Løsningsforslag
Eksamen SIE5040 Informasjonssikkerhet vår 2003

Oppgave1. Modeller

a) Konfidensialitet, autentisitet (integritet og ubenektelighet), tilgjengelighet
b) Økt tillit til utstyret. Klassifisering ved spesifikasjon innkjøp. Kan forenkle kontroll mot regelverk basert på evalueringsklasser. Risikoanalyse forenkles.
c) Se lærebok kap 4.2
d) Nedgradering av informasjon er ikke mulig innenfor modellen, f.eks. kan ikke subjekt klassifisert for topp hemmelig kommunisere til andre subjekter som er lavere klassifisert.
   Fokus er på konfidensialitet, i sivile omgivelser vil integritet være vel så viktig å sikre.
   Klassifisering er statisk.
e) Klassifisering i BLP-formalismen er statisk ("tranquility"), mens dynamisk klassifisering er essensielt i Kinamur-modellen.

Oppgave 2. Aksesskontroll

a) Abstrakt konsept for aksesskontroll som refererer til en abstrakt automat som formidler alle referanser fra subjekter til objekter. Tre egenskaper kreves: 1) Korrekt virkemåte 2) Fullstendig formidling 3) Beskyttet mot endring.
b) Utsagnet er en begrunnelse for å autentisere påstått brukeridentitet.
c) For: Det er en sikkerhetsrisiko fordi Superuser har alle rettigheter i opsys.
   Mot: Dette forenkler drift av systemet og dermed oversikt over korrekt sikkerhetskonfigurasjon.
d) Et operativsystem må, for å beholde sin egen integritet, beskyttes mot brukerprosesser. Dermed innføres det et skille, som oftest hardwarestøttet, mellom brukerprosesser og systemprosesser, og problemet oppstår hvordan switche mellom de to modi. "Styrt iverksetting" kobler mellom de to kjøremodi i Unix ved hjelp av Set UserID (SUID) program, f.eks. ved endring av passord av brukeren.
e) Se definisjon i lærebok avsnitt 12.2.1 side 205.

Oppgave 3. Sertifikater

a) Multiplikasjon av to store primtall er en enveisfunksjon.
b) Se læreboka avsnitt 10.2.1 side 168. Sterk kollisjonsfrihet medfører svak kollisjonsfrihet. Anvendelser: Konstruksjon av digitalsignatur. Konstruksjon av MAC.
c) X.509 sertifikat er en spesifikk format-standard for autentisering av offentlige nøkler. Innhold: Versjonsnr., serienr.,signaturalgoritme, utstedernavn, gyldighetsperiode, subjektnavn, subjektets offentlige nøkkel, utstederidentifikator, subjektidentifikator.
d) 1) Innenfor gyldighetsperiode? 2) Er utsteder tiltrodd? 3)Subjektnavn ok? 3) Signatur stemmer?
e) 1) Distribusjon av offentlige nøkler. 2) Utstedelse av aksessrettigheter 3) Autentiseringsprotokoller f.eks. SSL 4) Tillitshierarkier.
f) Se læreboka avsnitt 13.2.2 med figur 13.12. Handshake protocol.
g) KeyStore skal inneholde en privat nøkkel og tilhørende sertifikat, sammen med Root og ServerCerts sertifikatene. Det er ikke spesifisert hvem man skal stole på (forsvant fra oppgaveteksten). Antatt svar er da Root. Full pott gies

også til de som bemerker at det er udefinert. Å spesifisere at KeyStore = TrustStore er ikke direkte riktig.

Oppgave 4. Sikkerhetsanalyse

a) 68^5 < 10^10 < 68^6, dvs lengde 6 tegn.
b) 96^5 < 10^10 < 96^6, dvs. Lengde 6 tegn.
c) Antall passord uttestet innenfor 72 timer:
   10 ord/s * 3600 s/time * 72 timer = 2 592 000 ord
   Antakelse: Pr(treff innenfor 1/k av søkerommet) = 1/k = 10^-6
   Søkerom: n= 2 592 000 * 10^6 = 2,592 * 10^12
   log[base68](n) = 6,77 < 7 tegn.
d) 1) Passordet sendes åpent over radioforbindelse → beskytt passordet med kryptering, eller lag en autentiseringsprotokoll i stedet.
   2) Passordtabell må lagres i LM → Beskytt tabellen vhj. enveisfunksjon.
   3) Data sendes åpent over Bluetooth → sett opp en kryptert forbindelse.
   4) LM har ikke autentisert seg overfor brukeren → bruk en gjensidig autentiseringsprotokoll
   5) Uttesting av passord → detekter uttesting og gi avbrudd eller tidsforsinkelser.
   6) Uautorisert bruk av LM → utfør logging av viktige hendelser i LM
e) (68^6)^(2/3) = 68^4 = 21,4*10^6verdier i tabellen.
   Anta hver verdi kan komprimeres til 6 bytes, gir ca. 128 Mbytes, som kan lagres i primærminne.
f) Tabelloppslaget er neglisjerbart i forhold til beregningene.
   Beregningstid (68^6)^(2/3)*10^-3 s = 21381 s = 5,9 timer.
   Dette søket tar 1/12 av dimensjoneringstiden ovenfor, men avhenger av at verdien for det krypterte passordet er blitt tilgjengelig, f.eks. fra passordfilen lagret i LM.