Tentti S-38.3153 Tietoliikenteen tietoturva
Exam S-38.3153 Security of Communication Protocols

5.1.2007

Put your name, student number, course code and date to each exercise paper. This helps you to receive your credits in fast and reliable manner. Answers are accepted in Finnish, Swedish or in English. Answers are judged based on their quality and clarity. A short and down to the fact answer will get better points than an excursive one. You may explain things further but beware that errors may lower your points (even if they are in extra matter).

1. Miten kryptologiaa voidan käyttää tietoturvan toteuttamiseen ja parantamiseen? Mitä rajoitteita sillä on?
   How cryptology can be used to implement and improve data security? What limitations there exists?(6 p)
2. Turvamekanismit voivat perustua ensisijaisesti estämiseen, havaitsemiseen tai toipumiseen. Esitä kustakin tapauksesta havainnollinen ja perusteltu esimerkki.
   Security mechanisms can base primarily on prevention, detection or recovery. Present an example for each case with short reasoning. (6 p)
3. You are buying a new hiking equipment from a previously unknown shop from Internet using your credit card. What kind assumptions you make about security? How about if you are buying with advance bank transfer? What kind of possibilities you have to confirm your assumptions? (6 p)
   Olet ostamassa uusia retkeilyvälineitä aiemmin tuntemattomasta internet-kaupasta käyttäen luottokorttiasi. Mitä olettamuksia teet turvallisuudesta? Entä jos maksat ennakkomaksulla pankkiin? Mitä mahdollisuuksia sinulla on pyrkiä varmentamaan olettamuksiasi.(6 p)
4. Selitä IPSec-arkkitehtuuri ja mekanismit. (6 p)
   Explain IPSec architecture and mechanisms. (6 p)
5. You are outsourcing maintenance of company servers (contain both financial (accounting) and personal data). What questions you ask from the contractor and what you look for to ensure that the contractor security is sound. (6 p)
   Olet ulkoistamassa yrityksen palvelimien ylläpitoa (sisältävät sekä taloudellista (kirjanpito) että henkilötietoja). Mitä kysyt ja mihin kiinnität huomiota varmistuaksesi, että toimittajan turvallisuus on riittävällä tasolla?(6 p)

Markus Peuhkuri