T-110.2100 Johdatus tietoliikenteeseen (ruotsinkielinen tentti paperin toisella puolen)
Välikoe 1 8.3.2011
Kirjoita opiskelijanumerosi *selvästi* jokaiseen vastaus paperiin

1 Selitä **lyhyesti** seuraavaat tietoliikenteeseen ja tietoturvaan liittyvät käsitteet ja lyhenteet (6p)
a) Protokollapino (protocol stack)
b) SSL
c) Portti
d) Reititin
e) Vertainen (peer)
f) Saatavuus

2 **Perustele** lyhyesti mitkä seuraavista väitteistä pitävät paikkansa ja mitkä eivät (pisteet tulevat perusteluista) (6p)
a) Symmetrisessä salauksessa viestin eheyttä ei voida suojata yhtä hyvin kuin epäsymmetrisessä.
b) IP muodostaa virtuaalisen piirin lähettäjän ja vastaanottajan välille
c) Kun saat www-palvelimelta varmenteen, tiedät kenen kanssa olet yhteydessä.
d) Sekvenssinumero on tietoliikennepaketin numero.
e) Ethernet-verkon maksimikoko tulee sähkön nopeudesta johtimessa.
f) HTTP:n versioon 1.1 lisättiin Host-kenttä, koska versiota 1.0 käytettäessä yhdessä IPv4-osoitteessa voi olla vain yksi palvelu (esim. www.aalto.fi-verkkosivut)

3
a) Koodaat TCP/IP-protokollatoteutusta pieneen ja hitaaseen mobiililaitteseen nimeltä agenttikello. Minkä TCP:n ominaisuuden avulla voit varmistaa, että pienen päätelaitteesi puskuri ei ylivuoda, kun pyydät agenttikellon puskurin kokoa selkeästi enemmän salaista agenttitdataa palvelimelta? Kuvaile ominaisuuden toiminnan perusperiaate. (2p)
b) Kuvaile kaksi käyttötarkoitusta ICMP-protokollalle (2p)
c) Miksi IP-osoitteissa on verkko-osa ja laiteosa? (2p)

4
a) Arvioi verkkopankin tietoturvatarpeita CIA-mallia käyttäen. Mitä suojattavaa tietoa pankkijärjestelmässä on? Mikä ominaisuus on millekin tietotyypille olennaisinta ja minkä ominaisuuden kustannuksella sitä voisi parantaa? (3p)
b) Kuvaile miten salaat ja allekirjoitat viestin hybridisalausta käyttäen (3p)

5 Kahden koneen välillä on TCP-yhteys. Yhdessä pakettien reitin varrella olevista koneista on ruuhkaa, ja reitittimen puskuri on hetkellisesti täynnä.
a) Mitä tapahtuu reitittimessä? (1p)
b) Miten koneet havaitsevat tämän ja reagoivat ylläolevaan tapahtumaan?(3p)
c) Mikä on riskinä jos reitittimen puskuri on täynnä pidempään kuin hetkellisesti? Miten TCP varautuu tähän? (2p)