Tekno-juni

OPSec opstart

OPSec

Operations security kan tænkes som en række af overvejelser og praksisser som man gøre sig for at forsøge at garantere (informations-)sikkerheden af en aktivitet overfor fjendtlige aktørere.

- Forsvars strategier og metoder
- Trussels modeller, *threat actors*, praksisser og protokoller

Hvorfor kan det være relevant for dig?

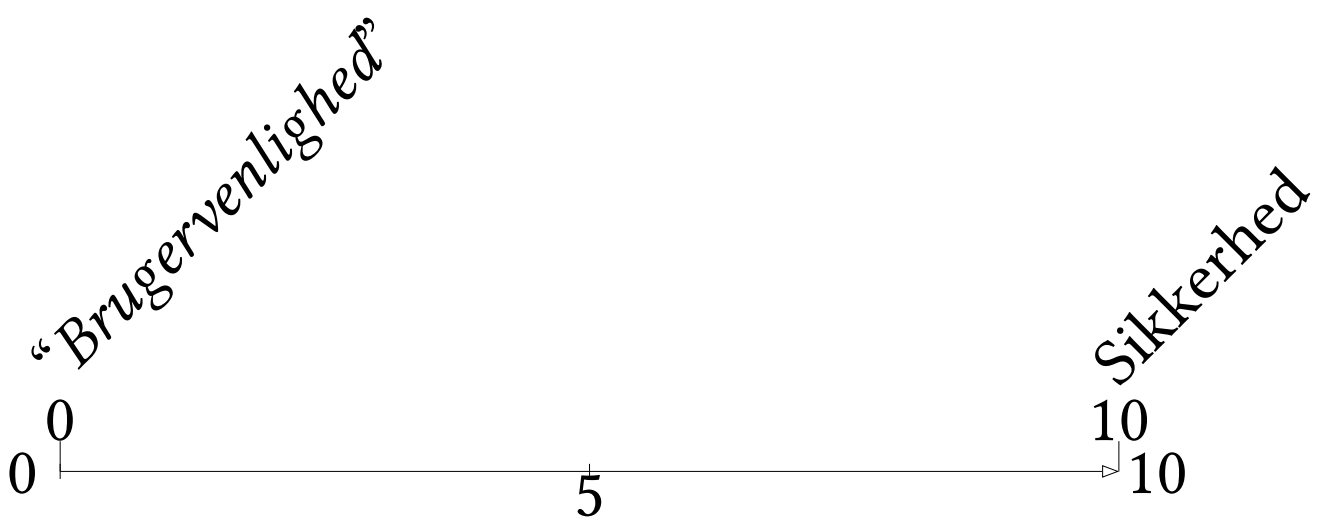
- Omgørelsen af Roe V. Wade og cyklus-app
- Aktivistisk og politisk engagment gavner af muligheden for privatliv og undgåelsen af overvågning
- Du vil have kontrol over din egen data[1]

Data akkumulation og profil opbygning

[1]Eks. kan der være ting som du synes ikke rager andre end dine venner.

Trussels modeller - din, min, vores

- **hvad** skal jeg holde hemmeligt?
- **hvem** skal jeg holde det hemmeligt fra?
- **hvilke** risikoer/ulejligheder er jeg villig til at tage?



Software og kildekode

Closed source	Open source
Kildekoden er privat-ejet og utilgængelig for brugeren	Kildekoden er tilgængelig for brugere til at modificiere, redistribuere og bruge
Licenser som EULA, og er under copy-right	Er licenseret under enten en permissive eller defensiv licens,[1] og er eksempler på copy-left

[1]Gnu Public License (GPL) er et eksempel på en defensiv licens som garantere at alle kopiere af koden forbliver under samme licens, mens at permissive licenser tillader ændring af licensen.

Enkryption

Hemmeligholdelsen af information ved at konvertere information fra *plain text* til *cipher text*, således at kun de tiltænkte kan få adgang til informtionen ved dekryption.

Symmetrisk	Asymmetrisk
Eks. en passphrase, p	Public-Private keypair $\text{keypair} = (\text{pub}; \text{private})$
Enkryption og dekryption er bundet til en værdi	Opdeling af processer

Symmetrisk	Asymmetrisk
	Enkryption, signature og validering

End-to-end enkryption

Mange ting er idag krypteret mellem bruger og server,[1] men det som man skal holde øje med er om det krypteret *end-to-end*.

- Fra afsender til modtager enkrypteret hele vejen.
- Værktøjs eksempel:
  - GPG oven på email
  - signal, simplex, briar

[1] De fleste web-tjenester idag bruger alle https til at garantere sig selv mod man-in-the-middle angreb.

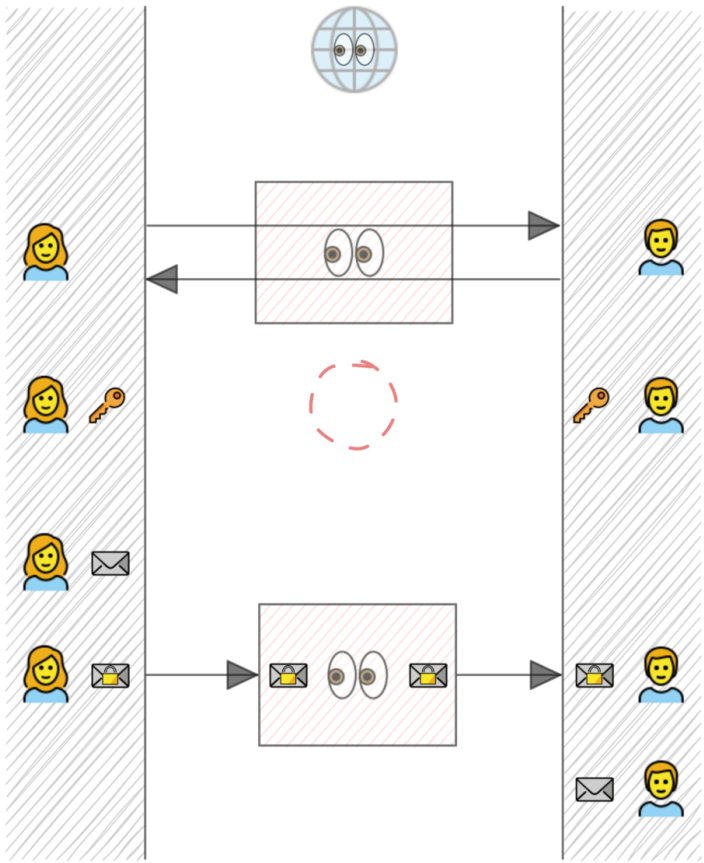


Figure 1: Wikipedia's illustration af e2ee.

Data

Stationær	Transit
Lokal data på harddrives og devices.	Data der transporteres mellem devices.
Enkryption af harddrives og filer	End-to-end enkryption
Fysisk angreb (tyveri)	Man-in-the-middle (MITM)[1] og *compromised* modtager

[1] I tilfælde af at man ikke har kunne bekræfte med sin modtager offline eller på en sikker kanal, kan man være i risiko hvis platformen agere malicious.

Metadata

Data om anden data. I tilfælde af tjenester med en central aktør eks. signal og protonmail:

- Tidspunkter, IP-addresser, modtager og afsender

Minimere mængden af metadata:

- Brug af overlay netværk (eks. Tor, VPN)
- Tjenester uden krav for konto oprettelse
- Peer-to-peer eller multi-node systemer[1]

[1]Her er det et tilfælde af at gøre det svære for en enkelt observatør at danne sig et overblik, hvis flere noder er i *kahoots* eller samarbejder kan de få adgang til at danne sig en metadata profil som fra centrale tjenester.

Fysisk sikkerhed og *threat actors*

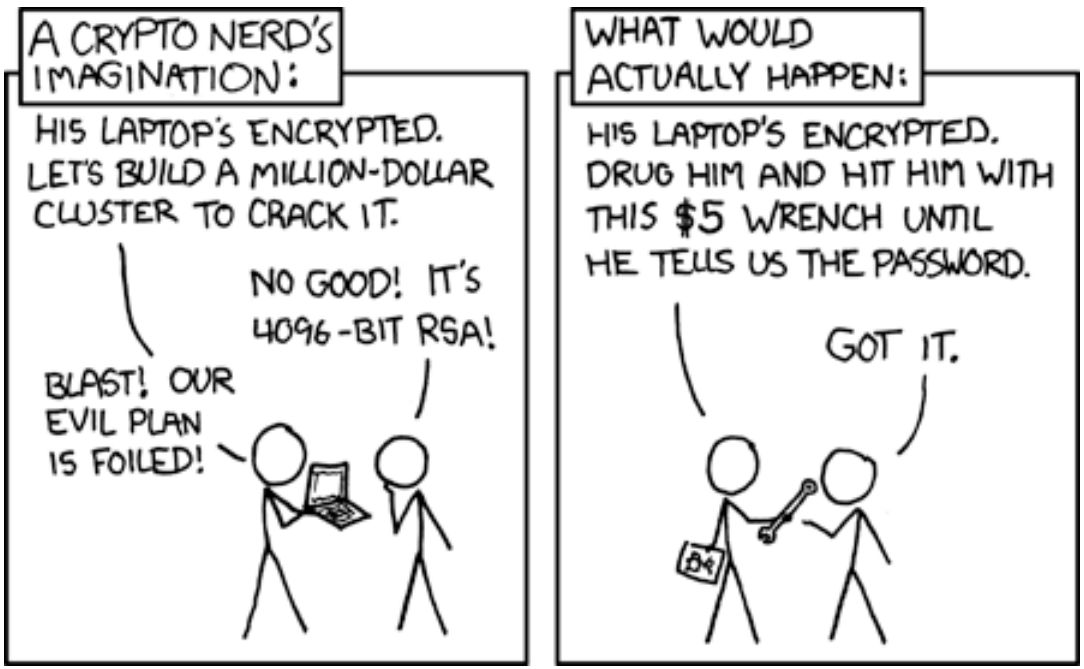


Figure 2: xkcd, Security. https://xkcd.com/538/

No silver bullets

Når uheldet er ude

Uheld	Plastre
Data leaks ved en service	e2ee
Zero day	Sandboxing
Fysisk konfiskation	Enkrypterede backups, sletningspraksis
Internet shutdowns	Radio, LoRa, Bluetooth
Backdoors	…

Retention[1] praksis

… mellem bevaring og at slette. Et spænd mellem datahoarding og ingenting.

- Sikkerhedshorisonter over tid.
- Data følsomhed og brugbarhed.[2]

[1] Bevaring, opretholdelse, tilbageholdelse.

[2] Både for sig selv og for trussels aktørere.

Identitets hygiene på online tjenester

Data akkumulation og -korelation kan bruges til at opbygge en profil af brugeren.

- Variation af brugernavne
- Udskiftning af brugernavne og sletning af konti
- Flere forskellige identiteter

Værktøjer:

- En god (offline) password manager[1]

[1]Det er svært at huske mange forskellige brugernavne og kodeord, og vi er generelt dårlige til det især at lave mange forskellige og lange kodeord som er svære at gætte. Password managers er gode værktøjer hertil.

Kommunikations kanaler

- Hvor mange?
  - *Single-point of failure* kontra distribueret risiko
- Hvad slags?
  - officielle, hemmelige, chat[1], message-boards, etc.?
- Backup planer i tilfælde af blackout?

[1]Om det eks. er single-lane eller multi-lane chat-tjenester.

Øvelse - Kortlægning

Snak sammen i grupper og kortlæg følgende for jeres gruppe:

- Hvad skal I holde hemmeligt?
  - Er noget information vigtigere end andet?
- Hvem er jeres *threats actors*?
- Hvordan kan I holde det hemmeligt?
  - hvilke værktøjer og praksisser?

I kan bruge EFF's Surveillance Self-Defense[1] som inspiration.

[1] Electronic Frontier Foundation's Surveillance Self-Defense guide https://ssd.eff.org

Afrunding

Online ressourcer:

- Electronic Frontier Foundation's Surveillance Self-Defense (SSD)[1]
- The Tor Project's hjemmeside og support-FAQ[2]

Vær opmærksom på ikke at få *security fatigue* og at falde i "OPSec" rabbit-holes på youtube.[3]

[1] https://ssd.eff.org

[2] https://support.torproject.org/

[3] At blive bevidst om sikkerheds hensyn skal helst ikke føre til at man bliver udbrændt eller irrationel paranoia som ødelægger ens dag.

Næste gang: Gentag kontrollen

- Right to repair og ejerskab
- Klima konsekvenser
- Åbne operativsystemer som løsning[1]

https://github.com/gnist-dev/tekno-juni

[1] Medbring gerne en USB-nøgle og en bærbar til workshop'en.

Gentag kontrollen

Kontrol og ejerskab af hardware gennem software.

Problemerne som plager

Computere og mange devices plages af ejerskab- og kontrol problemer som adskiller sig de man kender fra andre produkt-kategoriere.

- Transparens
- *Right to repair* og vedligeholdelse
  - Planned obsolescence
  - *Abandonware*[1]
  - End of life

[1]Software som er blevet efterladt af sine producenter, som fører til et limbo af utilgængelighed. Utilgængeligt for legal anskaffelse, udvikling og vedligeholdelse.

Computeren som system

1. Hardware
2. Operativ system
3. Userland

Windows 10´s EOL

Det grælle ved ophøret af windows 10´s sikkerheds opdateringer, er udelukkelsen fra windows 11 ved TPM 2.0 kravet.

- Brugere og computere efterlades i støvet
- Eksponering til fare
- Klima byrden
  - Funktionel hardware udelukkes
  - Anskaffelsen af nyt hardware påtvinges

Alternativet eller alternativerne?

- Erstat windows med et åbent operativ system
- Reduce, reuse, recycle - upcycle en gammel computer[1]
- Omgå windows 11's krav

[1]Evt til en server eller et dedikeret formål, som en retro spil konsol.

Åbne operativsystemer

Operativsystemer udviklet som opensource software.[1]

- Linux- og BSD-distributioner
- "*Demokratisering*" henover de sidste 10 år.

Hvad det åbner for af muligheder:

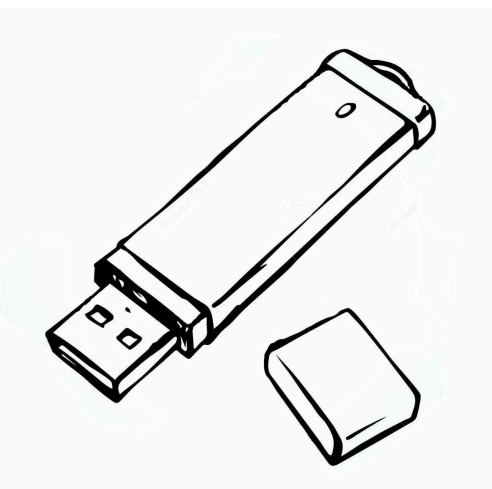
- Mulighed for et bedre ressource forbrug af hardware.

[1] Åbne også i den forstand at de er åbne for modifikation og tilpasning.

Øvelse - At boot fra en USB

Planen for idag:

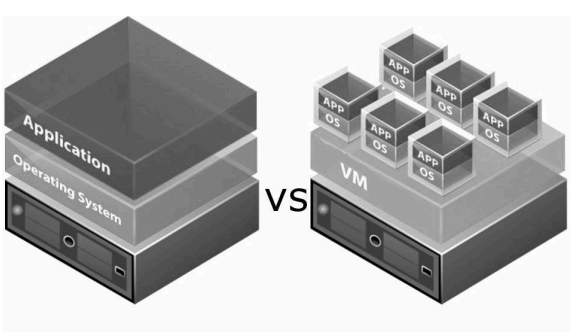
- Boot en linux distribution fra en USB
- Gennemgang af det fagre nye operativ system



(Intermediate) øvelse - Et virtuelt laboratorie

Virtualbox er en software pakke for at håndtere og bruge *virtual machines*.

- Opsætning af en virtual machine
- Installation af en linux distribution
- Gennemgang af det fagre nye operativ system



Onion Routing og Selfhosting

Hvor mange kender til ... ?

- TOR
- Selfhosting
- Servere

Hvad er en server?

Computeres rolle i et netværk.

- Clients og servere

Internettet i grove træk

world wide web:

- Domain name system (DNS), addressebogen
- IP-adresser

Hosting

At *serve* indhold og tjenester[1] over et netværk.

- Local Area Network (LAN)
- Internettet
  - Clearnet og “dark”-net

[1] En tjeneste kan rangere fra email, fil-upload, chat, multi-medie, etc.

Selfhosting

At stå for sine egne tjenester. Eksempelvis privat brug på et LAN eller over internettet:

Data tjenester	"Sociale" tjenester[1]
netflix ⟶ jellyfin / plex	twitter ⟶ mastodon
google drev ⟶ nextcloud / cryptpad	discord ⟶ matrix / xmpp
google images ⟶ immich	

[1]En tjeneste som er nødt til at være tilgængelig over internettet for andre, og kan ikke hostes på et privat lukket netværk som andre tjenester, idet at funktionaliteten bygger på interaktion mellem brugere.

Interaktioner med en computer

- Grafisk brugerflade
- Command line / terminal

The Internet's Own Boy

Aaron Scwartz