc* :
 - Andare alla *cartella Personale*.
 - Premere   per affiggere i file nascosti.
 - Fare clic sul simbolo della lente di ingrandimento nella barra dei menu e digitare *torrc* nella barra di ricerca.⁵
3. Aprire questo file *torrc* con un editor di testo (clic destro → *Apri con editor di testo*),
4. Aggiungere una riga contenente `ExitNodes {FR}`, quindi salvare e chiudere il file.
5. Avviare Tor Browser, navigare su alcuni siti e fare clic ogni volta sul lucchetto nella barra degli indirizzi per verificare che l'ultimo nodo sia ancora in Francia.

4. Anonimo, 2019, *Resoconto di un'ispezione CAF* [<https://nantes.indymedia.org/posts/45908/>].

Una volta terminate le attività amministrative, non dimenticate di chiudere immediatamente il Browser Tor e di modificare nuovamente il file *torrc* per rimuovere la riga aggiunta.

Per fare questo in Tails :

1. All'avvio, impostare una *password di amministrazione*⁶ e poi avviare *Tails*.
2. Connettersi a Tor, poi aprire un terminale (*Applicazioni* → *Strumenti di sistema* → *Terminale*).
3. Digitare `sudo gedit /etc/tor/torrc` nel terminale, premere *Invio* (o ritorno), quindi inserire la password di amministrazione configurata all'avvio. Si apre il file di configurazione di Tor.
4. Aggiungere la riga `ExitNodes {FR}` a questo file, quindi salvare e uscire dall'editor. *teur*.
5. Nel terminale, digitare `sudo service tor reload` per riavviare Tor con la nuova configurazione. Reinserire la password di amministrazione impostata all'avvio.
6. Riavviare il browser Tor, navigare in alcuni siti e fare clic ogni volta sul lucchetto nella barra degli indirizzi per verificare che l'ultimo nodo sia ancora in Francia.

Una volta completate le attività amministrative, riavviare *Tails*.

5. Se il Tor Browser viene installato da Tor Browser Launcher e la lingua del sistema operativo è il francese, il percorso dovrebbe essere il seguente:

`.local/share/torbrowser/tbb/x86_64/tor-browser_it/Browser/TorBrowser/Data/Tor/torrc`.

6. https://tails.boum.org/doc/first_steps/welcome_screen/administration_password/index.fr.html

Scelta dell'hosting web

🔄 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: Da mezz'ora a un'ora.*

Lo scopo di questa sezione è scoprire dove ospitare un documento sul web. Ci sono troppe possibilità per fornire una risposta "chiavi in mano" a questa domanda. Inoltre, non mi sembra una buona idea consigliare un breve elenco di provider di hosting, in cui sarebbero centralizzati molti contenuti "a rischio". Invece, questa ricetta vi darà alcune indicazioni per aiutarvi a fare la scelta migliore del provider di hosting.

È anche possibile ospitare il nostro documento in modo anonimo utilizzando i servizi di Tor a cipolla. Per farlo, è necessario consultare la ricetta sull'uso di da

OnionShare.

pagina
242
pagina
266
pagina
359

40.1 Alcuni criteri di selezione

Ci sono così tanti possibili host che ci si può sentire rapidamente persi nella giungla delle possibilità. Ecco alcuni criteri che vi aiuteranno a porre le domande giuste. Parleremo di documenti più avanti, ma questi criteri si applicano anche a un progetto più ambizioso, come un blog o un documentario video.

- **Tipo di organizzazione:** molti siti si offrono di ospitare documenti "gratis". Molti di questi sono servizi commerciali che trovano redditizio pubblicare i contenuti creati dai loro utenti. Ma ci sono anche associazioni o collettivi che ospitano progetti, a determinate condizioni.
- **Condizioni di hosting:** se il documento non piace all'host, nulla impedisce che lo cancelli senza nemmeno avvertirci. Lo statuto dell'host (che dobbiamo accettare quando ospitiamo il nostro documento) può spesso darci un'idea di ciò che l'host tollera o meno.
- **Requisiti di identificazione:** la misura in cui l'host ci richiede di fornire dettagli e garanzie sui nostri dati personali per poter utilizzare i suoi servizi.
- **Resistere alle pressioni:** lo Stato può anche voler impedire che il nostro documento rimanga online. In molti casi, sarà sufficiente intimidire l'host affinché cancelli il nostro documento. In effetti, a seconda dell'host scelto, può essere in grado di sopportare più o meno pressioni: alcuni aspetteranno che venga intrapresa un'azione legale, mentre altri cancelleranno il nostro documento non appena verrà inviata la prima e-mail leggermente minacciosa.
- **Cancellazione del documento:** al contrario, potreste voler cancellare il vostro documento a un certo punto. Tuttavia, poiché l'hosting dei documenti è un servizio affidato ad altre persone, di cui ci si può fidare o meno, noi non

pagina
240

non può garantire che i nostri file vengano effettivamente eliminati su nostra richiesta. In alcuni casi, conoscere meglio l'host può darci maggiori garanzie.

- **Rischi per l'host:** a seconda del contenuto del nostro documento, potrebbe mettere a rischio l'host, soprattutto se quest'ultimo non vuole collaborare con la polizia. In questi casi, è necessario chiedersi se si è disposti a mettere a rischio un host, che potrebbe scomparire in caso di arrivo della polizia.
- **Dimensioni del documento:** se il nostro documento è "troppo grande", alcuni host si rifiutano di accettarlo. Questo può accadere anche se il nostro documento è "troppo piccolo". Le dimensioni consentite sono specificate in alcune offerte, ma attenzione: alcuni host fanno pagare per funzioni come l'hosting di file molto grandi.
- **Durata dell'hosting:** a seconda del provider di hosting, ci sono molte offerte diverse per quanto riguarda la durata dell'hosting. Ad esempio, alcuni cancellano automaticamente il documento dopo un determinato periodo di tempo, altri se non viene scaricato per un certo periodo di tempo, e così via.
- **Condizioni di identificazione per la consultazione:** per ridurre al minimo la possibilità che l'host o i poliziotti siano in grado di identificare le persone che vengono a consultare il nostro documento, è importante non utilizzare un host sul quale potrebbero già essere identificate. Ad esempio, vanno evitati i social network e piattaforme simili (Facebook, Twitter, YouTube, ecc.).
- **Utilizzo tramite Tor:** per le stesse ragioni, è meglio assicurarsi che il documento possa essere depositato e/o consultato tramite il browser Tor, o anche tramite un servizio onion.
- **Conservazione dei log di connessione:** sia per l'invio che per la visualizzazione del documento, possono lasciare tracce compromettenti nei registri di connessione dell'host. La scelta di un host che non conserva questi registri o li cancella regolarmente riduce questo rischio.
- **Riservatezza del documento:** a seconda delle nostre esigenze, potremmo volere che il provider di hosting offra un sistema di crittografia in modo che il contenuto del documento non possa essere letto sul server, o al contrario, potremmo non preoccuparci, dato che il documento sarà pubblicamente accessibile.

40.2 Tipo di contenuto

Ora che abbiamo in mente alcuni criteri di selezione, cerchiamo di renderli più concreti. L'hosting giusto per il nostro progetto dipende dal tipo di contenuto che vogliamo pubblicare: testo, immagini, video, audio, ecc.

40.2.1 Pubblicare il testo

Pubblicare un testo è spesso la cosa più semplice da fare.

Se il testo da pubblicare è correlato a un altro testo già pubblicato, è spesso possibile inviare un commento, sia su un blog, un forum o un sito partecipativo. Per questo tipo di pubblicazione non è necessariamente richiesta la registrazione. Ciò non significa, tuttavia, che la pubblicazione sia anonima, a meno che non si prendano particolari precauzioni, come l'utilizzo del routing a cipolla. Inoltre, poiché il nostro testo è un commento e non un argomento principale, non viene necessariamente messo in evidenza sul sito.

È anche possibile pubblicare un testo su un sito o un blog esistente. In questo caso, dovrete inviarlo al sito in questione *tramite* un modulo o un'e-mail e la pubblicazione dipenderà dagli amministratori. Alcuni siti ¹ offrono la pubblicazione gratuita di articoli su un determinato tema.

1. Ad esempio, i siti della rete **Indymedia** [<https://fr.wikipedia.org/wiki/Indymedia>] e quelli della rete **Mutu** [<https://reseau.mutu.info>].

40.2.2 Avere un blog o un altro sito

Se volete pubblicare regolarmente dei testi, potete anche scegliere di amministrare un blog: molte organizzazioni offrono blog già configurati e facili da usare. Potreste anche gestire un sito web, ma questo richiede un po' di formazione.

In molte città, i gruppi di persone interessate al software libero o alla libertà di espressione su Internet possono essere una buona fonte di consigli. Alcuni elenchi sono disponibili anche sul web:

- un elenco di grandi piattaforme di blog su Wikipedia [https://fr.wikipedia.org/wiki/Cat%C3%A9gorie:H%C3%A9bergeur_de_blogs];
- un elenco di servizi web gratuiti sul wiki della comunità Ubuntu di lingua francese [https://doc.ubuntu-fr.org/liste_de_services_web_libres];
- c'è anche l'host noblogs.org [<https://noblogs.org/>].

40.2.3 Pubblicare file audiovisivi

Esistono diverse soluzioni per pubblicare immagini, video o suoni a corredo del testo di un articolo, ad esempio. In primo luogo, la maggior parte dei siti in cui è possibile pubblicare testi offre la possibilità di includere documenti audiovisivi. Questi siti offrono la possibilità di prelevare i file dal nostro computer (che saranno poi ospitati sul loro server), oppure di indicare l'indirizzo di file già ospitati su un altro server.

Esistono anche siti dedicati alla condivisione di file audiovisivi. Ecco alcuni esempi:

- L'*Internet Archive*, senza scopo di lucro, si propone di essere una [biblioteca digitale gratuita](https://archive.org/) [<https://archive.org/>].
- Il collettivo CHATONS ² gestisce un [elenco di numerosi strumenti e servizi gratuiti](https://entraide.chatons.org/) [<https://entraide.chatons.org/>], tra cui servizi di [video-salvataggio](https://www.chatons.org/search/by-service?service_type_target_id=152) [https://www.chatons.org/search/by-service?service_type_target_id=152] e [foto album hosting servizi](https://www.chatons.org/search/by-service?service_type_target_id=150) [https://www.chatons.org/search/by-service?service_type_target_id=150]. Alcuni servizi consentono anche di memorizzare i file in modo criptato sui loro server (nel caso dell'hosting di immagini, tuttavia, a seconda del server, ciò non è sempre automatico: potrebbe essere necessario richiedere esplicitamente la crittografia del file al momento dell'invio).
- Infine, è possibile utilizzare gli strumenti menzionati nella sezione successiva sulla condivisione dei file.

40.2.4 Condividere un file scaricabile

Per pubblicare i documenti che volete rendere scaricabili, non cercate altro che i servizi Direct Download *Link* (DDL).

In francese, questo significa "link di download diretto": "carichiamo" il nostro file su un server di download diretto e poi otteniamo un link (un indirizzo web) che, digitato in un browser web, avvia il download del file.

Esistono anche siti di file-sharing e di file-hosting. Ecco alcuni esempi:

- Il progetto Riseup, un collettivo che fornisce strumenti di comunicazione sicuri, offre anche uno strumento [leggero di condivisione dei file](https://share.riseup.net/) [<https://share.riseup.net/>].

2. [CHATONS](https://chatons.org/) [<https://chatons.org/>], per Collectif d'Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires, è un'iniziativa nata nel 2016. L'obiettivo di questo collettivo è quello di riunire le organizzazioni che desiderano offrire servizi che rispettino la privacy di che li utilizzano.

- Alcuni CHATONI ³ forniscono a [condivisione di file](https://www.chatons.org/search/by-service?service_type_target_id=148) [https://www.chatons.org/search/by-service?service_type_target_id=148].

Alcuni servizi, come quelli basati sul software *Lufi*, consentono di memorizzare i file crittografati sui loro servizi.

40.3 In pratica

Più concretamente, la prima cosa da fare è scegliere un file host. I criteri descritti sopra vi aiuteranno a fare questa scelta. È molto importante fare una scelta ben informata dell'host, poiché il nostro anonimato può dipendere in parte da questa scelta.

[pagina] È anche possibile criptare il file da ospitare. Esistono due modi per farlo: o criptare il
[305] file prima di ospitarlo online; o scegliere una società di hosting che cripta il
[pagina] file nel nostro browser web prima di memorizzarlo sui suoi server, come ad
347 esempio CHATONS.

Per ospitare il nostro file, il metodo esatto varia da host a host, ma il principio rimane lo stesso. Innanzitutto, apriamo il nostro browser web e lo usiamo con discrezione. Poi andiamo sul sito dell'host e troviamo la pagina in cui possiamo "caricare" il nostro file. A questo punto, dovreste seguire il metodo specifico dell'host per trasmettere il vostro file. In generale, questo metodo è facile da seguire e, sebbene vari, rimane relativamente simile da un host all'altro. Una volta completato il *caricamento*, viene visualizzato l'indirizzo web in cui è possibile trovare il file.

[pagina] A volte è necessario inserire un indirizzo e-mail per ricevere questo indirizzo web:
il caso d'uso sugli scambi di e-mail e il capitolo sulle identità contestuali ci
[293] permetteranno di decidere quale indirizzo e-mail fornire in questo caso.

[pagina] Una volta ottenuto il link, potete distribuirlo come meglio credete. Chi ha il link
243 può scaricare il file digitandolo nella barra degli indirizzi di un browser web.

3. CHATONS [https://chatons.org/], per Collectif d'Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires, è un'iniziativa nata nel 2016. L'obiettivo di questo collettivo è quello di riunire le organizzazioni che desiderano offrire servizi che rispettino la privacy di che li utilizzano.

Verifica di un certificato elettronico

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Da quindici a trenta minuti.*

Abbiamo già visto che, per stabilire una connessione crittografata, è spesso necessario fidarsi di un' autorità di certificazione (CA). Nella maggior parte dei casi, le CA sono già registrate sul computer, ad esempio nel browser web. Ma non è sempre così: il nostro browser web o altro software ci presenterà un messaggio che spiega che non è stato in grado di autenticare il certificato del servizio.

Può anche accadere che il servizio visitato, per mancanza di fiducia, non utilizzi un' autorità di certificazione. In questo caso, dobbiamo verificare noi stessi il certificato.

pagina
255

41.1 Verificare un certificato o un' autorità di certificazione

Per visualizzare il certificato di un sito web, in un browser web, fate clic sul lucchetto  nella barra degli indirizzi, poi su *Connessione sicura* e infine su *Più informazioni*. Si apre una nuova finestra in cui vengono visualizzate numerose informazioni sulla pagina web.

Facendo clic sul pulsante *Afficher le certificat*, è possibile esaminare più da vicino il certificato e scoprire, ad esempio, chi lo ha rilasciato, per quanto tempo *e così via*. In questa finestra sono solitamente presenti diverse schede, ognuna delle quali corrisponde a un certificato. La prima scheda corrisponde al certificato del sito stesso; le schede successive corrispondono alle autorità di certificazione che autenticano il certificato del sito (mediante una firma digitale).

Siamo particolarmente interessati al certificato presentato dal sito al nostro browser web. La sua impronta digitale SHA-256 si trova nella sezione *Impronte digitali* della prima scheda.

pagina
252

Per il certificato <https://guide.boum.org/> utilizzato il 13 dicembre 2021 ¹ad esempio, si otterrà la seguente stringa di caratteri :

```
72:7 E:9E: A3 :1E:2E: B9: E1 :5B: D5 :88:93:01:38:7 A:70:
8B: C6 :81: E2: F3: D0 :5F: CC:63:40:51: CF:22: EC:28:41
```

1. Questo certificato è disponibile sul sito <https://crt.sh/?id=5796332967>.

A volte il browser visualizza un avviso di sicurezza.



Attention : risque probable de sécurité

Le Navigateur Tor a détecté une menace de sécurité potentielle et n'a pas poursuivi vers `untrusted-root.badssl.com`. Si vous accédez à ce site, des attaquants pourraient dérober des informations comme vos mots de passe, courriels, ou données de carte bancaire.

Que pouvez-vous faire ?

Le problème vient probablement du site web, donc vous ne pouvez pas y remédier.

Si vous naviguez sur un réseau d'entreprise ou si vous utilisez un antivirus, vous pouvez contacter les équipes d'assistance pour obtenir de l'aide. Vous pouvez également signaler le problème aux personnes qui administrent le site web.

[En savoir plus...](#)

Retour (recommandé)

Avancé...

pagina

254

La nozione di "informazioni rubate" menzionata nel messaggio precedente si riferisce all'attacco del mostro nel mezzo. Una volta letto questo avviso, è possibile fare clic su *Avanzate...*, che rivelerà il motivo per cui il browser web non ha voluto accettare il certificato, come nella seguente schermata.



Attention : risque probable de sécurité

Le Navigateur Tor a détecté une menace de sécurité potentielle et n'a pas poursuivi vers `untrusted-root.badssl.com`. Si vous accédez à ce site, des attaquants pourraient dérober des informations comme vos mots de passe, courriels, ou données de carte bancaire.

Que pouvez-vous faire ?

Le problème vient probablement du site web, donc vous ne pouvez pas y remédier.

Si vous naviguez sur un réseau d'entreprise ou si vous utilisez un antivirus, vous pouvez contacter les équipes d'assistance pour obtenir de l'aide. Vous pouvez également signaler le problème aux personnes qui administrent le site web.

[En savoir plus...](#)

Retour (recommandé)

Avancé...

Quelqu'un pourrait être en train d'essayer d'usurper l'identité du site. Vous ne devriez pas poursuivre.

Les sites web justifient leur identité par des certificats. Le Navigateur Tor ne fait pas confiance à `untrusted-root.badssl.com`, car l'émetteur de son certificat est inconnu, le certificat est auto-signé ou le serveur n'envoie pas les certificats intermédiaires corrects.

Code d'erreur : `SEC_ERROR_UNKNOWN_ISSUER`

[Afficher le certificat](#)

Retour (recommandé)

Accepter le risque et poursuivre

Nel caso di un certificato autofirmato, ad esempio, si può leggere *Il certificato non è sicuro perché autofirmato*. È anche possibile che la data di validità del certificato sia passata, il che non ne impedisce necessariamente l'uso. In ogni caso, è sempre bene leggere questa sezione e chiedersi se si vuole continuare alla luce di queste informazioni. È quindi necessario verificare i certificati del sito e quelli di eventuali autorità di certificazione. In caso contrario, la connessione sarà crittografata, ma non *autenticata*. In altre parole, la comunicazione sarà criptata, ma non si saprà con chi si sta comunicando, il che è tutt'altro che ideale.

La verifica di un certificato consiste di solito nel visualizzare la sua impronta digitale e nel confrontare con un'altra fonte per assicurarsi che sia corretto. Noi

pagina

254

53

pagina

preferiamo utilizzare l'impronta digitale SHA-256, piuttosto che MD5oSHA-1² o SHA-1³ che non sono più considerati sicuri.

Resta da trovare altre fonti per ottenere questa impronta digitale. Esistono diverse tecniche per verificare l'autenticità di un certificato:

- Se una persona fidata nelle nostre vicinanze utilizza già il sito o la CA in questione e ne ha già verificato il certificato, possiamo confrontare l'impronta digitale del certificato che conosce con quella che ci viene presentata. Possiamo anche richiederlo via e-mail a persone che ce lo invieranno crittografato e firmato per una maggiore sicurezza. È ancora meglio se si è in contatto con diverse di queste persone, che avranno verificato il certificato utilizzando diverse connessioni Internet. In questo caso, è necessario seguire la procedura spiegata di seguito per trovare l'impronta digitale di un certificato già installato nei browser web di queste persone.
- Se abbiamo accesso a diverse connessioni Internet dalla nostra posizione, Ad esempio, in un'area urbana con molti accessi Wi-Fi, è possibile visitare il sito Web o scaricare il certificato della CA utilizzando diverse connessioni e confrontare l'impronta digitale del certificato presentata ogni volta.
- Se si utilizza il Tor Browser, si può approfittare del cambio di circuito, e quindi di nodo di uscita su Internet, per verificare più volte l'impronta digitale del certificato. In questo modo si eviterà che un malintenzionato che abbia le mani sul nodo di uscita, o che si trovi tra il nodo di uscita e il sito consultato, possa usurparne l'identità.

Per conoscere l'indirizzo IP del nodo di uscita utilizzato per accedere a un sito nel Browser Tor, fare clic sul lucchetto a sinistra della barra degli indirizzi, subito prima dell'indirizzo del sito. Appare quindi un inserto *Informazioni sul sito [...]*, che riporta, tra le altre cose, il *circuito Tor* utilizzato per questo sito. Il nodo di uscita è il penultimo nodo dell'elenco, subito prima del nodo corrispondente al sito visitato. La sua geolocalizzazione (paese) e l'indirizzo IP sono indicati. (Nota bene: non esiste un nodo di uscita quando si consulta un servizio onion, cioè un sito il cui nome di dominio è *.onion*).

Nello stesso inserto, è possibile cambiare il circuito Tor utilizzato per accedere a questo sito facendo clic sul pulsante *Nuovo circuito per questo sito*, situato appena sotto la rappresentazione del circuito corrente. È quindi possibile assicurarsi che l'IP del nodo di uscita cambi ogni volta che il circuito viene rinnovato.

Ogni volta che il nodo di uscita cambia, possiamo ricaricare il sito visitato o il certificato CA e confrontare le sue impronte digitali con quelle raccolte le volte precedenti. Dopo alcuni tentativi andati a buon fine, la probabilità che si tratti della

certificato giusto diventa sufficiente per accettarlo. Infine, è compito di noi essere giudicati sulla base della nostra politica di sicurezza!

Usate isolatamente, queste tecniche non sono necessariamente molto robuste, ma il loro uso combinato fornirà sufficiente credibilità al fatto che il certificato che stiamo per usare è quello giusto. E che nessuno è riuscito a ingannarci.

Si tenga presente, tuttavia, che questo non protegge da tutti gli attacchi alla crittografia delle connessioni.

Una volta accertato con sufficiente sicurezza che il certificato presentato corrisponde al sito che si desidera visitare, è possibile fare clic sul pulsante *Accetta il rischio e proseguire fino alla* pagina di avviso. Il certificato verrà quindi accettato dal browser web e il sito verrà visualizzato.

2. Chad R Dougherty, 2008, *MD5 vulnerabile agli attacchi di collisione* [<https://www.kb.cert.org/vuls/id/836068>] (in inglese).

3. Julien Cadot, 2017, *SHattered: Google ha rotto la funzione hash SHA-1* [<https://web.archive.org/web/20211122073218/https://www.numerama.com/tech/235436-shattered-google-aca-sse-la-metodo-de-chiffrement-sha-1.html>].

41.1.1 Il caso speciale dei servizi a cipolla

Attualmente è molto difficile ottenere certificati validi per i servizi onion (siti il cui nome di dominio termina con *.onion*), quindi si riceverà sempre un messaggio di avvertimento dal Tor Browser quando ci si vuole connettere a un sito di questo tipo in *https*.

Nella maggior parte dei casi, il certificato utilizzato dal servizio onion è autofirmato: ciò significa che il sito stesso ha firmato il proprio certificato. È quindi possibile verificare la validità del certificato con altri mezzi, come descritto nella sezione precedente.

[pagina]

323

Nel caso di servizi a cipolla che sono accessibili anche con un nome di dominio

Nella versione "classica", il certificato presentato è generalmente un certificato valido per questo nome di dominio, ma non per il nome *.onion*. È quindi sufficiente verificare che il nome di dominio per cui il certificato è valido corrisponda effettivamente al sito a cui ci si vuole collegare.

In ogni caso, la riservatezza e l'autenticità della connessione a un servizio onion sono garantite dal protocollo di routing onion e dal sistema di "rendezvous point": se si è certi che l'indirizzo *.onion* a cui ci si connette è corretto, allora si può essere convinti con un grado di sicurezza abbastanza elevato che si sta accedendo al servizio onion corrispondente.

[pagina]

261

[pagina]

266

41.2 Trovare l'impronta digitale di un certificato installato

Questa impronta digitale può essere visualizzata facendo clic su  nel nostro browser per aprire il menu di Firefox o Tor Browser e quindi andare su *Impostazioni*. Scegliere la pagina *Privacy e sicurezza*, quindi scorrere fino alla sezione *Certificati*. Qui, fare clic su *Afficher les certificats*. I certificati per i siti già installati possono essere trovati selezionando

la scheda *Server* nella finestra che si apre. Infine, selezionando il sito desiderato dall'elenco e facendo clic sul pulsante *Visualizza...*, è possibile visualizzare l'impronta digitale del certificato. La stessa operazione può essere eseguita per le autorità di certificazione selezionando la scheda *Autorità*.

Utilizzare una tastiera visiva in Tails

🔄 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.*

🕒 *Durata: pochi minuti.*

Nel primo volume abbiamo visto che un computer può essere compromesso nell'hardware...

in particolare, può contenere keylogger hardware in grado di registrare tutto ciò che viene digitato sulla tastiera. In particolare, può contenere keylogger hardware in grado di registrare tutto ciò che viene digitato sulla tastiera. I testi che scrivete, le azioni che eseguite, ma soprattutto le password che inserite.

In caso di dubbio se fidarsi o meno di un computer su cui si intende utilizzare Tails, è possibile utilizzare una tastiera visiva (precedentemente nota come "tastiera virtuale") per rendere inefficiente il recupero dei tasti dalla tastiera. Attenzione

Tuttavia, questo metodo non protegge da un errore nella registrazione della pagina 31 dello schermo.

Una tastiera visiva è un software che ha l'aspetto di una tastiera e consente di inserire i caratteri senza utilizzare la tastiera hardware del computer. Può essere utilizzata con diversi dispositivi di puntamento, come mouse, touch screen o touchpad.

L'ambiente desktop GNOME fornito da Tails consente di utilizzare una tastiera visiva tra le varie opzioni di accessibilità disponibili. Per farlo, fare clic sull'icona *Accesso universale* nella barra superiore, quindi attivare l'opzione *Tastiera visiva*. In alternativa, premere (**⌘**) su Mac), digitare **param**, quindi fare clic su *Impostazioni*: si può quindi attivare l'opzione *Tastiera visiva* nella sezione *Input* della pagina *Accessibilità*.

Una volta attivata, la tastiera visiva compare non appena si ha la possibilità di inserire del testo. È quindi sufficiente digitare le password utilizzando il mouse, il touchpad o un altro dispositivo di puntamento.

Va notato che questa tastiera visiva può essere attivata dalla schermata di benvenuto di Tails, quindi può essere utilizzata anche per inserire la passphrase per sbloccare il volume persistente.

Configurazione e utilizzo del client di posta Thunderbird

🔄 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: Da quindici a trenta minuti.*

Questa sezione descrive come configurare e utilizzare il client di posta elettronica Thunderbird per tutte le attività relative alla posta elettronica. È stata testata con la versione 91 di Thunderbird. L'interfaccia potrebbe essere leggermente diversa con versioni più recenti.

In Debian, se Thunderbird non è ancora installato, è necessario installare il pacchetto `thunderbird-l10n-it`¹ seguendo la ricetta per l'installazione del software.

pagina
135

43.1 Avviare Thunderbird

Avviare Thunderbird premendo  ( su Mac), digitare `thu` e cliccare su *Thunderbird Messaging*.

Quando si avvia Thunderbird e non è stato impostato alcun account di posta elettronica, appare una scheda di configurazione intitolata *Configura l'indirizzo di posta elettronica esistente* per aiutare ad aggiungere il primo account a un indirizzo di posta elettronica esistente.

Tuttavia, in genere è meglio prendersi un po' di tempo per impostare alcune opzioni di privacy di Thunderbird prima di configurare questo primo account di posta elettronica: si può quindi chiudere questa scheda facendo clic su *Annulla*, in modo da poter eseguire le operazioni descritte di seguito. Se invece si desidera configurare subito un account di posta elettronica, si può passare direttamente alla sezione corrispondente.

prossimo
pagina.

43.2 Configurazione del routing a cipolla per Thunderbird

Se si utilizza Tails, Thunderbird è già configurato per funzionare con Tor. Potete passare direttamente al passo successivo

Se si utilizza Thunderbird su un sistema Debian e si vuole che utilizzi la rete Tor per connettersi al server di posta, è necessario configurarlo di conseguenza.

Per prima cosa, installare il Browser Tor, se non è già installato. Poi :

- aprire la scheda *Preferenze* accedendo a  per accedere al menu di Thunderbird.

1. Il protocollo OpenPGP, utilizzato per la crittografia delle e-mail [pagina 295], è stato integrato e attivato per impostazione predefinita dalla versione 78.2.1 di Thunderbird. Non è quindi più necessario installare il componente aggiuntivo Enigmail, che era richiesto nelle versioni precedenti.

pagina
successiva
pagina
pagina 261
pagina 313

- Assicuratevi di essere nella sezione *Generale* nella colonna di sinistra.
- Scorrere fino alla sezione *Connessione*.
- Cliccate su *Impostazioni...* in *Configura come Thunderbird si connette a Internet*.
- Controllare la *configurazione del proxy manuale*.
- Compilare il campo *Host SOCKS* con **127.0.0.1** e *Porta* con **9150**.
- Controllare *SOCKS v5*.
- Selezionare *Usa DNS remoto quando SOCKS v5 è attivo*.
- Fare clic sul pulsante *OK*.
- Chiudere la scheda delle preferenze facendo clic sul pulsante corrispondente✕.

D'ora in poi, con questa nuova configurazione, per poter inviare e ricevere e-mail, si dovrà sempre aprire Tor Browser e connettersi a Tor. Se, per qualche motivo, Tor Browser non funziona, non funzionerà nemmeno l'invio e la ricezione di e-mail.

43.3 Impostare una password principale in Thunderbird

Per impostazione predefinita, Thunderbird propone di ricordare le password per l'accesso agli account di posta elettronica configurati. Inoltre, se si desidera utilizzare le funzioni di crittografia OpenPGP o di firma digitale descritte nel prossimo capitolo, Thunderbird dovrà memorizzare la *chiave privata* nella sua configurazione.

Per limitare l'accesso alle password e alle chiavi private memorizzate da Thunderbird, occorre innanzitutto definire una *password principale*. Questa passphrase verrà richiesta ogni volta che Thunderbird viene aperto.

Per farlo, in Thunderbird, cliccate su☰ per aprire il menu, quindi su *Preferenze*. Nell'elenco a sinistra, scegliete *Privacy e sicurezza* e scorrete fino alla voce *Password*. Selezionate la casella *Usa password principale*. Si apre una nuova finestra che chiede una password per proteggere la chiave. Scegliere una buona passphrase, digitarla due volte e fare clic su *OK*. Viene visualizzato un messaggio di conferma della modifica della password principale. Confermare con *OK*, quindi chiudere la scheda delle preferenze facendo clic sul pulsante corrispondente✕.

43.4 Impostazione di un account e-mail

Per aggiungere un nuovo account di posta elettronica esistente a Thunderbird, fare clic su☰ per accedere al menu di Thunderbird e andare su➕ *Nuovo* → *Account di posta esistente*.
scheda *Configura l'indirizzo e-mail esistente*.

È quindi necessario compilare i primi due campi: *Nome e cognome* e *Indirizzo e-mail*. Il nome che inseriamo nel campo *Nome completo* apparirà nelle e-mail che inviamo e sarà quindi leggibile dai nostri corrispondenti e dagli intermediari che inoltrano i nostri messaggi. Vi suggeriamo pertanto di compilare questo campo con lo pseudonimo che desiderate far comparire nelle intestazioni delle vostre e-mail.

Tuttavia, non è necessario compilare il campo *Password*, a meno che non si voglia che Thunderbird ricordi la password per connettersi a questo account di posta elettronica (in tal caso si consiglia vivamente di impostare prima una *password principale* come descritto sopra).

Una volta inseriti i dati, fare clic su *Continua*.

Se la *configurazione viene trovata nell'affiche del provider di posta*, la configurazione automatica ha funzionato. Se Thunderbird non riesce a trovare la configurazione automatica, è possibile consultare la documentazione ufficiale del nostro host di posta per verificare le impostazioni specifiche per IMAP, POP e SMTP. Se

Questa informazione non si trova sul sito web dell'host di posta, ma è possibile trovare il contatto di posta degli amministratori e chiederlo a loro.

La procedura guidata offre quindi la possibilità di scegliere tra due protocolli, IMAP o POP. Selezionate quello più adatto a voi e fate clic su *Fine*, quindi chiudete la scheda di configurazione dell'account facendo clic sul pulsante corrispondente **X**.

pagina
292

Thunderbird è ora pronto a ricevere i messaggi. Potete ripetere la procedura se desiderate aggiungere altri account di posta elettronica. Altrimenti, potete passare alla sezione successiva, dedicata alla configurazione avanzata di Thunderbird.

43.5 Configurazione avanzata di Thunderbird

Una volta che Thunderbird è stato configurato per un account di posta elettronica, è possibile ottimizzare la sua configurazione per renderlo più facile da usare o per ridurre i rischi per la sicurezza informatica.

Per farlo, fare clic su  per aprire il menu di Thunderbird, quindi scegliere *Impostazioni account*. Non faremo un tour esaustivo delle opzioni di configurazione, ma solo di quelle che ci sembrano utili.

43.5.1 Tempo di conservazione del messaggio

Innanzitutto, se avete scelto di utilizzare il protocollo POP, nella sezione *Impostazioni del server* potete impostare il tempo dopo il quale i messaggi saranno cancellati dai server dopo il rimpatrio. Questo, naturalmente, non offre grandi garanzie e dipende in particolare da...

possiamo solo sperare che cancelli davvero la pagina 42 dei nostri dati.

43.5.2 Porte utilizzate

Infine, se si verificano problemi nell'invio o nella ricezione di e-mail, è possibile che le porte di protocollo utilizzate non siano quelle corrette con le impostazioni predefinite. In questo caso, è necessario apportare modifiche in base alle informazioni di configurazione disponibili presso l'host di posta elettronica.

Per accedere a queste impostazioni, fare clic sull'indirizzo e-mail nella colonna di sinistra, quindi su *Impostazioni account* nell'angolo in alto a destra. Si apre una nuova scheda in cui è possibile modificare la porta SMTP nella sezione *Server in uscita (SMTP)* in basso. Cliccate quindi su *Modifica server SMTP...* e infine cambiate il numero di *porta* con quello fornito dal nostro host. Per modificare il server in entrata, tornare alla colonna di sinistra, selezionare *Impostazioni server* e modificare la *Porta* corrispondente *al tipo di server* scelto in precedenza (IMAP o POP3).

43.5.3 Utilizzo di un servizio di cipolle

Se l'host di posta ha impostato i servizi onion, è possibile configurare Thunderbird per utilizzare gli indirizzi onion corrispondenti.

pagina
266

Per trovarli, è necessario cercare le informazioni pubblicate dal nostro host di posta: gli indirizzi onion e le relative porte per i servizi SMTP, IMAP e/o POP. Queste informazioni non sono sempre facilmente reperibili. È possibile effettuare una ricerca su Internet utilizzando le seguenti parole chiave: "*configurazione servizio smtp onion [e il nome dell'host di posta]*". Se non riuscite a trovare quello che cercate, potete anche chiedere direttamente alle persone che amministrano il servizio di hosting di posta.

Una volta trovati gli indirizzi delle cipolle :

- configurare il routing a cipolla in Thunderbird come descritto sopra.

pagina
329

- Per il server POP o IMAP: nella colonna di sinistra sotto l'account e-mail in questione, andare alla sezione *Impostazioni del server*, quindi sostituire l'indirizzo indicato in *Nome del server* con l'indirizzo del servizio POP o IMAP della cipolla.
- Per modificare l'indirizzo del server SMTP, accedere alla sezione *Server in uscita (SMTP)* all'estremità della colonna di sinistra, selezionare l'account di posta elettronica interessato, fare clic su *Modifica...* e infine sostituire l'indirizzo del server SMTP in *Nome server* con l'indirizzo del servizio SMTP della cipolla.

Utilizzare la crittografia OpenPGP in Thunderbird

Lo standard Internet ¹ OpenPGP è un formato crittografico che consente di creare e verificare firme digitali e di crittografare e decrittografare messaggi e file.

Questo capitolo descrive come utilizzare OpenPGP in Thunderbird per gestire le chiavi e crittografare o firmare i messaggi. Tuttavia, alcuni usi di OpenPGP che non sono possibili in Thunderbird sono trattati nel capitolo successivo.

pagina

343

44.1 Creare una coppia di chiavi

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Da 15 minuti a un'ora.*

Questo strumento illustra la creazione e parte della gestione di una coppia di chiavi di crittografia. Vale la pena di ricordare alcune nozioni di base da tenere sempre presenti:

pagina

249

- Non tutte le chiavi di crittografia utilizzano lo stesso algoritmo. Abbiamo parlato della crittografia RSA, ma ne esistono diverse altre.
- L'algoritmo non definisce rigorosamente la dimensione della chiave, che può essere variata per giocare con i livelli di sicurezza.
- Alcune chiavi hanno una data di scadenza, altre no.

pagina

251

44.1.1 Generare una coppia di chiavi

Prima di tutto, prima di generare una coppia di chiavi OpenPGP, è necessario aver definito una *password principale*, come descritto nel capitolo precedente. Questa passphrase viene richiesta ogni volta che si apre Thunderbird. Viene utilizzata per limitare l'accesso non solo alle password registrate, ma anche alla chiave privata che si sta per creare.

pagina

330

Per creare la nostra nuova coppia di chiavi, in Thunderbird, cliccate su  → *Strumenti*

→ *Gestore di chiavi OpenPGP*. Scegliere *Generazione* → *Nuova coppia di chiavi*. Si apre la finestra *Aggiungi una chiave OpenPGP personale per [...]*. Controllare che l'*identità* selezionata corrisponda all'*identità contestuale* utilizzata e all'indirizzo e-mail ad essa associato.

pagina

243

È consigliabile scegliere una data *di scadenza della chiave*. Se è la prima volta che si crea una coppia di chiavi, scegliete una data di scadenza compresa tra un anno e

1. Wikipedia, 2014, *Internet Standard* [https://fr.wikipedia.org/wiki/Standard_Internet].

due anni, ad esempio. Per non dimenticare di rinnovare la chiave in tempo, è bene annotare la data di scadenza da qualche parte.

Nelle *impostazioni avanzate*, il *tipo di chiave* predefinito è *RSA*. È consigliabile selezionare *ECC (curva ellittica)*, poiché gli algoritmi crittografici corrispondenti offrono una sicurezza equivalente alle chiavi di tipo *RSA*, pur essendo più efficienti. È comunque possibile utilizzare una chiave *RSA*.

Se si sceglie *RSA* come *tipo di chiave*, la *dimensione* predefinita di 3072 bit è considerata sicura fino a oltre il 2030.² ma se si desidera proteggere le proprie comunicazioni in modo più efficace o più a lungo, si consiglia di scegliere la dimensione della chiave più alta disponibile, cioè 4096 bit. Nel caso delle chiavi *ECC*, invece, non è attualmente possibile scegliere la dimensione della chiave.

Una volta selezionati i parametri della chiave, fare clic su *Generate key* e poi su *Confermare*.

L'operazione può essere quasi istantanea o richiedere diversi minuti. Questo è il momento di muovere il mouse, usare la tastiera o anche il disco rigido, se possibile, per aiutare il computer a generare dati casuali. Questi sono necessari per il processo di generazione della chiave.³

Una volta completata questa operazione, la nostra chiave apparirà in grassetto nell'*OpenPGP Key Manager*. Può capitare che la chiave non sia visibile. In questo caso, spostatevi in alto o in basso nell'elenco delle chiavi.

44.1.2 Salvare la chiave privata

Una volta completata la fase di creazione della chiave, è il momento di pensare a come salvare la nostra coppia di chiavi, e in particolare la nostra chiave privata: essendo segreta, non dobbiamo lasciarla in giro. La chiave privata deve essere accessibile solo alla persona che deve accedervi. Il modo migliore per farlo è conservare la coppia di chiavi su un volume crittografato, che sia una chiavetta USB, un disco rigido interno o esterno, o l'*assistenza Tails*.

Se si sta salvando con la persistenza *Tails*, è una buona idea avere un backup del sistema attivo:

* Dal *Gestore chiavi OpenPGP*, selezionare la chiave e scegliere *File* → *Salva una o più chiavi segrete in un file*.

* Scegliere dove collocare il file e il suo nome, quindi fare clic su *Salva*.

* Scegliete quindi una passphrase per proteggere il backup della chiave segreta. Può essere la stessa passphrase scelta in precedenza come *password principale di Thunderbird*, poiché si tratta praticamente delle stesse informazioni che stiamo proteggendo: la nostra chiave segreta. Quindi fate clic su *OK*.

* Una finestra di dialogo dovrebbe confermare che *le chiavi sono state salvate correttamente*. È possibile chiuderlo.

* Verificare che il backup sia in un luogo sicuro.

44.1.3 Tenere al sicuro un certificato di revoca

Se gli avversari mettono le mani sulla nostra chiave privata, o se semplicemente la perdiamo, dobbiamo *revocarla*, in modo che i nostri corrispondenti sappiano che l'abbiamo persa.

1. Agence nationale de la sécurité des systèmes d'information, 2020, *Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf], p. 20.

2. Zvi Gutterman, Benny Pinkas, Tzachy Reinman, 2006, *Analysis of the Linux Random Generatore di numeri* [<http://www.pinkas.net/PAPERS/gpr06.pdf>].

non deve più utilizzare la chiave pubblica corrispondente. A questo scopo si utilizza un *certificato di revoca*.

Il certificato di revoca si presenta sotto forma di un file o di poche righe di testo, che dovremo conservare in un luogo sicuro, ad esempio su una chiavetta USB crittografata, presso una persona fidata o su un pezzo di carta ben nascosto. Chiunque abbia accesso a questo file può revocare la nostra chiave pubblica, impedendoci di comunicare in forma criptata.

Quando si crea una coppia di chiavi OpenPGP, Thunderbird crea automaticamente un certificato di revoca, ma lo nasconde nella sua cartella di configurazione. Per trovarlo :

- lanciare Files: premere  ( su Mac), digitare `file` e poi fare clic su *File* ;
- nel pannello di sinistra, andare alla *cartella Personale* ;
- fare clic su  e poi su *Afficher les fichiers cachés* ;
- aprire la cartella `.thunderbird` ;
- trovare la cartella con il nome strano che termina con `.default` (per esempio `7u6xu6tq.default` o `profile.default`) e aprirlo;
- il certificato di revoca della nostra chiave privata è memorizzato in un file il cui nome inizia con l'identificativo della chiave e termina con `_rev.asc`⁴ e termina con `_rev.asc` (ad esempio `0xC7BF166A096820DA_rev.asc`);
- fare doppio clic sul file per aprirlo.

A seconda della nostra scelta, possiamo quindi :

- salvarlo facendo clic su  e poi su *Salva con nome...* e scegliere un nome di file chiaro. Ad esempio *Certificato di revoca per la chiave 0xC7BF166A096820DA.asc* ;
- stamparlo facendo clic sull'icona della stampante nel menu .

Se la nostra chiave privata venisse compromessa, utilizzeremmo questo certificato per revocare la chiave pubblica associata.

pagina
340

44.1.4 Impostazione della crittografia per un account e-mail

La crittografia asimmetrica può essere utilizzata per crittografare o firmare le e-mail, o per entrambe le cose. È quindi necessario configurare l'account e-mail che si desidera utilizzare con la coppia di chiavi appena generata.

Per farlo:

- * fare clic su  per aprire il menu di Thunderbird, quindi aprire *Impostazioni account*;
- * fare clic sulla sezione *Crittografia end-to-end* dell'account di posta da modificare;
- * scegliere la chiave corrispondente alla nostra identità contestuale invece di *None. Non utilizzare OpenPGP per questa identità.*

Più in basso, in *Impostazioni predefinite per l'invio di messaggi*, è possibile selezionare diverse opzioni.

Per impostazione predefinita, le e-mail non sono crittografate e la crittografia deve essere attivata manualmente per ogni e-mail. È possibile *attivare la crittografia per i nuovi messaggi*; sarà poi necessario disabilitare la crittografia per scrivere a qualcuno che non utilizza OpenPGP.

Possiamo anche selezionare la casella *Firma messaggi non crittografati* per firmare tutte le e-mail inviate da questo account (i messaggi crittografati sono sempre firmati).

4. In caso di dubbio, è possibile trovare l'identificativo della nostra chiave (senza lo 0x iniziale) nella cartella di Thunderbird *OpenPGP Key Manager*, di fronte all'identità contestuale corrispondente.

firmato per impostazione predefinita). Ciò consente ai destinatari di autenticare tutte le e-mail, comprese quelle non crittografate. Inoltre, mostra loro che viene utilizzato OpenPGP. Attenzione, però, perché questo dimostra criticamente che l'e-mail è stata inviata da una persona in possesso della chiave segreta corrispondente, il che non è sempre auspicabile.

44.2 Esportare e condividere la nostra chiave pubblica

🔄 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: pochi minuti.*

Per inviarci e-mail crittate e verificare la nostra firma e-mail, i nostri corrispondenti hanno bisogno della nostra chiave pubblica. Ma prima di poterla utilizzare, devono anche aver verificato l'impronta digitale di questa chiave.

pagina
338

44.2.1 Inviare la nostra chiave pubblica via e-mail

È possibile inviare la nostra chiave pubblica via e-mail. Nella finestra del messaggio, fare clic sul pulsante  a destra del pulsante  *Attach*, quindi selezionare *My OpenPGP public key*. La nostra chiave verrà automaticamente aggiunta come allegato al momento dell'invio dell'e-mail.

44.2.2 Pubblicare la vostra chiave pubblica sui server delle chiavi

Se l'esistenza dell'identità contestuale a cui corrisponde la chiave non è di per sé riservata, possiamo pubblicare la nostra chiave pubblica su un server di chiavi, in modo che chiunque voglia inviarci e-mail crittate possa scaricarla a tale scopo.

Si inizia esportando la propria chiave pubblica in un file, che può essere condiviso su un server o tramite una chiave USB crittografata. La procedura è la stessa sotto Tails o con una Debian crittata:

- In Thunderbird, fate clic su  → *Strumenti* → *Gestione chiavi OpenPGP*.
- Selezionate la chiave OpenPGP che desiderate esportare; nel menu, fate clic su *File* → *Esporta chiavi pubbliche in un file*; scegliete un percorso di esportazione e un nome per il file, quindi fate clic su *Salva*.

Quindi pubblicare la chiave su un server di chiavi:

- Aprire Tor Browser e inserire l'indirizzo <https://keys.openpgp.org/>.
- Fare clic su *Carica*.
- Cliccare su *Sfoglia...* e scegliere il file in cui è stata esportata la chiave pubblica.
- Fare clic su *Carica*. Una pagina conferma la ricezione della chiave.
- Visitare il link contenuto nell'e-mail di conferma (copiandolo e incollandolo nella barra degli indirizzi del browser Tor) per confermare che siamo noi dietro l'indirizzo e-mail associato alla chiave pubblicata.

pagina
315

44.2.3 Ottenere un'impronta digitale della chiave

Se trasmettiamo la nostra chiave pubblica con mezzi non autenticati, dobbiamo inviare alla nostra corrispondente l'impronta digitale (vedi pagina 54) della nostra chiave con mezzi autenticati, in modo che possa verificare che si tratti della chiave giusta appartenente alla persona giusta.

Per ottenere l'impronta digitale della nostra chiave :

- In Thunderbird, fate clic su  → *Strumenti* → *Gestione chiavi OpenPGP*.
- Fare doppio clic sulla chiave OpenPGP per visualizzare le *proprietà della chiave*.

- Annotare o copiare l'impronta digitale della chiave per una condivisione sicura.

Di seguito vengono illustrati i metodi per condividere l'impronta digitale su un canale sicuro e per verificare l'autenticità della chiave (vedere la pagina successiva).

44.3 Importare, verificare ed esportare chiavi pubbliche

C Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

🕒 Durata: Da pochi minuti a mezz'ora.

Utilizziamo le chiavi pubbliche di altre persone per crittografare le e-mail che inviamo loro e per verificare l'autenticità dei messaggi che hanno firmato.

Per ottenere queste chiavi pubbliche, dobbiamo importarle. Prima di utilizzarle, è necessario verificarne l'autenticità, per assicurarsi di avere la chiave pubblica giusta dalla persona giusta. A volte è anche utile esportare queste chiavi in un file per utilizzarle in altri software.

questa
pagina

prossimo
pagina

339

44.3.1 Importare una chiave pubblica

Lo scopo di questo capitolo è importare una chiave OpenPGP, che verrà utilizzata per verificare le firme digitali o criptare i messaggi. La procedura è la stessa sotto Tails o con una Debian criptata.

Importare una chiave non significa verificare che appartenga effettivamente al presunto proprietario. Vedremo nella prossima sezione che questo richiede altre operazioni, come lo studio della firma o dell'impronta digitale.

In Thunderbird, l'importazione delle chiavi avviene attraverso l'*OpenPGP Key Manager*. Per accedervi, cliccate su  → *Strumenti* → *OpenPGP Key Manager*.

prossimo
pagina.

Se la chiave è disponibile in un file

In *OpenPGP Key Manager*, fare clic su *File* → *Importa chiavi pubbliche da file*. Nella finestra che si apre, selezionare il file contenente la chiave, quindi fare clic su *Apri*.

Si può quindi procedere alla fase di conferma dell'importazione (vedi pagina successiva).

Se volete cercare la chiave online

Sempre in *OpenPGP Key Manager*, fare clic su *Key server* → *Ricerca le chiavi online*.

Nella finestra che si apre, digitate l'indirizzo e-mail o l'identificatore corrispondente alla chiave che state cercando, ad esempio guide@boum.org, `0x326F9F67250B0939`⁵ o `D4874FA4F6B688DC0913C9FD326F9F67250B0939` e selezionare *OK*. È necessario controllare l'impronta digitale in seguito, come vedremo più avanti.

pagina
329

Si noti che se si è precedentemente configurato Thunderbird per l'utilizzo del routing a cipolla, è necessario che sia attivo anche Tor Browser affinché la ricerca di chiavi online funzioni.

5. Si tratta dell'identificatore breve di una chiave, che non è sufficiente per selezionare in modo univoco una chiave. Riseup, 2017, *Best practices for using OpenPGP* [<https://help.riseup.net/it/security/message-security/openpgp/best-practices#-don't-know-%C3%A0-identifier-de-cl%C3%A9>].

Conferma dell'importazione

Una volta che Thunderbird ha trovato la chiave (nel file specificato o online, a seconda della procedura utilizzata poco prima), si apre una finestra di risultati che mostra l'identificativo completo della chiave e gli indirizzi e-mail associati. Se si tratta della chiave che si desidera importare, selezionare *Accettata (non verificata)* e fare clic su *OK*.

Se l'importazione è riuscita, si apre una finestra con *le chiavi importate correttamente* e un riepilogo delle informazioni sulle chiavi. Chiuderla con *OK*.

La chiave importata dovrebbe ora essere visibile in *OpenPGP Key Manager*.

È comunque necessario verificarne l'autenticità.

44.3.2 Verificare l'autenticità di una chiave pubblica

Quando si utilizza la crittografia asimmetrica, è fondamentale assicurarsi di avere la vera chiave pubblica del proprio corrispondente. In caso contrario, ci si espone all'attacco del mostro di mezzo.

Prima di tutto, dobbiamo scegliere un metodo per assicurarci di avere la chiave pubblica giusta. Poi diremo a Thunderbird che ci fidiamo di questa chiave.

A seconda dei requisiti del nostro modello di minaccia e delle nostre possibilità, possiamo scegliere diversi modi per verificare l'autenticità di una chiave pubblica. Supponiamo di dover verificare l'autenticità della chiave pubblica di Ana.

Trasmettere la chiave a se stessi tramite un canale sicuro...

Quando è possibile, il modo più semplice è quello di consegnare il file contenente la chiave pubblica, ad esempio utilizzando una chiave USB. Ana esporta quindi (vedi pagina a fianco) la sua chiave pubblica in un file, che memorizza su una chiave USB, eventualmente crittografata (vedi pagina 145), e che poi ci consegna. Noi importiamo (vedi pagina precedente) la chiave pubblica di Ana direttamente da questo file.

... o trasmettersi l'impronta digitale tramite un canale sicuro.

Uno degli svantaggi del metodo precedente è che richiede il trasferimento di un file informatico con un mezzo sicuro. Questo non è sempre possibile. Fortunatamente non è necessario: è sufficiente ottenere, con un mezzo sicuro, una somma di controllo della chiave pubblica, nota come "impronta digitale".

Ana può pubblicare la sua chiave pubblica su Internet, ad esempio sul suo blog o su un server di chiavi. Da parte nostra, scarichiamo questa chiave non autenticata, quindi verificiamo che l'impronta digitale della chiave corrisponda a quella che Ana ci ha inviato *autenticata*. Per vedere l'impronta digitale della chiave di Ana ottenuta da Internet, è necessario importarla (vedi pagina precedente) in *OpenPGP Key Manager*, quindi fare doppio clic sulla sua chiave.

Cosa si guadagna utilizzando questo metodo? Invece di dover passare un file, è sufficiente passare una riga di caratteri come questa:

```
A490 D0F4 D311 A415 3 E2B B7CA DBB8 02 B2 58 AC D84F
```

Ad esempio, Ana, che è una persona ben organizzata, può portare sempre con sé una copia della sua chiave pubblica scritta su un pezzo di carta. Basterà poi passargliela: non c'è bisogno di un computer o di una chiave USB.

Se non possiamo incontrarla, Ana può anche inviarci la stampa per posta e noi possiamo chiamarla per leggerla al telefono. La verifica non sarà come quella di vedersi direttamente, ma è comunque più difficile da fare.

per gli avversari di inviarci posta con la sua chiave e di rispondere al numero di telefono di Ana leggendo la sua impronta digitale e imitando la sua voce.

Le cose si complicano ulteriormente se non conosciamo Ana. In questo caso, dovremo fidarci delle persone che affermano di conoscerla. Anche in questo caso, non esiste una formula magica, ma la combinazione di diversi mezzi di verifica può facilitare il compito di eventuali avversari che vogliono sferrare un "attacco a metà": possiamo chiedere a diverse persone che affermano di conoscere Ana piuttosto che a una sola, usare diversi mezzi di comunicazione e così via.

pagina
254

Registrazione della fiducia in una chiave

Una volta stabilita la fiducia nella chiave di Ana, è utile informare Thunderbird che può fidarsi di questa chiave.

Per farlo, aprite il *Gestore delle chiavi OpenPGP* di Thunderbird facendo clic su  → *Strumenti* → *OpenPGP Key Manager*.

Una volta individuata la chiave di Ana nella finestra principale, fare doppio clic su di essa per visualizzarne i dettagli. Verificare che si tratti della chiave giusta, ad esempio verificando l'impronta digitale. Nella scheda *La tua accettazione*, selezionare *Sì, ho verificato di persona che l'impronta digitale di questa chiave sia corretta*, quindi convalidare facendo clic su *OK*.

Thunderbird ora sa che la chiave di Ana è affidabile.



PER SAPERNE DI PIÙ...

In Thunderbird, quando ci si fida di una chiave, la scelta rimane solo sul nostro computer. Per far funzionare la rete di fiducia (vedere pagina 257), il protocollo OpenPGP consente di firmare una chiave e di rendere pubblica la firma, in modo che qualsiasi utente della rete di fiducia possa beneficiare delle verifiche effettuate.

Per il momento non è possibile utilizzare l'interfaccia di Thunderbird per la firma pubblica. È possibile solo nel portachiavi OpenPGP del sistema, a cui si può accedere, ad esempio, con l'applicazione *Kleopatra*.

44.3.3 Esportazione di una chiave pubblica in un file

Lo scopo di questo strumento è esportare una chiave OpenPGP, ad esempio per utilizzarla con altri software.

Il file creato da questa operazione conterrà la chiave pubblica necessaria per criptare i messaggi destinati all'identità corrispondente o per verificare le firme apposte da questa identità.

Per farlo:

- In Thunderbird, fate clic su  → *Strumenti* → *Gestione chiavi OpenPGP*.
- Selezionate la chiave OpenPGP che desiderate esportare; nel menu, fate clic su *File* → *Esporta chiavi pubbliche in un file*; scegliete un percorso di esportazione e un nome per il file, quindi fate clic su *Salva*.

44.4 Gestire la coppia di chiavi: estenderla, modificarla o revocarla

Quando abbiamo creato la nostra coppia di chiavi, abbiamo potuto scegliere una data di scadenza. Prima che la coppia di chiavi scada, è possibile modificare la data di scadenza per estenderne la validità. Tuttavia, con l'evoluzione delle tecnologie, potremmo voler cambiare la nostra coppia di chiavi e passare a una nuova. Infine, a volte capita che una chiave privata sia compromessa e debba essere revocata.

44.4.1 Estensione della coppia di chiavi

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: pochi minuti.*

Se la nostra coppia di chiavi sta per scadere, ma non c'è motivo di passare a una nuova coppia, possiamo estenderne la validità.

Per farlo:

- in Thunderbird, fare clic su  → *Strumenti* → *OpenPGP Key Manager* ;
- fare doppio clic sulla nostra coppia di chiavi;
- cliccare su *Modifica data di scadenza* ;
- selezionare *La scadenza della chiave* e scegliere un numero di mesi, ad esempio dodici o ventiquattro mesi (uno o due anni);
- fare clic su *OK* per convalidare.

Rieccoci per un'altra stagione con la nostra coppia di chiavi!

44.4.2 Transizione a una nuova coppia di chiavi

 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: Da 15 minuti a un'ora.*

Prima che la nostra coppia di chiavi scada, o quando i progressi della crittografia ci costringeranno a usare chiavi più sicure, dovremo creare una nuova coppia di chiavi.

A tal fine, utilizzare lo strumento *Crea coppia di chiavi* (vedere pagina 333).

Esporteremo quindi la nostra nuova chiave pubblica (vedi pagina precedente) e la invieremo alle persone con cui comunichiamo.

Qualche tempo dopo, saremo in grado di revocare la nostra vecchia chiave (vedere questa pagina).

Tuttavia, conserveremo la nostra vecchia chiave privata, in modo da poter decifrare i messaggi ricevuti in precedenza, crittografati con la vecchia chiave pubblica.

44.4.3 Revocare una coppia di chiavi

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.*

 *Durata: Da quindici a trenta minuti.*

Se la nostra coppia di chiavi è compromessa, ad esempio se abbiamo perso il nostro sistema o sospettiamo che sia stato violato, la chiave è informare i nostri corrispondenti. In questo modo, sapranno che la chiave non è più affidabile e potranno smettere di usarla.

A tale scopo, utilizzeremo il certificato di revoca creato in precedenza (vedere pagina 334) con la nostra coppia di chiavi.



Attenzione: le istruzioni che seguono revocano in modo irreversibile la nostra chiave. Utilizzatele solo se necessario!

Preparazione del certificato di revoca

Prima di tutto, dobbiamo trovare il certificato di revoca che abbiamo salvato quando abbiamo creato la nostra coppia di chiavi. Lo abbiamo conservato in un luogo sicuro, ad esempio su una chiave USB crittografata, presso una persona fidata o su un pezzo di carta ben nascosto.

pagina

334

Se era su un pezzo di carta, è necessario creare un file contenente le informazioni sul certificato di revoca:

- avviare l'Editor di testo: premere  ( su Mac), digitare `gedi` poi fare clic su *Editor di testo* ;
- nel documento, digitare esattamente la parte che inizia con `-----BEGIN PGP PUBLIC KEY BLOCK-----` e termina con `-----END PGP PUBLIC KEY BLOCK ;`
- Salvare il file in formato `.asc`, ad esempio `revocation.asc`.

Altrimenti, se il file contenente il certificato di revoca è stato salvato su un altro supporto (chiave USB criptata o simile), è necessario prima :

- aprire questo file facendo clic con il tasto destro del mouse su di esso, quindi *Apri con un'altra applicazione*;
- in *Scegliere un'applicazione*, selezionare *Editor di testo* e fare clic su *Seleziona* ;
- rimuovere il carattere `:` all'inizio della riga `-----BEGIN PGP PUBLIC KEY BLOCK-----`;
- fare clic su *Salva* e chiudere l'editor di testo.

Il certificato di revoca è pronto. Ora possiamo usarlo per revocare la nostra chiave.

Revocare la chiave OpenPGP

Per revocare una chiave OpenPGP, è necessaria la chiave pubblica corrispondente. Se la nostra chiave privata è stata compromessa, potremmo non avere più accesso al sistema in cui si trovava. Pertanto, se non si dispone della chiave pubblica che si desidera revocare, è necessario iniziare a importarla (vedere pagina 337).

Successivamente, importare il certificato di revoca.

In Thunderbird, aprite il *gestore delle chiavi OpenPGP* facendo clic su  →

Strumenti → *OpenPGP Key Manager*. Poi :

- scegliere *File* → *Importazione di revoche da un file* ;
- selezionare il file contenente il certificato di revoca, quindi fare clic su *Apri*;
- la chiave revocata appare in grigio.

Se avete già pubblicato la vostra chiave pubblica su un server di chiavi, ora dovete pubblicare lì la chiave revocata, seguendo la ricetta qui sotto.

Pubblicare la chiave pubblica revocata

Se la nostra chiave pubblica è stata precedentemente pubblicata su un server di chiavi, la cosa migliore da fare è pubblicare nuovamente la nostra chiave revocata, in modo che la nostra chiave pubblica sia ora revocata anche lì, consentendo a tutti i nostri corrispondenti di essere avvisati aggiornandola dal server di chiavi.

Per farlo, sia con Tails che con Debian, seguite la ricetta per pubblicare la vostra chiave pubblica sui server di chiavi.

pagina

336

Una volta completata la sincronizzazione, non resta che informare i nostri corrispondenti.

Notificare ai nostri corrispondenti la revoca della chiave

Il passo più importante per revocare la nostra chiave è quello di informare i nostri corrispondenti in modo che non la utilizzino più.

A tal fine, è possibile scegliere :

- inviare via e-mail il certificato di revoca, che potrà essere importato per revocare la nostra chiave pubblica nel loro portachiavi;
- esportare la nostra chiave pubblica revocata (vedere pagina 339) e poi inviargliela via e-mail, in modo che possa importarla di nuovo;
- chiedere loro di aggiornare la nostra chiave revocata dal server delle chiavi su cui l'abbiamo pubblicata; non esiste una ricetta pronta per questo, tra l'invio di un'e-mail criptata, l'avviso di persona, ecc.

44.4.4 Revoca della chiave pubblica di un corrispondente

Se uno dei nostri corrispondenti ci ha informato che la sua coppia di chiavi è stata compromessa e l'ha revocata, dobbiamo aggiornare la sua chiave sul nostro computer in modo che Thunderbird tenga conto di questa revoca.

Per farlo:

- se il nostro corrispondente ci ha inviato il certificato di revoca della sua chiave, seguite la ricetta precedente per importare questo certificato;
- se ha inviato la sua chiave pubblica revocata, deve essere importata di nuovo (vedere pagina 337);
- se ha pubblicato la sua chiave pubblica revocata su un server di chiavi, è necessario aggiornare la nostra copia della chiave importandola nuovamente dal server di chiavi (vedere pagina 337).

44.5 Crittografare e/o firmare le e-mail in Thunderbird

 Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

 Durata: pochi minuti.

[pagina] Una volta avviato e configurato Thunderbird :

329

- fare clic sul pulsante *Scrivi* per iniziare a scrivere un nuovo messaggio;
- si apre la finestra *Redaction*, in cui scriveremo la nostra e-mail;
- se si desidera crittografare l'e-mail, fare clic sul pulsante  *Encrypt*, se non è già selezionato (il lucchetto è barrato quando la crittografia è disattivata); è anche possibile attivare la crittografia dell'e-mail facendo clic nel menu *Sicurezza* → *Crittografia*;
- se si desidera firmare digitalmente l'e-mail, fare clic su  *OpenPGP* → *Firma digitale* o nel menu *Sicurezza* → *Firma digitale* ;
- Se il nostro corrispondente non possiede già la nostra chiave pubblica, è possibile allegarla automaticamente all'e-mail facendo clic sul pulsante  alla destra del pulsante *Attach* e selezionando *My OpenPGP public key* ;
- una volta completata l'e-mail, cliccare su *Invia*.

[pagina]

252

Se la persona che riceve l'e-mail utilizza anche Thunderbird, vedrà un'icona Pulsante *OpenPGP* con :

- un lucchetto chiuso se l'e-mail è crittografata;
- un timbro se l'e-mail è firmata.

Facendo clic su questo pulsante si visualizzano i dettagli della crittografia e della firma.

Se la persona non possiede la chiave privata per la quale il messaggio è stato crittografato, al posto del corpo dell'e-mail viene visualizzato il messaggio *La chiave segreta necessaria per decrittografare questo messaggio non è disponibile.*

Utilizzare la crittografia OpenPGP in l'ufficio

Lo standard Internet ¹ OpenPGP è un formato crittografico che può essere utilizzato per creare e verificare firme digitali e per criptare e decriptare messaggi e file.

La maggior parte degli strumenti di questa guida utilizza OpenPGP, utilizzando Thunderbird quando possibile per gestire le chiavi OpenPGP, poiché la sua interfaccia è più ergonomica e funziona così in Tails. Tuttavia, alcuni usi di OpenPGP che non sono possibili in Thunderbird sono raggruppati in questo capitolo.

pagina
333

Thunderbird e il resto dell'ambiente desktop (sia che si utilizzi Debian o Tails) utilizzano due portachiavi OpenPGP diversi. Le chiavi che vorremmo avere in entrambi i portachiavi devono essere esportate manualmente da uno e poi importate nell'altro.

45.1 Importare una chiave nel portachiavi di Office

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: pochi minuti.*

Lo scopo di questo strumento è importare una chiave OpenPGP nel portachiavi OpenPGP del desktop. Si noti che questo portachiavi non è lo stesso di Thunderbird.

Se si utilizza una Debian criptata, occorre innanzitutto installare il pacchetto software *Kleopatra*, che contiene lo strumento di gestione delle chiavi che si utilizzerà. Se si sta ascoltando Tails, il pacchetto installato.

pagina
119
pagina

134



Quando Kleopatra viene lanciato, potrebbe apparire un messaggio di avvertimento intitolato *Risultati del test automatico di Kleopatra*, in cui la *verifica della configurazione di sdaemon* sembra essere fallita. Non si tratta di un problema grave, ma può diventare rapidamente fastidioso. Per evitare che questo messaggio appaia ogni volta che Kleopatra si avvia, si può deselezionare la casella *Avvia questi test all'avvio* e poi fare clic su *Continua*. Un'altra possibilità è quella di installare il pacchetto sdaemon, anche se non ci sarà utile.

pagina

135

45.1.1 Importare una chiave segreta

Potrebbe essere necessario importare la propria chiave segreta (detta anche chiave privata) nel portachiavi di Office, ad esempio per firmare o decifrare file o per firmare chiavi pubbliche.

1. Wikipedia, 2014, *Internet Standard* [https://fr.wikipedia.org/wiki/Standard_Internet].

[pagina] Se si trova nel portachiavi di Thunderbird, iniziare a salvare la chiave segreta, sotto
334 forma di file con estensione .asc.

Quindi importatela nel portachiavi del desktop facendo doppio clic su di essa.

Viene visualizzata la finestra *Hai importato una chiave privata*. Il software chiede *È questa la propria chiave?* Rispondere *Sì*.

Viene visualizzata una nuova finestra *Risultato importazione certificato*. Confermare con *OK*.

45.1.2 Importare una chiave pubblica

L'importazione di una chiave pubblica nel portachiavi OpenPGP del desktop consente di verificare le firme digitali o di crittografare i file.

Se si è ricevuto o scaricato un file contenente la chiave (di solito con estensione .asc o .pub), è sufficiente fare doppio clic sul file per importarlo nel foro del desktop.

[pagina] Se si desidera recuperare una chiave già presente nel portachiavi di Thunderbird, è
339 necessario esportarla per ottenere il file contenente la chiave da importare. È quindi possibile importare la chiave facendo doppio clic sul file.

Viene visualizzata la finestra di dialogo *Hai importato un nuovo certificato (chiave pubblica)*. Il software propone di guidare l'utente attraverso il processo di certificazione della sua autenticità. È buona norma selezionare *Sì* se si dispone di una chiave segreta (necessaria per firmare la chiave appena importata).

45.2 Firma di una chiave

 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: pochi minuti.*

[pagina] Lo scopo di questo strumento è firmare una chiave OpenPGP nel portachiavi
119 OpenPGP del desktop. Si noti che questo portachiavi non è lo stesso di Thunderbird.

[pagina] Se si utilizza una Debian criptata, è necessario installare prima il pacchetto
134 software *Kleopatra*, che contiene lo strumento di gestione delle chiavi che si utilizzerà. Se si sta ascoltando Tails, il pacchetto installato.

 Quando *Kleopatra* viene lanciato, potrebbe apparire un messaggio di avvertimento intitolato *Risultati del test automatico di Kleopatra*, in cui la *verifica della configurazione di sddaemon* sembra essere fallita. Non si tratta di un problema grave, ma può diventare rapidamente fastidioso. Per evitare che questo messaggio appaia ogni volta che *Kleopatra* si avvia, si può deselezionare la casella *Avvia questi test all'avvio* e poi fare clic su *Continua*. Un'altra possibilità è quella di installare il pacchetto sddaemon, anche se non ci sarà utile.

[pagina] 135

[pagina] 338 Ma perché firmare una chiave? Diciamo che abbiamo prima verificato l'autenticità della chiave di Ana seguendo la ricetta descritta nel capitolo precedente. È quindi utile informare OpenPGP che può fidarsi di questa chiave. Questa operazione si chiama firma della chiave. *Kleopatra* la chiama anche *certificazione della chiave*. La procedura è la stessa sotto Tails o con una Debian criptata.

[pagina] precedente Per poter firmare una chiave, dobbiamo prima importare la nostra chiave segreta in *Kleopatra*. Avanti:

- Andate su *Kleopatra*, premendo  ( su Mac) per aprire la panoramica delle attività, quindi digitate *kleo* e fate clic sul software corrispondente.

- Se la chiave che si desidera firmare non è presente, importarla.
- Una volta individuata la chiave di Ana nella finestra principale, fare doppio clic su di essa per visualizzarne i dettagli. Verificate che si tratti della chiave giusta, ad esempio controllando l'impronta digitale (che si trova in fondo alla finestra).
- Quindi fare clic su *Certifica*.
- Inserire la passphrase per la nostra chiave segreta nella finestra di dialogo che si apre, se necessario.².
- Dovrebbe apparire la finestra *Certificazione riuscita*. Fare clic su *OK*.

OpenPGP ora sa che la chiave di Ana è attendibile.

45.3 Verifica di una firma digitale

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: pochi minuti.*

Lo scopo di questo strumento è verificare l'autenticità di un file con una firma digitale OpenPGP.

Se si utilizza una Debian criptata, è necessario installare il pacchetto software *Kleopatra*, che contiene lo strumento di gestione delle chiavi che si utilizzerà. Se si utilizza Tails, questo pacchetto è già installato.



Quando Kleopatra viene lanciato, potrebbe apparire un messaggio di avvertimento intitolato *Risultati del test automatico di Kleopatra*, in cui la verifica della configurazione di *scdaemon* sembra essere fallita. Non si tratta di un problema grave, ma può diventare rapidamente fastidioso. Per evitare che questo messaggio appaia ogni volta che Kleopatra si avvia, si può deselezionare la casella *Avvia questi test all'avvio* e poi fare clic su *Continua*. Un'altra possibilità è quella di installare il pacchetto *scdaemon*, anche se non ci sarà utile.

Per verificare la firma digitale di un file, è necessario trovare la chiave pubblica della persona o del gruppo che ha prodotto la firma e importarla nel portachiavi di Office. In genere, la chiave pubblica necessaria per verificare la firma può essere scaricata dal sito web in cui sono stati recuperati il file e la sua firma. Se la firma è stata creata da uno dei nostri corrispondenti, è la sua chiave pubblica che deve essere utilizzata per verificare la firma.

Questa firma assume la forma di un piccolo file, solitamente con lo stesso nome del file contenente i dati firmati, con estensione *.sig*,

.sig o *.asc*.

45.3.1 Eseguire la verifica della firma

- Se il file di firma termina con l'estensione *.sign*, fare clic con il pulsante destro del mouse e scegliere *Rename....* Rimuovere la *n* finale in modo che finisca in *.sig*.
- Andate su *Kleopatra*, premendo il tasto ( su Mac) per aprire la panoramica delle attività, poi digitate *kleo* e infine fate clic sul software corrispondente.
- Nella barra degli strumenti nella parte superiore della finestra, fare clic su *Decriptare/Verificare....*
- Nella finestra che si apre, selezionare il file di firma.

Viene visualizzata la finestra *Verifica file*. Essa contiene l'avanzamento e poi il risultato della verifica.

². Se la passphrase è già stata digitata poco prima, non verrà più richiesta. OpenPGP la tiene in memoria per dieci o trenta minuti.

45.3.2 Interpretare il risultato della verifica

- *Firma valida* significa che il file è stato firmato dalla chiave specificata in *Con certificato*.
- *L'impossibilità di verificare i dati* può significare due cose:
 - Se la casella dei risultati mostra *Con certificato* seguito dal nome di una chiave del nostro portachiavi, significa che il file è effettivamente firmato dalla chiave specificata, ma che non abbiamo confermato l'autenticità di questa chiave. Se si desidera verificarlo, seguire lo strumento corrispondente (vedere pagina 338), quindi firmare la chiave (vedere pagina 344).
 - Se la casella dei risultati mostra *Con certificato non disponibile* seguito da un identificatore di chiave, significa che il file è effettivamente firmato, ma che la chiave pubblica necessaria per verificare la firma non è presente nel portachiavi OpenPGP del desktop. In questo caso, trovare la chiave e importarla nel portachiavi del desktop (vedere pagina 343) utilizzando il pulsante *Importa*.
- *Firma non valida* significa che il file verificato non corrisponde a quello firmato. È possibile che sia stato caricato un file sbagliato, un file di firma errato o che sia stato vittima di un attacco. In tutti i casi, il file scaricato non può essere considerato autentico.

45.4 Dati di firma

 Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

 Durata: pochi minuti.

[pagina 252] Lo scopo di questo strumento è quello di firmare digitalmente i dati. In particolare, può consentire ad altre persone di autenticare un messaggio, un documento, un software, ecc. come proveniente da noi. Questo strumento richiede la creazione di una coppia di chiavi e l'importazione della relativa chiave segreta nel portachiavi OpenPGP del desktop.

[pagina 333] **45.4.1 Testo della firma**
[pagina 343]

Questo metodo funziona solo per firmare il testo. Per firmare qualsiasi altro tipo di file, seguire la sezione successiva.

Per firmare il testo :

- Andate su *Kleopatra*, premendo  ( su Mac) per aprire la panoramica delle attività, quindi digitate *kleo* e fate clic sul software corrispondente.
- Nella barra degli strumenti in alto, fare clic su *Blocco note*.
- Nella scheda *Blocco note*, digitare o incollare il testo da firmare.
- Andare alla scheda *Destinatari*.
- Selezionate *Firma come* (scegliendo la giusta identità contestuale se ne avete più di una).
- Deselezionare *Crittografia per me* e *Crittografia per gli altri*.
- Fare clic su *Segno del blocco note*.
- Inserire la passphrase per la nostra chiave segreta nella finestra di dialogo che si apre, se necessario.³

Il testo firmato si trova nella scheda *Blocco note*. Può essere copiato e incollato in un file.

3. Se la passphrase è già stata digitata poco prima, non verrà più richiesta. OpenPGP la tiene in memoria per dieci o trenta minuti.

45.4.2 Firma di un file

Per firmare un file, dobbiamo prima importare la nostra chiave segreta nel portachiavi di Office.

pagina
343

Per firmare il file :

- Andate su *Kleopatra*, premendo  ( su Mac) per aprire la panoramica delle attività, quindi digitate *kleo* e fate clic sul software corrispondente.
- Nella barra degli strumenti nella parte superiore della finestra, fare clic su Firma/cancellazione...
- Selezionare il file da firmare e fare clic su *Apri*.
- Selezionate *Firma come* (scegliendo la giusta identità contestuale se ne avete più di una).
- Deselezionare *Crittografa per me* e *Crittografa per gli altri*.
- Fare clic su *Firma*.
- Inserire la passphrase per la nostra chiave segreta nella finestra di dialogo che si apre, se necessario.⁴
- Dovrebbe essere visualizzato un messaggio di *successo della firma*.

Il processo di firma può richiedere fino a diversi minuti, a seconda delle dimensioni del file e della potenza del computer utilizzato. Una volta completata, la firma assume la forma di un piccolo file con lo stesso nome del file originale, ma che termina con l'estensione *.sig*, situato nello stesso punto del file originale. Ogni volta che si trasmette il file originale, questo file di firma deve essere allegato in modo che i destinatari possano verificarne l'autenticità. Inoltre, affinché i destinatari possano verificare la nostra firma, dovranno aver importato in precedenza la nostra chiave pubblica.

45.5 Crittografia dei dati

 Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.

 Durata: pochi minuti.

Lo scopo di questo strumento è quello di criptare digitalmente i dati. Può essere utilizzato, ad esempio, per trasmettere uno o più documenti riservati su un supporto non crittografato che contiene già dei dati, oppure per mettere online questi stessi documenti.

pagina
249

Se si utilizza una Debian criptata, è necessario installare prima il pacchetto software *Kleopatra*, che contiene lo strumento di gestione delle chiavi che si utilizzerà. Se si sta ascoltando Tails, il pacchetto

pagina
119
pagina
134

installato. Quando Kleopatra viene lanciato, potrebbe apparire un messaggio di avvertimento intitolato *Risultati del test automatico di Kleopatra*, in cui la *verifica della configurazione di sddaemon* sembra essere fallita. Non si tratta di un problema grave, ma può diventare rapidamente fastidioso. Per evitare che questo messaggio appaia ogni volta che Kleopatra si avvia, si può deselezionare la casella *Avvia questi test all'avvio* e poi fare clic su *Continua*. Un'altra possibilità è quella di installare il pacchetto sddaemon, anche se non ci sarà utile.

pagina
135

Per iniziare:

- Andate su *Kleopatra*, premendo  ( su Mac) per aprire la panoramica delle attività, quindi digitate *kleo* e fate clic sul software corrispondente.
- Nella barra degli strumenti nella parte superiore della finestra, fare clic su Firma/cancellazione...

4. Se la passphrase è già stata digitata poco prima, non verrà più richiesta. OpenPGP la tiene in memoria per dieci o trenta minuti.

- Selezionate il file da crittografare e fate clic su *Apri*.

È possibile scegliere di crittografare il file con una o più chiavi pubbliche o di utilizzare una passphrase.

45.5.1 Crittografia dei dati con una passphrase

Se utilizzate una passphrase, dovrete condividerla con le persone che devono decifrare i dati.

- Deselezionare la voce *Firma con nome*.
- Deselezionare anche *Crittografia per me* e *Crittografia per gli altri*.
- Selezionare *Crittografia con password*.
- Fare clic su *Crittografia*.
- Immettere due volte la *frase segreta*, quindi fare clic su *OK*.
- Dovrebbe essere visualizzato un messaggio di *successo della crittografia*.

Il processo di crittografia può richiedere fino a diversi minuti, a seconda delle dimensioni del file e della potenza del computer utilizzato. Una volta completata l'operazione di crittografia, il file crittografato viene visualizzato accanto al file originale non crittografato, con la scritta

estensione `.gpg` alla fine del suo nome.

45.5.2 Crittografare i dati con una o più chiavi pubbliche.

Se si esegue la crittografia con chiavi pubbliche, è necessario avere nel portachiavi le chiavi pubbliche di *tutte le* persone con cui si desidera condividere il file. Se non l'avete ancora fatto, dovrete importarle.

- Deselezionate *Firma come*, a meno che non vogliate firmare il file digitalmente. In questo caso, dovrete scegliere l'identità contestuale giusta (se ne avete più di una).
- Se si desidera crittografare il file anche per la propria chiave, selezionare *Crittografia* anche *per me*.
- Selezionate *Crittografia per altri* e selezionate le chiavi delle persone con cui desiderate condividere il file.
- Fare clic su *Crittografia* (o *Firma/Crittografia*).
- Un messaggio di *successo della crittografia* (o di *successo della firma e della crittografia*) deve essere inviato.

Il processo di crittografia può richiedere fino a diversi minuti, a seconda delle dimensioni del file e della potenza del computer utilizzato. Una volta completata l'operazione di crittografia, il file crittografato viene visualizzato accanto al file originale non crittografato, con la scritta

estensione `.gpg` alla fine del suo nome.

45.6 Decriptare i file

 *Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

 *Durata: pochi minuti.*

pagina

249

Lo scopo di questo strumento è quello di decifrare un file crittografato digitalmente. In particolare, può essere utilizzato per leggere documenti riservati trasmessi in forma criptata.

pagina

119

pagina

134

Se si utilizza una Debian criptata, è necessario installare prima il file *Kleopatra* software. Se si utilizza Tails, questo pacchetto è già installato.

 Quando Kleopatra viene lanciato, potrebbe apparire un messaggio di avvertimento intitolato *Risultati del test automatico di Kleopatra*, in cui la *verifica della configurazione di sddaemon* sembra essere fallita. Non si tratta di un problema grave, ma può diventare rapidamente fastidioso. Per evitare che questo messaggio appaia ogni volta che Kleopatra si avvia, si può deselezionare la casella *Avvia questi test all'avvio* e poi fare clic su *Continua*. Un'altra possibilità è quella di installare il pacchetto sddaemon, anche se non ci sarà utile.

pagina

135

 **Attenzione:** spostare sempre il file da decifrare nella posizione in cui si desidera memorizzarlo nella sua forma decifrata. Ad esempio, se il file crittografato è memorizzato su una chiave USB non crittografata, è molto importante spostarlo prima di decifrarlo, altrimenti il file decrittografato verrà memorizzato in chiaro sulla chiave USB.

Per decifrare il file :

- Andate su *Kleopatra*, premendo  ( su Mac) per aprire la panoramica delle attività, quindi digitate *kleo* e fate clic sul software corrispondente.
- Nella barra degli strumenti nella parte superiore della finestra, fare clic su *Decriptare/Verificare...*
- Selezionare il file da decifrare e fare clic su *Apri*.
- Inserire la passphrase condivisa o la passphrase della nostra chiave segreta nella finestra di dialogo che si apre ⁵.
- Se il file non è solo crittografato ma anche firmato, il risultato della verifica della firma viene visualizzato come quando si verifica una firma semplice. In caso contrario, un messaggio indica *Decryption Success*.
- Fare clic su *Salva tutto* per salvare il file decrittografato.

pagina

346

5. Se la passphrase è già stata digitata poco prima, non verrà più richiesta. OpenPGP la tiene in memoria per dieci o trenta minuti.

Utilizzare la messaggistica istantanea con

OTR

🔄 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: Da mezz'ora a un'ora.*

Lo scopo di questo strumento è quello di dialogare con una persona utilizzando la messaggistica istantanea con crittografia e autenticazione. Per raggiungere questo obiettivo, utilizzeremo il protocollo OTR ¹ che aggiunge crittografia, autenticazione e riservatezza persistente a una serie di protocolli di messaggistica istantanea.

pagina
258

Per poter utilizzare OTR per chattare con la nostra corrispondente, quest'ultima deve anche attivare OTR nel suo software di messaggistica istantanea. Per farlo, può anche seguire le istruzioni fornite in questo capitolo.

46.1 Installare il client di messaggistica istantanea Pidgin

A tale scopo utilizzeremo il client di posta elettronica Pidgin. Pidgin supporta la crittografia OTR. Supporta anche diversi protocolli di messaggistica istantanea, come XMPP ² o IRC ³ tra gli altri. ⁴ Questo software è installato nel sistema Tails live, ma sono supportati solo i protocolli XMPP e IRC, mentre gli altri sono difficili da anonimizzare. Su una Debian criptata, è necessario iniziare installando i pacchetti `pidgin` e `pidgin-otr`.

pagina
119
pagina
135

46.2 Avviare Pidgin

Per aprire il software di messaggistica istantanea, aprire la panoramica delle attività premendo (`⌘`) su Mac), quindi digitare `pidgin` e infine fare clic su *Pidgin Internet Messaging*.

1. Wikipedia, 2014, *Off-the-Record Messaging* [[https://fr.wikipedia.org/wiki/Off-the-Record Messaging](https://fr.wikipedia.org/wiki/Off-the-Record_Messaging)].

2. Wikipedia, 2014, *Protocollo estensibile di messaggistica e presenza* [[https://fr.wikipedia.org/wiki / XMPP](https://fr.wikipedia.org/wiki/XMPP)].

3. Wikipedia, 2014, *Internet Relay Chat* [https://fr.wikipedia.org/wiki/Internet_Relay_Chat]. IRC normalmente accetta l'uso senza creare un account. Oggi, la maggior parte dei server IRC rifiuta le connessioni *tramite* Tor; fanno eccezione alcuni server, tra cui OFTC [<https://www.oftc.net/Tor/>]. L'uso di IRC non è spiegato in questa guida.

4. Per un elenco esaustivo dei protocolli supportati da Pidgin, consultare il [sito web](https://www.pidgin.im/) [<https://www.pidgin.im/>].

46.3 Impostazione di un account e-mail

Quando si apre Pidgin e non è stato impostato alcun account di posta elettronica, appare una finestra che propone di aggiungere un nuovo account.

Per impostare un nuovo account, fare clic *sul* pulsante Aggiungi.

Si apre la finestra *Aggiungi account*. Se disponete già di un account di messaggistica istantanea, compilate le informazioni necessarie, iniziando a selezionare il *protocollo* che desiderate utilizzare.

46.4 Creare un account di messaggistica istantanea XMPP

Come per l'account di posta elettronica, è necessario disporre di un login e di una passphrase (vedere pagina 103). Per evitare di utilizzare sempre la stessa, o di correre il rischio di dimenticarla, è possibile utilizzare un gestore di password (vedere pagina 355).

È anche possibile utilizzare i server della comunità dove la registrazione è gratuita. Ad esempio, sul sito jabberfr.org sono disponibili elenchi di server XMPP gratuiti. ⁵

Una volta creato l'account sul server prescelto e inserite le informazioni necessarie nella finestra di Pidgin, selezionare la casella Crea questo nuovo account sul server. ⁶ informazioni necessarie nella finestra di Pidgin, selezionate la casella *Crea questo nuovo account sul server*.

46.5 Crittografia della connessione al server

Per impostazione predefinita, Pidgin configura il nuovo account per crittografare la comunicazione con il server.

Se il certificato è firmato correttamente da un'autorità di certificazione, la connessione avverrà senza problemi e Pidgin salverà il certificato del server nella sua configurazione.

Se il certificato del server non è firmato, o se per qualche motivo Pidgin non è in grado di verificarne l'autenticità, è necessario utilizzare le stesse tecniche di verifica di un certificato nel browser web, altrimenti gli avversari potrebbero usurpare l'identità del server.

In questo caso, alla prima connessione, Pidgin visualizza una finestra che chiede se vogliamo *accettare il certificato per [example.org]*? Ci spiegherà anche perché non vuole accettare il certificato (*Il certificato è autofirmato. Non può essere verificato automaticamente*, se ad esempio il certificato non è firmato da un'autorità di certificazione). Facendo clic su *Visualizza certificato...*, Pidgin visualizza l'impronta digitale del certificato, consentendoci di verificarlo.

46.6 Attivare il plugin OTR (*Off-the-Record*)

Ora è necessario attivare la crittografia end-to-end con OTR.

Nel menu *Strumenti* di Pidgin, fare clic su *Plugin*. Individuare la riga "Off-the-Record confidential messaging" e selezionare la casella corrispondente per attivare il plugin. Fare clic su *Configura plugin* per selezionare opzioni quali *Non archiviare le conversazioni OTR*.

5. Un elenco di server XMPP comunitari [https://wiki.jabberfr.org/Serveurs#Serveur_s_communautaires]. Se la creazione di un account fallisce con un server, non esitate a provare con un altro.

6. Per maggiori dettagli su come creare un account XMPP, consultare il sito web di Linuxpedia [<https://www.linuxpedia.fr/doku.php/internet/pidgin-jabber>].

46.7 Impostare una conversazione privata

46.7.1 Aggiungere un contatto o partecipare a una chat

A seconda della situazione, dovremo aggiungere a Pidgin il contatto con cui vogliamo parlare, oppure dovremo iscriverci alla lounge dove lo troveremo.

Aggiungere un contatto

Per aggiungere un contatto in Pidgin, fare clic su *Contatti* nella barra dei menu del software e andare su *Aggiungi un contatto* Compilare quindi le informazioni di contatto pertinenti e fare clic su *Aggiungere*.

Il nostro contatto riceverà quindi una richiesta di autorizzazione per essere aggiunto al nostro elenco di contatti. Una volta che il nostro contatto avrà accettato la richiesta, potremo iniziare a chattare.

Partecipare a una chat room

Se invece volete entrare in una chat room dove probabilmente si trova la persona con cui volete chattare, cliccate su *Contatti* nella barra dei menu del software e andate su *Entra in chat* Allo stesso modo, compilate le informazioni necessarie e cliccate su

Chat.

Purtroppo non sarà possibile utilizzare la crittografia end-to-end nelle chat room di Pidgin. Il protocollo OTR non funziona per le chat room di Pidgin.

46.7.2 Avviare una conversazione privata

Per avviare una conversazione privata, fare doppio clic su un nome nella colonna di destra della finestra di chat in cui ci si trova, oppure fare clic sul nome dell'interlocutore nella finestra principale di Pidgin. Si apre una finestra di conversazione. Fare clic sul menu *OTR* → *Avvia una conversazione privata*.

Se è la prima volta che si utilizza OTR con questo account, Pidgin genererà una chiave privata e visualizzerà la finestra *Generazione chiave privata*. Questa chiave è unica per un determinato account. Se si possiedono più account di messaggistica istantanea, si avranno quindi più chiavi. Quando si afferma che la generazione di questa chiave è *completa*, si può chiudere questa finestra facendo clic su *Convalida*.

Pidgin afficherà poi *Ana non è stato ancora autenticato. È necessario autenticare questo contatto*. Ciò significa che la nostra conversazione è criptata, ma un avversario potrebbe impersonare Ana. Per essere sicuri di parlare con Ana, è necessario autenticare la conversazione.

pagina
254

46.7.3 Autenticare un corrispondente

Per autenticare un corrispondente, è necessario aver concordato in precedenza un segreto, oppure disporre di un mezzo di comunicazione diverso dalla messaggistica istantanea, considerato sicuro. Può trattarsi di una conversazione dal vivo, di una e-mail criptata, ecc.

OTR offre tre modi per autenticare un contatto:

- con domanda-risposta: definiamo una domanda e la sua risposta. La domanda viene poi posta al nostro corrispondente;
- con un segreto condiviso: viene richiesto un segreto noto solo ai due interlocutori per verificare che stiamo effettivamente parlando con la persona con cui vogliamo parlare;

- verifica manuale dell'impronta digitale: controlliamo che l'impronta digitale della chiave della persona con cui stiamo per avere una conversazione criptata sia la stessa che ci è stata fornita da un mezzo *autenticato*.

Una volta scambiati i segreti, le domande e le risposte o le impronte digitali, fare clic su *OTR* → *Autentica contatto*. Scegliere il metodo di autenticazione sotto *Come si desidera autenticare il contatto*, quindi rispondere alle domande. Infine, fare clic su *Autentica*.

Se l'autenticazione ha successo, lo stato della conversazione passa a *Privato*, il che significa che non è solo crittografata, ma anche autenticata.

[pagina

116

Se si utilizza un sistema non live o si è attivata la persistenza di Pidgin in Tails, questa fase di autenticazione deve essere eseguita solo una volta per un determinato contatto.

46.7.4 Terminare una conversazione

Una volta completata la finestra di dialogo, fare clic su *OTR* → *Termina conversazione privata*. In questo modo si cancella dalla RAM del computer la chiave di crittografia temporanea generata per questa conversazione. Anche se gli avversari dovessero ottenere le nostre chiavi private, non avrebbero accesso alla chiave che consente loro di decifrare la conversazione *a posteriori*.

Gestione delle password

C Poiché il software si evolve, si consiglia vivamente di utilizzare la versione più aggiornata di questo strumento, disponibile sul sito Web <https://guide.boum.org/>.

🕒 Durata: Da quindici a trenta minuti.

Quando si crea un indirizzo e-mail, un account su un sito web e così via, questo account è solitamente protetto da una password.

È importante non utilizzare la stessa password per account diversi o per scopi diversi.

È inoltre importante non utilizzare la stessa password per diverse identità contestuali, in modo che la compromissione di una non comprometta le altre.

pagina
243

Esistono due buone scuole per la gestione delle password:

- Scegliere e ricordare una passphrase diversa per ogni utilizzo;
- generano password in modo casuale e le memorizzano in un *gestore di password*, che a sua volta è protetto da una passphrase.

47.1 Scegliere una buona passphrase

La prima scuola ha il vantaggio di non richiedere supporti di memorizzazione: le passphrase sono sempre con voi. Per applicarla, consultare la passphrase giusta (vedere pagina 103).

Tuttavia, quando si moltiplicano gli account e le identità contestuali, le passphrase da ricordare possono essere davvero tante.

47.2 Utilizzare un gestore di password

Il secondo metodo può essere utile. In pratica, avremo una passphrase da ricordare per ogni identità, mentre il nostro gestore di password si occuperà di memorizzare le varie password collegate a questa identità. Questo può essere fatto su un sistema Debian criptato o su un sistema live amnesico usando la persistenza.

pagina
119

47.2.1 Installare il gestore di password

Utilizzeremo il gestore di password KeePassXC. Se non è installato sul nostro sistema, installare il software *KeePassXC* (vedere pagina 134). KeePassXC è installato di default in Tails.

pagina
113
pagina
116

47.2.2 Avviare KeePassXC

Premete  ( su Mac) per aprire la panoramica delle attività, quindi digitate `keepassxc` e fare clic sull'icona di *KeePassXC*.

47.2.3 Creare e salvare un database di password

Un database di password è un insieme di password memorizzate nello stesso database di KeePassXC e crittografate con la passphrase associata.

Se si sceglie di utilizzare KeePassXC in Tails, è necessario prima attivare la persistenza (vedere pagina 116) e abilitare l'opzione *Dati personali*.

Quando si avvia KeePassXC, è necessario creare un nuovo database di password e salvarlo per un uso futuro. Per creare un nuovo database di password, selezionare *Crea nuovo database*.

Per memorizzare il database delle password appena creato per un uso futuro, inserire un nome e, facoltativamente, una descrizione. Quindi fare clic su *Continua*.

È quindi possibile impostare i *parametri di crittografia del database*, che possono essere modificati anche in un secondo momento. Fare clic su *Continua*.

Successivamente, è necessario scegliere una passphrase che verrà utilizzata per decifrare il database delle password. Poiché questo database conterrà alcune delle nostre password, è importante scegliere una buona passphrase (vedere pagina 103). Specificare la passphrase due volte nella casella di testo *Password*.



PER SAPERNE DI PIÙ...

Possiamo anche decidere di *aggiungere un'ulteriore protezione* generando o indicando un *file chiave* composto da byte casuali; tuttavia, dobbiamo mantenere questo file segreto e non perderlo: senza il file chiave, sarà impossibile accedere al nostro database.

Il vantaggio di questa protezione è che possiamo memorizzare questo file chiave su un supporto diverso dal nostro database di password, ad esempio una chiave USB crittografata da tenere in un luogo sicuro. Oltre alla nostra passphrase, dovremo avere con noi questa chiave USB per poter accedere alle password contenute nel database; e chi riesce a indovinare la nostra passphrase non sarà in grado di decifrare il database senza il nostro file chiave.

D'altra parte, il rischio di questa tecnica è quello di smarrire la chiavetta USB contenente il file chiave: se non avessimo fatto una copia di backup del nostro file chiave, saremmo completamente impossibilitati ad accedere al nostro lavoro.

Al termine, fare clic su *Fine*.

Successivamente, è necessario indicare a KeePassXC dove salvare il database. Se si utilizza Tails, la posizione predefinita è la cartella *Persistent*: lasciarla così, in modo che il database venga salvato nel volume persistente di Tails. Altrimenti, scegliere la posizione desiderata per salvare il database. Fare clic su *Salva*.

Poiché conterrà alcune delle nostre password, ricordatevi di eseguire regolarmente una copia di backup (vedere pagina 151) di questo database.

47.2.4 Generare e salvare una password casuale

KeePassXC consente inoltre di generare password casuali più robuste di quelle che si possono ricordare.

In KeePassXC, fare clic su *Voci* e poi © *Nuova voce* Compilare i campi pertinenti. Per il campo *Password*, fare clic sul pulsante a forma di dado (⌘), situato a destra del campo di immissione.

Si apre una finestra contenente varie opzioni di generazione della password.

Tra le opzioni disponibili, è meglio utilizzare lettere minuscole, maiuscole e numeri, quindi aumentare il numero di caratteri della password (ad almeno 32), poiché non sarà necessario ricordarla. I caratteri speciali possono talvolta causare problemi con alcuni programmi software o siti web.

Per selezionare i caratteri desiderati, fare clic sui pulsanti corrispondenti nella sezione *Tipi di carattere*. Quando un pulsante è evidenziato (in verde), la password sarà generata con questo tipo di carattere; quando il pulsante è deselezionato (cioè quando appare in grigio chiaro), i caratteri corrispondenti non saranno utilizzati nella password generata. Facendo clic sull'occhio barrato (👁) a destra della password generata, si rende visibile la password, consentendo di verificare ciò che è stato generato.

L'indicatore *Entropia* misura la robustezza della password generata. È direttamente collegato al tipo di caratteri selezionati e alla lunghezza della password. L'entropia minima consigliata è di 128 bit.

Fare clic su *Conferma password*, quindi su *OK*.

47.2.5 Ripristino e sblocco del database delle password

Se si desidera utilizzare un database di password precedentemente registrato, è necessario sbloccarlo. Per farlo, avviare KeePassXC. In genere, se lo trova, KeePassXC suggerisce automaticamente di aprire l'ultimo database di password utilizzato. Indica quindi *Sblocca database KeePassXC*, seguito dal nome del file corrispondente. Se questo è il database che si desidera aprire, si può saltare il paragrafo successivo.

In caso contrario, o se *KeePassXC* non suggerisce automaticamente un database da sbloccare, andare nel menu *Database*, cliccare su *Apri un database*, quindi

sfogliare l'elenco delle cartelle per trovare il file *.kdbx* corrispondente al database che si desidera aprire. Selezionare questo file e fare clic su *Apri*.

Sia che KeePassXC abbia trovato automaticamente il database da aprire, sia che lo abbiate specificato voi stessi, vi chiederà di sbloccarlo. A tal fine, nel campo *Inserisci password*, inserire la passphrase configurata al momento della creazione del database. Se sono stati definiti altri identificatori per proteggere il database (ad esempio un file di chiavi), anche questi devono essere inseriti qui. Infine, fare clic su *OK*.

Se la passphrase non è corretta, viene visualizzato il seguente messaggio di errore:



Errore di lettura del database: sono stati forniti identificatori non validi, riprovare.
Se il problema si ripete, il file del database potrebbe essere danneggiato.

47.2.6 Utilizzare una password registrata

Una volta ripristinato e sbloccato il database delle password, è possibile utilizzare le password in esso memorizzate.

La password registrata può essere utilizzata in due modi: manualmente, copiando e incollando il nome utente e la password, oppure con l'inserimento automatico.

Ingresso automatico

KeePassXC può registrare "associazioni di finestre", che collegano una voce con il nome di una finestra e con una sequenza di completamento automatico, cioè con le informazioni della voce da digitare direttamente in questa finestra.

A tal fine, è necessario aprire la finestra in cui si desidera eseguire l'inserimento automatico, ad esempio il browser web con la pagina di accesso alla mailbox.

Quindi, cercare in KeePassXC la voce che si desidera utilizzare per questa finestra, quindi fare doppio clic su di essa per modificarla. I campi *Nome utente* e *Password* devono essere compilati. Nella colonna di sinistra, andare su *Completamento automatico*. Assicurarsi che la casella *Abilita il completamento automatico per questa voce* sia selezionata. Fare clic sul simbolo **+** in fondo alla sezione *Associazioni di finestre* per creare una nuova associazione. Dal menu a discesa *Titolo della finestra* sulla destra è possibile scegliere la finestra a cui associare la voce. Cliccare infine su *OK*: le impostazioni sono terminate.

D'ora in poi, è possibile utilizzare la sequenza di inserimento automatico posizionando il focus ¹ nella finestra in cui si desidera inserire i dati di accesso, ad esempio il campo e-mail nel browser della casella di posta elettronica. Passate quindi a KeePassXC su

la voce corrispondente e avviare il completamento automatico. Questo avviene con la combinazione

del  + ² o facendo clic sull'icona della tastiera 

+t

nella barra degli

strumenti superiore.



Attenzione: l'autofill può essere utilizzato anche per commettere errori molto insidiosi, come incollare la password in una finestra di messaggistica istantanea... e inviare il messaggio automaticamente. Fate quindi molta attenzione a dove posizionate il cursore prima di eseguire il riempimento automatico.

Questo metodo di inserimento automatico potrebbe non funzionare per tutti i tipi di interfaccia. In questo caso, è necessario passare all'inserimento manuale.

Ingresso manuale

In KeePassXC, per recuperare il nome utente dagli appunti, andare alla voce che si desidera utilizzare, quindi fare clic con il pulsante destro del mouse e scegliere *Copia nome utente* oppure

combinazione di tasti  . Incollare quindi il contenuto della cartella carta nel campo della finestra in cui inserire il login. Procedere allo stesso modo per copiare la password facendo clic con il tasto destro del mouse sulla voce e scegliendo

Copiare la password o utilizzare il campo   +  e poi inserirlo nella cartella di immissione della password.

1. Il punto in cui appariranno i caratteri successivi durante la digitazione.

2.  è la notazione del tasto shift. Questo tasto si trovano sotto varie notazioni a seconda della tastiera:



Utilizzo di OnionShare

🔄 *Poiché il software si evolve, si consiglia vivamente di usare la versione più aggiornata di questo strumento, disponibile sul sito web <https://guide.boum.org/>.*

🕒 *Durata: Da cinque a dieci minuti.*

Per rendere uno o più file disponibili ad altri, è possibile ospitarli su un server web.

pagina
319

Tuttavia, non c'è alcun motivo *a priori* per fidarsi delle persone o delle amministrazioni che gestiscono questi server.

Se preferite non affidarvi a terzi, potete ospitare voi stessi i documenti che volete condividere e farlo *tramite* un servizio a cipolla.

pagina
266

Uno dei vantaggi di questo sistema è che protegge fortemente la posizione del server di hosting, che in questo caso è il nostro computer. Tuttavia, questo sistema di anonimizzazione non è infallibile.

pagina
267

Per farlo, utilizzeremo il software OnionShare, che in pochi clic consente di creare un servizio Onion e di ospitarvi i file di vostra scelta.

48.1 Utilizzo di OnionShare in Tails

OnionShare è installato di default in Tails. È possibile seguire la documentazione ufficiale di Tails, disponibile presso qualsiasi supporto Tails, anche senza una connessione a Internet.

Avviare prima Tails. Sul desktop, fare doppio clic sull'icona della *documentazione di Tails*. Nell'indice che si apre, cercate la sezione *Internet anonimo e senza censura* e fate clic sulla pagina *Condividi i file con OnionShare* sotto *Applicazioni Internet*. Questa è la pagina da seguire.

pagina
115

48.2 Usare OnionShare in Debian

Se non l'avete ancora fatto, iniziate a installare il software *OnionShare*. Per avviarlo, aprite la panoramica delle attività premendo  (⌘ su Mac), quindi digitate *onion* e fate clic su *OnionShare*.

pagina
131

OnionShare si conetterà *tramite* Tor. Potete lasciare che il software vi guidi scegliendo il file che volete condividere.

817210X
BUG 12378
817210X

Chi parla?

Purtroppo non abbiamo una risposta semplice a questa domanda, ma vorremmo spendere qualche parola al riguardo.

Innanzitutto, ci sono diverse ragioni per cui riteniamo importante pubblicare un libro in forma anonima. Uno di questi, che abbiamo sviluppato nella prefazione, è che alla domanda "Niente da nascondere?", rispondiamo all'unisono "Sì!". L'anonimato è quindi prima di tutto un modo per proteggere noi stessi. Inoltre, abbiamo scelto di non esporci individualmente, per tenere il *chi lontano* dai riflettori e il *cosa sotto i riflettori*.

In secondo luogo, fin dai primi numeri di questa *guida*, il numero di persone che hanno partecipato, da vicino o da lontano, alla sua stesura, correzione e redazione, rende il collettivo che dà vita a questo progetto ampio, in evoluzione e non chiaramente definito.

Infine, riteniamo di aver lasciato in queste pagine tracce sufficienti per consentire a chi legge di collocarci, almeno in parte, nel nostro rapporto con l'informatica, sia essa tecnica, politica o etica.

*

* *

Due caratteristiche di quest'opera, tuttavia, ci costringono ad affrontare le domande sulla sua provenienza da alcuni punti di vista. Da un lato, quest'opera pretende di trasmettere conoscenze tecniche e know-how, solitamente riservati agli specialisti. Dall'altro lato, l'accuratezza delle informazioni fornite può avere implicazioni per la tranquillità di chi le utilizza. Piccoli errori che possono esserci sfuggiti possono avere gravi conseguenze.

È quindi importante spendere qualche parola sulle persone che hanno contribuito a questa guida. Chiarire la portata delle nostre conoscenze e del nostro know-how - e i loro limiti - ci aiuta a trovare un rapporto di apprendimento più appropriato con questo documento, ma anche a decidere il livello di fiducia *tecnica* che merita. Diciamo quindi che, nell'ambito del progetto :

- le questioni sollevate da questa guida sono importanti per noi, sia dal punto di vista tecnico che politico, da oltre un decennio;
- gestiamo laboratori di trasmissione e forniamo consulenza alle persone che necessitano di privacy digitale;
- abbiamo una certa familiarità con il funzionamento di alcuni sistemi o p e r a t i v i , i n particolare Debian GNU/Linux;
- abbiamo una buona base di crittografia, ma siamo ben lontani dal poter affermare di averne la padronanza.

E infine, affermare un'ultima volta che la parola portata da questo libro, come ogni parola *guida*, deve essere presa con le pinzette commisurate alle conseguenze in gioco.

Indice

- CA, *vedere* autorità di certificazione
- amministratori, *vedere*
- amministratori amministratori, **206**
- admins, *vedere*
- indirizzo admins
 - Indirizzo .onion, *vedere* servizio onion Indirizzo IP, **202**, **205**, **217** Indirizzo MAC, *vedere* hardware indirizzo
 - indirizzo fisico, **198**, **215**
 - indirizzo privato, **205**
 - indirizzo pubblico, **205**
- ADSL, **199**
- algoritmo, **48**, **333**
- AMD Platform Security Processor, *vedi* Intel Management Engine
- AMD PSP, *vedere* Intel Management Engine
- anonimato, **243**
- set di anonimato, **268**
- applicazione, **22**
- architettura, **17**
- archiviazione, **89**
- argomento, **98**
- ARPANET, **197**
- AS, *vedere* Sistema autonomo di autenticità, **53**
- self-hosting, **242**, **319**
- autorità di certificazione, **255**, **323**
- backbone, *vedi* backbone
- backdoor, *vedi* libreria
- backdoor, **23**
- binario, **17**
- BIOS, **20**, **76**, **107**, **126**
- bit, **17**
- BitTorrent, **200**
- avvio, *vedere* avvio della casella Internet, **205**, **215**
- scatola nera, **269**
- ponte, *vedere*
- interruttore
- ponte Tor, **267**, **268**, **314**
- bug, **29**
- cache, **43**, **213**
- scheda madre, **16**
- scheda di rete, **198**
- CD o DVD, **171**
- censura amministrativa, **233**, **234**
- certificato elettronico, **255**, **323**
- percorso del file, **98**, **142** Trojan cavallo, **32** crittografia, **47**, **47**, **249**, **347**
 - crittografia end-to-end, **251**, **333**, **343**, **352**
- crittografia ripudiabile, **52** crittografia di un disco rigido, **145**
- crittografia di un sistema, **119**
- crittografia di una chiave USB, **145**
- chipset, **20**
- tastiera virtuale, *vedere*
- tastiera visiva tastiera visiva, **327**
- client di posta, *vedere* client di posta
- client di posta, **292**, **333**
- chiave di crittografia, **48**, **50**, **249**, **333**, **343**
- Codice della sicurezza interna, **32**, **224**, **229**, **237**
- Codice di procedura penale, **31**, **52**
- Codice penale, **51**
- codice sorgente, **39**
- attacco cold boot, **27**, **50**, **75**
- collisione, **53** switch, *vedere*
- riservatezza degli switch, **47**
- cookie, **214**, **222** CPU, *vedi* crittoanalisi del processore, **47**
- crittografia, **47**
 - crittografia asimmetrica, **55**, **249**, **333**
 - crittografia simmetrica, **55**
- crittologia, **51**
- Debian, **22**, **119**

- ispezione profonda dei pacchetti, *vedere* ispezione profonda dei pacchetti
- Déjà Dup, **153**
- avvio, **107**
- deposito di pacchetti, **136**
- dereferenziazione, **234**
- DHCP, **204**
- disco rigido, **18, 42**
- Disco SSD, *vedere* memoria flash, *vedere anche*
 - distribuzio
 - ne dei dischi
 - rigidi, **23, 40**
 - DNS, **210, 232**
 - dominio di primo livello, **232**
 - DPI, *si veda* l'esame approfondito delle pa-
quette
 - plausible deniability, *vedi*
crittografia affidabile
 - deposito di pacchetti, **23**
 - sovrascrittura dei dati, **42**
 - cancellazione, **42**
 - elettricità, **21**
 - impronta, *vedere* intestazione
checksum,
202, 217
 - incapsulamento, **201**
 - registratore di battute, **35**
 - spina dorsale, **208**
 - scambio di sp a z i o n i, v. memoria
vir-
tuale
 - Ethernet, **199**
 - esame approfondito dei pacchetti,
217, 230, 236
 - ext2, ext3 o ext4, **24**
 - Facebook, **222**
 - ISP, *vedere* Internet Service Provider
 - FAT32, **24**
 - fibra ottica, **199**
 - filtraggio, *vedere* filtraggio del
phishing,
236
 - firewall, *vedere* firewall
 - firmware, *vedere* firmware
 - funzione hash, **53, 161**
 - forza bruta, **77**
 - formato di file, **24**
 - formattazione, **24, 44, 146**
 - Provider di servizi Internet, **205, 224**
 - GAFAM, **31, 224**
 - Gestore di macchine virtuali, **84, 163**
 - gestore di password, **355**
 - Gestore di pacchetti Synaptic, **23, 135**
 - GNU/Linux, **22, 40**
 - GnuPG, **49**
 - Google, **221**
 - hash, *vedi* funzione hash phishing, **234**
 - ibernazione, **28**
 - storico, **29**
 - uomo al centro, *vedi* mostro al centro
 - HTTP, **200, 217, 291**
 - HTTPS, **200, 255, 291**
 - sistemazione, **211, 233, 242, 285, 319,**
359
 - identità contestuale, **243**
 - immagine disco, **114, 169**
 - Immagine ISO, **114, 123, 169**
 - IMAP, **200, 292, 331**
 - IMAPS, **200, 255, 292**
 - stampante, **36**
 - installatore, **119**
 - Intel Management Engine, **20, 33** Intel
ME, *vedere* Intel Management Engine.
gine Internet,
205, 209, 239
 - Protocollo Internet, **202**
 - interoperabilità, **199**
 - integrità, **53**
 - IP, *vedi* protocollo
Internet IPv4, *vedi*
protocollo Internet IPv6,
vedi protocollo Internet
IRC, **200, 351**
 - Java, **214, 241**
 - JavaScript, **214, 241**
 - disboscamento, **43**
 - giornali, **29, 215, 216, 218, 224**
 - KeePassXC, **355**
 - keylogger, *vedi* keylogger
 - LAN, *vedi* rete
locale biblioteca,
vedi licenza di
biblioteca
 - licenza libera, **40, 132**
 - licenza di proprietà, **39**
 - linea di comando, **97**
 - elenco autorizzato, **66**
 - elenco
 - bloccato, **66** log,
vedere log del
software, **22, 131**
 - installazione del software, **131**
 - spyware, **32**
 - software libero, **39, 40, 132**
 - malware, **31, 32, 76** software
 - open source, **40** software
 - portatile, **44**
 - software proprietario, **39, 39**
 - leggi, **31**
 - legge per la fiducia nell'economia digitale,
225

- Legge sull'intelligence, **32**
- Legge per rafforzare la lotta al terrorismo
 - criminalità organizzata, terrorismo [...], **31**
- loi renforçant les dispositions relatives à la lutte contre le terrorisme, **52**
- LOPPSI2, **231**
- requête légale, *vedi* réquisition judiciaire
- LUKS, **50, 145**
- MAC, *vedi* indirizzo hardware
- macchina centrale, *vedi* mostro centrale
- macchina-in-the-middle, *vedi* mostro malware in the middle, *vedi* software dannoso
- uomo al centro, *vedi* mostro al centro
- MAT2, **185**
- memoria
 - memoria flash, **18, 20, 42, 140**
 - memoria di sola lettura, *vedere*
 - memoria per-memoria
 - persistente sistante, **18**
 - memoria virtuale, **25, 28, 44, 73**
 - memoria vivente, **18, 27**
- messaggistica istantanea, **351**
- metadati, **30, 218, 221** microcodice, *vedere* firmware, *vedere* firmware, **20, 76, 107, 120** aggiornamento, **175**
- modem, **199, 205**
- modem-router, *vedere* modello di
- minaccia Internet box, **63**
- mostro al centro, *vedi* mostro al centro
- mostro nel mezzo, **254**
- password, **41, 355**
- NAT, **205**
- neutralità della rete, **207**
- nome di dominio, **210, 232**
- nucleo, **22**
- NTFS, **24**
- digitalizzazione, **17**
- Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, **231, 233**
- cipolla, **261, 313**
 - .cipolla indirizzo, *vedere*
- Servizio OnionShare, **359**
- servizio cipolle, **266, 326, 331, 359**
- onde, **21**
- open source, **40**
- OpenPGP, **333, 343**
- opzione, **98**
- OS, *vedi* sistema operativo OTR, **351**
- Outlook, *vedi* client di posta
- kpeayckpaagier, **60, 135**
- pacchetto (rete), **202, 217**
 - firewall, **203**
- punteggio, **23**
- peering, **207**
- periferica, **20**
- phishing, *vedi* phishing
- passphrase, **47, 103**
- Pidgin, **351**
- pilota, **22**
- punto di accesso, **204**
- politica di sicurezza, **65** bridge, *vedere* switch Tor bridge, *vedere* bridge Tor POP, **200, 292, 331**
- SCHIOPPI, **200, 255, 292**
- porta, **203**
- portale vincolato, **216**
- porta posteriore, **39, 216**
- forriell, **31, 32, 296**
- processore, **16**
- programma, **22**
- protocollo
 - protocollo applicativo, **200, 217**
 - protocollo di comunicazione, **199**
 - protocollo IP, *vedi* Internet Protocol
 - collare
 - protocollo di rete, **202, 217**
- pseudonimato, **243**
- radio, *vedi* Wi-Fi
- RAM, *vedere* requisizione giudiziaria RAM, **51, 228**
- requête légale, *vedi* réquisition judiciaire
- rete locale, **204**
- rischi
 - valutazione del rischio, **63**
 - riduzione del
- rischio, **61** RJ-45, *vedere* Robot Ethernet, **296**
- rootkit, **32**
- instradamento, **208**
- router, **205, 207, 208, 217** VPN, *vedere* VPN
- Rete privata virtuale, *vedere*
- Conservazione dei dati VPN, **224**
- backup, **151**

- backup automatici, **29**
- cancellazione sicura, **139**
- triturare, **142**
- Segnale, **200**
- firma digitale, **55, 345**
- firma steganografica, **36**
- sito specchio, **231**
- Skype, **201**
- SMTP, **200, 291, 331**
- SMTSP, **200, 255, 291**
- checksum, **53, 161** spam,
vedere spam spyware,
vedere spyware
- SSD, *vedere* memoria *flash*, *vedere*
anche
 - Disco
 - rigido SSL, *vedere*
 - TLS
- archiviazione web locale, **214**
- steganografia, **36**
- superficie di attacco, **66**
- scambio, **25, 28**
- interruttore, **204**
- Synaptic, *vedi* gestore di pacchetti
 - Synaptic
- sintassi, **98**
- sistema autonomo, **206**
- file system, **24, 43**
- sistema operativo, **22** installazione
del sistema, **119** sistema host,
84
sistema ospite, **84**
sistema *live*, **22, 44, 82, 113, 113**
- Coda, **44, 82, 113, 175, 267, 280, 295,**
301, 327, 343, 359
- memorizzazione persistente, **151, 356**
- TCP, **202**
- terminale, **97**
- Thunderbird, *vedi* clienti di posta
- TLD, *vedere* dominio di primo livello
- TLS, **255, 258**
- dominio di primo livello, *vedi*
dominio di primo livello
- Tor, **261, 313**
- tracce, **27, 213**
- transistor, **17**
- transito, **207, 209**
- TrueCrypt, **40**
- UDP, **202**
- UEFI, **20, 76, 126, 128**
- aggiornamento, *vedere* Aggiornamento
- USB,
20
- vigilia, **28**
- VeraCrypt, **52**
- Virtual Private Network, *vedere*
- virtualizzazione VPN, **83, 163**
macchina virtuale, **212**
virtualizzazione hardware, **164**
- virus, **32**
- VPN, **227**
- watermarking, *vedi* firma stegano-grafica webmail, **291**
- WebRTC, **215**
- Wi-Fi, **199, 204**
- Finestre, **82, 165**
- cancellare, *vedere* sovrascrittura dei dati
- XMPP, **200, 351, 352**

Crediti

Copertina, quarta di copertina e disegni alle pagine **i**, **xvi**, **8**, **188** e **360** realizzati dal team della Guida digitale all'autodifesa.

Foto pagina **16** di Darkone, licenza CC BY-SA 2.5, trovata su:

https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:ASRock_K7VT4A_Pro_Mainboard.jpg.

Foto pagina **16**, di pubblico dominio, trovata su:

<https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:Pentium-60-back.jpg>.

Foto pagina **18**, di Topory, licenza CC BY-SA 3.0, trovata su:

https://fr.wikipedia.org/wiki/M%C3%A9moire_vive#/media/Fichier:RAM_n.jpg.

Foto pagina **18**, di pubblico dominio, trovata su:

<https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:Hdd-wscsi.jpg>.

Foto pagina **19**, dominio pubblico, trovata su:

https://commons.wikimedia.org/wiki/File:MSATA_SSD_16_GB_Sandisk_-_SDSA3DD-016G-2494.jpg.

Foto pagina **20** di Zac Luzader Codeczero, licenza CC BY 3.0, trovata su:

https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:AT_Motherboard_RTC_and_BIOS.jpg.

Disegno a pagina **77** di XKCD, licenza CC BY-NC 2.5, trovato su: <https://xkcd.com/538/>.

Foto pagina **199** di David Monniaux, licenza CC BY-SA 3.0, trovata su:

https://commons.wikimedia.org/wiki/File:Ethernet_RJ45_connector_p1160054.jpg.

Foto pagina **207** di Geek2003, licenza CC BY-SA 3.0, trovata su:

https://commons.wikimedia.org/wiki/File:Avaya_Secure_Router_2330.jpg.

Foto pagina **211** di Victor Grigas, licenza CC BY-SA 3.0, trovata su:

https://commons.wikimedia.org/wiki/File:Wikimedia_Foundation_Servers-8055_08.jpg.

Diagramma pagina **263** di HANtwister, licenza CC BY-SA 3.0, trovato su:

https://en.wikipedia.org/wiki/Onion_routing#/media/File:Onion_diagram.svg.

Diagrammi alle pagine **264**, **265**, **265** e **266** di Nos Oignons e Electronic Frontier Foundation, licenza CC BY, trovati su :

<https://nos-oignons.net/Diffusez/index.fr.html>.

Icone di testo basate su Font Awesome 4 di Dave Gandy, licenza SIL OFL 1.1 (<https://fontawesome.com/v4/>).

Icona "per andare oltre" di Mr Minuvi di The Noun Project; icona "contenuto della finestra" di Gregor Cresnar di The Noun Project; icona "testo di legge" di Handicon di The Noun Project; icona "dettagli" di Coloureatype di The Noun Project: Licenza CC BY 3.0 (<https://thenounproject.com/>).

Gli altri diagrammi sono stati realizzati dal team della guida e utilizzano le icone: da GNOME Project, licenza CC BY-SA 3.0; da Silvestre Herrera, licenza GPLv2, reperibile su <http://>.

www.silvestre.com.ar/; dal pubblico dominio, all'indirizzo <https://openclipart.org>.