

TTKK / Tietoliikenne / J.Koskinen
8306000 Tietoturvallisuuden perusteet
Tentti 13.8.2001

Vastaa viiteen tehtävään, ja tehtävissä 2 ja 3 a-kohtaan lisäksi vain joko b- tai c-kohtaan.

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 lisäpistein.

1. Jos kaikki tietoturvaohjelmat pitäisi luokitella, mitä muuta pitäisi ottaa huomioon kuin ne asiat, jotka esiintyvät Howardin taksonomiassa? Siinähan esitellään taulukkomuodossa toisensa poissulkevat luonnehdinnat hyökkääjälle, hänen käyttämälleen välineelle, keinolle päästä käsiksi tietoon, tulokselle jonka hän saa aikaan suhteessa tietoon sekä tavoitteelle, joka hänet motivoi.
2. Sovelletaan hash-funktiota h tuhat kertaa peräkkäin satunnaislukuun r ja kerrotaan tulos turvallisesti palvelimelle.
 - a) Miten tästä saadaan autentikointimenetelmä ja miksi se on turvallinen?
 - b) Miten menettelyä voi (alustuksen jälkeen) nopeuttaa, jos autentikoituminen voi tapahtua myös sellaiselta asiakaslaitteelta, jossa h :ta ei voi laskea kovin nopeasti?
 - c) Missä suhteessa a-kohtaa heikompi on OPIE-menettely, jossa r kerrotaan palvelimelle?
3. Rabinin kryptosysteemissä on julkinen avain n ja yksityiset avaimet p ja q . (p ja q ovat suuria alkulukuja, joiden jakojäännös modulo 4 on 3; $n=pq$.)
 - a) Miten salataan viesti m , joka halutaan lähettää n :n omistajalle ja miten tämä saa sen auki? (Avaamisen tarkkoja kaavoja ei vaadita mutta sellainen tarkkuus kylläkin että syy redundanssin käyttötarpeelle selviää.)
 - b) Jos avain n eli moduuli on 500-bittinen ja viesti m on 100-bittinen, mitä m :lle pitää tehdä ennen salauksen soveltamista ja miksi?
 - c) Jos viesti onkin sitten 100 000-bittinen, se pitäisi käsitellä 200 lohkona. Miksei näin kuitenkaan yleensä tehdä ja mikä on tavallisempi menettely (kuten RSA:ssakin)?
4. Etsi esimerkki tietokannasta, jossa yhtäältä joudutaan vastaamaan kyselijälle mutta toisaalta joudutaan pimitämään jotain samalta henkilöltä. Mainitse kolme mekanismia, joilla pimitystä voidaan toteuttaa.
5. Missä mielessä toimikortilla oleva prosessori on turvallinen? Millä valmistusvaiheen menettelyillä turvallisuus saavutetaan?
6. Esittele viisi menettelyä, joilla yritys voi torjua työntekijöidensä tahallisesti aiheuttamia tietoturvarikkomuksia.
7. Yhden pisteen kysymyksiä, eli vastaa/selitä juuri sen verran, että lukija vakuuttuu että tiedät mistä on kyse:
 - Makrovirus
 - Tietosuoja
 - Digitaalinen allekirjoitus
 - Common Criteria (CCITSE)
 - Kertakirjautuminen
 - Digitaalinen vesileima

12