T-110.4206 Information Security Technology
Exam 29.10.2009

1 **Explain** briefly the following concepts and acronyms related to data security. (6 p)
- a) Intrusion Detection System
- b) Malware
- c) Whitelist filter
- d) Authorization
- e) Integrity
- f) Reference monitor

2 **Justify** briefly the following statements as either correct or false. (6 p)
- a) Including a Javascript function in a form to verify the input is a good way to move security related computation off the server.
- b) A company should store copies of important encryption keys.
- c) A replay attack can be prevented by encrypting the contents of each message.
- d) Installing a firewall starts by reading the organization's security policy.
- e) When an intrusion is suspected, the most important thing is to disconnect the company network from the Internet.
- f) TLS or IPsec are not needed when using the Internet from a mobile telephone, as mobile communications are already encrypted.

3
- a) Firewalls can operate on the layers 3-4 of the TCP/IP model (packet filtering firewalls) or on layer 5 (or 7, application filter). Give two **examples** of what an application layer firewall can do that a packet filter can not do. (1.5 p)
- b) A firewall can also be an application in a workstation. Give two **justifications** for why a workstation should have a software firewall if there already is a network firewall. (1.5 p)
- c) You have been put in charge of a software project, where experienced **intranet** programmers are implementing an **Internet** application for the first time. You are afraid that the programmers will leave vulnerabilities to the code. Briefly describe two software production practices and one relevant standard that you will use to prevent the vulnerabilities. (3 p)

4 Protecting information (6 p)
- a) What encryption keys are needed to send an encrypted and signed e-mail message, in a practical situation and with largish message content? Describe how each key is used and where the key is obtained from. (3 p)
- b) A TLS handshake starts by the client presenting its cipher algorithms and a nonce; the server replies by its algorithms, nonce and certificate; and so on. Why is a handshake needed and what is the result of the handshake? (3 p)

5 Several theoretical data security models have been presented during the course, like simple Bell-LaPadula, Bell-LaPadula with lattice, static Biba, subject low watermark Biba, object low watermark Biba, Chinese Wall and Clark-Wilson. **Describe and justify** which model would be best suited to apply in each following case. Include the assumptions on which you base your justification. (6 p)
- a) Cern is an international research institution doing big and expensive experiments, resulting in huge amounts of original measurement **data** that not transferred from Cern, but scientist can run their software at the Cern computers.
- b) The balance of your bank account is just a number in a database. When you pay a bill through the bank, you or a bank employee use the system to change the value of a field belonging to your and recipient's account.
- c) A police officer may read a telephone eavesdropping report from the database if she is senior enough and if she is participating in the investigation of that particular crime.
- d) A young **motorist** may join any motorbike gang, however after joining up, he may not change his membership to another gang, as he knows the secret handshake.