Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver med løsningsforslag

Teori 2 (Del 2): Systemsikkerhet

Oppgave 1: Tillitsanker

Hva menes med begrepet «tillitsanker» i systemsikkerhet?

Løsningsforslag

Et tillitsanker for systemsikkerhet er et element som danner grunnlag for å etablere/garantere sikkerhet i andre deler av systemet. Tillitsankeret må i utgangspunktet ha høy sikkerhet/robusthet, fordi det ikke fins andre elementer som kan etablere/garantere sikkerhet for tillitsankeret.

1. Et eksempel på tillitsanker er fastvare (firmware) for sikker oppstart med UEFI, der fastvare-koden ligger lagret i ROM (Read Only Memory) som er en fysisk brikke integrert i systemet. Det er vanskelig å angripe fastvare-koden i ROM-brikken, slik at den i utgangspunktet har høy sikkerhet. Dette tillitsankeret brukes for å etablere/garantere integritet av OS-kernel og drivere under systemoppstart.
2. Et annet eksempel på tillitsanker er rotsertifikater i en PKI. Validering av underliggende sertifikater, som f.eks. serversertifikater for nettsteder, avhenger av et rotsertifikat. Hvis rotsertifikatet er korrupt/falskt, vil underliggende sertifikater ikke gi noen kryptografisk sikkerhet. Det betyr at angripere f.eks. kan lese kryptert trafikk eller sende falske data.

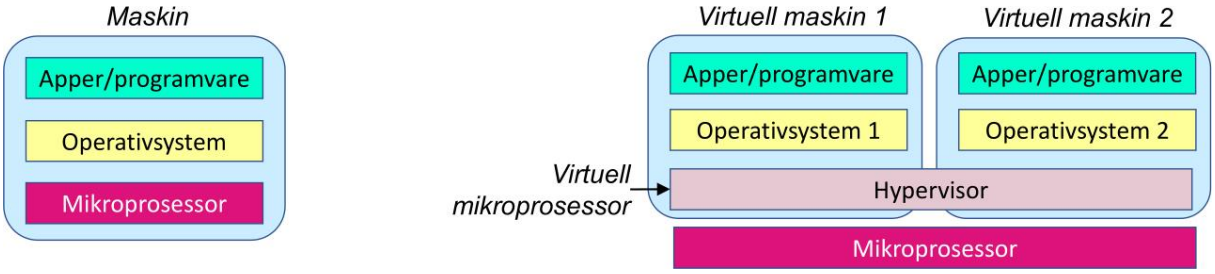
Oppgave 2: Virtualisering

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?

Løsningsforslag

a. Et virtuelt system er noe som etterligner og har mange av de samme egenskaper som det egentlige systemet. For eksempel, den verden vi ser i VR-briller er virtuell. Når vi setter på VR-briller føler vi at vi er i en verden som har en del av de samme egenskaper som den virkelige verden, og typisk også mange egenskaper som ikke fins i den virkelige verden.
b. En virtuell maskin i sammenheng med datamaskiner er et operativsystem som kjører over en hypervisor. Slike operativsystemer kalles ofte gjeste-OS, og er egentlig helt vanlig operativsystemer. Man sier at de er virtualisert fordi de kjører over en hypervisor som jo er en virtuell mikroprosessor. Med virtualisering er det

altså mulig å kjøre mange separate virtualiserte gjeste-OS-er med tilhørende apper/programvare på samme fysiske maskinvare. Figuren nedenfor illustrerer forskjellen på en «maskin» og en «virtuell maskin».



c. Bruk av virtuelle maskiner kan støtte sikkerhet på forskjellige måter, f.eks.
   i. Det gjør at operativsystemer er separert fra hverandre. Det betyr at et kompromittert operativsystem eller en kompromittert app ikke kan skade/påvirke andre operativsystemer eller apper på andre operativsystemer.
   ii. Ved kompromittering er det lett å slette det kompromitterte operativsystemet og den virtuelle maskinen, og starte en ny virtuell maskin som i utgangspunktet har integritet.
   iii. Ved testing/analyse av skadevare er det nyttig å la skadevaren kjøre på en virtuell maskin, slike at skadevaren ikke kan skade hele systemet, bare operativsystemet der skadevaren kjøres.
   iv. Enkelt å ta et snapshot (dump av minnet) av en virtuell maskin for å analysere hva som skjer, f.eks. når skadevare kjøres eller noe krasjer.
   v. Ved å sette likhetstegn mellom virtualisering og skytjenester (på den måten at skyleverandører tilbyr et virtuelt datasenter) unngår man at et eget fysisk datasenter er sårbart for direkte fysiske angrep. Denne strategien gjorde bl.a. at Ukraina i stor grad kunne opprettholde sine digitale forretningsprosesser under den russiske invasjonen i 2022.

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?

Løsningsforslag

a. Privilegienivåer for ulike prosesser i VM-arkitektur Type 1 (native/direkte).
   i. Bruker: privilegienivå 3
   ii. Administrator/Root: privilegienivå 0
   iii. Hypervisor: privilegienivå -1
b. Privilegienivåer for ulike prosesser i VM-arkitektur Type 2 (hosted/vertsbasert).
   i. Bruker: privilegienivå 3
   ii. Administrator/Root: privilegienivå 3
   iii. Hypervisor: privilegienivå 3

c. UEFI/BIOS avgjør hvilket OS eller hvilken hypervisor som skal lastes når datamaskinen starter. Det kan tolkes slik at UEFI/BIOS har høyere privilelgienivå (lavere tall) enn OS og hypervisor, som dermed blir privilegienivå -2. Mikroprossoren har innebygd mikro-OS som kalles ME (Management Engine). Så lenge det er strømtilførsel kjører ME selv om datamaskinen er avslått. ME har full kontroll over mikroprosessoren uansett hvilket OS eller hvilken hypervisor som er lastet av UEFI/BIOS. Det kan tolkes slik at ME kjører med høyere privilegienivå (lavere tall) enn UEFI/BIOS, som dermed blir privilegienivå -3.

d. Intel ME (Management Engine) er et lite subsystem som er integrert med Intel mikroprosessorer. Dette mini-systemet er basert på operativsystemet MINIX og er fullstendig innebygd i CPU-en. Så lenge mikroprosessoren har strøm er ME aktivt til enhver tid, dvs. uansett om plattformen kjører normalt, er i dvale eller er skrudd helt av. Med andre ord er ME aktiv så lenge computeren er koblet til strømkontakten eller har strøm på batteri. ME har svært lavt strømforbruk, slik at det knapt merkes at ME kjører. ME har full tilgang til systemmaskinvare, inkludert systemminne, skjerm, tastatur, kamera, mikrofon, periferiutstyr og nettverk.

e. Intel AMT (Active Management Technology) er en teknologi for fjernadministrasjon av computere innen virksomheters datanett. AMT er altså for virksomheters administrasjon av computere, ikke for administrasjon av private computere. AMT er basert på ME (Management Engine) som er uavhengig av operativsystemet på en computer. Ettersom ME støtter nettverkskommunikasjon over internett kan en virksomhet gjennom fjernadministrasjon f.eks. starte en computer som er skrudd av, konfigurere og installere nytt operativsystem.

f. ME har full kontroll over Intel-prosessorer, og er derfor den mest privilegerte funksjonen til en Intel-basert computerplattform. AMT gjør at en computer kan fjernstyres, og er dermed en potensiell bakdør. Et relevant trusselscenario er f.eks. at angripere klarer å ta kontroll over ME via ekstern tilgang basert på AMT. Så lenge ME og AMT ikke har sikkerhetssårbarheter er det intet problem, men hvis det oppdages sårbarheter vil det potensielt være svært alvorlig.

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.

Løsningsforslag

Mulige tiltak for å hindre at avanserte trusselaktører kan spore en mobiltelefon er:

- Ta ut batteriet
- Sørg for at batteriet er helt utladet
- Oppbevar mobiltelefonen i et faradaybur (lomme med (tykt) metall rundt)
- Legg igjen mobiltelefonen hjemme, da vil trusselaktøren kanskje tro du er hjemme selv om du er et annet sted.

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?

Løsningsforslag

a. Hver prosess har et eget virtuelt minneområde som operativsystemet oversetter til fysiske minneadressen. En prosess kan bare aksessere sitt eget virtuelle minneområde og kan derfor ikke nå andre prosessers fysiske minne.
b. Stack canaries er en mekanisme mot en type buffer-overflow exploit som ved å manipulere instruksjonspekere på stacken kan gjenbruke legitime programinstruksjoner fra forskjellige programvaremoduler og eksekverer disse som skadelig kode. En måte å utføre dette er å overskrive returadressen i stack-rammen til et metode- eller funksjonskall til plassen hvor skadelig kode ligger. En stack canary er en tilfeldig verdi eller sjekksum som kan brukes for å sjekke om returadressen har blitt endret og prosessen termineres dersom det er tilfellet.
c. ASLR er også en mekanisme mot buffer-overflow. En exploit trenger å vite den nøyaktige plasseringen av kodeinstruksjonene i minnet. ASLR sørger for at minnesegmenter av det virtuelle adresseområdet blir lastet til tilfeldige steder når programmoduler starter. Det er relativt lett å utnytte buffer-overflow til å injecte data på stacken. ASLR gjør det vanskelig (men ikke umulig) for en exploit å manipulere instruksjonspekere gjenbruke legitim kode fra kjente minneadresser.

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.

Løsningsforslag

a. TPM-funksjoner:
   i) Autentisert oppstart: Rapporter programmers integritetsstatus under oppstart. Sikker oppstart: Stopp oppstart hvis et program har ødelagt integritet.
   ii) Forseglet lagring (Sealed Storage): Kryptering / dekryptering med hemmelige nøkler basert på TPM, og potensielt basert på korrekt plattformintegritet,
   iii) Fjernattestering: rapportering av en computers identitet og systemstatus til en ekstern part gjennom datanett/internett

b. Bitlocker bruker forseglet lagring (Sealed Storage).

c. TPM beskytter ikke mot nulldagssårbarheter mens computeren kjører, fordi TPM eventuelt bare beskytter oppstartsprosessen. Kompromittering av operativsystemet gjennom en nulldagssårbarhet kan potensielt bli oppdaget neste gang computeren starter. Detektering av kompromittert operativsystem kan baseres på sikker oppstart som vanligvis gjøres med UEFI (Unified Extensible Firmware Interface), men som i teorien også kan baseres på TPM . Annen skadevare og kompromittering av programvaremoduler som ikke dekkes av sikker oppstart vil heller ikke bli detektert gjennom sikker oppstart. Deteksjon av slik skadevare kan potensielt gjøres med antivirusprogrammer eller gjennom monitorering av systemer og nettverk.