PGP, UNA CONFIDENZIALITÀ ABBASTANZA SICURA

Ignifugo - HOD 2022

TEMPI E TEMI

- breve storia generale e perchè
- DEMO creazione chiavi PGP usando Tails

COSA NON QUI, MA CERCATELE:

- RSA - Rivest, Shamir e Adleman(1976)
- Diffie-Hellman (1977)
- AES - Advanced Encryption Standard (1997)

https://it.wikipedia.org/wiki/Portale:Crittografia

E DIVULGATE! B)


crypto keys
diffie hellman public keys exchange* is about sharing a secret without sending it over the wire!
sends prime p and its primitive root g
* it uses the power of modular arithmetics where two different integers divided by the same number give the same remainder
server calculates g^a modulo p
client calculates g^b modulo p
public server key
public client key
calculates the module p of the client public key^b
send over the wire
calculates the module p of the server public key^a
same remainder
same remainder
* a and b are integers reused in each operation
* the module operation finds the remainder of an integer divided by another
remainder becomes the common secret to secure further communication!

PGP (1991)

https://it.wikipedia.org/wiki/Pretty_Good_Privacy

CHE SERVE?

- firma
  - verifica integrità
  - verifica identità
- cripta
  - intimità
  - confidenzialità

Anche su canali non sicuri (e2e)

TIPS

- cifratura ed anonimato sono due cose molto diverse
- cifrare è solidarietà
- dopo è troppo tardi
- non chiuderti fuori da sol_

TIPS

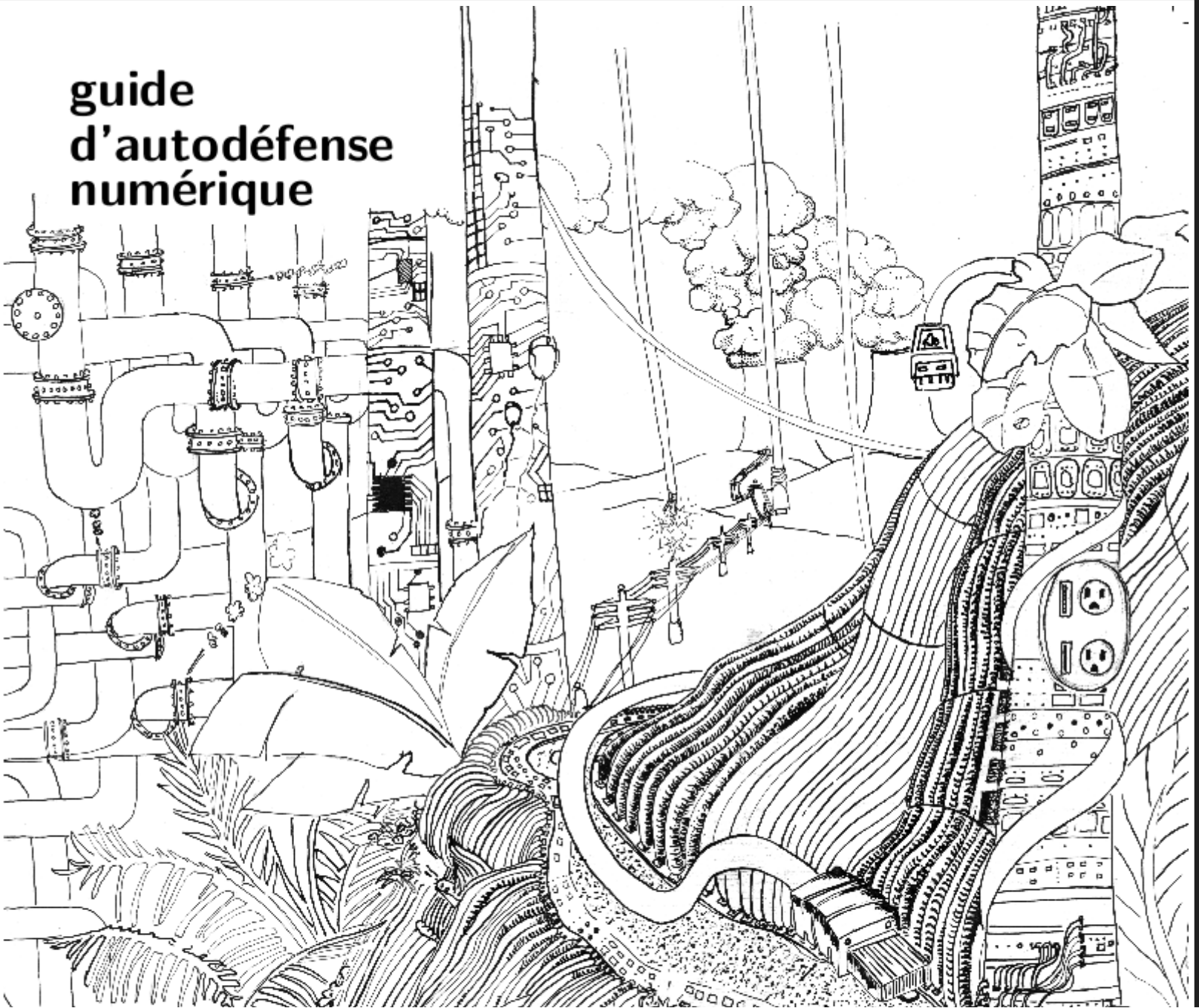
- questo talk non ti basta
- fai dei periodi o ambienti di test
- la lunghezza della chiave conta (>4096bit)
- backups (privata e revoca)
- metti le scadenze vicino a qualche data che ricordi!

https://it.wikipedia.org/wiki/RSA_(crittografia)

TIPS

- diverse chiavi per diverse cose
- passfrase forti
- calcola la Web of Trust

guide d'autodéfense numérique



guide d'autodéfense numérique

Volume 1 - escluse le connessioni

Alcune nozioni di base sui computer

Cominciamo dall'inizio.

Un *computer* non è un cappello da mago dove riporre i conigli e portarli fuori quando ne hai bisogno, e che permetterebbe, premendo il tasto destro, di avere una finestra aperta dall'altra parte del mondo.

Un computer è costituito da un insieme di macchine più o meno complesse, collegate tra loro da connessioni elettriche, cavi e talvolta onde radio. Tutto questo *materiale* immagazzina, trasforma e replica i segnali per manipolare le informazioni che possono essere visualizzate su un bellissimo schermo con molti pulsanti su cui fare clic.

Capire come si articolano questi componenti principali, capire le basi di ciò che fa funzionare tutto, questo è il primo passo per capire dove sono i punti di forza e di debolezza di queste macchine, a cui affidiamo molti dei nostri dati. .

LA SICUREZZA È UN PROCESSO

PGP È IL CRIPTOSISTEMA PIÙ USATO AL MONDO E PROBABILMENTE IL PIÙ VICINO ALLA CRITTOGRAFIA DI LIVELLO MILITARE

NON SI PUÒ ESSERE SICUR_ SENZA CAPIRE COME FUNZIONA


Utente
Applicazione
Sistema operativo
Hardware

CATENA DI FIDUCIA DEL SOFTWARE:

- progetto / blueprint o whitepaper
- codice
- software compilato
- distribuzione

APPLICAZIONI "MODERNE" CON PGP

- conversazioni sensibili via mail
- password manager (segreti di gruppo)
- ansible vault (configurazioni di server)
- OpenPGP (2007) - (volendo in 2fA)
- release di software pacchettizzato

TAILS

THE AMNESICO INCOGNITO LIVE SYSTEM

- partizione cifrata
- portatile
- rete anonimizzata (TOR)
- o amnesico o partizione cifrata, per volta

VEDIAMO DI

- verificare l'immagine
- creare una chiave OpenPGP
- vederne i dettagli con gpg da cli

- https://tails.boum.org/install/linux/index.it.html
- https://tails.boum.org/install/expert/index.en.html

BIBLIOGRAFIA:

- https://numerique.noblogs.org 2020-21
- https://guide.boum.org 2017
- https://git.lattuga.net/cisti/facciamo
- https://tails.boum.org
- https://digitalfirstaid.org/en/
- https://www.accessnow.org/cms/assets/uploads/2019
  Security-Start-Booklet-digital-Aug2019.pdf