TTKK / Tietoliikenne / J.Koskinen

8306000 Tietoturvallisuuden perusteet

Tentti 22.1.2001

Vastaa viiteen tehtävään.

1. Sovittele virustorjunnan eri vaiheita ja menetelmiä seuraaviin luokkiin. Enintään yksi luokka saa jäädä tyhjäksi.
   - Välttäminen (avoidance)
   - Pelottaminen (deterrence)
   - Estäminen (prevention)
   - Havaitseminen (detection)
   - Toipuminen (recovery)
   - Korjaaminen (correction)

2. Mikä erottaa tietoturvamallin (jollainen esim. Bell-LaPadula on) ja tietoturvapolitiikan? Mitä yhteistä niillä voi olla? Miten tietoturvasuunnitelma sitten liittyy näihin?

3. Mainitse kolme turvallisuusongelmaa, jotka liittyvät salasanapohjaiseen autentikointiin. Minkä ongelman ratkaisuyritys on seuraavanlainen? Autentikoituja lähettää todentajalle tiedot:
   id, r, t, h(id, r, t, pw),
   missä id=käyttäjätunnus, r=satunnaisluku, t=aika, h=hash-funktio, pw=salasana.

4. Oletetaan, että saat A:lta salatun PGP-viestin, jonka hän on myös allekirjoittanut. Mistä PGP-ohjelmasi saa avaimet salauksen purkuun ja allekirjoituksen todennukseen? Kumpaa se tarvitsee ensin (eli kumpi operaatio on ulompana)? Millä perusteilla sinä voit luottaa, että juuri A on allekirjoittanut viestin?

5. Millä tavoin palomuurilla edistetään tietoturvaa: toisin sanoen, mitä sillä konkreettisesti tehdään ja miten se vaikuttaa?

6. Yhden pisteen kysymyksiä, eli vastaa/selitä juuri sen verran, että lukija vakuuttuu että tiedät mistä on kyse:
   - Salakirjoituksen kerta-avain-systeemi (one-time pad)
   - Troijan hevonen (nykyaikainen)
   - SET, Secure Electronic Transactions
   - PICS, Platform for Internet Content Selection
   - Julkisen avaimen systeemeissä lasketaan kokonaisluvuilla, mutta miksi tämä tehdään modulo jokin iso kokonaisluku, eli ottamalla aina jakojäännös tämän luvun suhteen?
   - Lähetät kaverillesi jonkin dokumentin levykkeellä, mutta olet aiemmin käyttänyt levykettä myös yksityisiksi tarkoittamiesi tiedostojen käsittelyssä. Miksei näiden tiedostojen tuhoaminen, deletointi, riitä luottamuksellisuuden säilyttämiseen?