**TTKK / Tietoliikenne / J.Koskinen**

**8306000 Tietoturvallisuuden perusteet**

**Tentti 5.3.2001**

Vastaa viiteen tehtävään.

*Kun olet saanut vastaukset valmiiksi, merkitse vastauspaperin alkuun tehtävien numerot siinä järjestyksessä kuin arvioit osanneesi niihin vastata, paras ensimmäiseksi, huonoin viimeiseksi. Jos arvostelu tuottaa saman järjestyksen, saat lisäpisteen.*

1. a) Mitä ovat seittiselauksen evästeet (eli cookiet eli piparit)? (1p)
   b) Miksei niiden kautta voi tapahtua hyökkäystä koneesi eheyttä vastaan? (1p)
   c) Millä tavoin ne voivat aiheuttaa ongelmia yksityisyytesi kannalta? (2p)
   d) Millä tavoin seittiselaus yleisesti heikentää yksityisyyttäsi, evästeistä riippumatta? (2p)

2. Ensimmäisellä luentokerralla esiteltiin lyhyesti seuraavat 22 informaatiollista tietoturvamekanismia:

   salakirjoitus -- tarkistussumma (yleisemmin: tiivistefunktio) -- allekirjoitus -- nimettömyys (anonymiteetti) -- tunnistus (identification) -- olion autentikointi -- pääsynvalvonta -- erottelumekanismit -- auditointi -- oikeutus, auktorisointi -- omistusoikeus -- valtuutus, delegointi -- validointi, kelpuutus -- varmentaminen (certification) -- aikaleimaus -- todistaminen (witnessing) -- kuittaus -- konfirmointi -- kiistämättömyys -- peruutus (revocation) -- tietoliikennemekanismit -- toipumismekanismit

   Valitse näistä kolme sellaista, joilla ei ole mitään tekemistä virustorjunnassa. Selitä miksi ei ja mihin ne sitten liittyvät.

3. Oletetaan, että A ja B ovat sopineet symmetrisestä avaintensalausavaimesta K, jota he käyttävät päivittäin vaihdettavien datansalausavainten salaukseen seuraavien kahden vuoden ajan. Mitä avaintenhallintaan liittyviä tapahtumia voidaan niiden bittien elinkaaressa erotella, joista K muodostuu?

4. Jos jätetään jälkikäteen ohjelmiin tartutetut virukset huomiotta, mitä toimia ohjelman oikean toiminnan takaamiseksi voivat suorittaa ohjelmien tekijät, hankkijat ja ajajat?

5. Esittele kolme erilaista tapaa, joilla henkilö A voi vakuuttaa etäällä olevan henkilön B siitä, että K on A:n julkinen avain. Ainakin yhden tavan pitää toimia ilman kolmatta osapuolta ja ainakin yhdessä sellainen pitää olla.

6. Yhden pisteen kysymyksiä, eli vastaa/selitä juuri sen verran, että lukija vakuuttuu että tiedät mistä on kyse:
   - Hash-funktio.
   - Riskianalyysi.
   - Päättely tietoturvaongelmana tietokannoissa.
   - Tehtävässä 4 ei ole tarpeen esitellä Common Criteriaa eli CC:tä, mutta CC:n noudattamisesta voi silti olla hyötyä tehtävässä mainituille kolmelle toimijaryhmälle. Mikä niistä joutuu eniten CC:n kanssa tekemisiin? (Pelkkä arvaus ei riitä.)
   - Tunnelointi.
   - SSL, Secure Socket Layer.