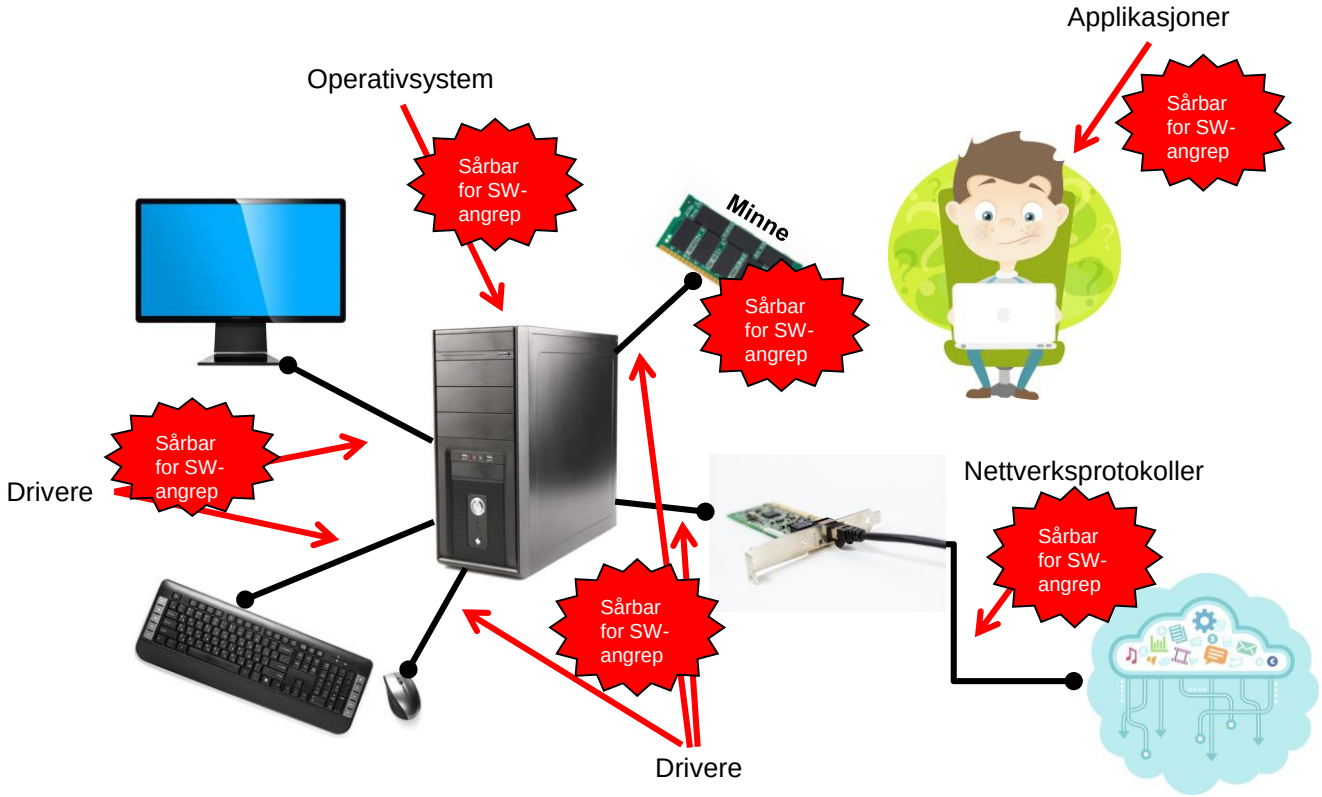
UiO : Institutt for informatikk

Datateknologi og sikkerhet

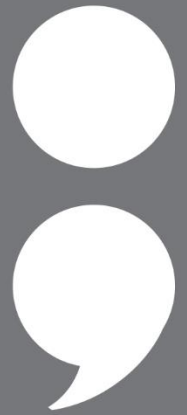
IN1020 – Introduksjon til datateknologi

Datasikkerhet temavideo 9: Sikre datasystemer

Kristin Skar
kritisk@ifi.uio.no


Applikasjoner
Operativsystem
Sårbar for SW-angrep
Sårbar for SW-angrep
Minne
Sårbar for SW-angrep
Sårbar for SW-angrep
Drivere
Nettverksprotokoller
Sårbar for SW-angrep
Sårbar for SW-angrep
Drivere

Systemsikkerhet



UiO : Institutt for informatikk

Sikkerhet i operativsystemet

Dere har tidligere lært:

- *Kjernen* i operativsystemet styrer alt.
- Kjernen kommuniserer med *periferenhetene* i datamaskinen gjennom *drivere*.
- Brukerprosesser må kommuniserer via kjernen for å kunne benytte periferenhetene.
- Minnet i en datamaskin benyttes (bl.a.) til mellomlagring.

Sikkerhet i operativsystemet (forts)

1. Kjerne og drivere er dataprogrammer

- Kan inneholde sårbarheter

2. Kjernen kjører i *supervisor mode* og har tilgang til «alt»

- En sårbarhet i kjernen er kritisk

Ekstremt viktig å holde både operativsystem og drivere fri for sårbarheter:

- Sørge for trygg programvare
- Holde programvaren oppdatert vha. *sikkerhetoppdateringer*.

Bufferoverskridelse

- **Et buffer** er en sammenhengende seksjon i minnet i datamaskinen, avsatt til å inneholde data.
- En feil i et dataprogram, som gjør at programmet når det kjøres kan *overskride bufferets grenser* i minnet, kalles **bufferoverskridelse** (*buffer overflow)*.

Bufferoverskridelse kan utnyttes

- En *bufferoverskridelse* kan krasje et program, føre til korrupte data, eller i verste fall utnyttes av angripere.
- Kreative programmerere kan utnytte en slik sårbarhet:
  - Plassere skadevare på steder i minnet hvor det ligger *kjørbar kode.*
  - Endre en funksjons returadresse til å isteden peke til adressen i minnet der skadevare er plassert.
- Mottiltak
  - Programmere trygt - *desinfisere* all input til programmer
  - Vanskeliggjøre utnyttelse av minnet ved f.eks. uforutsigbare adresserom og sjekksum for data i minnet.

Sikkerhet fra laveste nivå

Ved oppstart av en datamaskin:

1. Starter bootloader fra BIOS
2. Bootloader laster kjernen i operativsystemet

Dilemma: Er programvaren som startes identisk med den vi antar at startes og kjører?

Applikasjonssikkerhet

UiO : Institutt for informatikk

Sikre applikasjoner

Design og utvikling med tanke på trygg bruk:

- I designfasen:
  - Kartlegge potensielle trusler
  - Identifisere tiltak som kan iverksettes for å motvirke truslene
- I programmeringsfasen:
  - Unngå å skape eller tilrettelegge for sårbarheter
- I produksjonsfasen:
  - Holde all programvare oppdatert

Ressurser: OWASP Top 10

«The Open Web Application Security Project»

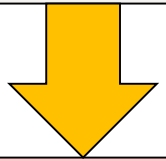
OWASP Top-10 2021:

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery

Kilde: https://owasp.org/Top10/

Konklusjon: Helhet er nødvendig

Sikkerhet i applikasjonsprogramvare er ikke sikrere enn sikkerheten i datamaskinen den kjører på.



Sikkerhet i datamaskinen avhenger av sikkerhet i systemprogramvare, boot-prosess, maskinvare.

UiO : Institutt for informatikk

Takk!

mn.uio.no/ifi