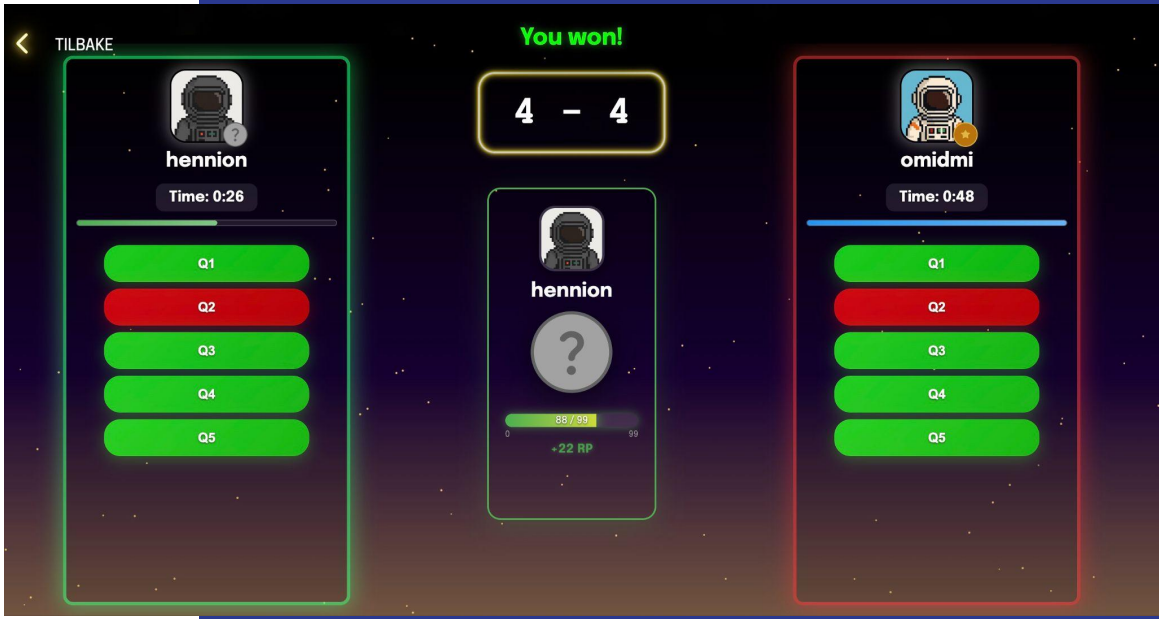
Uke 5 - IN1020

Velkommen!

Lever oblig i løpet av dagen!

Agenda

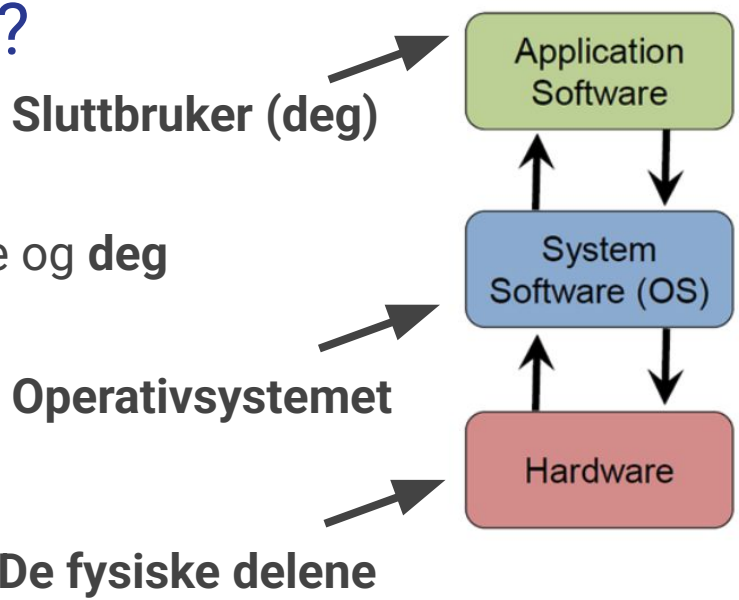
- Operativsystemer
- Hvordan hacke
- Kahoot
- Oppgaver på universet / ukesoppgaver

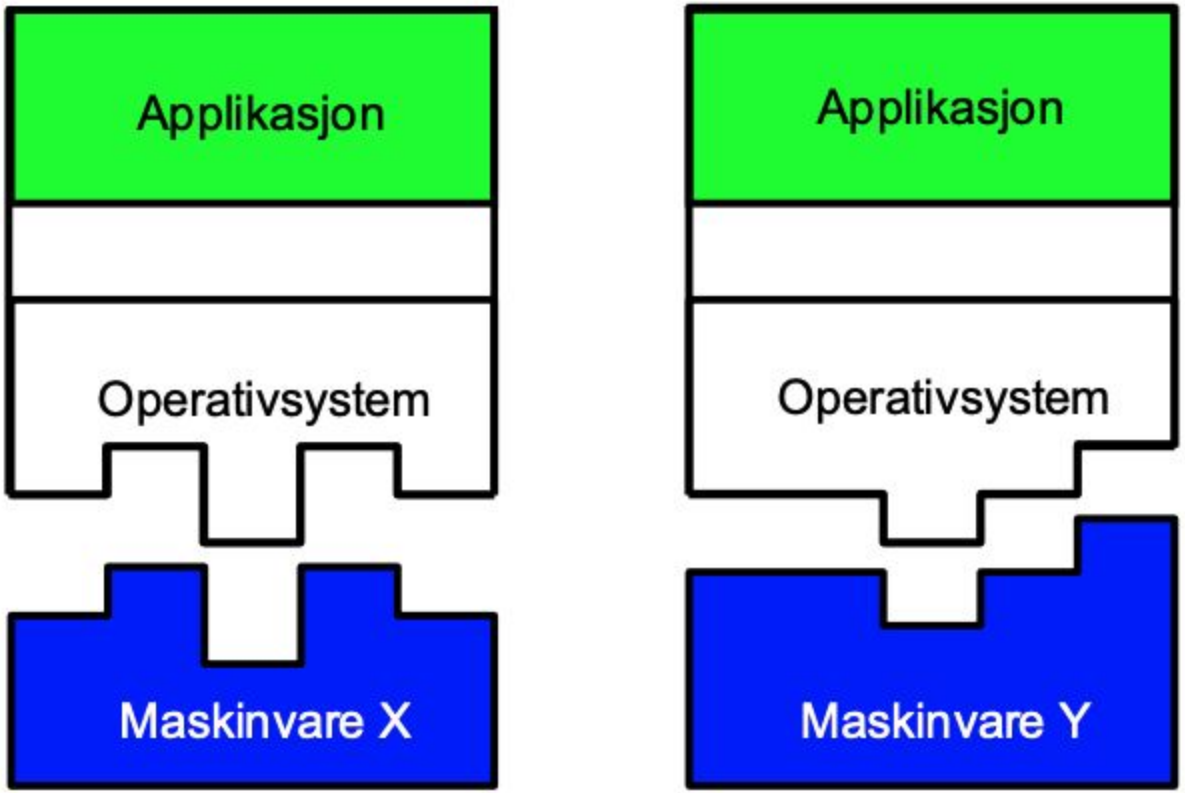


Operativsystemer

Hva er et operativsystem?

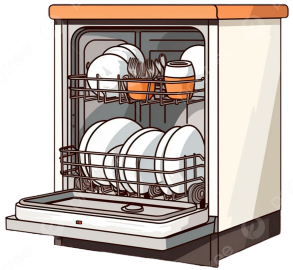
- Dirigenten i datamaskinen 🎼
- Mellommann mellom maskinvare og **deg**
- Skjuler kompleksitet




Applikasjon
Operativsystem
Maskinvare X
Applikasjon
Operativsystem
Maskinvare Y


SHARP

Hvor finner vi et operativsystem?

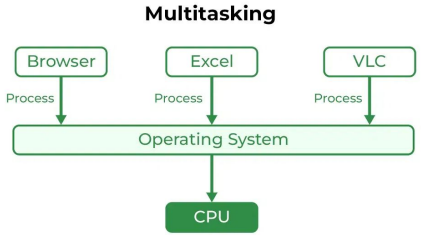






- PC-er💻
- Mobiltelefoner 📱
- Innebygde systemer (biler, kamera, vaskemaskiner) 🚗📷
- Sanntidssystemer (fly, roboter, medisinsk utstyr) ⏱️
- Klokker, IoT osv.

Typer operativsystemer



- **Single-user, single-task**
  Én bruker kan kjøre **ett program om gangen**. Eksempel: veldig gamle PC-er, gamle PDA-er.

- **Single-user, multitasking**
  Én bruker, men **flere programmer samtidig** (f.eks. Word + Spotify). Vanlig på moderne PC og mobil.

- **Multi-user, multitasking**
  Mange brukere samtidig, hver med egne programmer. Typisk på **servere** og UNIX-baserte systemer.

- **Distribuert OS**
  Samler flere maskiner i ett system – ressursene ser ut som de kommer fra én datamaskin. Brukes i **dataklynger**.

- **Real-time OS (RTOS)**
  Reagerer innenfor strenge tidskrav. Eksempler: **bilmotorer, fly, medisinsk utstyr, roboter**.

- **Embedded OS**
  Bygd inn i små enheter for spesifikke oppgaver: **mikrobølgeovn, vaskemaskin, smartlåser, kamera**.

Komponenter

- **Brukergrensesnitt (CLI/GUI)**

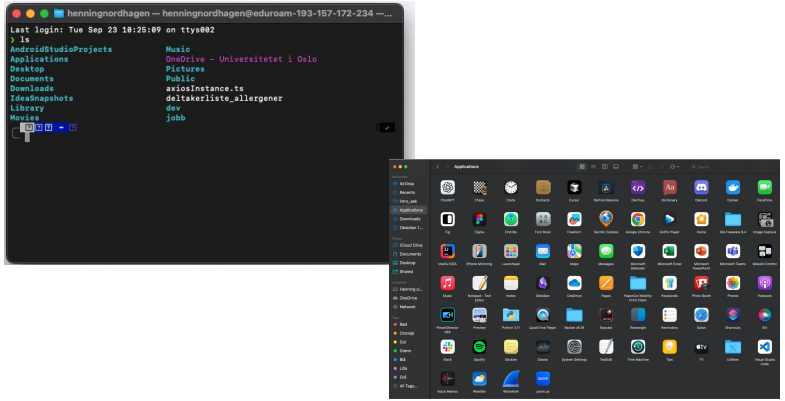
  Hvordan brukeren snakker med maskinen.
  Kommandolinje (terminal) eller grafiske vinduer.

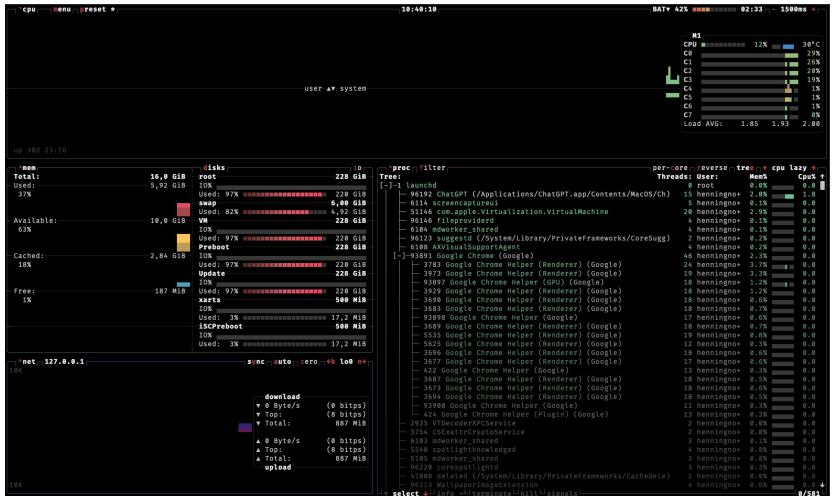
- **Prosesskontroll (CPU)**

  Hvem får kjøre når? Planlegging, bytte mellom prosesser (multitasking).

- **Minnehåndtering**

  Gir hvert program sitt område i RAM, beskytter mot at programmer overskriver hverandre.





Komponenter



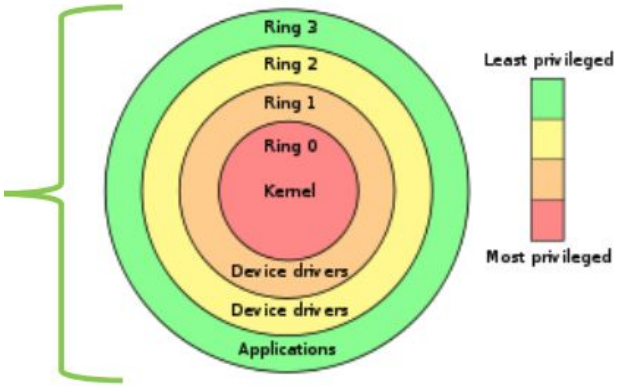
- **Filsystem**
  Organiserer data i mapper og filer, håndterer lagring og rettigheter.

- **Enhetskontroll**
  Styrer maskinvare via drivere (tastatur, skjerm, nettverk).

- **Kommunikasjonstjenester**
  Gjør at programmer kan snakke med hverandre (IPC) og med andre maskiner (nettverk).

Systemkall

- **Hva:** Grensesnittet programmer bruker for å snakke med kjernen.
- **Hvorfor:** Programmer kan ikke direkte aksessere maskinvare (sikkerhet).



- **Beskyttelse:**
  a. **Brukernivå:** begrensede rettigheter.
  b. **Kjernenivå:** full tilgang til maskinvare.

Eksempel: Lese fra fil (Disclaimer, under panseret)

Brukernivå vs. Kjernenivå (Beskyttelse)

Brukernivå (user mode)

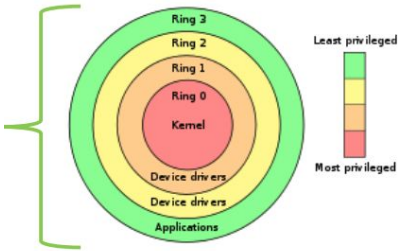
- **Vanlige programmer** kjører her (Word, nettleser, spill).
- Har **begrenset tilgang**:
  - Får bare bruke sitt eget minneområde.
  - Kan ikke snakke direkte med maskinvare.
  - Må gå via **systemkall (API)** for å be operativsystemet om hjelp.

👉 Tenk på dette som **gjester** i et hus: de får bruke stua og kjøkkenet, men ikke strømnettet eller sikringsskapet direkte.

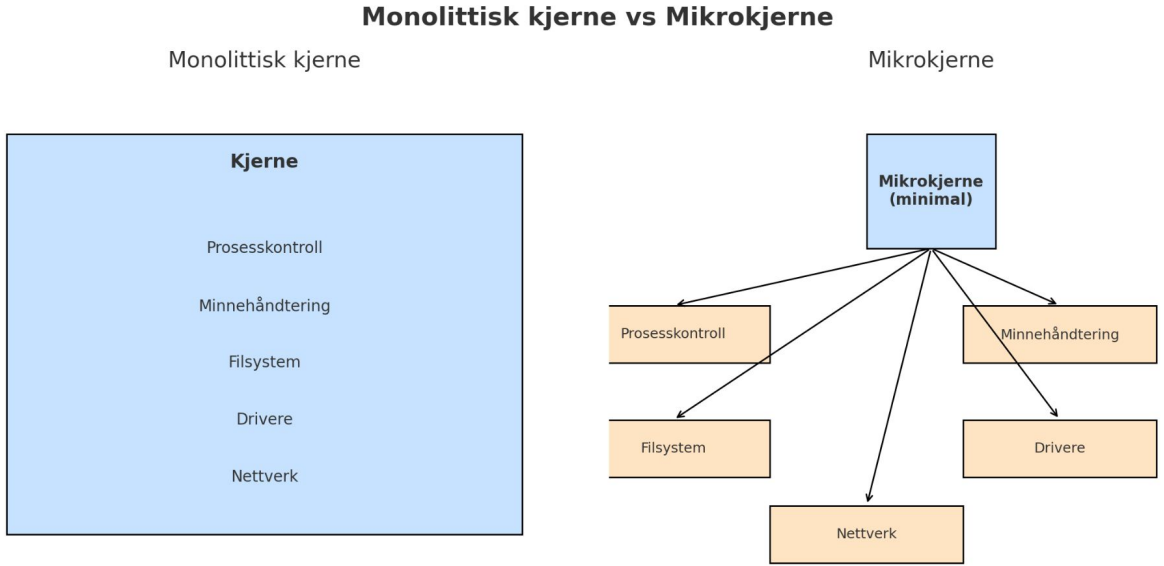
Kjernenivå (kernel mode)

- **Operativsystemet** kjører her.
- Har **full makt**: kan bruke hele minnet, snakke direkte med maskinvare og kjøre alle instruksjoner.
- Ingen sikkerhetsbegrensninger → hvis noe går galt her, kan hele systemet krasje.

👉 Tenk på dette som **admin** eller “superbruker”.



Organisering av operativsystemer



Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	○	○
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	○	○
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.	○	○
Operativsystemet sørger for at flere programmer kan kjøre samtidig.	○	○
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.	○	○
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.	○	○
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.	○	○
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.	○	○

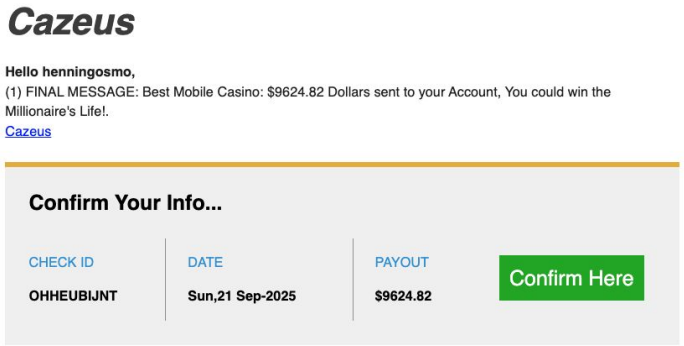
Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	✔	
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		✔
Operativsystemet sørger for at flere programmer kan kjøre samtidig.	✔	
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.	✔	
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.	✔	
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		✔
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		✔

Hvordan hacke?

Google© - This message was sent from a trusted sender.

Phishing



🎯 Phishing (generelt)

- Svindel via e-post/sms/nettsider som prøver å stjele info eller få deg til å klikke.

📨 Mass-phishing (spray & pray)

- Masseutsendelse til mange; generisk innhold: «Oppdater passordet».
  Lav målretting, høy volum.



🎯 Spear-phishing (spyd-phishing)

- Målrettet angrep mot én person eller organisasjon; personlig og troverdig.
- Krever research (f.eks. LinkedIn) — farligere.



SQL injection

Sender kode som påvirker databasen, inn i input felt

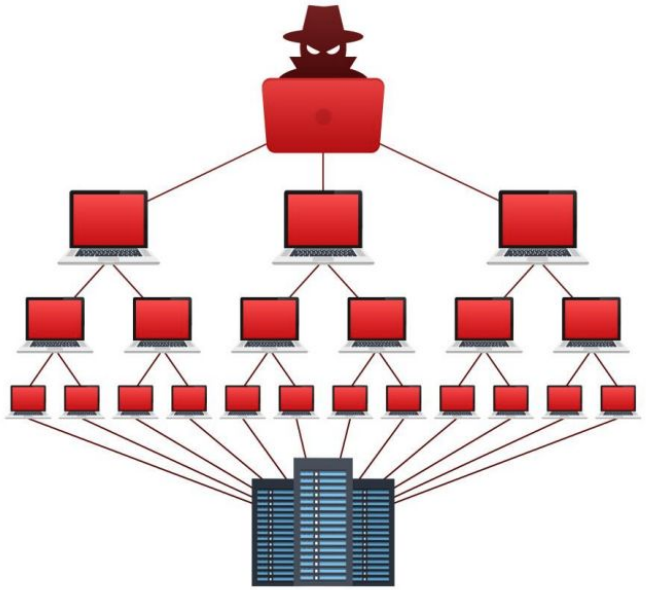
Feks

Username:

Password: —-



DDoS




BRACE YOURSELVES
THE PACKETS ARE COMING
memegenerator.net

Ulike former for skadevare / angrepsvektorer

 Virus	Kjennetegnes ved at det sprer seg hver gang en fil med virus blir åpnet av bruker eller systemet.
 Dataorm	Skadevare som på egenhånd er i stand til å spre seg og finne nye ofre.
 Trojaner	Skadevare som utgir seg for å være et nyttig program.
Bakdør	En ubeskyttet og ukjent åpning inn i et datasystem, laget av en angriper.
 Spionvare	Programvare for å spionere på en bruker i håp om å få tak i f.eks. informasjon, passord, kontoinformasjon.
 Tastelogger (Keylogger)	En enhet eller programvare som er koblet til tastatur eller maskin og som lagrer eller videresender alle tastetrykk. En variant av spionvare.
Rootkit	Skadevare som endrer eller erstatter funksjoner i OS eller applikasjoner, med mål å ta kontroll over en maskin eller et system.
Exploit	Et program, en sekvens med data, eller en oppskrift på hvordan en sårbarhet kan utnyttes.

Hvordan beskytte oss selv?

Hvordan beskytte oss selv?

🧱 Brannmur

- Slipper inn / blokkerer trafikk ut og inn 🚦
- Basert på regelsett (tilgangskontroll)
- Kan være programvare eller dedikert maskinvare

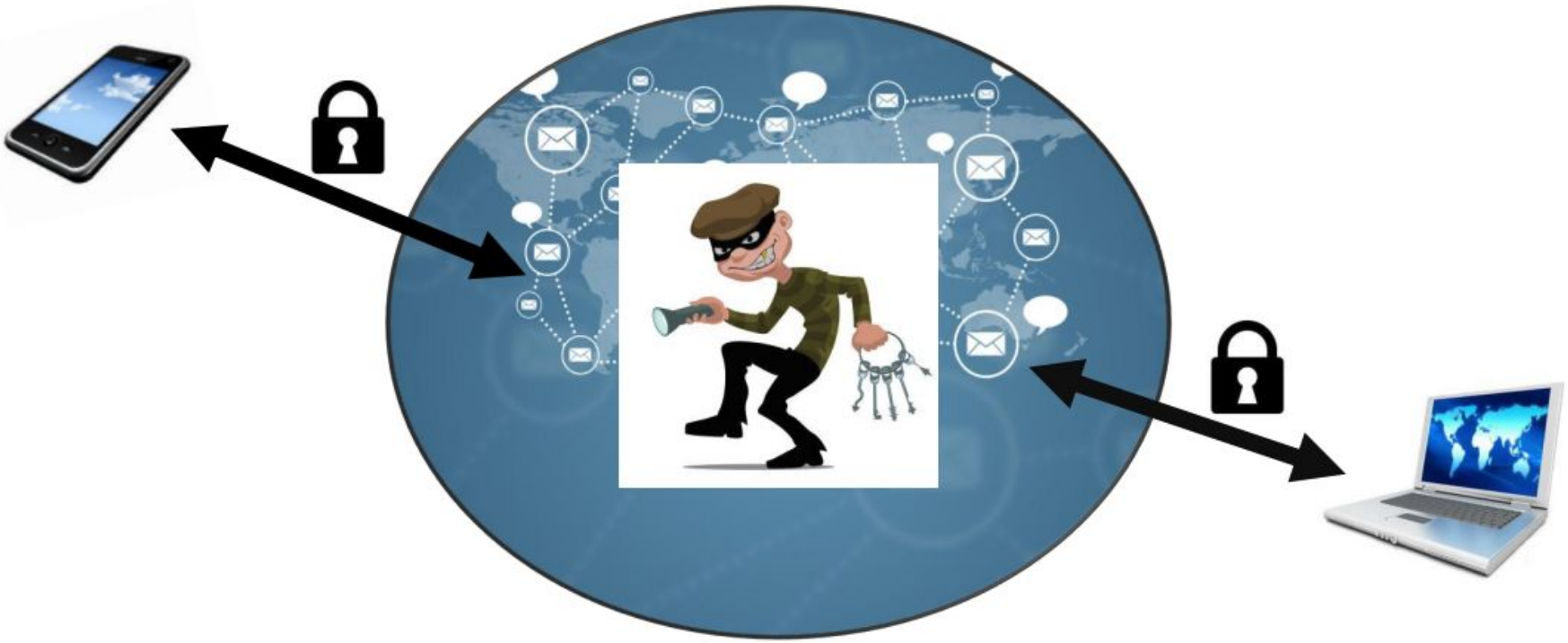
🕵️ Inntrengningsdeteksjon (IDS)

- Overvåker trafikk i nettverket 👀
- Oppdager forsøk på innbrudd 🚨
- Kan se virus, malware og DoS-angrep 💣

Kort sagt: **Brannmur stopper trafikk**, **IDS oppdager angrep**.

Og med kryptering, det husker dere fra forrige uke

Tradisjonell sikkerhetsmodell:
Stoler på endesystemene, nettverket anses upålitelig.



Brudd på sikkerhetsmål

Angi hvilket sikkerhetsmål som typisk brytes som resultat av hvert av følgende angrep:

Finn de som passer sammen:

	Autentisitet	Integritet	Tilgjengelighet	Konfidensialitet
Løsepengevirus	○	○	○	○
Identitetstyveri	○	○	○	○
DDoS-angrep	○	○	○	○
DNS-modifisering	○	○	○	○
Spionprogramvare	○	○	○	○
Forfalskning av nettside	○	○	○	○

Brudd på sikkerhetsmål

Angi hvilket sikkerhetsmål som typisk brytes som resultat av hvert av følgende angrep:

Finn de som passer sammen:

	Tilgjengelighet	Autentisitet	Integritet	Konfidensialitet
Spionprogramvare	○	○	○	○ ✔
DDoS-angrep	○ ✔	○	○	○
Identitetstyveri	○	○ ✔	○	○
DNS-modifisering	○	○	○ ✔	○
Løsepengevirus	○ ✔	○	○	○
Forfalskning av nettside	○	○ ✔	○	○