Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 7: Systemsikkerhet

Spørsmål 1

a. Hvorfor bruker operativsystemer virtuelle adresseområder og virtuell adressering i stedet for fysiske minneadresser for aktive prosesser?
b. Hva er fordeler og ulemper med å bruke virtuell adressering?

Spørsmål 2

a. Hva er DEP (Data Execution Prevention) (dataeksekveringsblokk) og hva er hensikten med denne mekanismen?
b. Hva er ASLR (Address Space Layout Randomization) og hva er hensikten med denne mekanismen?

Spørsmål 3

a. Hva er forskjellen mellom følgende konsepter?
   - *"et tiltrodd system"*
   - *"et tillitsverdig system"*
b. Forklar betydningen av følgende utsagn.
   - *"Et tiltrodd system kan fører til brudd på informasjonssikkerhet"*.

Spørsmål 4

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

a. Forklar de tre hovedtjenestene støttet av TPM: i) Autentisert oppstart (Authenticated Boot), ii) Forseglet lagring (Sealed Storage), iii) Fjernattestering (Remote Attestation).
b. Hvilken TPM-tjeneste brukes av Bitlocker diskkryptering i Windows?
c. Anta at en computer har en null-dagssårbarhet som utnyttes av en exploit til å ta kontroll over computeren. Svar Ja/Nei til om TPM kan beskytte mot denne trusselen, og forklar hvorfor/hvorfor ikke.

Spørsmål 5

Hva er forskjellen mellom sikker oppstart og autentisert/målt oppstart?

Spørsmål 6

For at kjøre virtualisering på en computer er det nødvendig å aktivere BIOS-instillingen 'hardware-virtualisering'. Hvorfor er ‘hardware-virtualisering’ ofte deaktivert i nye computere, slik at brukeren manuelt må aktivere innstillingen for å kunne kjøre en hypervisor?

Spørsmål 7

a. Hva er Intel ME (Intel Management Engine)?
b. Hva er hensikten med Intel ME?
c. Hva er MINIX?
d. Hva er Intel AMT (Active Management Technology)?
e. På hvilken måte kan Intel ME og AMT eksponere computeren for cybertrusler?

Spørsmål 8

Anta at du ønsker å implementere en "tillitsrot for måling" basert på TPM.

a. Hvor ville du foreslå å lagre programmodulen?
b. Hvor ville du absolutt ikke lagre programmodulen?
c. Diskuter hvorfor eller hvorfor ikke med referanse til a) og b) ovenfor.

Spørsmål 9

a. Forklar prinsippet om sikker oppstart med UEFI (Unified Extensible Firmware Interface).
b. Hvorfor kan man si at dette ikke er et eksempel på tiltrodd oppstartsprosess?