TiTe/Pj
13.2.2008 **CT30A3500 Tietoturvan Perusteet**

1. Ovatko seuraavat lauseet totta vai tarua? Perustele vastauksesi?
Oikea vastaus +1p, oikea/hyvä perustelu +2p, väärä vastaus huonolla tai puuttuvalla perustelulla -1p

a) Biometriikkaan perustuva autentikointi on parempi kuin salasanaan perustuva autenikointi
b) Matojen avulla voidaan hankkia zombieita.
c) Kekseillä (cookie) voidaan levittää viruksia.
d) Liikenneanalyysiä vastaan ei auta edes 512-bittinen symmetrinen salaus.

(12p)

2. Autentikointi

Mainitse kaksi menetelmää joiden avulla voidaan suojautua.

a) Matoja
b) DoS: ia
c) Kotitietokoneelle murtautumista
d) Sisäpiiriläisiä

vastaan. Kerro myös kuinka menetelmä tämän suojauksen hoitaa.

(**12p)**

3. Matti saa sähköpostissa liitteenä viestin Maijalta. Matti tallentaa viestin koneensa kovalevylle salattuna symmetrisellä AES algoritmilla käyttäen 256-bittistä avainta. Salausavain on tallennettuna USB tikulla, josta tiedon lukeminen vaatii biometrisen autentikoinnin.

a) Onko Matti toiminut järkevästi viestin turvauksessa? Mitä muuta Matin kannattaisi tehdä tiedon turvaamiseksi? Olisiko jotain mitä Matin tulisi tehdä toisella tavalla?

b) Marjatta on kovasti kiinnostunut Matin ja Maijan välisestä sähköpostiliikenteestä. Mitä keinoja Marjatalla on edellä mainittujen suojausten jälkeen hankkia tietoonsa viestin sisältö. Kuinka näitä keinoja vastaan voidaan suojautua?

Tarvittaessa voit itse määrittää mahdollisia lisädetaljeja kuten käytetyn prosessorin merkki ja Matin kenkien väri.

Vinkki: Tehtävän ratkaisu vaatii annettujen oppien soveltamista koko kurssin alueelta.

(16p)

4. *Vertaile* steganografiaa ja kryptografiaa suojausmenetelminä.
(Huomasithan että tehtävän määritys alkaa sanalla vertaile)

(**10p)**

Ei laskimia
Ei materiaalia