CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Engineering

Tentamensskrivning i Tillämpad datasäkerhet EDA261 för D4 och LEU 321 för Di3, ChL
torsdag den 21 augusti 2003, kl 08.45 - 12.45
Examination in Applied Computer Security IMP 261 for the International Master’s Program in Dependable Computing Systems Thursday 21 August 2003, 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 solution may be given in English or Swedish.

Grades will be posted before Tuesday 2 September 2003 at 10.00 a.m. on the Department's notice board and on the course's homepage.

Please contact the examiner if you want to review your exam.

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

Grade: The grade is normally determined as follows:

$24\text{p} \leq \text{grade } 3 < 36 \text{ p} \leq \text{grade } 4 < 48 \text{ p} \leq \text{grade } 5$

1. Security aspects

Give the three traditional aspects of security and explain them in view of the “delivery-of-service” concept. (6p)

2. UNIX security

a) Explain the concepts of real UID and effective UID in a UNIX operating system.
b) An example of the file permissions in UNIX is `-rwsr-sr-x.` Explain these file permissions. Which is the use of the bit named `s`? Give an example of a program where the `s`-bit is needed. Explain why.
c) What happens with the real and effective UID’s when a system call such as `setuid(181)` is executed? (10p)

3. Buffer overrun

Describe how a buffer overrun (buffer overflow) attack works, what is accomplished, why it is possible, etc. (6p)

4. Kerberos

Kerberos is a system for authentication. Give an exhaustive description of its general function (i.e. not all the details are needed) based on a figure and a message exchange chart. The description must include explanation of the fundamental concepts of Kerberos. Which were the original requirements that were set up when the development of the system started? Also discuss the applicability of Kerberos. (10p)

5. Database security

a) The course has covered four different (query) attack types on database systems. Name these and explain how they work.
b) The course has also covered three fundamental database protection methods. Name and describe these.
c) Discuss broadly the concept of “polyinstantiation”. (10p)

6. Risk analysis

What is a risk analysis? Define and discuss the different steps of such an analysis. Discuss its use, advantages and drawbacks as well as its applicability. (6p)

7. Cryptographic security

Discuss the security of cryptography from a broad and applied perspective. (Circa 3-5 pages.) The discussion must reflect what you want to achieve by cryptography. It must also cover the problems you meet, possible reasons for not achieveing your goals as well as potential remedies for the problems. Examples of possible sub-topics might be (not exhaustive, nor obligatory): goals; security aspects; vulnerbilities; cryptographic methods (in principle); implications for the system, the user, other applications; organizational issues etc
Note: This type of question can have many answers, none of which is exhaustive, so there is no single “correct” answer. The judgement of the answer will be based on the the technical contents, but also on the how the answer is structured and how the topic is generally treated and which items are covered. The answer should clarify the student’s understanding of the general problem. (12p)