Johdatus tietoliikenteeseen 2010, kierros 2 arvosteluohje

Tehtävä 1

a. Voimassa 12.2.2010 - 11.2.2013. (1p). Varma ei voi olla, mutta valistuneesti voi arvata, että sertifikaatti olisi luotu osapuilleen silloin kun sen voimassaolo alkaa. Näkyvästä ajattelusta 1p.

b. Sonera Class 2 CA (1p), pelkkä Sonera riittää.

c. Firefoxissa Tools->Options->Advanced->Encryption ja View Certificates -nappi. (tai sama suomeksi). 1p

d. Avaimet generoidaan satunnaisesti. (1p) Oodi ei tunnista avaimen perusteella (1p), mutta tunnistaa toki sisäänkirjautumistietojen perusteella.

e. X.509-speksi tarjoaa mahdollisuuden sertifioida dns-tietueen lisäksi esimerkiksi sähköpostiosoitteen, jonka voidaan katsoa identifioivan henkilön. (1p, ei tarvitse olla kauhean formaalisti) Tällä tavoin Oodi voisi tunnistaa sertifikaattia tarjoavan selaimesi (eli käytännössä sinut) ilman sisäänkirjautumisprosessia (1p). Tähän on olemassa toteutuksia, mutta ne eivät yleensä ole kovin levinneitä.

Tehtävä 2

a. Nähdäksemme se on hyvä asia, koska todennäköisyys sille, että joudut maksamaan varastetulla kortilla tehtyjä ostoksia pienenee (1p). Myös päinvastaista mieltä voi olla perustellusti.

b. Mielipiteestä 1p, artikkelista löydetyistä perusteluista 2p ja hyvin rakennetusta vastauksesta viimeinen 1p.

c. Vastauksesta ja perusteluista 2p. Käytännössä koko sirukorttijärjestelmän tarkoitus oli poistaa maksuvelvollisuus kauppiaalta asiakkaalle varastetun kortin käyttötapauksissa. Järjestelmän heikkous ei sinänsä aiheuta kauppiaalle mitään riskiä, vaan riskin kantaa pankki. Toisaalta jos järjestelmä osoittautuu järjettömän helpoksi kiertää, saattavat pankit sysätä taas vastuuta kaupoille.

Tehtävä 3

a. Ei oikeastaan (1p). Osoitteet ovat aika selvä tapaus: koneella saattaa olla monta osoitetta (esimerkiksi eri verkkokortteja), joten pelkästään se, että paketit tulevat oikealle käyttöjärjestelmälle ei mitenkään voi riittää tiedon ohjaamiseksi oikealle ohjelmalle.

Jos lähdekoneen portti poistetaan, ei koneesta a voi ottaa koneella b olevalle palvelinkoneelle kuin yhden yhteyden kerrallaan.

Jos kohdekoneen portti poistetaan tai korvataan esimerkiksi protokollan nimellä tai tyypillä, ei kohdekoneessa voi olla kuin yksi tiettyä protokollaa palveleva sovellus (vrt. esim. Apache ja Tomcat samalla palvelimella).

Perustelluista 1p.

a. UDP:llä (1p). TCP-yhteydessä paketin uudelleenlähetys saattaa aiheuttaa lägin, jota on käytännössä mahdotonta sovellusprotokollatasolla arvioida. (2p). NTP toimii siten, että se ensin arvioi asiakkaan ja aikapalvelimen välistä viivettä verkossa, ja saatuaan riittävän arvion viiveestä käyttää tätä rviota osana kellon säätöä.

b. Järkevästä arviosta 1p. Abstraktiotasolla ei ole väliä. Voi esimerkiksi arvioida että “yhteyden päät voivat olla eri mieltä yhteyden kohtalosta” tai voi miettiä, että yhden osapuolen aloittama molempien päiden katkaisu saattaa johtaa jonkin tiedoston siirron katkeamiseen ja tiedon korruptoitumiseen, mikä rikkoo TCP:n tarjoamaa palvelutasoa vastaan.