T-110.2100 Johdatus tietoliikenteeseen
Välikoe 1 09.03.2010
Kirjoita opiskelijanumerosi *selvästi* joka paperiin

1 Selitä **lyhyesti** seuraavaat tietoliikenteeseen ja tietoturvaan liittyvät käsitteet ja lyhenteet (6p)
- a) Protokollapino (protocol stack)
- b) SSL
- c) Soketti
- d) Eheys (integrity)
- e) Asiakas-palvelin ja peer-to-peer protokollat
- f) Ajax (tietotekniikassa; ei mytologiassa, jalkapallojoukkue tai pesuaine)

2 **Perustele** lyhyesti mitkä seuraavista väitteistä pitävät paikkansa ja mitkä eivät (pisteet tulevat perusteluista) (6p)
- a) Hybridisalausta käytetään siksi, että symmetrinen salaus on aina vahvempaa kuin asymmetrinen.
- b) TCP-otsakkeen tarkistesummana voitaisiin käyttää kryptografista allekirjoitusta, jossa kaikki osapuolet tietävät avaimen.
- c) Kun saat www-palvelimelta itseallekirjoitetun varmenteen, tiedät kenen kanssa olet yhteydessä.
- d) Käyttäessäsi IT-palvelukeskuksen DNS-palvelinta joudut luottamaan siihen, että se kertoo sinulle oikean osoitteen www.cs.helsinki.fi -palvelimelle.
- e) TCP tarjoaa luotettavaa tavuvirtaa, koska vastaanotaja osaa pyytää uudelleen kadonneita paketteja.
- f) Kuvaus palvelimen nimestä IP-osoitteeseen on bijektio (jokaista nimeä vastaa tasan yksi osoite ja jokaista osoitetta tasan yksi nimi)

3 **TCP ja IP**
- a) Jos TCP/IP-pinossa IP vaihdettaisiin tismalleen vastaavan palvelun ja rajapinnan tarjoavaan Aalto-protokollaan (AP), mitä muutoksia ylä- ja alapuolella oleviin TCP- ja Ethernet-protokolliin pitäisi tehdä? Entäpä jos AP tarjoaisi luotettavaa (paketit tulevat järjestyksessä ja virheettöminä ylemmälle tasolle) pakettien siirtoa. Mitä TCP-protokollan ominaisuuksia ei silloin tarvitsisi toteuttaa? (3p)
- b) Jos TCP tarjoaisi yksisuuntaista luotettavaa tavuvirtaa, montako pakettia TCP-yhteyden avaamiseen ja sulkemiseen tarvittaisiin? Perustele (3p)

4 **Tietoturva**
Oodi-palvelu sisältää opiskelijoiden suoritustiedot, kurssien toteutustiedot, kursseille ilmoittautumiset ja (pian) kurssipalautteet.
- a) Arvioi Oodin sisältämän tiedon tietoturvatarpeita CIA-mallia käyttäen. Mikä ominaisuus on millekin tietotyypille olennaisinta ja minkä ominaisuuden kustannuksella sitä voisi parantaa? (3p)
- b) Oodiin on mahdollista olla yhteydessä vain SSL-salatun yhteyden avulla. Miksi luulet, että yhteys on salattu? Mikä on suojattu tieto ja suojataanko tiedon eheyttä, saatavuutta vai luottamuksellisuutta? (2p)
- c) Jos Oodia vastaan tehtäisiin palvelunestohyökkäys esimerkiksi virolaisella botnetillä, voitaisiinko hyökkäys osittain torjua palomuuriasetuksilla? (1p)

5 **Sovelluskerros**
- a) Oheisessa http-kutsussa määritellään yhteyden olevan tyyppiä "keep-alive" ja vastauksessa

suostutaan tähän. Minkä protokollan yhteyttä pidetään auki? (1p)

b) Miksi tällainen ominaisuus on tehty HTTP-protokollaan? Onko oletettavaa, että sen käyttö lisääntynyt tai vähentynyt www:n alkuajoista nykypäivään? Perustele. (2p)

c) Jos HTTP-protokollakutsusta poistettaisiin Host:-rivi, miten tämä vaikuttaisi Internetiin? (3p)

```
GET /tteekkar/esimerkki.html HTTP/1.1
Host: www.cse.tkk.fi
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.7)
Gecko/20091221 Firefox/3.5.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

```
HTTP/1.x 200 OK
Date: Thu, 21 Jan 2010 12:57:12 GMT
Server: Apache/1.3.41 (Unix) PHP/4.4.7 DAV/1.0.3 mod_ssl/2.8.31 OpenSSL/0.9.8j
Etag: "2f80a6-1d9-4b585a30"Accept-Ranges: bytes
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```