Uppdaterad 2019 för nya kursboken.

Tentamen i Säkerhet (EDA625) för IT-programmen

070816, kl 14

Tillåtna hjälpmedel: Miniräknare

Maxpoängen för provet är totalt 60 poäng. För betyget 3 krävs minst 30 poäng som får vara fördelade godtyckligt mellan uppgifterna. Lycka till !

1. Inom krypteringstekniken finns en mängd olika begrepp för att åstadkomma integritetsskydd, bl.a., hash funktioner och digital signatur. Förklara dessa utförlig och hur de hänger ihop. (10p)

Kort svar:

Hash funktion är en sk envägsfunktion; det är lätt ett beräkna f(x) men den är svårt, praktisk inte genomförbart, att bestämma x så att f(x) är ett givet värde, och likadant att det är svårt att hitta x och y så att f(x)=f(y). Digital signatur är värdet på en sträng som genom en beräkning är kopplad till ett meddelande så att det är lätt att verifiera att en given person har skapat signaturen (utföra beräkningen), att enbart innehavaren av en hemligt kan utföra beräkningen, samt att den som har skapat signaturen inte kan neka denna handling (non-repudiation). Innan man skapar en digital signatur av ett meddelande så beräknas först dess hash värde, dvs man signerar hash värdet istf själva meddelande. Hashning är också nödvändig vid RSA signering för att förhindra att man kan miskruka den multiplikativa strukturen.

2. RSA kryptering är grunden till många olika kryptosystem. När man dimensionerar att RSA system så väljar man två primtal p och q. Låt p=17 och q=31. Låt den publika exponenten vara e=3.
   a. Bestäm den privata nyckel d (5 p)
   b. Kryptera medelandet m=5. (2,5p)
   c. Avkryptera kryptomedelandet c=7 (2,5p)

Kort svar: uppgiften var denna gång lite speciellt

a) Man kan inte använda e=3 eftersom e delar q-1=30, alltså kan d ej bestämmas

b) 5^3 mod (p q) = 125

c) Det går inte

3. Ett annat begrepp är authentisering.
   a) Vad vill man åstadkomma med en autentiseringsmetod? (5 p)
   b) Ger ett exempel på tvåfaktorautentisering (2,5p)
   c) Beskriv skillnaden mellan en synkron och en asynkron autentiseringstoken (2,5p)

Kort svar:

a) Man vill säkerställa identiteten på ett sådan sätt att metoden ej gör det möjligt för utomstående att autentisera sig genom att observera en eller flera autentiseringar

b) En bank token med PIN kod.

c) Synkron token: token och server har en synkron klocka och responsen är beroende på kockans värde. Responsen av ett asynkron token förutsätter ingen synkronisering av en klocka eller räknare.

4 a) Vad är en DMZ (demilitariserad zon) (2,5p)

b) Vilka hot kan finnas mot en brandväggslösning? (2,5p)

c) Definiera 1) mask, 2) trojansk häst och 3) virus 4) macrovirus (5p)

Kort svar:

a) DMZ är ett internet domän som ligger mellan ett intranät och internet med syfta att vara ett kontrollerad (från intranät hållet) domän för att antal förbestämda (servar) funktioner så som email, externa web sidor som ska vara nåbar från internet.

b) 1) att underhållet är bristfälligt, 2) att personalen inte är kunnig nog att konfigurera brändväggen på ett korrekt sätt, 3) att bakom liggande system har svagheter som gör att men vi öppna protokol, tex http, kan ta sig in bakvägen och sedan ta kontroll.

c) se kursmaterialet

5. a) Vad menas med [illegible]ation i datorsammanhang och vari ligger risken (hur och varför kan [illegible]en angripare). (2,5p)

b) En vanlig referensmodell när det gä[illegible]byggnaden av ett OP-system är Bell-LaPadula. Vad är modellens g[illegible]amn minst två regel i modellen.

(4p)

c) Vad är en replay attack och nämn minst två tekniska tillvägagångsätt att blockera sådana attacker. (3,5p)

Kort var:

a) *Att exekvering av program inte direkt görs i anroparens namn men i namn av den som äger programmet. Det kan leda till att man kan få någon annans rättigheter om vid ett exekveringsfel av ett sådant program man hänger kvar i som programägarens namn istf för att komma tillbaka till den ursprungliga anroparens.*

b) *Modellen beskriver accesskontrol ur perspektivet att upprätthålla konfidentialitet. Modellen ger objekt och subjekt säkerhetsnivåer och beskriver ett regelverk för access där ingen information (objekt) på en viss säkerhetsnivå kan läsas av subjekt som inte har tillräckligt behörighet (read-up) samt att det inte går att objektet görs tillgänglig för en icke behörig subjekt (write-down).*

c) *Vid en replay attack används information inspelad vid ett tidigare förlopp. Slumptal eller räknare (tid) kan användas för binda ett förlopp till det aktuella händelse.*

6 SSL, TLS, samt Ipsec är tre protokoll som används ofta för att säkra Internet förbindelse.

a) Förklara skillnaden mellan SSL, TLS och Ipsec. (5 p)
b) Ipsec: vad betyder AH och ESP? (2,5p)
c) Vad händer och i vilken ordning under en TLS handshake (2,5p)

Kort svar:

a) SSL och TLS är båda protocol på TCP nivå som realiserar authentisering, integritetsskyd, skydd mot replayattacker samt konfidentilitet. SSL är ett gammal protokoll som inte underhålls längre. TLS underhålls av IETF. Man använder ofta också namnet "SSL" där man i praktiken använder TLS. Ipsec är ett protokoll på IP nivå som förutsätter att man har redan etablerat ett nyckel par mellan de två noder som använder protokollet. IPsec kan ge integritetsskyd, skydd mot replayattacker samt konfidentilitet. Det finns olika protokoll sätt inom IPsec med olika skydd. Det sk Authentication-Header protokoll ger inget konfidentialitetsskydd.

b) Se kursmaterialet om IPsec

c) Se kursmaterialet om TLS