TTY / TIE / J. Harju

TIE-03100 Tietoverkot ja tietoturva

Tentti 16.12.2016

Tentissä ei saa käyttää laskinta. Tätä tehtäväpaperia ei tarvitse palauttaa.

1. Tarkastellaan SSL/TLS-protokollaa, jota käytetään yleisesti turvallisessa verkkoasioinnissa.

   a) Kerro, miten osapuolten *todentaminen* tapahtuu, esimerkiksi miten asiakas todentaa palvelun, johon hän on ottanut yhteyden selaimensa avulla? (3p)

   b) Miten yhteyden *luottamuksellisuus* toteutetaan? (3p)

2. Reititys ja IP-osoitteet ovat Internetin toiminnan keskeisimpiä asioita.

   a) Mitä tarkoitetaan aliverkolla, miten se määritellään IP-osoitteiden avulla ja mikä on sen merkitys reitityksen kannalta? (3p)

   b) Kun IP-paketti matkalla kohteeseensa saapuu johonkin välillä olevaan reitittimeen, niin miten tämä reititin pystyy tietämään, mihin ulosmenevään liittymään sen pitää kyseinen paketti lähettää, jotta paketti etenisi kohti lopullista kohdettaan? (3p)

3. Tarkastellaan TCP/IP-protokollia ja kerrosmallia.

   a) Mitä tarkoitetaan end-to-end eli päästä-päähän-protokollilla? Mille kerroksille ne tyypillisesti asettuvat? Onko IP end-to-end-protokolla? Entä TCP tai HTTP? Perustele vastauksesi. (2p)

   b) Miksi TCP ja IP muodostavat tarkoituksenmukaisen protokollaparin Internetin tietoliikenteessä? (2p)

   c) Miten asiakkaan lähettämä sovellustason data osataan palvelimen päässä antaa juuri oikealle sovellukselle? Entä miten palvelimen vastaus osataan antaa juuri oikealle sovellukselle asiakkaan päätelaitteessa? (2p)