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

9.5.2005

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. Why denial of service is hard to protect from in current Internet? Is there something that can be done for that (6 p)
   Miksi nykyisessä Internetissä on vaikea suojautua palvelunesothyökkäyksiltä? Onko jotain, mitä asialle voitaisiin tehdä. (6 p)
2. 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)
3. Explain design principles for encryption system (Kerckhoff, Shannon) (6 p)
   Selitä salausjärjestelmien suunnitteluperiaatteet (Kerchoff, Shannon) (6 p)
4. Describe UMTS security system. (6 p)
   Kuvaile UMTS:n turvajärjestelmät (6 p)
5. You are acquiring a new server system for a company and want to ensure that the system is secure as it will contain both financial and personal data. How you can ensure that the system is sound in security-vice. (6 p)
   Olet hankkimassa uutta palvelinjärjestelmää yritykselle ja haluat varmistua, että järjestelmä on turvallinen koska siinä on sekä taloudellista että hankilötietoja. Kuinka voit varmistua että järjestelmä on eheä turvallisuusmielessä? (6 p)

Markus Peuhkuri

Tentti S-38.3205 Henkilökohtainen kurssi tietoliikenteen tietoturvasta
Exam S-38.3205 Indivudual course on Security of Communication Protocols

9.5.2005

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).

This set of questions is only to those who have taken other security courses on TKK and cannot have S-38.3153 course in their records

1. Why denial of service is hard to protect from in current Internet? Is there something that can be done for that (6 p)
   Miksi nykyisessä Internetissä on vaikea suojautua palvelunesothyökkäyksiltä? Onko jotain, mitä asialle voitaisiin tehdä. (6 p)
2. Describe different firewall types, usage scenarios and usage topologies (6 p)
   Kuvaile eri palomuurien tyypit, käyttötavat ja -topologiat. (6 p)
3. Protocols related on IPSec and typical IPSec usage scenarios (6 p)
   IPSec:iin liittyvät protokollat ja tyypilliset käyttötilanteet. (6 p)
4. Describe UMTS security system. (6 p)
   Kuvaile UMTS:n turvajärjestelmät (6 p)
5. Explain Kerberos 5 authentication. Why there is not need to trust much on each computer?
   Kuvaile Kerberos 5 autentikointi. Miksi jokaiseen koneeseen ei tarvitse luottaa täydellisesti? (6 p)

Markus Peuhkuri