T-110.4206 Information Security Technology

Exam 18.12.2006 Timo Kiravuo

1 Explain briefly the following concepts and acronyms related to data security. (6 p)

a) Malware
b) Reference monitor
c) Bell-LaPadula model
d) Trojan (horse)
e) One time pad
f) TCB (Trusted Computing Base)

2 Justify briefly the following statements as either correct or false. Grading is based on the justification you give. (6 p)

a) One of the benefits of ACL (access control list) is that it is easy to see all the rights that one subject has.
b) An intrusion detection system prevents attacks.
c) An encryption system based on public mechanisms is more likely to be secure than a system, which working mechanisms are secret.
d) Cryptographic methods can be used to protect confidentiality, but not integrity or availability.
e) The goal of information security is to protect against all damage.
f) Encrypting all information increases security.

3 Explain each of the attacks below and describe at least one method of protection against each attack. Describe the main principle of the method, not just its name (6 p)

a) Man in the middle
b) Buffer overflow
c) Denial of service
d) Eavesdropping

4 a) Below are several terms, explain using them how a system for identifying people and enabling electronic contracts, such as the FINEID works. (3 p)
Certificate, PKI, public key encryption, hash, certificate revocal list, smart card

b) If you want to assure to your customer that a software implementation is secure, how would you do it? (2 p)

c) How steganography works? (1 p)

5 If a system for returning homework were to be designed for this course, it would consist of at least

- A WWW based user interface for returning a homework
- A database for storing the returns and related information
- A teacher's user interface for giving feedback and grading the homework

The obvious threats are:

- Being able to see another student's homework
- Being able to change the grading for yourself

Describe four techniques or methods related to software engineering that you could use to thwart the threats. These techniques are for example the design principles and security models discussed in the lectures. Describe at which part of the design process you would use the technique and what is its use. (6 p)