Remember to mark each paper you return with the course code, the exam date, your full name and student number!

The exam has two parts, both of which have to be passed. The passing limit for the first part is 10 points.

FIRST PART (Questions 1-2)

1: Terms (12 points)

Explain the following terms briefly (2-3 lines/explanation is enough) ***and*** **give an example** that describes the practical role of that term in the field of computer security.

a) vulnerability
b) non-repudiation
c) social engineering attack
d) covert channel
e) certificate
f) buffer overflow

2: More terms (8 points)

Explain briefly the following terms and their relationship to each other:
a) Identification, authentication and authorization. (4 points)
b) Worm, virus and Trojan horse. (4 points)

SECOND PART (Questions 3-6)

3: IPsec (5 points)

Answer briefly the following questions:
What is IPsec? (1p)
What problems does IPsec solve? (2p)
How does IPsec protect e-mail? (2p)

4: Access control (5 points)

Give a short comparison of the benefits and downsides of using the following structures for access right management: access control matrices, access control lists (ACL) and capabilities.

5: Firewalls (4 points)

Compare the advantages and disadvantages of packet filtering firewalls and application level firewalls.

6: Essay (20 points)

This exam has one essay question which is graded 0-20 points. **Choose one and only one** of the following themes (a, b, c, and d) and write an essay about it on a separate paper. Some themes have guidance about what is expected from the answer, for other themes the title is self-explanatory.

Mark clearly the letter of the theme you have chosen on your answer.

If you write about more than one theme, you will get points according to your weakest answer.

The recommended length of the essay is 2 to 4 pages of text.

The alternative themes for the essay:

a) **Confidentiality models**
Describe briefly the Bell-LaPadula and Chinese Wall security policy models. Compare the background of the models and the fields where they are applied. Analyze the problems of the models and compare them, for example do the same information leak mechanisms work in both models?

b) **Intrusion detection**
Tell about different ways how intrusion detection can be done and about their advantages and limitations. In general, what kind of difficulties there are in detecting attacks coming through a network? When is it reasonable to use an intrusion detection system? How does intrusion detection relate to other security arrangements?

c) **Smart card security and using smart cards for authentication**

d) **Security at different stages of the lifecycle of software**