CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering

Examination in Computer Security EDA263 for the International Master's Program in Secure and Dependable Computing Systems et al, Tuesday 11 January 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.

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. Password cracking

a) Explain, by means of a step-by-step-description, how an off-line brute-force or dictionary password attack against a UNIX system is accomplished. (You may assume that the password file is accessible and readable, i.e. no “shadow file”).

b) There is one “spicy” ☺ UNIX security feature, which aims to make such attacks less effective. Explain how this feature is set up and how it works. Also, explain the aims of it and how they are accomplished. (8p)

2. User identification in UNIX

a) Processes in UNIX have at least two identities, the Real UID (RUID) and the Effective UID (EUID). Describe the functionality and use of these two identities

b) What is a SUID (Set-UID) program? What is the use of such a program? Give an example!

c) **User1** (with UID=27055) is running a program **Prog** with the following access rights:

```
-rws r-x r-x root root /bin/Prog
```

Give **User1**’s EUID and RUID when **Prog** is started.

d) The program **Prog** contains a system call

```
setuid (User1)
```

which is executed within the program. Give **User1**’s EUID and RUID after execution of the system call.

e) At a later occasion (the person behind) **User1** logs in as **User3** (with UID=27057). Which EUID and RUID will **User1** get after the log-in? (8p)

3. Firewalls

a) The book mentions four different types of firewalls. Describe these types and their characteristics and function.

b) There are two types of default policies (also called “stances”) for a packet filtering firewall. Describe and discuss those briefly.

c) Give four examples of situations when a firewall would not present a sufficient level of protection. (10p)

4. Buffer overflows

Explain how a typical stack-based buffer overflow attack works. Your answer should include a picture of the stack with the most relevant stack fields marked. A “canary” is the name of a defence method for buffer overflows. Please explain in some detail how this method works and discuss the prerequisites for its function. (8p)

5. Clark-Wilson Security Policy

Clark and Wilson proposed a commercial security policy for what they called “well-formed transactions”. In which context can this policy be used and what is the purpose of it? The policy is defined in terms of an “access triple”. Give and explain this triple. Also give an illustrating example of the use of this model by means of a block diagram. (8p)

6. 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)

7. Miscellaneous questions

Give a brief but informative answer to the following questions.
(a-d gives 1point each, e-f gives 2 points each).
a) What is the idea and goal of intrusion tolerance?
b) What is meant by a key escrow system? What is the idea and potential benefit behind it?
c) What is meant by data remanence?
d) What is a honeypot?
e) The Common Criteria defines a set of potential security requirements. Those requirements fall into two main categories. Which ones? What is the use of them?
f) Which are the main differences between an asymmetric and symmetric crypto? Make a comparison of the main characteristics. (8p)