Tietoturvan perusteet, erilliskoe 5.6.2012

Kirjoita jokaiseen vastauspaperiin kokeen nimi, pvm, oma nimesi, henkilötunnuksesi tai opiskelijanumerosi ja allekirjoituksesi. Numeroi sivut. Jätä ensimmäisen sivun yläreunaan leveä marginaali.

1. Luennoilla on esitelty kymmenen turvallisen suunnittelun periaatetta. Esittele näistä viisi mielestäsi tärkeintä. Anna jokaisen säännön yhteydessä myös esimerkki, minkälainen tietoturvaongelma voi syntyä, jos sääntöä ei noudateta.

2. **a)** Kuvaile, mieluiten piirroksen avulla, salalohkojen ketjutusmenetelmä CBC (cipher block chaining).

   b) Miten RSA-allekirjoituksen verifiointi tapahtuu. Erityisesti selitä varmenteiden rooli tässä yhteydessä.

3. Ensimmäinen X.509 standardi määritteli kolminkertaiseen kättelyyn perustuvan todennusprotokollan, jossa oli kuitenkin turvallisuusaukko. Protokolla oli seuraava:

   1. $A \longrightarrow B: \quad t_A,\ r_A,\ ID_B,\ E_B(K_{AB}),\ Sig_A(t_A, r_A, B, E_B(K_{AB}))$
   2. $B \longrightarrow A: \quad t_B,\ r_B,\ A,\ r_A,\ E_A(K_{AB}),\ Sig_B(t_B, r_B, A, r_A, E_A(K_{AB}))$
   3. $A \longrightarrow B: \quad r_B, Sig_A(r_B)$

   Yllä r_A and r_B ovat satunnaislukuja, nonsseja, t_A ja t_B ovat aikaleimoja, Sig_A tarkoittaa allekirjoitusta A:n salaisella avaimella, E_B tarkoittaa salausta B:n julkisella avaimella ja K_{AB} on generoitu istuntoavain (joka ei ole tärkeä tässä tarkastelussa). X.509-dokumentti toteaa, että aikaleimojen tarkistus on vapaaehtoista. Tarkastellaan kuitenkin seuraavaa esimerkkiä: Oletetaan, että A ja B ovat käyttäneet protokollaa jossain aikaisemmassa tilanteessa ja että vastustaja C on siepannut nuo aikaisemmat sanomat. Oletetaan lisäksi, ettei aikaleimoja käytetä, vaan ne kaikki on asetettu nollaksi (kuten standardi mahdollistaa). Nyt C haluaa tekeytyä A:ksi kommunikoidessaan B:n kanssa. C lähettää ensimmäisen aikaisemmin sieppaamansa viestin B:lle:

   $$C \longrightarrow B: \ 0,\ r_A,\ ID_B,\ E_B(K_{AB}),\ Sig_A(0, r_A, B, E_B(K_{AB})).$$

   B vastaa luullen kommunikoivansa A:n kanssa:

   $$B \longrightarrow C: \ 0,\ r'_B,\ A,\ r_A,\ E_A(K_{AB}),\ Sig_B(0, r'_B, A, r_A, E_A(K_{AB})).$$

   C houkuttelee jollain tavalla A:n aloittamaan uuden istunnon C:n kanssa. A lähettää C:lle:

   $$A \longrightarrow C: \ 0,\ r'_A,\ ID_C,\ E_C(K'_{AB}),\ Sig_A(0, r'_A, C, E_C(K'_{AB})).$$

C vastaa A:lle käyttäen samaa nonssia kuin B on käyttänyt C:n kanssa kommunikoidessaan:

$$C \longrightarrow A: \;\; 0,\; r'_B,\; A,\; r'_A,\; E_A(K'_{AB}),\; Sig_B(0, r'_B, A, r'_A, E_A(K'_{AB})).$$

A vastaa sanomalla

$$A \longrightarrow C: \;\; r'_B, Sig_A(r'_B).$$

Tämä on juuri sitä mitä C tarvitsee vakuuttaakseen B:lle, että B juttelee A:n kanssa, joten C toistaa sanoman B:lle:

$$C \longrightarrow B: \;\; r'_B, Sig_A(r'_B).$$

Näin B luulee, että kommunikoi A:n kanssa kun todellisuudessa C kommunikoi C:n kanssa. Laadi yksinkertainen korjaus protokollaan, joka estää tämän hyökkäyksen. Älä myöskään käytä aikaleimoja!

4. Esittele vastatoimenpiteitä haittaohjelmia vastaan.