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 13 april 2004, kl 08.45 - 12.45

Examination in Applied Computer Security EDA261 for the International Master's Program in Dependable Computing Systems Tuesday 13 April 2004, 08.45 - 12.45

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

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 27 April 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. Security and dependability

Give definitions for the four concepts: reliability, availability, safety and security and describe their interrelation (if any). Further, discuss for each of these concepts how they could be measured or given some quantitative assessment. (8p)

2. Authentication

a) Define what is meant by authentication.
b) Define what is meant by authorization.
c) Define what is meant by a capability.
d) Describe the four steps of an authentication procedure.
e) The information used for authentication can be of three (or potentially four) fundamentally different kinds. Describe and examplify those. (10p)

3. Firewalls

a) What is a firewall?
b) There are two types of stances (i.e. security philosophies) for a firewall system. Describe and discuss those briefly.
c) Give three examples of different firewall systems. Also describe their characteristics.
d) Give four weaknesses for firewall systems. (10p)

4. Security modelling

Describe the Bell-La Padula security model. In particular define (mathematically) the two properties that characterize the model. Also, discuss what kind of model it is and its use.(10p)

5. Intrusion detection

Discuss broadly the role of intrusion detection systems (IDS) as a security mechanism in today’s and tomorrow’s computer systems. Among other things your answer could cover the following sub-topics: functionality, IDS wrt other security mechanisms, advantages and drawbacks, its potential for the future, etc. (8p)

6. Malicious code

Explain how an intruder could use the path definition (“sökväg”) in Unix to create a security hole in the system, e.g. to launch a trojan horse? Give details. (4p)

7. Miscellaneous questions

Explain briefly the following terms:
a) key escrow
b) query analysis
c) principle of least privilege
d) Chinese wall
e) serialization flaw
f) link encryption
g) reference monitor
h) TOCTTOU flaw
i) teleology
j) social engineering (10p)