CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
Examination in Computer Security EDA263 (DIT641) for the International Master's Program in Secure and Dependable Computing Systems, Wednesday 18 August 2010, 08.30 -12.30

Examiner: Professor Erland Jonsson, Ph. 031-772 1698, email: erland.jonsson@chalmers.se

Solutions: No solutions will be posted.

Language: Answers and solutions must be given in English.

Grades will be posted before Monday 6 September, 2009.

A review of the exam after correction is possible. The date and time will be announced on the course home page.

You are **not** allowed to use any means of aid.
However, according to general rules printed English language dictionaries are allowed.

Grade: The grade is normally determined as follows:

30 p ≤ grade 3 < 38 p ≤ grade 4 < 46 p ≤ grade 5 (EDA263)

30 p ≤ pass < 46 p ≤ pass with distinction (DIT641)

1. Security and dependability concepts

a) List the traditional security and dependability attributes/aspects.
b) Group the attributes in protective and behavioural, where applicable. Explain their functionality and relation to the object system. Draw an illustrating figure.
c) Explain the interaction between attacks, vulnerabilities and failures and the object system in terms of its protective and behavioural attributes. (10p)

2. Set-UID programs

a) What is a SUID (set-UID) program? Explain the functionality and intended use of such a program. How does it show that a program is SUID?
b) Explain why and how SUID programs can be a security problem.
c) Define and explain the function of RUID and EUID and their relation to SUID programs. (6p)

3. Network authentication

Describe by means of a diagram and a bulleted list the Kerberos authentication scheme. Further, name the most important elements (e.g. ticket, session key, etc) that are used in the protocol and describe the use of them. (No protocol details are needed.) (8p)

4. Intrusion detection systems

Give a brief and comprehensive overview of Intrusion detection systems, including usage, principles, types, performance, etc, etc. (10p)

5. Protection in operating systems

The course book mentions three different methods to control access to objects ("files") in an operating system. Define and explain these methods by means of a figure for each of them. (8p)

6. Database security

What is SQL injection? What is accomplished with it? Describe what makes SQL injection possible (in principle) and how to protect against it. (4p)

7. Miscellaneous questions

Give a short (i.e. less than ca 10 lines) but exhaustive answer to each of the following questions: (The answer must include not only the function, usage, principle etc, but also the (security) context into which the object of the question would be applicable.) (14p)

a) What is meant by a covert channel?
b) What is SYN flooding? What is the use of it?
c) What is the context, goal and basic principle of the Chinese Wall security policy?
d) What is query analysis? What is the reason for applying it?
e) Describe three basically different methods to achieve unauthorized access to a password. Also give a countermeasure for each of them.
f) What is a security policy and security plan?
g) What is meant by Security Target and Protection Profile? Which is the difference?