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 17 August 2011, 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 Friday 9 September, 2011.

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. Authentication

a) Define what is meant by authentication.
b) Define what is meant by authorization.
c) Describe the four steps of an authentication procedure.
d) The information used for authentication can be of three (or potentially four) fundamentally different kinds. Describe and exemplify those. (8p)

2. Cryptography

a) Describe the basic principles and characteristics of asymmetric crypto systems.
b) Suppose A wants to send a symmetric encryption key to B, so that nobody else can intercept and read it. Suggest how this can be done using asymmetric cryptography.
c) Suggest an improved method, which ensures that the symmetric key came from A. (8p)

3. Intrusion detection

a) The function of an intrusion detection system (IDS) can be described by the false alarm rate. Define what is meant by this term. There are (at least) two other terms that describe the basic function of an IDS in terms of the attack vs alarm relation. Name and give a definition of these.
b) There is a fundamental reason why the false alarm rate is one of the biggest problems for IDS's, a reason that is generally applicable to many types of systems that have certain characteristics, and not only to IDS's. Describe this problem in some detail and explain why it is applicable to IDS's. Give a numeric example. (8p)

4. The Bell-La Padula security model

Each operating system has a set of subjects *S* and a set of objects *O*. For each subject *s* in *S* and object *o* in *O* there is a "security class" *C(s)* and *C(o)* respectively.
Give a detailed description of the Bell-La Padula security model and name the two properties that characterize the model. Give a mathematical description of those properties. Also, discuss what kind of model it is and its use. There is a "twin" model to the Bell-La Padula model that reflects another security aspect. Describe very briefly the twin model and its relation to the Bell-La Padula model. (8p)

5. A basic system model of security and dependability.

a) The course has suggested a system model for the integrated concept of computer security and dependability. The model describes security and dependability attributes, such as e.g. reliability and availability. The model can also describe the system's interaction with its users and environment, e.g. in terms of attacks and failures. Draw a figure that describes the model, and give a thorough explanation of it.
b) The model can be used to define fundamental security "defence lines", i.e. basic methods to avoid system failures. Please explain.
c) Finally, discuss the concept of (failure) latency in the model and its implication for the behavioural attributes. (10p)

6. Inference in databases

Please make a comprehensive discussion of the problem of inference in databases. Among other things you should explain what inference is and why it is a problem, how it can be accomplished and what kind of counter measures there are. **(**10p)

Note: The answer to this question can be given in many different ways and not everything can be covered. The answer will judged based on the approach taken, i.e. what you select to incorporate in your description and how it is structured and presented.

7. Miscellaneous questions

Give a short (i.e. less than ca 20 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.) (8p)

a) What is a covert channel? How is it used? Are there different kinds?

b) What is a Man-in-the-middle-attack? What is achieved by it?

c) Operating system security is largely based on *separation*. Describe available types and how they are used.

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