Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 1: Grunnleggende sikkerhetsbegreper

Spørsmål 1

a. Les definisjonene på konfidensialitet, integritet og autorisering i X.800 (http://www.uio.no/studier/emner/matnat/ifi/IN2120/h18/docs/x800.pdf) .
   i. Er definisjonene på konfidensialitet og integritet fra X. 800 meningsfulle i forhold til hvordan autorisering er definert? Hvorfor eller hvorfor ikke?
   ii. Er den amerikanske «Computer Fraud and Abuse Act» meningsfull fra samme perspektiv? Se f. eks «18 U.S. Code § 1030 - Fraud and related activity in connection with computers» http://www.law.cornell.edu/uscode/text/18/1030
   iii. Foreslå en definisjon på «autorisering» som gjør at definisjonene på konfidensialitet og integritet i X.800 blir menmingsfulle, og også den amerikanske «Computer Fraud and Abuse Act».
b. Er læreboka (Harris & Maymí CISSP, 7Th Edition) tydelig på tolkningen av autorisering? Se f.eks. s.725, 2. og 3. avsnitt. (Ch. 5, Sec. «*Identification, Authentication, Authorization, and Accountability*» (*Identifisering, autentisering, autorisering og sporbarhet*)
c. Hvordan er "autorisering" definert på wikipedia? https://en.wikipedia.org/wiki/Authorization
d. Forklar om Wikipedias definisjon er kompatibel med definisjoner på konfidensialitet, integritet og tilgjengelighet i X.800 og ISO 27000.

Spørsmål 2

a. Nevn relevante trusler mot trinnene i konfigurasjonsfasen av IAM (identitets- og tilgangshåndtering).
b. Nevne relevante trusler mot trinnene i driftsfasen av IAM (identitets- og tilgangshåndtering).

Spørsmål 3

a. Hvilke sårbarheter er hovedsakelig utnyttet av phishing-angrep?
b. Foreslå sikkerhetstiltak for å forhindre eller mitigere phishing-angrep.

Spørsmål 4

Artikulere en enkel sikkerhetspolicy for din personlige laptopp, som uttrykker hvem som er autorisert til å få tilgang til å bruke den.

Spørsmål 5

X.800 angir sikkerhetstjenester for datanettverk, for eksempel OSI-og TCP/IP-baserte datanettverk. Sjekk tabell 1 (s. 15) i X.800 for å se hvilke sikkerhetsmekanismer (tiltak) som kan brukes til å støtte kommunikasjons sikkerhetstjenestene nedenfor, og forklar hvordan hver mekanisme tilbyr tjenesten.

a. Forbindelsesløs konfidensialitet (dvs. meldingskonfidensialitet)
b. Forbindelsesløs integritet (dvs. meldingsintegritet)

Spørsmål 6

En bruker har autentisert seg på en webtjeneste på Internett ved starten av en økt, og sender data til Web-serveren via klientcomputeren. Forklar i hvilken grad tjenestetilbyder kan ha visshet om at dataene som mottas i løpet av økten er autentisk basert på brukerautentiseringen.

Spørsmål 7

a. Forklar hvorfor personopplysningsvern ikke kan oppnås kun ved å innføre tiltak for informasjonssikkerhet (KIT-egenskaper).
b. Forklar hvorfor personopplysningsvern avhenger av informasjonssikkerhet.