TIE-30301 Tietoturvallisuuden jatkokurssi Ei laskimia.
Tentti 12.5.2017 / Jarmo Harju

Tehtäviä on viisi ja ne arvostellaan asteikolla 0-6 pistettä eli maksimipistemäärä on 30 p. Tähän lisätään välikokeen ja harjoitusten bonuspisteet ja siitä vähennetään harjoitustöiden mahdolliset sakkopisteet, jolloin saadaan kokonaispistemäärä. Läpipääsyyn tarvitaan normaalisti kokonaispistemäärä 15 p.

1. Bell-LaPadula-malli (BLP) pyrkii sääntöjen avulla tekemään monia tasoja sisältävästä tietoturvamallista turvallisen käyttää. Selosta BLP:n sääntöjä ja kerro malliin kohdistetusta kritiikistä.

2. Kuvaa lyhyesti Diffie-Hellmannin (D-H) avaintenvaihdon toimintaperiaate ja kerro millaiseen matemaattiseen tekniikkaan se perustuu. D-H on haavoittuva tietynlaiselle hyökkäystyypille. Perustele tätä väitettä ja kerro, miten sitä vastaan voidaan suojautua.

3. Miten perusmuotoinen MAC eli Message Authentication Code -menetelmä viestien alkuperän ja eheyden varmistamiseksi toimii? HMAC on paljon käytetty menetelmä samaan tarkoitukseen. Miten tämä menetelmä eroaa perus-MACista ja mitkä syyt ovat johtaneet siihen, että HMAC on syrjäyttämässä perus-MACin.

4. Anna esimerkkejä palvelunestohyökkäyksissä käytetyistä menetelmistä. Kerro esimerkkejä, minkä tyyppistä liikennettä hyökkäyksen uhrille lähetetään, miten hyökkäykseen saadaan liikennevolyymia, ja miten hyökkääjät voivat halutessaan piilottaa oman identiteettinsä.

5. Kerro, miten Tor-verkon piilotetut palvelut on teknisesti toteutettu ja miksi palvelun tarjoajaa ja palvelun käyttäjää on tyypillisesti mahdotonta jäljittää.