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

8.5.2008

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. Tarkastele kolmea järjestelmää, jotka toteuttavat suojauksen Biba, Bell-LaPadula ja Chinese Wall-mallien mukaan. Järjestelmä saastuu haittaohjelmalla. Selitä miten saastuminen etenee järjestelmässä eri vaihtoehdoissa. Onko merkitystä mikä osa järjestelmästä saastuu tai haittaohjelman tyypillä? (6 p)
   Review three systems that implement Biba, Bell-LaPadula and Chinese Wall models. System gets infected with malicious software. Explain how infection proceeds in system in different alternatives. Does it matter which part of system gets infected or what is type of malvare?(6 p)
2. Yrityksesi tarjoaa web-hotellipalvelua sekä tietoliikenneyhteyksiä yrityksille. Millaisia turvamekanismeja on järkevää käyttää? Mitkä niistä perustuvat estämiseen, havaitsemiseen tai toipumiseen. (6 p)
   Your company provides web hotel services and network access services to companies. What kind of security mechanims are reasonable to use? What of those base on prevention, detection or recovery. (6 p)
3. Miten salausta käytetään tietoliikenteessä? Millaisia vaatimuksia tietoliikennejärjestelmissä käytetyille salausjärjestelmille on? (6 p)
   How encryption is used in data communication? What kind of requirements there are for encryption systems used for communications(6 p)
4. Kuvaile UMTS:n turvajärjestelmät (6 p)
   Describe UMTS security system. (6 p)
5. Millaisia käyttäjän autentikointimenetelmiä voidaan käyttää? Eroaako tilanne, jos tunnistaminen tapahtuu paikallisesti tai verkon yli?
   What kind of authentication methods can be used? Is there a difference if authentication is done locally or over network?(6 p)
6. Mitä kirjaa/joja käytit opiskeluun (½ p)

   What book(s) you used for studying (½ p)

Markus Peuhkuri