T-110.4200

T-110.4206 Information Security Technology

Exam 28.8.2008

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

a) DAC (Discretionary Access Control)
b) Malware
c) SSO (Single Sign On)
d) ACL (Access Control List)
e) Biometrics
f) Non-repudiation

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

a) An IDS system should react to an attack by automatically breaking into the attacking machine and preventing its operation.
b) An encryption system based on public mechanisms is more likely to be secure than a system, which working mechanisms are secret
c) An e-commerce service can be designed so that breaking the security of the front end web server does not give access to the whole system.
d) Cryptographic methods can be used to protect confidentiality, but not integrity or availability.
e) Common Criteria is a standard for operating system security.
f) Encrypting all information always increases security..

3 Attacks and defenses (6 p)

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

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

4 Security policy models (6 p)

Which of the security policy models discussed on the course (simple Bell-LaPadula, lattice version of Bell-LaPadula, static Biba, subject low watermark Biba, object low watermark Biba, Chinese Wall, Clark-Wilson) do the following cases resemble the most? Jystify your answer by describing what properties or rules of the models can you find in these examples?

a) A tuning fork gives a certain pitch for *a*-note, according to which other instruments are tuned. The tuning fork is never tuned according to the other instruments.

b) A back-up system reads all users' home directories from disk and writes them on a tape. None of the users can read data from the back-up tape; only the administrators can break the rules and copy data from the tape back to the disk.

c) A widely known celebrity is imprisoned and wants to give an exclusive interview to some magazine. He can choose to give the interview to any magazine, but after he has done so he can not give another interview to any other media within a certain time.

d) In the kitchen of a large catering service the foodstuffs have two categories: those that will not be cooked (salad, sushi etc) can only be handled with carefully washed hands and tools, whereas those that will be cooked can be handled without washing the tools and hands all the time. Already cooked food (e.g. roast beef) can be cooled down under well defined conditions (fast cooling) and after that will be treated the same way as food that will not be cooked. There is a bookkeeping process to keep track of which dishes are made and by whom.

5 Remote use of a home server (6 p)

You have a home server, containing an excellent collection of music and your digital picture archive. When traveling, you have a laptop computer with you and you want to retrieve music from your home server. You also want to be able to back up to the server your newest purchases of music and your digital pictures.

You don't want to let anybody break in to your server and change the files, you don't want anybody to be able to watch you pictures without permission and you have to protect the music, too, so that you would not have problems with the copyright authorities.

Write an essay, where you explain how you protect the server against threats from the network, how you transfer the files and how you control the access permissions. Also explain how you define the security requirements in terms of confidentiality, integrity and availability.

You may draw a picture to illustrate your essay, but the main answer should be in the written essay. Your solutions should be reasonably practical and justified.