CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Engineering

Tentamensskrivning i Tillämpad datasäkerhet EDA261 för D4/5
(även LEU 321 för ChL och INN 641 för GU) tisdagen den 24 augusti 2004, kl 14.15 - 18.15

Examination in Applied Computer Security EDA261 for the International Master's Program in Dependable Computing Systems Tuesday 24 August 2004, 14.15 - 18.15

Examiner: Professor Erland Jonsson, tel. 772 1698, email: erland.jonsson@ce

Solutions: No solutions will be posted.

Language: The examination is written in English. Answers and solutions may be given in English or Swedish.

Grades will at the latest be posted before Tuesday 7 September 2004, at 10.00 a.m. on the Department's notice board and the course's homepage.

Please contact the examiner if you want to review the coorection of the exam.

You are **not** allowed to use any means of aid.

Grade: The grade is normally determined as follows:

24p ≤ grade 3 < 36 p ≤ grade 4 < 48 p ≤ grade 5

1. Operating system security

a) The security of an operating system normally relies on different types of *separation.* Describe four such types of separation. (4p)

b) 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. (7p)

c) Explain briefly the meaning of the term "capability" in this context. (1p)

d) How would you go about it to develop a secure operating system? Give the answer in the form of a bulleted list. (3p)

2. Attacks and other security concepts

Give a brief explanation to the following terms:

a) polymorphic virus

b) backdoor

c) masquerading

d) hoax virus

e) DDOS attack (5p)

Explain in some detail and illustrate with a figure the following terms:

f) attack tunneling

g) honeypot

h) TOCTTOU flaw (6p)

Give a detailed explanation, including a figure, of how the attack below is accomplished.

i) buffer overflow (buffer overrun) attack (4p)

3. Passwords

a) Give three fundamentally different methods for how to get illicit (Sw: ung. "olovlig") access to a password. Illustrate with examples. (3p)

b) The Chalmers CDKS portal is enforcing a password policy for its users. An acceptable password has to have the following properties:

- it has to have at least 8 characters
- it has to have at least 4 unique characters
- at least 4 of the characters have to be alphabetic
- at least 1 character must be a number
- at least 1 character must be a "special character", i.e. a character other than a number or an alphabetic character.

Discuss the requirements above from a security viewpoint, including both attack and protection aspects. (4p)

4. Intrusion detection

One specific aspect of the detection functionality of an intrusion detection system (IDS) is described by the false alarm rate. Define what is meant by this term. There are two other terms that describe two other aspects of an IDS's detection functionality. Name and give a definition of these. Put all those three terms into the same context.
The false alarm rate is one of the biggest problems for IDSs and there is a fundamental reason for this. Motivate and explain in detail why this is so. Give a numeric example. (8p)

5. The Bell-La Padula security model

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. . (10p)

6. Social engineering

What is social engineering? What is the purpose of it? In which respects is social engineering effective? Which are the advantages to the one who uses it? (5p)