CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Engineering

Tentamensskrivning i Tillämpad datasäkerhet EDA261 för D4 och LEU 321 för Di3, ChL
Lördagen den 14 december 2002, kl 08.45 - 12.45
Examination in Applied Computer Security EDA261/IMP 261 for the International Master's Program in Dependable Computing Systems Saturday 14 December 2002, 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 at the latest be posted before January 8th, 2003 at 10.00 a.m. on the Department's notice board and on the course's homepage.

A review of the exam may take place January 8th, 2003 at 10.00 a.m. at 13.30 - 14.00 pm.

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

Grade: The grade is normally determined as follows:

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

1. A biological approach to security

The course has suggested that there is a biological analogy to computer security. Describe and explain this analogy. Give examples. (8p)

2. Passwords

Suppose you want to acquire a secret password by means of a so-called brute force attack ("uttömmande sökning"). You have succeeded in reading the encrypted version from a password file. You have reason to believe that the cleartext password contains 8 small letters only and no other characters. Suppose you can use a network of ***N*** computers for the attack and that each computer can make ***k*** attempts per second with a negligible parallelisation penalty.

a) Derive an expression for the mean search time to crack the password. Explain how you arrive at your suggested solution.

b) Suppose the password also contained capital letters. How would that affect the time to crack it? Explain why.

c) Suppose this was a UNIX operating system with "salt" functionality. How would that affect the time to crack the password. Explain why. (8p)

3. Covert channel

What is a covert channel? Explain how it works and a "typical environment" for a covert channel. There are several types of covert channels. Please name these and explain how they work. What kind of performance metric is normally used for covert channels? (8p)

4. Malicious code

Describe in detail how (and why) a buffer-overrun attack works. Which are the flaws utilized, if any? Illustrate with an example, e.g. from the Internet worm. Which is the result that the attacker achieves? (8p)

5. PGP message exchange

Suppose ***A*** wants to send a message to ***B*** that is read protected and signed according to the PGP method. How does encryption/decryption and signing work in this case? What keys are used and when? Give a detailed step-by-step explanation of the procedure. You may assume that both ***A*** and ***B*** already have a public/private key pair before starting the procedure. (8p)

6. Secure storage

Your employer has given you the task of developing a distributed file storage system, in which the files are stored in remote untrusted hosts. The requirements on the system are that the confidentiality as well as the availability of the files must be protected. Encryption tools can not be used for legal reasons.

How would you design your system? Give a functional description. Explain the functionality of your design and the reasoning behind it. Finally, try to evaluate your system and assess to what extent the requirements are fulfilled. Are there any remaining flaws?

It may not be possible to design such a system. In that case, give a detailed explanation why this is so. (8p)

7. Miscellaneous questions

Explain the meaning of the following terms. In particular address their security relevance:

a) authentication
b) No-Write-Down
c) rule-deontology
d) query analysis
e) call-back
f) Chinese Wall
g) demilitarized zone
h) trapdoor
i) fraud detection
j) Certification Authority
k) honey-pot
l) key escrow (12p)