Tik-79.159 Tiedon salaus ja suojaus	kevät 97
Laskuharjoitus 11, viikko 16	Tuomas Aura, Antti Huima

1. Miten korjatussa 1-, 2- ja 3-suuntaisessa X.509-autentikoinnissa (viimeinen sanoma: $N_B, B, S_A(N_B, B)$) vastaanottaja varmistuu sanomien tuoreudesta?

2. Esitä avainpalvelijan tietorakenteet ja toiminta-algoritmi yksinkertaistetussa Kerberos-protokollassa. Muista turvallisuuden kannalta tarpeelliset tarkistukset.

   Protokolla on Schneierin sivulla 60, mutta tässä on vielä askeettisempi versio:

1.	$A \to T:$	A, B
2.	$T \to A:$	$E_A(T_T, B, K_{SES}), E_B(T_T, A, K_{SES})$
3.	$A \to B:$	$E_B(T_T, A, K_{SES})$

3. Mitä vikaa on tehtävän 2 Kerberos-protokollan seuraavissa optimoinneissa?

   (a)

1.	$A \to T:$	A, B
2.	$T \to A:$	$B, E_A(T_T, K_{SES}), E_B(T_T, K_{SES})$
3.	$A \to B:$	$A, E_B(T_T, K_{SES})$

   (b)

1.	$A \to T:$	A, B
2.	$T \to A:$	$E_A(B, K_{SES}), E_B(A, K_{SES})$
3.	$A \to B:$	$E_B(A, K_{SES})$

   (c)

1.	$A \to T:$	A, B, N_A
2.	$T \to A:$	$E_A(N_A, B, K_{SES}), E_B(N_A, A, K_{SES})$
3.	$A \to B:$	$E_B(N_A, A, K_{SES})$

   (N_A on Alicen **nonssi** eli Alicen generoima (pseudo)satunnaisluku. Sen arvo on joka protokolla-ajossa eri, eikä kukaan muu kuin Alice voi lukua näkemättä arvata sitä.)

4. Schneier (s. 515 alalaita) esittää Diffie–Hellman-protokollasta myös version, jossa käyttäjien julkiset DH-avaimet ovat allekirjoitettuina julkisessa hakemistossa. Istuntoavain kahden käyttäjän välille luodaan joka kerta näitä samoja DH-avaimia käyttäen.

   (a) Mitä ongelmia aiheutuu avaimen tuoreudelle?

   (b) Miten tuoreusongelma on ratkaistavissa? Salliiko protokolla edelleen lähettäjän aloittaa salauksen ennen avaintenvaihtoa?

5. Onko Otway–Rees-protokollan (Schneier s. 59) autentikointi implisiittinen vai eksplisiittinen (erikseen kumpaankin suuntaan)? (Vihje: protokolla ei ole aivan niin luotettava kuin Schneier antaa ymmärtää. Parantaisiko sarjanumeron korvaaminen satunnaisluvulla tilannetta?)

6. Millainen relaatio on osapuolten välinen luottamus

   (a) PGP:n luottamusverkossa?

   (b) X.509-autentikointihierarkiassa?