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

31.8.2006

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 seuraavia tapauksia: perustele lyhyesti mitä tekisit tilanteen ratkaisemiseksi ja miksi (2 p/tapaus).
   Evaluate following cases: what would you do to resolve situation and why? (2 p/case) (6 p)
   a) Yrityksessä käytettävästä tekstinkäsittelyohjelmasta on löytynyt vakava haavoittuvuus, johon ei ole korjausta saatavissa. Haavoittuvuutta hyödyntävä esimerkkikoodi on saatavissa verkosta. Yrityksen toimintaan kuuluu olennaisesti tarjousdokumenttien (k.o. ohjelmalla tehtyjen) käsittely. Mitä teet?
   A vulnerability has been found from the word processing software used by company. There is no patch available and proof-of-concept code is available from Internet. Handling world processing documents (with the program in question) is critical part for company. What you do?
   b) Sattumalta käy ilmi, että eräs työntekijä on liittänyt yrityksen verkkoon luvattoman WLAN-tukiaseman. Sinut määrätään selvittämään onko niitä muitakin. Mitä teet?
   It is found out by a change that some employee has installed a WLAN accesspoint on company network without permit. You are commanded to find out if there are more. What do you do?
   c) Käytettyäsi luokkatilassa ollutta PC:tä poislähtiessäsi havaitset näppäimistöjohdossa epäilyttävän välipalikan. Mitä teet?
   After you finish using classroom PC you notice a suspicious device on keyboard cable. What you do?
2. Miten turvallisuusmekanismit voidaan sijoittaa tietoliikennejärjestelmien eri kerroksille. Mitä hyötyjä ja haittoja kustakin sijoituksesta on? (6 p)
   Security mechanisms can be deployed on multiple layers of communications systems. What benefits and disadvantages there are on each layer? (6 p)
3. Millaisia vaatimuksia tietoliikennejärjestelmissä käytetyille salausjärjestelmille on.
   What kind of requirements there are for encryption systems used for communications(6 p)
4. Selitä IPSec-arkkitehtuuri ja mekanismit. (6 p)
   Explain IPSec architecture and mechanisms. (6 p)
5. Suunnittelet protokollaa tiedon turvalliseen siirtämiseen useamman järjestelmän välillä. Mitä asioita sinun tulee ottaa huomioon? (6 p)
   You are designing a protocol for secure information transmit between multiple systems. What aspects you must take into account? (6 p)

Markus Peuhkuri