**T-110.4200 Tietoturvallisuustekniikka**
Tentti 18.12.2006 Timo Kiravuo

1 Selitä lyhyesti seuraavat tietoturvallisuuteen liittyvät käsitteet. (6 p)
   a) Haittaohjelma (malware)
   b) Referenssimonitori (Reference monitor)
   c) Bell-LaPadula -malli
   d) Troijalainen (Trojan)
   e) One time pad
   f) TCB (Trusted Computing Base)

2 Perustele lyhyesti mitkä seuraavista väitteistä pitävät paikkansa ja mitkä eivät. (6 p)
   a) Yksi ACL:n (access control list) hyvistä puolista on, että sen avulla on helppo selvittää yhden subjektin kaikki oikeudet.
   b) Intrusion detection -järjestelmä estää hyökkäyksiä.
   c) Salausjärjestelmä, jonka toimintaperiaatteet ovat julkisia, on todennäköisesti turvallisempi kuin salausjärjestelmä, jonka toimintaperiaate on salainen.
   d) Kryptografisilla menetelmillä voidaan suojata luottamuksellisuutta, mutta ei eheyttä eikä käytettävyyttä (saatavuutta).
   e) Tietoturvan tavoitteena on kaikkien vahinkojen torjuminen.
   f) Kaiken tiedon salaaminen (kryptaaminen) lisää tietoturvaa.

3 Kerro mitä kukin alla oleva hyökkäys tarkoittaa ja kuvaile ainakin yksi tekniikka kutakin kohden, jolla kyseistä hyökkäystä vastaan voi suojautua. Pelkkä tekniikan nimi ei riitä, vaan myös sen toimintaperiaate pitää kuvata. (6 p)
   a) Man in the middle -hyökkäys
   b) Puskurin ylivuoto (Buffer overflow)
   c) Palvelunestohyökkäys
   d) Salakuuntelu

4 a) Alla on joukko termejä, selitä niitä käyttäen miten HST-järjestelmän tapainen ihmisten tunnistamisen ja sähköiset sopimukset mahdollistava järjestelmä toimii. Varmenne, PKI, julkisen avaimen salaus, tiiviste, sulkulista, toimikortti (3 p)
   b) Jos haluat vakuuttaa asiakkaan toteuttamasi ohjelmiston turvallisuudesta (turvan laadusta), miten tekisit sen? (2 p)
   c) Miten steganografia toimii? (1 p)

5 Jos tälle kurssille suunniteltaisi harjoitustöiden palautusjärjestelmä, siinä olisi komponentteina ainakin
   - WWW-pohjainen käyttöliittymä oman harjoitustyön palauttamiseen
   - Tietokanta harjoitustöiden ja niihin liittyvän tiedon säilyttämiseen
   - Opettajan käyttöliittymä palautteen antamiseen ja työn arvostelemiseen

   Ilmiselviä uhkia ovat:
   - Toisen oppilaan harjoitustyön näkeminen
   - Oman arvostelunsa muuttaminen

   Kuvaile neljä **ohjelmistotyöhön** liittyvää tekniikkaa tai menetelmää joita käyttäen pyrit varmistumaan siitä, että edellä mainitut uhat torjutaan. Näitä tekniikoita ovat esimerkiksi luennoilla käsitellyt suunnitteluperiaatteet ja turvamallit. Kuvaile missä vaiheessa suunnittelua käytät mitäkin tekniikkaa ja mitä hyötyä siitä on. (6 p)