Cripto libretto

Unit hacklab - unit@paranoici.org

24 Gennaio 2019

Contents

1 Per una corretta igiene digitale

2 Usiamo software libero e a sorgente aperta

https://gnu.org/philosophy/free-sw.it.html

3 Una buona password

Non usare la stessa password per diversi servizi.

Usa una passphrase, ossia una frase di accesso compresa di spazi, facile da ricordare, ma difficile da indovinare persino per un computer, ad esempio questa contiene sia maiuscole che numeri che caratteri buffi. È molto lunga, ma è difficile da dimenticare.

```
Nel Mezzo Del Cammin Di Nostra Vita 19!
```

4 Il password manager

Le password da ricordare sono troppe, KeePassX è un software per la gestione di password che offre un luogo sicuro dove scriverle, ma non dimenticare la password principale.

https://keepassxc.org

```
apt-get install keepassxc
```

5 Accecare la telecamera del portatile

Attaccare un pezzo di scotch nero da elettricista sulla telecamera del portatile. Il fatto che non si accenda la lucina non significa che sia spenta.

6 Navigazione consapevole

Usiamo Firefox.

La gestione dei containers e dei profili ci permettono di creare ambienti isolati

Multi-account-containers è un componente aggiuntivo (add-on) per creare schede contenitore (tab) e compartimentare le preferenze del sito, le sessioni registrate e i dati di tracciamento. Un sito non avrà dunque accesso ai dati (cookies) delle altre tab aperte. Questo permette di separare facilmente il lavoro dalla navigazione personale.

I Profili sono delle diverse sessioni del browser, per compartimentare anche gli add-on, si possono aprire scrivendo nella finestra di navigazione:

`about:profiles`

Add-ons:

- multi-account containers
- https-everywhere: preferisce https a http
- ghostly: blocca i tracker della nostra navigazione
- no script: blocca gli script
- ublock origin: blocca la pubblicità

7 Navigazione anonima

Tor, **T**he **O**nion **R**outer è un protocollo per l'anonimizzazione del traffico web. Scaricare, installare e usare il programma Tor browser bundle per navigare in rete anonimamente.

https://torproject.org

Attenzione. Non presumere che il tutto funzioni per magia. Studia, prova, chiedi.

8 Navigazione paranoica

Tails è un sistema operativo smemorato, amnesiac e incognito. Si installa e si avvia da penna Usb con un sistema GNU/Linux già configurato per la navigazione anonima e cambia il MAC address, l'identificativo univoco assegnato all'interfaccia di rete. Una volta spento non ricorda nulla di quello che è successo. In altre parole usa Tor per navigare in internet e permette di usare un computer in prestito senza doverci installare nulla né lasciarvi tracce dell'utilizzo. Utile in viaggio e in zone di guerra. Decidi tu in che zona vivi.

L'installazione di Tails si basa sul sistema della rete di fiducia. Ad esempio se conosci qualcun* che lo usa, basterà installare Tails su una penna Usb vuota partendo dalla sua Tails.

https://tails.boum.org/index.it.html

9 Usare un sistema operativo libero

Usiamo GNU: software libero o almeno a sorgente aperta, il quale viene raccolto e assemblato assieme al kernel Linux per formare un sistema operativo in quella che viene chiamata distribuzione. Ogni distro ha il suo perché. Noi ne elenchiamo tre:

- Linux Mint: https://linuxmint.com

Un desktop familiare. Facile da usare e da installare. Il nonno lo usa e non ha mai chiamato per fare domande. Può avviarsi direttamente da Cd o da Usb (live). Preferisce un computer moderno con almeno 4Gb di Ram. Basata su Debian e Ubuntu.

- Bunsenlabs: https://www.bunsenlabs.org

Minimale, leggera e funzionale. Buona sia per un pc moderno che non. Erede della distro Crunchbang. Usandola si imparano cose utili. Live. Basata su Debian.

- Debian: https://www.debian.org

Il sistema operativo universale. Sapendo già cosa si vuole è la miglior cosa.

9.1 Scaricare e installare una distribuzione GNU/Linux

Ad esempio Debian. Dal sito individuare e scaricare l'immagine. Mentre scriviamo la più recente è la 9.6. Per un comune computer moderno usare amd64. Verificare la checksum e masterizzare l'immagine su di un Cd, Dvd o penna Usb.

Inserire la penna Usb e scoprire dove è stata montata

```
ls -l /dev/disk/by-id/*usb*
```

Nell'esempio che segue la penna è in /dev/sdb, copiarvi Debian:

il contenuto della penna sarà cancellato

```
dd if=debian-9.6.0-amd64-netinst.iso of=/dev/sdb bs=4M; sync
```

Riavviare il Pc dalla penna Usb tenendo premuto **F12**

Se il Pc non avvia automaticamente dalla penna, entrare nel Bios e scegliere Usb come dispositivo d'avvio. A seconda del modello tenere premuto all'avvio uno di questi tasti: ESC, DEL, F1, F2, F8, F10. Una volta nel Bios, editare l'ordine di avvio mettendo per prima la penna Usb.

Nella procedura di installazione si verrà guidati a scegliere la lingua da usare, la zona geografica, il nome del Pc, la rete e la creazione dell'utilizzatore. Durante la partizione guidata formattare l'intero disco senza complicazioni. In conclusione installare Grub bootloader nel Master Boot Record.

Il disco del Pc verrà formattato e cancellato, non ci saranno altri sistemi operativi oltre a GNU/Linux Debian. È possibile effettuare al momento dell'installazione scelte diverse per casi particolari

È possibile durante l'installazione crittografare l'intero disco e in questo caso si dovrà mettere una passhprase ad ogni avvio, in aggiunta alla password di login. Consigliabile per un portatile, in caso venga smarrito non ci si dovrà preoccupare della perdita dei dati. Ricordare che senza la passphase non è possibile accedere al disco.

9.1.1 Migrare la posta di Thunderbird da quel sistema a GNU/Linux

Prima di cominciare fare un backup zippando la cartella di Thunderbird,

Poi compattare le cartelle di Thunderbird

`Thunderbird: Menu > File > Compact Folders`

Infine copiare il profilo da un pc all'altro. Il profilo si trova, a seconda per Gnu/Linux, MacOSX, WindowsXp, Windows7, in:

```
/home/tu/.thunderbird/[nome profilo]
/Users/tu/Library/Thunderbird/Profiles/[nome profilo]
C:\Documents and Settings\tu\Application Data\Thunderbird\Profiles
C:\Users\tu\AppData\Roaming\Thunderbird\Profiles\[nome profilo]
```

In caso di problema, far partire thunderbird con profile manager e sistemare:

`thunderbird -profilemanager`

Se il problema persiste:

Chiudere e riaprire

Controllare i permessi

Verificare il path in ./thunderbird/profiles.ini

```
nel mac era: Path=Profiles/76gighirz.default
su debian è: Path=76gighirz.default
```

Cancellare questi files che comunque si rigenerano da soli

```
compreg.dat
extensions.cache
extensions.ini
extensions.rdf
pluginreg.dat
```

10 GnuPG, la crittografia pesante a doppia chiave

Gnu Privacy Guard https://gnupg.org è la versione libera del software di crittografia asimmetrica Pgp, Pretty Good Privacy.

Si usa per cifrare, cioè per nascondere il contenuto di un messaggio. E per firmare, cioè per autenticare un messaggio. Dunque anche per decifrare e per verificare una firma.

Il suo scopo è permettere una comunicazione sicura tra persone che non si sono incontrate di persona e frustrare chi intercetta i messaggi ma non ha la chiave per decifrarli.

10.1 Installazione

Si può usare da terminale o con la grafica, in entrambi i casi si vorrà integrarne l'uso con l'email, dunque *gpg+mutt* o *gpg+enigmail+thunderbird*.

Installare GnuPG, il client di posta grafica e il suo plugin (che può gestire Gpg fin dalla creazione delle chiavi)

```
apt-get install gnupg thunderbird enigmail
```

10.2 Configurazione e creazione delle chiavi

```
gpg --gen-key
```

oppure

```
Aprire thunderbird > enigmail
```

Creare la coppia di chiavi, indicando una email, assegnando una passphrase e specificando una scadenza. Otterremo una chiave pubblica (pubkey) e una chiave privata (privkey). La privkey viene conservata privatamente, la pubkey viene divulgata liberamente.

10.3 Uso

- Si usa la propria privkey per firmare un documento o una email
- Si usa la pubkey di qualcun* per verificare la sua firma al messaggio
- Si divulga la propria pubkey perché il nostro corrispondente possa scriverci segretamente
- Si ottiene la pubkey del nostro corrispondente per scrivergli segretamente
- Si usa la propria privkey per decifrare un messaggio a noi indirizzato
- Si usa la pubkey di qualcun* per cifrare un messaggio ad ess* destinato

Solitamente si invia un messaggio segreto sia cifrandolo che firmandolo ed è ragionevole aspettarsi di ricevere dei messaggi segreti firmati, ma quando non si vuole nascondere il contenuto ma solo avere la certezza di stare dialogando con la persona giusta, si firma solo.

La crittografia a doppia chiave è semplice, ma non è facile. Usarla nel quotidiano permette di sperimentare e capire attraverso la pratica. Trovare un corrispondente

Una guida con infografiche: https://emailselfdefense.fsf.org/it

10.4 Verifica

Ogni coppia di chiavi ha una fingerprint che la identifica univocamente. È buona pratica, prima di inserire la chiave nella nostra rete di fiducia, chiedere alla persona con cui voglio corrispondere di leggere al telefono la sua fingerprint per verificare che corrisponda con quella della pubkey che ci siamo scambiat*. E viceversa. Gpg è una rete sociale.

10.5 Fingerprint, revoca e backup

Ottenere la fingerprint di una chiave

```
gpg --fingerprint [email o Key-ID]
```

È meglio creare subito un certificato di revoca delle chiavi

```
gpg -o ~/.gnupg/RevocaCertificato.asc --gen-revoke [fingerprint]
```

Fare un backup della cartella nascosta .gnupg da conservare altrove con cura

```
tar -zcpf ~/backup-gnupg.tar.gz ~/.gnupg
```

È possibile usare una penna Usb cifrata con VeraCrypt per contenere il backup di gpg e altri dati importanti come le mailbox.

11 VeraCrypt, il lucchetto alla penna Usb

VeraCrypt è un software che permette di proteggere con una passphrase una penna Usb. Utile per trasportare dei documenti in viaggio senza preoccuparsi di perderla.

Durante la configurazione la penna verrà formattata e sarà sempre necessario usare VeraCrypt per montarla e accedere al contenuto.

https://veracrypt.fr

12 Verificare l'integrità di un software scaricato

Alcuni software sono distribuiti accompagnati dal risultato della somma di controllo (checksum) oppure da una firma digitale a lato (.sig) e la sua fingerprint.

Verificare che la stringa alfanumerica univoca (hash) che risulta applicando l'algoritmo sha256 coincida con quella pubblicata

```
openssl sha256 debian-9.6.0-amd64-netinst.iso
c51d84019c3637ae9d12aa6658ea8c613860c776bd84c6a71eaaf765a0dd60fe
```

Verificare una firma

```
gpg --import VeraCrypt_PGP_public_key.asc
key 821ACD02680D16DE: public key "VeraCrypt Team" imported
(è stato troncato ciò che non interessa all'esempio)

gpg --fingerprint VeraCrypt
```

```
5069 A233 D55A 0EEB 174A  5FC3 821A CD02 680D 16DE
(coincide con la fingerprint pubblicata sul sito?)

gpg --verify veracrypt-1.23-setup.tar.bz2.sig
Good signature from "VeraCrypt Team"
(Bene. Il warning indica solo che non ho firmato la chiave)
```

Non è necessario firmare una chiave per usarla. Firmarla serve a ricordare (e nel caso si usi il web of trust, a dichiararlo al mondo) che ci si fida di quella chiave. È giusto farlo dopo averla verificata con una telefonata. P.S. non chiamare al telefono Debian, tantomeno all'ora di cena.

13 Collegarsi a un pc usando ssh con scambio di chiavi

Nella crittografia asimmetrica quando si usa una passphrase per sbloccare una chiave, la decrittazione avviene in locale, perciò la passphrase non viaggia per internet. Questa viene chiamata cifratura *end to end* ed è più sicura.

Creare la coppia di chiavi per collegarsi al pc

```
ssh-keygen -b 8192 -t rsa -f chiave
```

Caricare sul pc la chiave pubblica e rinominarla in ~/.ssh/authorized_keys con i giusti permessi

```
cat chiave.pub | ssh tu@pc "mkdir -p ~/.ssh && \
chmod 700 ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

Avviare ssh-agent e usare la chiave privata

```
eval `ssh-agent` ; ssh-add chiave
```

Collegarsi al pc

"tu" è il nome utilizzatore e "pc" è il nome o l'indirizzo IP della macchina remota

```
ssh tu@pc
```

Dopo verifica sarà possibile disabilitare sul pc l'accesso ssh via password specificando *PasswordAuthentication no* in */etc/ssh/sshd_config*

14 Self hosting con Nextcloud

Per avere una copia di riserva dei propri dati, sincronizzare una rubrica e un calendario con un dispositivo mobile e condividere documenti non è obbligatorio usare i servizi commerciali, i quali non sono gratuiti, ma costano in libertà. Quando i nostri dati vengono sparpagliati e utilizzati come risorse per creare profitto, subiamo un danno all'integrità del nostro *mio* digitale. Self hosting significa gestire autonomamente uno spazio digitale. Si può fare in gruppo e collettivizzare le risorse e i costi. È meno facile che usare i servizi commerciali.. ma no, è il paragone che non regge. La guida per fare un orto verticale non deve giustificarsi dicendo che è meno facile che andare al supermercato.

Installare e configurare Nextcloud (con mariadb, apache2, php7, ufw e fail2ban) su una VPS o un Pc, con già Debian 9

```
apt-get install curl
```

```
curl -sSL https://raw.githubusercontent.com/ \
nextcloud/nextcloudpi/master/install.sh | bash
```

Conservare le password e seguire le info di post installazione

https://github.com/nextcloud/nextcloudpi/wiki

Se si ha un (sub)dominio a disposizione si può ottenere da LetsEncrypt un certificato SSL

```
ncp-config
```

Configurare nextcloud creando gli utilizzatori e attivare calendario, rubrica e quel che serve.

15 Mettere un software in scatola

Per mettere un software dentro una scatola (sandbox) usare firejail. Utile per far girare un software del quale non ci si fida, limitandolo in un ambiente chiuso dal quale non potrà uscire, per evitare che faccia danni al sistema

```
apt-get install firejail
```

Mettere in scatola firefox, in modo che lo script di un sito non possa accedere al disco. Notare che non sarà possibile caricare una foto dal disco alla rete, perché firefox non potrà accedere al disco

```
firejail firefox
```

Ad esempio mettere in scatola vlc ed impedirgli di collegarsi in rete

```
firejail --net=none vlc
```

https://firejail.wordpress.com

16 Comunicazione sicura dal telefonino

Premessa: consideriamo che gli smartphone sono insicuri per definizione.

- **Signal.org** è una app per comunicare privatamente
- **Conversations.im** è una app per comunicare privatamente con protocollo federato
- **lineageos.org** è un sistema operativo per telefonini basato su Android

Il progetto **Privacy matters on my phone** affronta il discorso privacy su smartphone per livelli

https://unit.abbiamoundominio.org/pmomp

17 Backup incrementale sicuro e remoto con duplicity

Usando duplicity, ssh e gpg si può crittografare un backup e conservarlo in modo sicuro su un pc remoto. Attenzione a conservare a parte una copia della

chiave gpg che serve per il recupero

```
apt-get install duplicity
```

In questo esempio avviene un backup della Home, con scambio chiavi ssh, definendo la chiave gpg da usare per la cifratura, con esclusione della cartella *Downloads*, sul pc chiamato *pc*, nella directory *backup* dell'utilizzatore con lo stesso nome, in questo esempio chiamato *tu*.

Nei giorni successivi usare stesso comando per eseguire un backup incrementale

```
duplicity --use-agent --encrypt-sign-key [Key-ID] \
--exclude ~/Downloads $HOME/ sftp://tu@pc//home/tu/backup
```

Verificare il backup

```
duplicity verify -v9 sftp://tu@pc//home/tu/backup /home/tu
```

Recuperare il backup nella cartella *recupero*

```
mkdir recupero
duplicity sftp://tu@pc//home/tu/backup /home/tu/recupero
```

Esiste un front-end grafico di duplicity, chiamato Deja Dup

```
apt-get install duplicity deja-dup
```

18 Risorse

Autistici/Inventati offre ad attivisti, gruppi e collettivi piattaforme per una comunicazione più libera e strumenti digitali per l'autodifesa della privacy, come per esempio email, blog, mailing list, instant messaging e altro.

https://www.autistici.org

19 Link

Liberati dai programmi globali di sorveglianza

https://prism-break.org/it

20 Consigli

Il computer non ha un cervello, usa il tuo,

e non fidarti troppo di chi ti dà consigli.

21 Storia

Il criptolibretto nasce dentro Unit hacklab per avere un pieghevole da distribuire come promemoria e appunti al cryptoparty organizzato in Macao a Milano il 15 aprile 2018. Continua con l'intento di essere un sintetico supporto aggiornato perché la causa della libertà nel 21esimo secolo è inestricabilmente connessa alla resistenza alla sorveglianza elettronica.

Il metodo (DIY) per la creazione del libretto può essere utilizzato da singole o gruppi per fare e pubblicare autoproduzioni. Nel caso, fatecelo sapere!

Questo (cripto) libretto è stato scritto e impaginato usando software libero (LaTeX)

- Scrittura usando sintassi markdown
- Conversione in pdf usando pandoc
- Conversione in PostScript con ghostscript
- Foliazione (signature) effettuata con psbook
- Scala delle pagine da A4 ad A5 usando psnup
- Automazione usando make

Il sorgente è disponibile:

https://git.abbiamoundominio.org/unit/criptolibretto

unit hacklab, Milano 2019