

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 aktører.

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

Hvorfor kan det være relevant for dig?

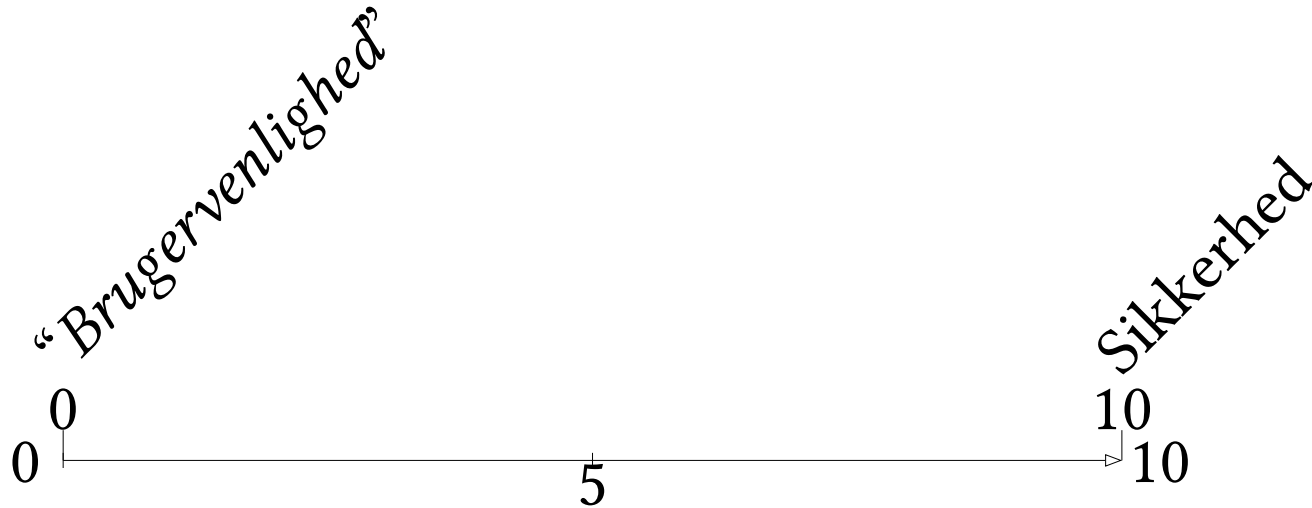
- Omgørelsen af Roe V. Wade og cyklus-app
- Aktivistisk og politisk engagement gavner af muligheden for privatliv og undgåelsen af overvågning
- Du vil have kontrol over din egen data¹

Data akkumulation og profil opbygning

¹Eks. 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

¹Gnu 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 informationen ved dekryption.

Symmetrisk	Asymmetrisk
Eks. en passphrase, p	Public-Private keypair keypair = (pub; 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

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

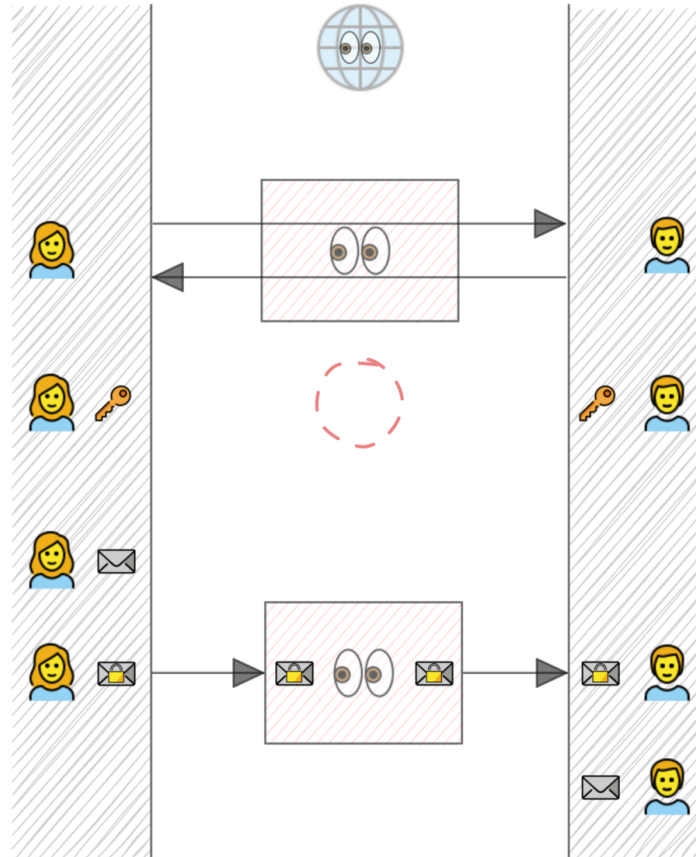


Figure 1: Wikipedia's illustration af e2ee.

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 <i>compromised</i> modtager

¹I 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-adresser, 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 systemer¹

¹Her 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*

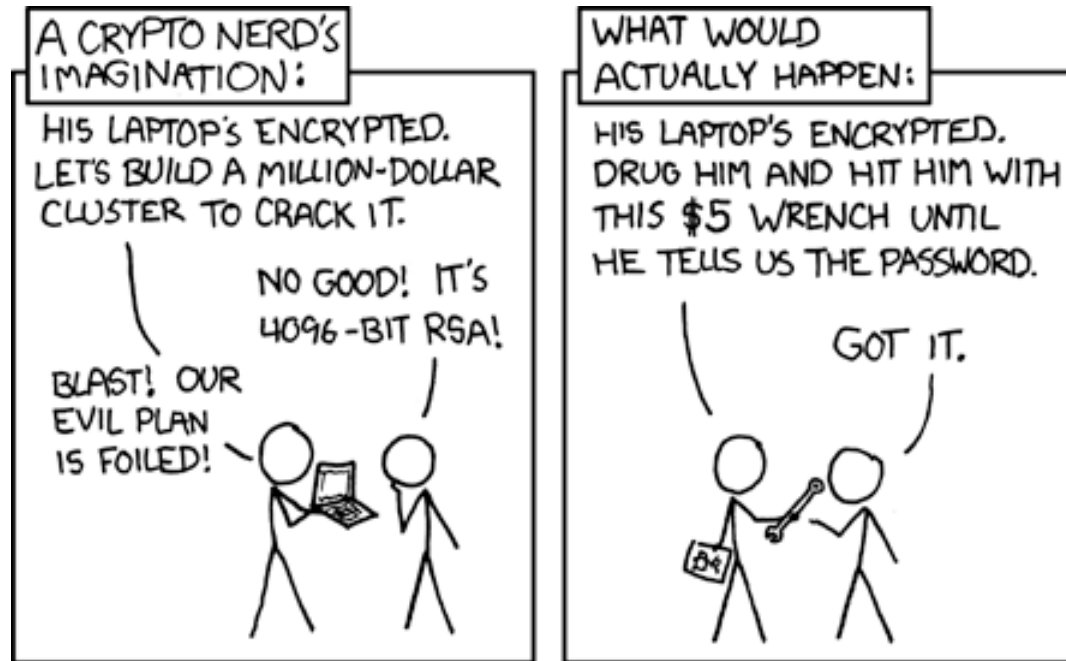


Figure 2: xkcd, Security. <https://xkcd.com/538/>

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

¹Bevaring, opretholdelse, tilbageholdelse.

²Både for sig selv og for trussels aktører.

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 manager¹

¹Det 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, chat¹, message-boards, etc.?
- Backup planer i tilfælde af blackout?

¹Om 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-Defense¹ som inspiration.

¹Electronic 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-FAQ²

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/>

³At 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 løsning¹



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

¹Medbring 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:

- Manglende transparens ind i softwaren
 - Overvågning og konfiguration
- *Right to repair* og vedligeholdelse
 - Planned obsolescence
 - *Abandonware*¹
 - End of life

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

Computeren som system

Computere er komplekse i deres sammensætning, og er afhængige af store socio-tekniske systemer for at kunne fungere og blive produceret. Forsimplet forholder vi os til følgende, hvad angår vores mulighed eller mangel deraf for kontrol:

1. Hardware
2. Operativ system
3. Userland¹

¹Userland (også kendt som userspace) er kode og programmer som kører udenfor styresystemets kernel. Det dækker programmer rangerende fra bruger-programmer som en web-browser til baggrund processer og den grafiske brugerflade.

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?

Hvis man finder sig ramt af Windows 10's *EOL* eller træt af Big Tech udviklede operativ systemer.

- Erstat windows med et åbent operativ system
- Reduce, reuse, recycle - upcycle en gammel computer¹
- Omgå windows 11's krav²

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

²Det er muligt at omgå Microsoft's installations krav ved at lave "registry edits". Man er dog i risiko for at ved opdatering at skulle ligge og bøvl med at genopsætte disse "registry edits".

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.
- At selv være i kontrol over styresystemet
- Undgå backdoors²

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

²Ved operativsystemer som MacOS og Windows har vi ingen mulighed for at bekræfte eller afkræfte tilstedeværelsen af backdoors.

Hvad er en distribution?

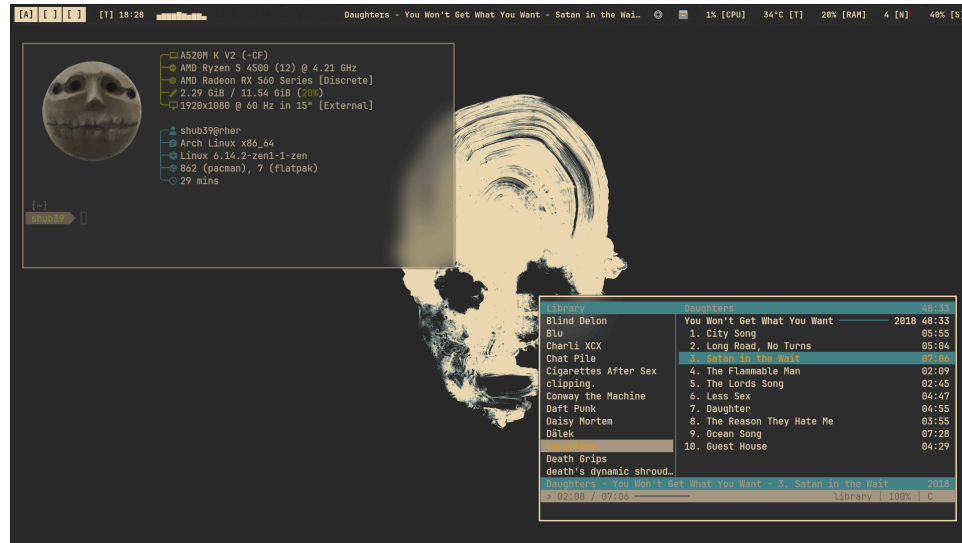
I modsætning til Windows og MacOS, er der for linux flere forskellige udbydere af “linux” styresystemer, som er indbyrdes forskellige i hensyn til deres sammensætning:¹

- Desktop Environment (Den grafiske brugerflade)
- *Target audience* og brugscenarie²
- Community- eller firma-udviklede
- Opdateringssystem og pakke format

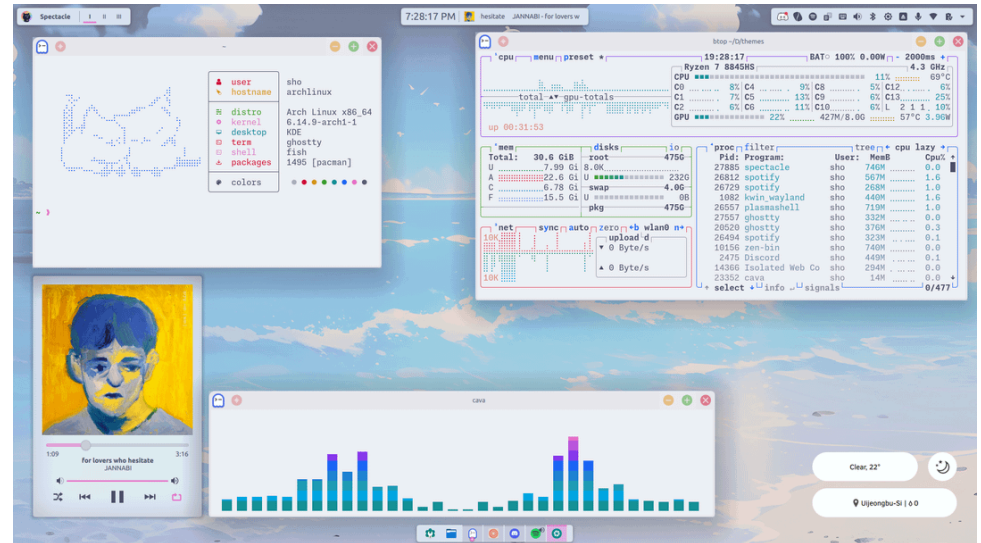
¹Her rangeret efter relevans for nye brugere/ikke-tekniske brugere.

²Samt hvilke design principper de følger for *User Experience*.

Hyprrland



Customized KDE



Eksempler på distributioner

Distributioner for general brug:

- *Stable release*: Debian, ubuntu, linux mint, fedora, OpenSUSE
- *Rolling release*: Arch, NixOS(unstable)

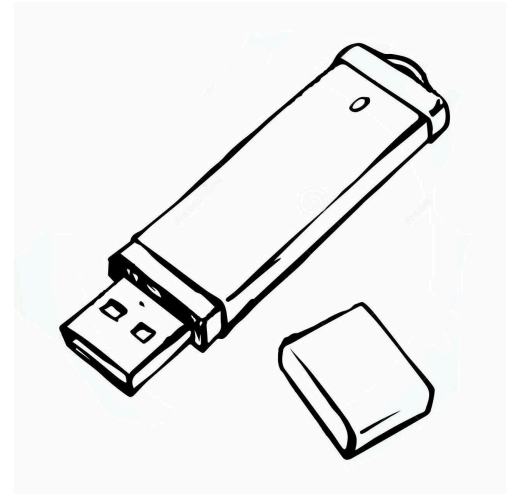
Distributioner med specialiserede brugsscenarier:

- Tails
- Whonix
- QubesOS
- Kali linux

Øvelse - At boot fra en USB

Planen for idag:

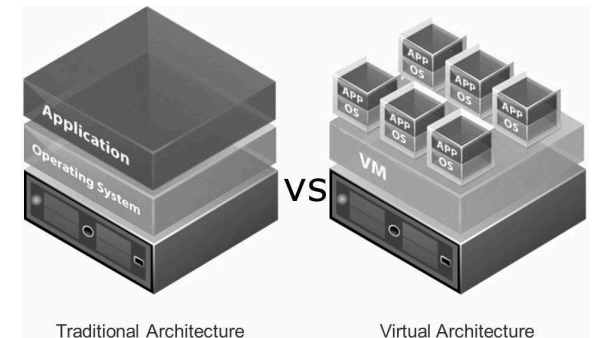
- Boot en linux distribution fra en USB
- Gennemgang af det fagre nye operativ system



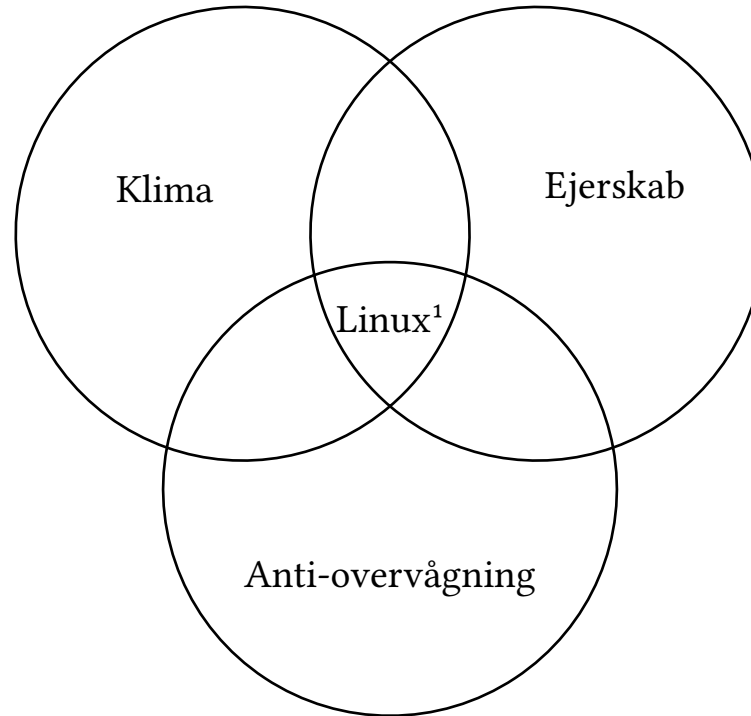
(Intermediate) øvelse - Et virtuelt laboratorium

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



Afrunding



¹... Og andre open source styresystemer

Næste gang: Onion Routing og Selfhosting

- Hvordan undgår man overvågning og censur på internettet?
 - Opsætning og brug af Tor
- Hvad er fordelene ved selv at hoste og have sin egen “server”?
 - Eksempler og hjælp til at starte begynder-projekter
 - Data-kooperativer som alternativ til Big Tech



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

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), adressebogen
- IP-adresser

Hosting

At *serve* indhold og tjenester¹ over et netværk.

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

¹En 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	

¹En 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 Schwartz