Gruppetime 5
25.09.2025



Sørg for at alle sitter ved siden av noen



Velkommen til gruppetimen! ☺

Rask REP

- Hva er forskjellene mellom Symmetrisk og Asymmetrisk kyptering
- Hvorfor bruker vi hashing algoritmer?
- Hva er en digital signatur?
- 3-veis håndtrykk er en del av hvilken tjeneste i transportlaget? (SYN, ACK..)

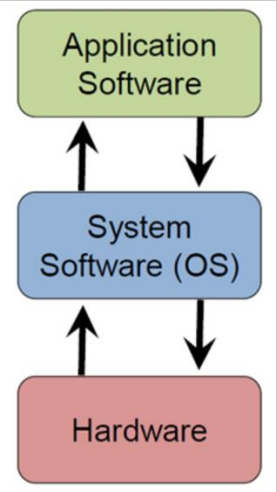
Oblig snakk ?

Operativ-systemer

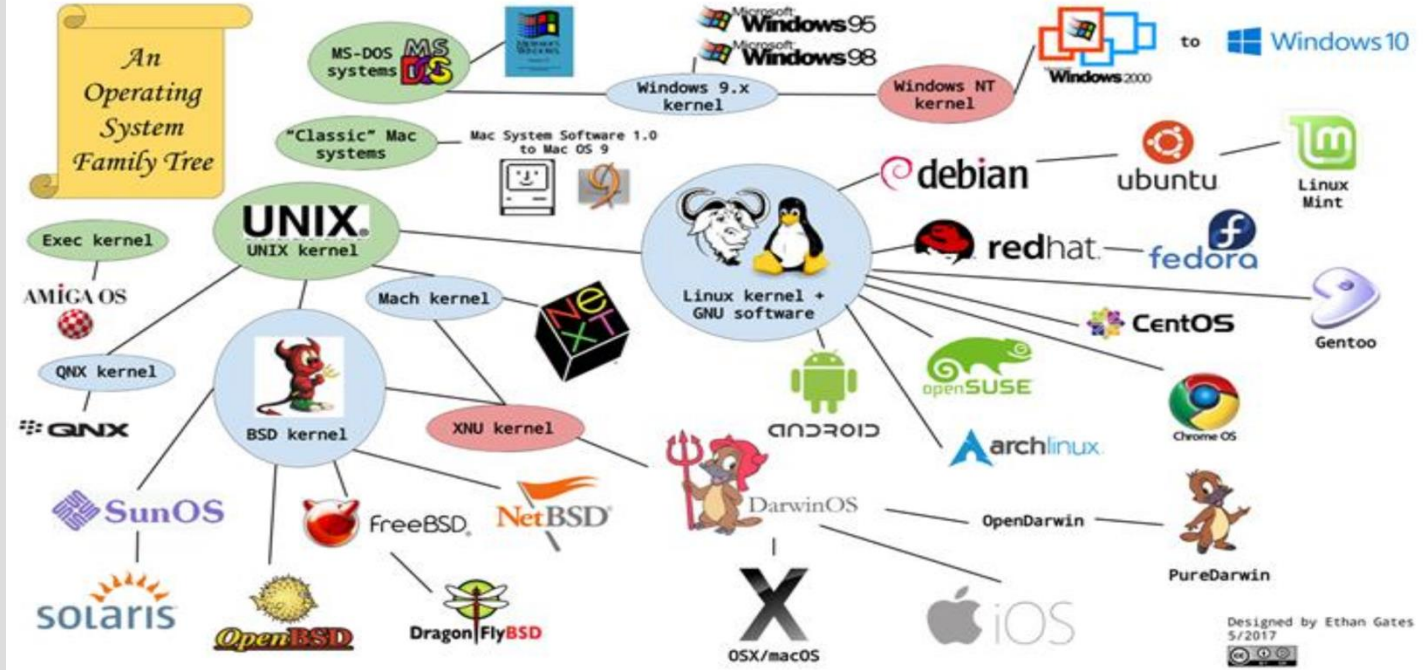


Dirigenten i datamaskinen

- Sørge for at flere brukere kan dele en datamaskin
- Sørge for at flere programmer kan kjøre samtidig
- OS: «mellomnivå» mellom maskinvare og programvare



OS "SLEKTTRE"

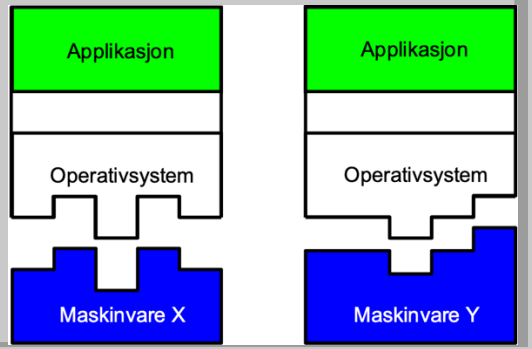

An Operating System Family Tree
MS-DOS systems
Microsoft Windows95
Microsoft Windows98
Windows 9.x kernel
Windows NT kernel
Windows 2000
to
Windows 10
"Classic" Mac systems
Mac System Software 1.0 to Mac OS 9
UNIX
UNIX kernel
Exec kernel
AMIGA OS
QNX kernel
QNX
Mach kernel
BSD kernel
XNU kernel
Linux kernel + GNU software
debian
ubuntu
Linux Mint
redhat
fedora
CentOS
Gentoo
openSUSE
ANDROID
Chrome OS
archlinux
SunOS
FreeBSD
NetBSD
DarwinOS
OpenDarwin
PureDarwin
solaris
OpenBSD
Dragon FlyBSD
OSX/macOS
iOS
Designed by Ethan Gates
5/2017

Hvordan fungerer de?

Finnes masse forskjellig maskinvare, OS sørger for at alle “lagene” over har alt det trenger i en forventet form uansett maskinvare

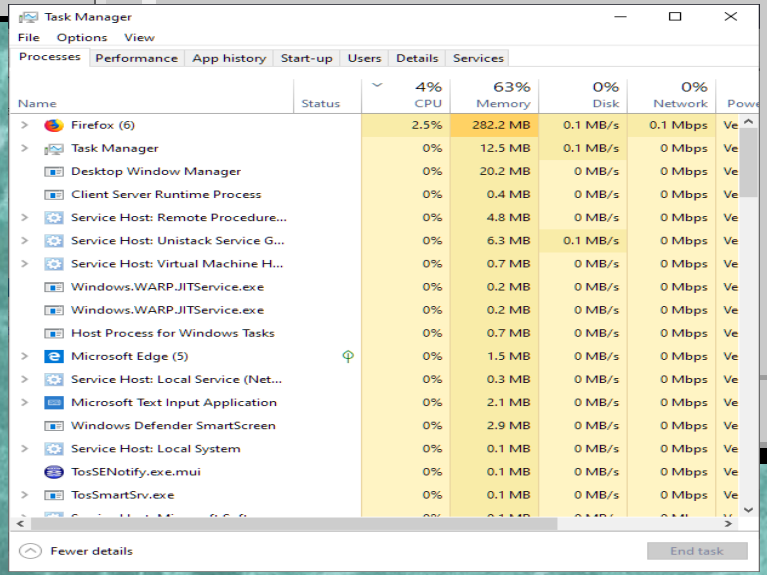


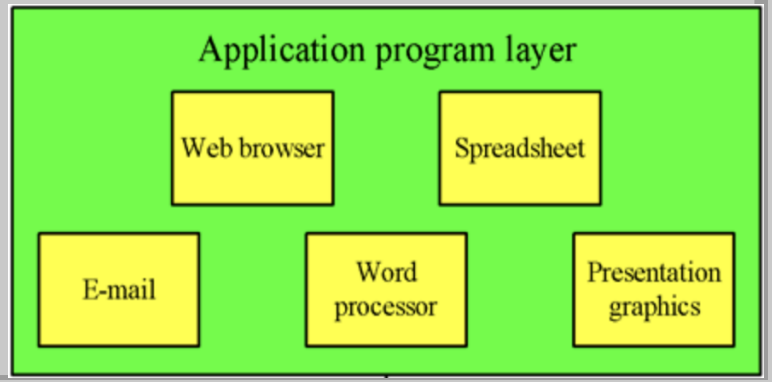




Hvordan fungerer de?

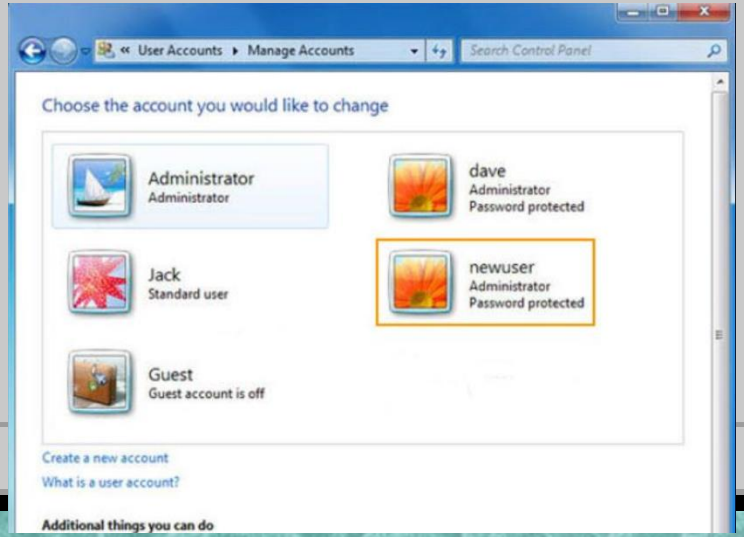
En datamaskin kjører MANGE prosesser i parallell, det er OS'et som tilatter datamaskinen dette.





Hvordan fungerer de?

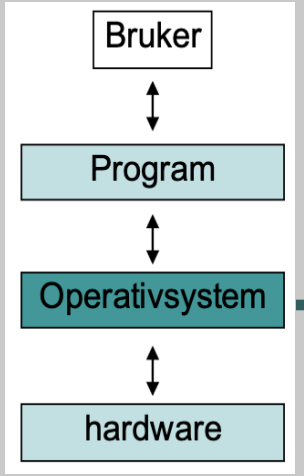
En datamaskin kan ha mange brukere

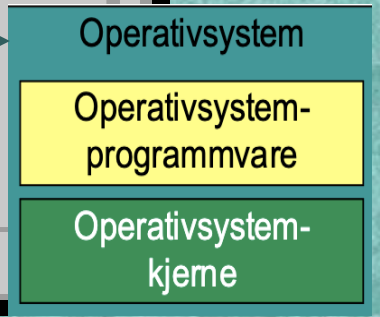


"Definisjon av OS"

- Det er en enkel maskin (ovenfra og ned)
- Skjuler kompliserte detaljer
- Presenterer en «virtuell maskin», enkel å bruke

- Det er en resurshåndterer (nedenfra og opp)
- Hvert program for sin tid/plass i resursene.





Datamaskiner



Mobiler



Konsoller



Biler

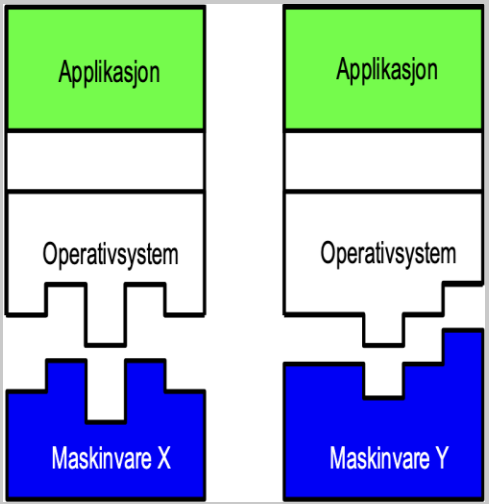


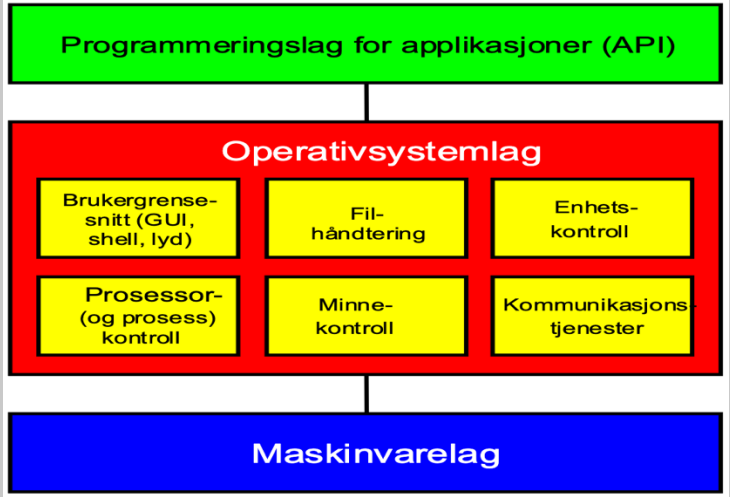
Hvor finner man OS?

Forskjellig typer OS

- Enkel-bruker, enkel-oppgave: Historisk og veldig sjelden
- Enkel-bruker, multi-oppgaver: Sjelden
- Multi-bruker, multi-oppgaver: Servere, Pcer, arbeidsstasjoner… (vanlig)
- Distribuert OS: Kontollere ressurser på flere datamaskiner (uvanlig)
- Real-time OS: Støtte for systemeter hvor sanntid er viktig: biler, fly…
- Embedded OS: IoS (Internet of shit), bygd inn for å løse et konkret problem

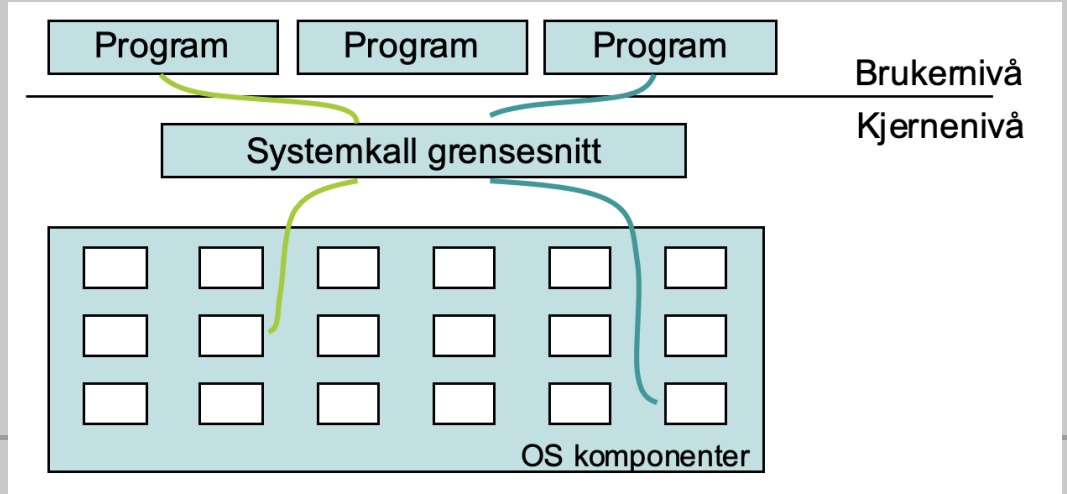
Hovedkomponenter





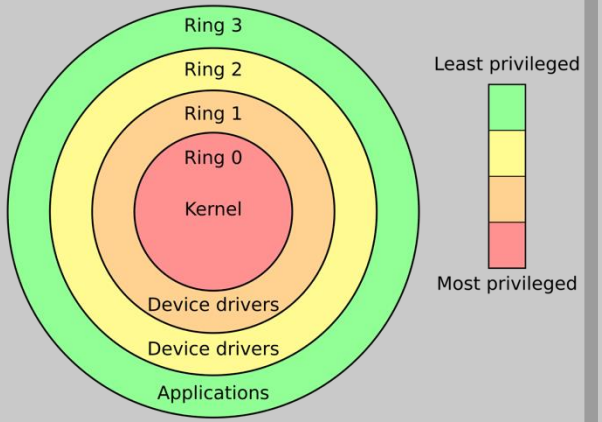
Systemkall

Mellom operativsystemet og programmer (bruker) har vi et systemkall

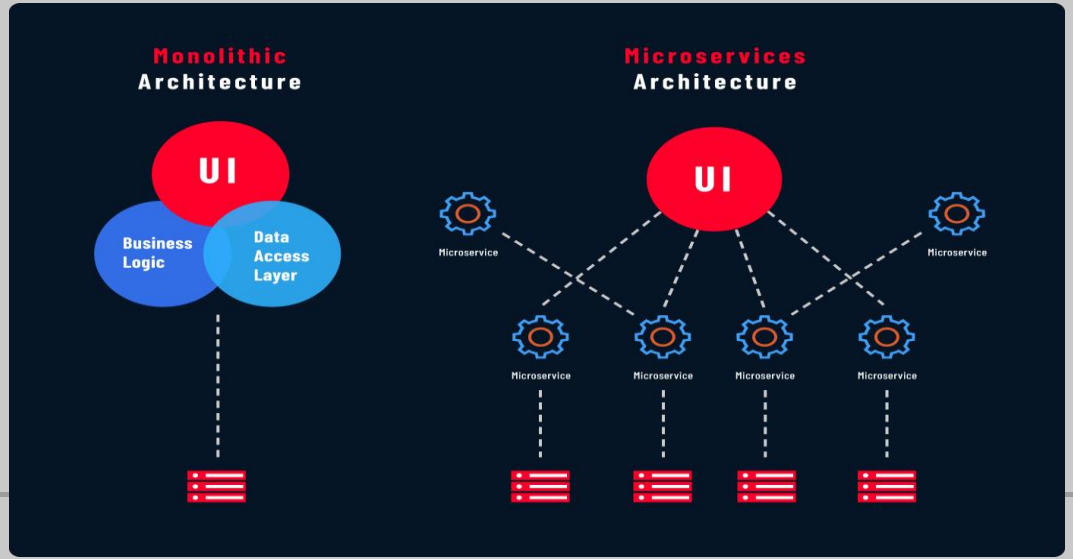


Brukernivå vs. Kjernenivå

- Handler om sikkerhet og beskyttelse I OS
- OS kjører I kjernemodus (alle tilganger)
- Vanlige programmer kjører I brukernivå



Organisering av OS



Hvordan hackes vi?

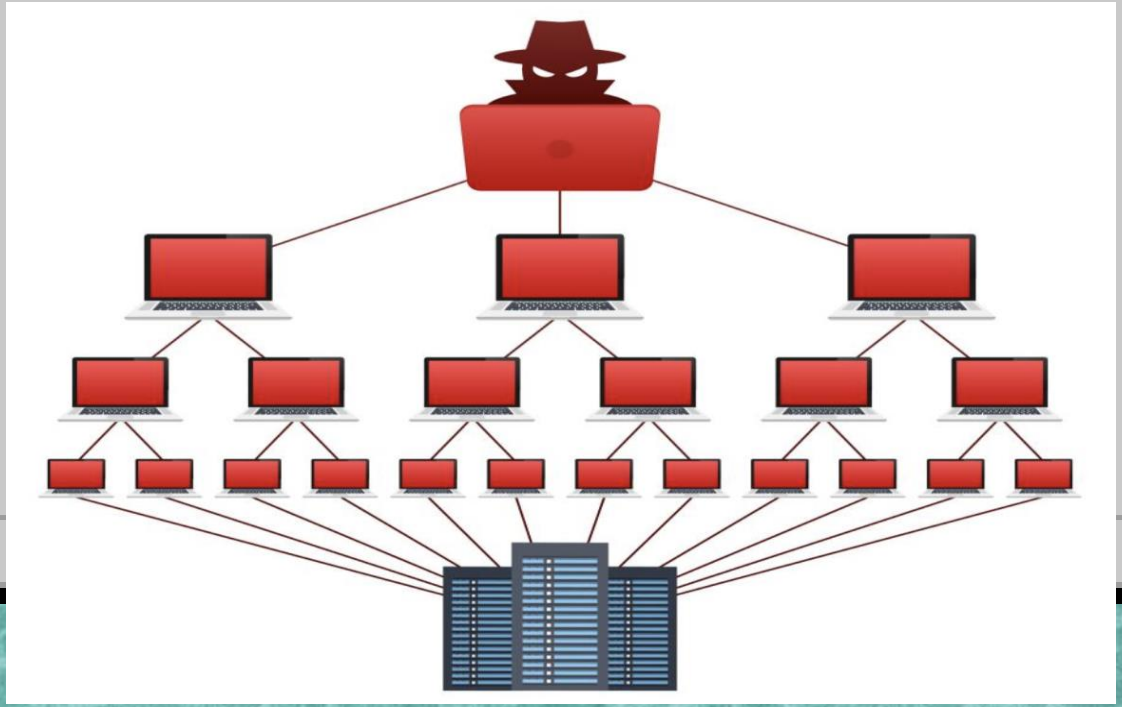
Datanettsikkerhet (skallforsvar/perimetersikring)

- Brannmur:
- Filtrerer trafikk basert på regler for å beskytte nettverket

- Inntrengningsdeteksjon:
- Overvåker trafikk for å oppdage innbrudd og angrep.



Tjenestenektangrep (Dos eller DDoS)



Definisjoner

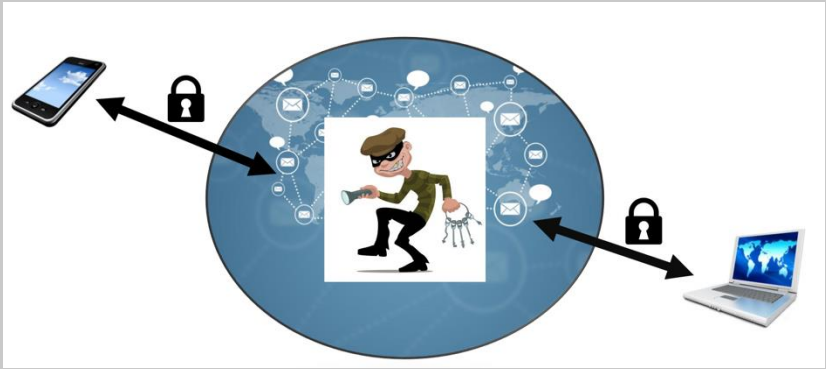
- Digital sårbarhet: En feil i et IKT-system som kan utnyttes
- Nulldags-sårbarhet: Sårbarhet som noen har kunnskap om, før produsenten/leverandøren eller brukerne av systemet/programvaren kjenner til den.
- Skadevare: Samlebetegnelse på programvare som har som mål å gjøre skade.
- Angrepsvektor: Metoden en angriper bruker for å utføre et angrep på en
- datamaskin, et nettverk eller et datasystem
- Sårbarhetsflate: Summen av (de potensielle) sårbarhetene i et system som kan nås og utnyttes av en angriper.

Et utvalg av typer skadevare:

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.

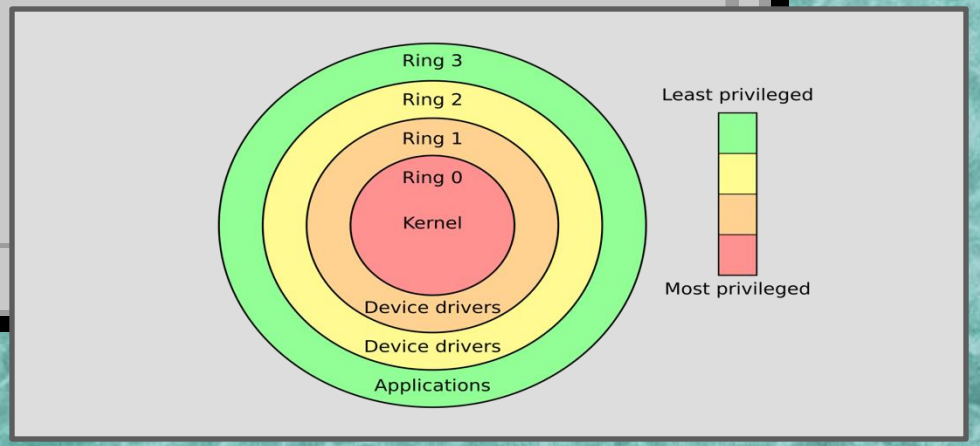
Husk dette!

- Sikkerhetsmodell: Man stoler på endesystemer og man anser nettverket som upålitelig!



Sikkerhet i OS

- OS styrer ulike brukeres tilgang til ressurser (prinsipp om minste privilegium)
- Kjernen I operativsystemet styrer alt
- Kjernen kommuniserer med periferenhetene i datamaskinen gjennom drivere
- Brukerprosesser kommuniserer via kjernen for å kunne benytte periferenhetene.



Vanlige sikkerhetssårbarheter

• **XSS:** Angriperen injiserer skadelig kode i et nettsted for å kjøre i brukerens nettleser.

• **SQL Injection:** Manipulerer databasespørringer for å få uautorisert tilgang eller endre data.

• **Buffer Overflow:** Overfyller en buffer med data og kan kjøre ondsinnet kode.

Husk dette!

Ingenting er sikrere enn det svakeste ledd



Vi er ofte det svakeste leddet

Bedragere lurte ansatt til å utbetale en halv milliard kroner

- Oslo-politiet har samarbeidet med FBI
- Ingen pågrepet så langt

Politiet på bar bakke i Norfund-saken: 100 millioner borte etter digitalt angrep

Norfund bekrefter å ha tapt store summer i en avansert, digital svindel. Politiet har etterforsket saken i det skjulte.

UiT svindlet for 12 millioner

UiT betalte ut 12 millioner kroner til det som viste seg å være svindel. Pengene gikk til det som så ut som en faktura for en røntgenmaskin.

Etterbørs Musikk

Utenlandske «direktørsvindlere» stjal 770.000 kroner fra festspillene i Nord-Norge

Med falske epostadresser og god norsk klarte svindlere å få festspillene i Nord-Norge til å overføre store summer til kontoer i England og Tyrkia.

Spørsmål?

Jobbe med oblig? ☺