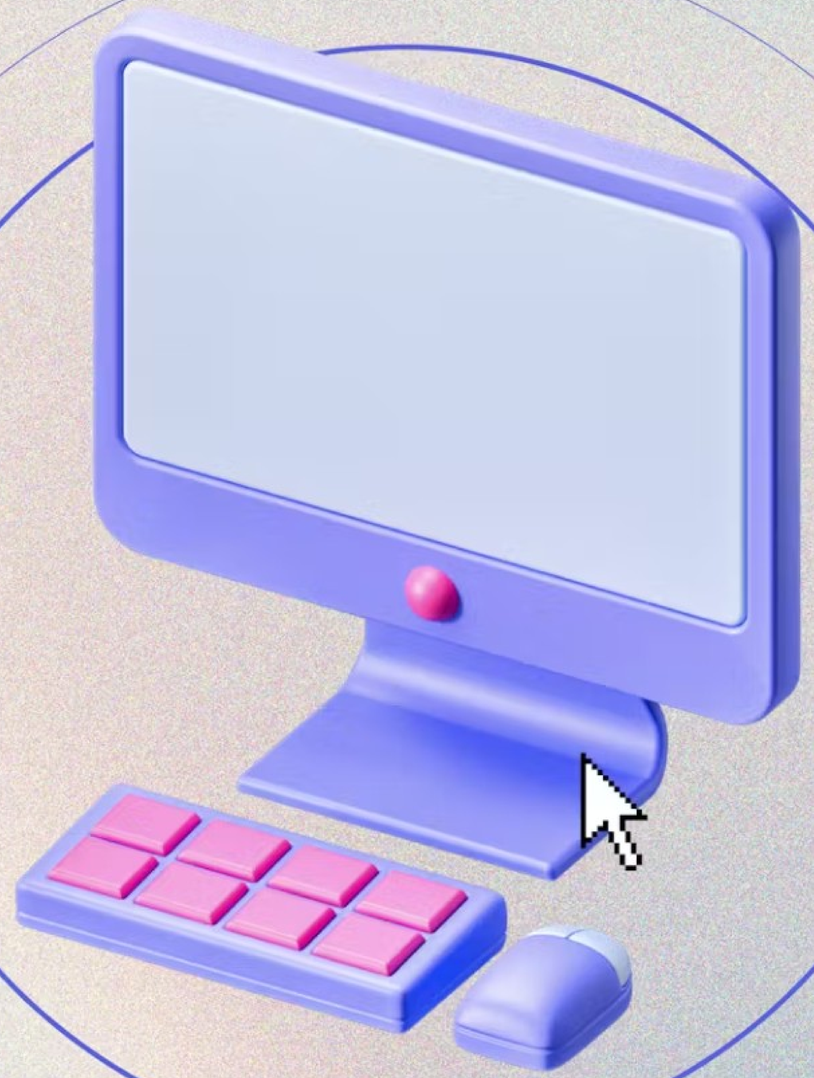
OPERATIVSYSTEMER OG SIKKERHET



Mentimeter

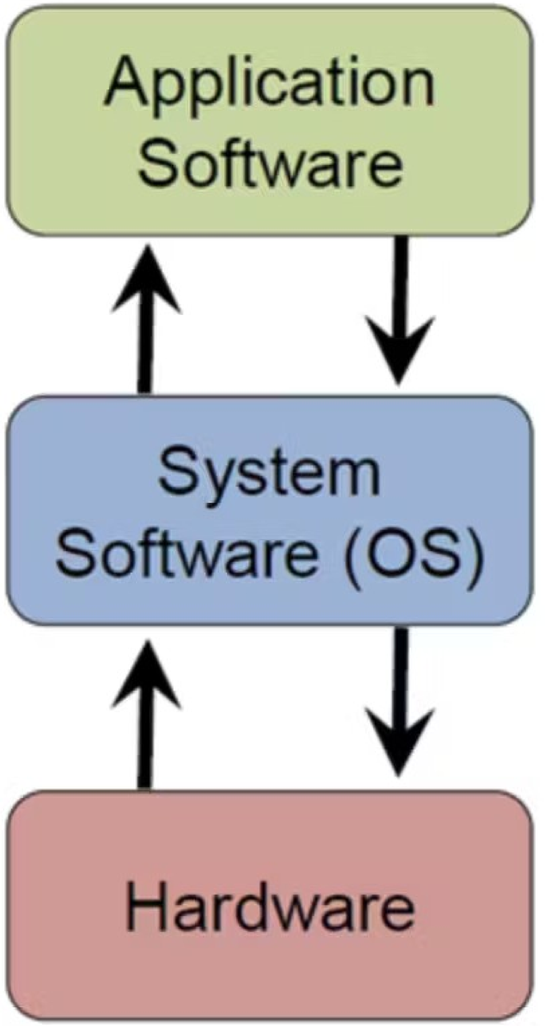
Hva er et operativsystem?

- Mellomledd mellom maskinvare og programvare
  - Hvordan snakker CPU med skjerm, harddisk eller nettverkskort? OS fikser dette!
- Deler prosessor, minne og filer mellom alle prosesser slik at alle flyt blir rettferdige og sikre
- Beskytter programmene mot hverandre

Mentimeter

Eksempler på situasjoner

- Flere programmer oppe samtidig mens du skriver oblig
  - Hva skjer?
- Når du lagrer noe inne i et program - OS oversetter "lagre" -> systemkall til harddisken
- Hva hadde skjedd om OS ikke stoppet prosesser fra å se hverandres minne?

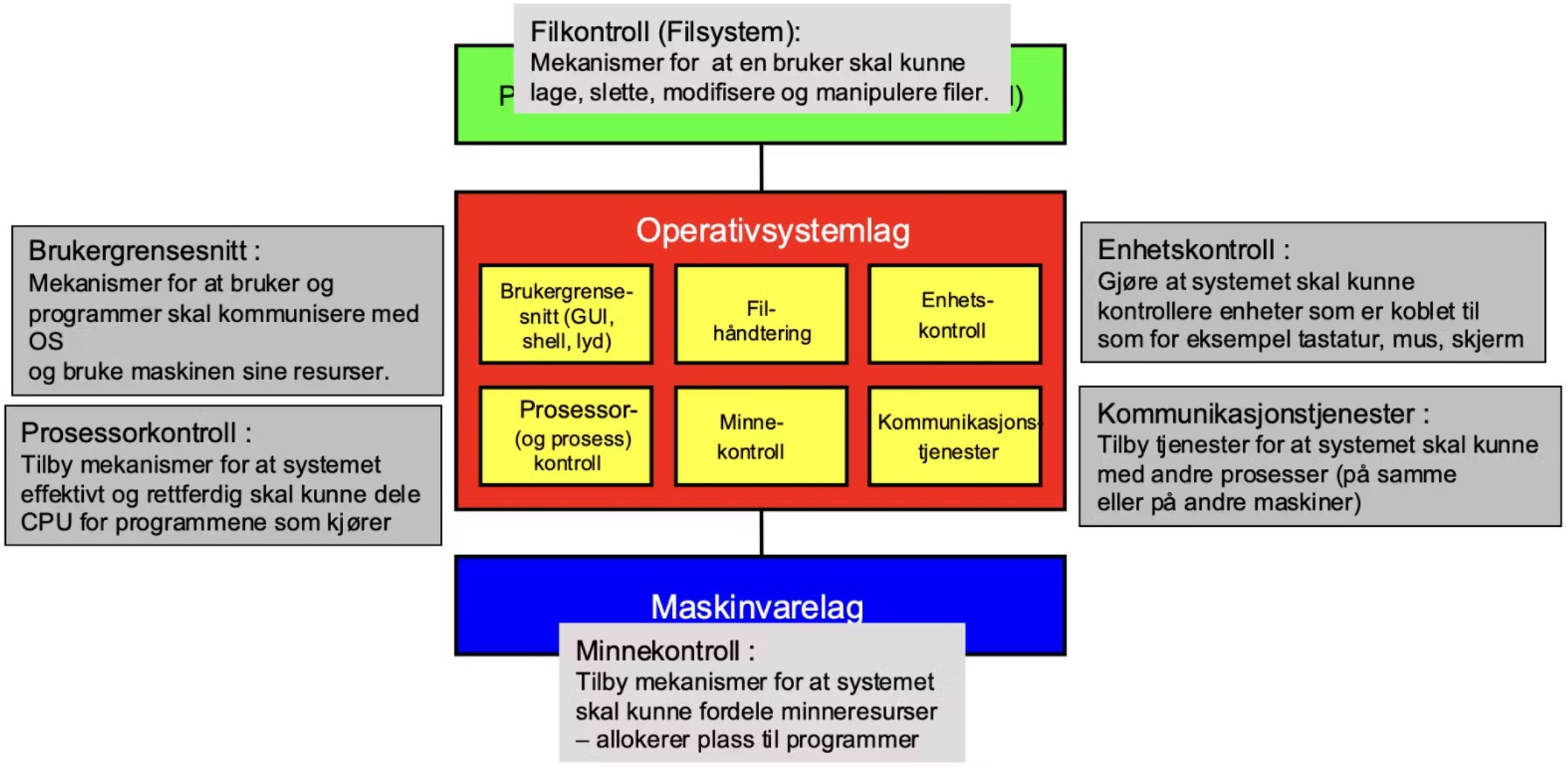


Mentimeter

Hvor finner vi operativsystemer?

- Overalt
  - Linux, Mac, Windows
- Trenger ikke være stort, mange systemer kan inneholde OS som bare styrer en spesifikk funksjon
  - Vaskemaskiner, Tesla, IoT
- Hva skjer hvis operativsystemet i en vaskemaskin eller en bil blir hacket? Er det mindre viktig enn et PC-angrep, eller kan konsekvensene være vel så store?

Mentimeter


Filkontroll (Filsystem):
Mekanismer for at en bruker skal kunne lage, slette, modifisere og manipulere filer.
Operativsystemlag
Brukergrense-snitt (GUI, shell, lyd)
Fil-håndtering
Enhets-kontroll
Prosessor- (og prosess) kontroll
Minne-kontroll
Kommunikasjons-tjenester
Maskinvarelag
Brukergrensesnitt :
Mekanismer for at bruker og programmer skal kommunisere med OS
og bruke maskinen sine resurser.
Prosessorkontroll :
Tilby mekanismer for at systemet effektivt og rettferdig skal kunne dele CPU for programmene som kjører
Enhetskontroll :
Gjøre at systemet skal kunne kontrollere enheter som er koblet til som for eksempel tastatur, mus, skjerm
Kommunikasjonstjenester :
Tilby tjenester for at systemet skal kunne med andre prosesser (på samme eller på andre maskiner)
Minnekontroll :
Tilby mekanismer for at systemet skal kunne fordele minneresurser – allokerer plass til programmer

Mentimeter

Sikkerhet- hva vil hackere?

- Lese data de ikke skal (konfidensialitet)
  - Identitetstyveri på sosiale medier
- Endre slik data (integritet)
  - Tukling av databaser
- Gjøre den utilgjengelig (tilgjengelighet)
  - Løspengevirus som krypterer alt

Mentimeter

Beskytte lagret info

- Kryptering
- Backup
  - 3-2-1 regelen: 3 kopier på 2 forskjellige enheter hvor 1 er off-site
  - Versjonering: Beholder gamle versjoner, hjelper mot ransomware
  - En kopi som ikke kan nås/endres fra produksjon (snapshots, WORM/immutable buckets, bånd)
  - Bør oppbevares separert fra originalene
- Trygg sletting
  - "Slett" fjerner ofte bare referanser til filene-> innholdet kan gjenopprettes
  - Secure erase/overwriting**:** Programvare som skriver over hele lagringsområdet
  - Crypto-erase: Hvis disken er kryptert, kan du tilintetgjøre nøkkelen så alt innhold blir ubrukelig med en gang

Mentimeter

Risiko

- Trådløst nett:
  - Radiobølger, alle kan lytte
  - Falske aksesspunkt - fake gratis wifi
- Kablet nett
  - Tryggere pga fysisk tilgang, men angriper kan bare bruke egen kabel
- Konkrete eksempler:
  - Man in the middle angrep: angriper sitter mellom to aktører/brukere og endrer informasjon
  - Avlytting på åpent wifi, passord kan bli lest etter hver kobling på https

Mentimeter

Skallforsvar og brannmur

- Brannmur: portvakt, har regler
- IDS: overvåking etter unormal oppførsel
- Kan en brannmur stoppe alt?

Mentimeter

DoS/DDoS

- DoS = én angriper sender masse trafikk
- DDoS = mange maskiner (ofte et botnett) angriper samtidig
- Eksempel
  - 1000 roboter ringer kundeservice og sperrer linjen for ekte kunder
- Hvilket sikkerhetsmål trues av DDoS?

Mentimeter

Skadevare

- Virus = sprer seg når filer åpnes
  - Trenger et vertsprogram -> de legger seg i en fil, og sprer seg når filen åpnes
  - Hvorfor: mange programmer lar data og kode blandes
- Orm = sprer seg selv over nettverk
  - Sprer seg automatisk, har ikke bruk for brukeren
  - Hvorfor: Systemer som ikke er oppdatert og står åpne på nett er utsatt
- Trojaner = ser ut som noe nyttig, men skjuler skade
- Keylogger = spionerer på tastetrykk
  - Hacker kan få tak i ditt passord uten å måtte lete
  - Kan skje gjennom en trojaner
- Rootkit = skjuler seg dypt i OS, gir angriper full kontroll, gjemmer seg for antivirus

Mentimeter

Sikkerhet i operativsystemet og applikasjonssikkerhet

- OS styrer brukeres tilgang
  - Programmer og brukere skal kun ha de rettighetene de trenger, ikke mer
- Kjernen har tilgang til alt
  - Sårbarhet i kjernen = kritisk
- SQL injeksjon
  - OR blir alltid true med 1OR1 -> hacker vil kunne få inngang ved passordspørring feks
- Cross-Site Scripting
  - Angriper legger ondsinnet kode på nettside
  - Når andre åpner siden, kjøres koden i nettleseren deres
- Hva er likheten mellom SQL-injeksjon og XSS? -> Utnyttelse av brukerinput!

Mentimeter

Sosial manipulasjon

- Angrep som utnytter mennesker, ikke teknologi
  - Phishing, spear-phishing, whaling
    - Fake e-post fra noen "kjente" som ber deg betale en faktura
    - Melding om en pakke med lenke til falsk nettside
    - Whaling: rettet mot ledere

Mentimeter

Oblig?