1: Terms (8 points)

Explain briefly the following concepts:

a) DAC (Discretionary Access Control)
b) One-way hash function
c) Replay attack
d) Non-repudiation
e) DMZ (Demilitarized Zone)
f) SSO (Single Sign On)
g) ACL (Access Control List)
h) Steganography

2: Justify whether the following claims are right or wrong. (6 p)

a) An IDS system should react to an attack by automatically breaking into the attacking machine and preventing its operation.
b) A certificate must always have the information to uniquely identify to whom the certificate has been issued to.
c) Unix provides multilevel security (MIS).
d) A typical WLAN network can often be eavesdropped from two kilometer distance.
e) The most important requirement for getting a Common Criteria certification is that the product must be protected against all attacks known at the time of certification.
f) Kerberos is based on shared secrets.

3: Security policy models (4 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? 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.

4: Exploits (6 p)

a) This fall there has been a rootkit in addition to the music on the CDs from Sony BMG. Explain briefly what is a rootkit, how it works, and why is it being used. (3p)
b) List three attacks targeted at passwords and tell how to defend against these attacks. (3p)

5: Security vulnerabilities (6 p)

Server software, like WWW or email servers, may have vulnerabilities or security holes, which enable an attacker to gain access to the server host. How are these weaknesses created? Describe on the general level two of these vulnerabilities and how they are exploited. How would you prevent the creation of security vulnerabilities when leading a software project (list at least two methods you would use)?

6: 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.