Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver

Teori 2 (Del 2): Systemsikkerhet

Oppgave 1: Tillitsanker

Hva menes med begrepet «tillitsanker» i systemsikkerhet?

Oppgave 2: Virtualisering

a. Hva er forskjellen mellom et generelt «system» og et «virtuelt system»?
b. Hva er en virtuell maskin når man snakker om datamaskiner?
c. På hvilken måte kan virtualisering støtte sikkerhet?

Oppgave 3: Privilegienivåer

Søk og finn artikkelen «Det er ikke Windows, Linux eller MacOS som har den egentlige kontrollen over pc-en din», eller besøk nettsiden
https://www.digi.no/artikler/det-er-ikke-windows-linux-eller-macos-som-har-den-egentlige-kontrollen-over-pc-en-din/411596

a. Anta VM-arkitektur Type 1 (native/direkte): Hvilke privilegienivåer har prosesser for (i) en bruker i en VM, (ii) administrator/root i en VM, og (iii) hypervisor?
b. Anta VM-arkitektur Type 2 (hosted/vertsbasert): Hvilke privilegienivåer har prosesser for (i) en bruker i en VM, (ii) administrator/root i en VM, og (iii) hypervisor?
c. Teknisk sett støtter mikroprosessorer privilegienivåene fra -1 til 3. Uformelt snakkes det også om at privilegienivåene -2 og -3 finnes. Hva menes med disse nivåene?
d. Hva er Intel ME (Management Engine)?
e. Hva er Intel AMT (Active Management Technology)?
f. På hvilken måte kan man si at Intel ME og AMT utgjør sårbarheter?

Oppgave 4: Hindre sporing av mobiltelefoner

På samme måte som med vanlige datamaskiner, er mikroprosessoren i en smarttelefon aktiv så lenge telefonen har strøm. Trusselaktører med tilstrekkelig kompetanse kan utnytte dette til å spore en mobiltelefon selv når den er helt avslått. Foreslå tiltak som hindrer at en mobiltelefon kan bli sporet på denne måten.

Oppgave 5: Beskyttelse av minnet

a. Mange prosesser kjører samtidig på en computer. Forklar hvorfor en brukerprosess (med privilegienivå 3) ikke kan aksessere minneområdet (data og kode) til andre prosesser.
b. Hva er stack canaries og hva er formålet med det?
c. Hva er ASLR (Address Space Layout Randomization) og hva er hensikten med det?

Oppgave 6: TPM (Trusted Platform Module)

TPM (Trusted Platform Module) er spesifisert av TCG (Trusted Computing Group).

a. Forklar de tre viktigste TPM-støttede tjenestene: i) autentisert/sikker oppstart, ii) forseglet lagring (Sealed Storage), iii) fjernattestering (Remote Attestation).
b. Hvilken TPM-tjeneste brukes av Windows Bitlocker-diskkrypteringsapplikasjonen?
c. Anta at en computer har en nulldagssårbarhet som en exploit utnytter for å ta kontroll over computeren. Kan TPM beskytte mot denne trusselen? Forklar hvorfor / hvorfor ikke.