CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
Examination in Computer Security EDA263 (DIT641) for the International Master's Program in Computer Systems and Networks, Thursday 17 January 2013, 14:00—18:00

Examiner: Assistant professor Magnus Almgren, Ph.031-772 1702,
email: magnus.almgren@chalmers.se

Teacher available during exam: Prof. Erland Jonsson, Ph. 031-772 1698.

Solutions: No solutions will be posted.

Language: Answers and solutions must be given in English.

Grades: will be posted before Tuesday 5 February, 2013.

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. Insiders

What is meant by an “insider” (as opposed to an “outsider”). Please give a brief definition. Give a general and comprehensive discussion of the ”insider” problem in computer security. At least the following aspects should be covered: Characterize insider threats and compare them to outsider threats? Different types of insiders? What kind of countermeasures are there? Is there a time aspect to the problem? (8p)

2. Security and dependability concepts

a) List the traditional security and dependability attributes/aspects.
b) Group the attributes in protective and behavioural, where applicable. Explain their functionality and relation to the object system. Draw an illustrating figure.
c) Explain the interaction between attacks, vulnerabilities and failures and the object system in terms of its protective and behavioural attributes. (8p)

3. 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)

4. Side Channel Attacks

a) Define what is meant by a side-channel attack and its characteristics. (1p)
b) Describe three (3) different types of side-channel attacks. (3p)
c) Discuss possible countermeasures for the attacks in (b). (3p)

5. Malware

a) One of the most common types of malware is the *virus.* Please explain the three parts that a virus usually contains, and the four phases a virus may go through during its lifetime.
b) Explain what a Trojan Horse is and what can happen if the compiler on the system is in reality a Trojan horse.
c) Explain what a backdoor is. Are there any legitimate uses for using a backdoor? (9p)

6. The Bell-La Padula security model

a) In the Bell-La Padula security model, two properties characterize the flow of information. Give a mathematical description of these two properties.

Now consider the following situation at an antivirus company. The following three people are employees at the company:

- Aron, cleared for (Top Secret, {Sweden, Vulnerability})
- Caleb, cleared for (Secret, {Vulnerability})
- Kate, cleared for (Confidential, {Vulnerability})

Remember that the clearance of a person has the same form as the classification of a piece of information: <rank; compartments>. The use of compartments helps to enforce the *the need-to-know rule,* where individuals shall only have access to those data that they need in order to perform their jobs.
Hint: The Security Level <L,C> dominates <L',C'> if and only if L'≤L and C'⊆C.

There are at least three compartments at the company:
{Sweden, Vulnerability, Malware}.
Furthermore: "Top Secret"(TS) > "Secret" (S) > "Confidential" (C) > "Unclassified" (U)

Each employee keeps his/her own working diary classified in accordance to their clearance. Thus, Kate also uses the document D_{Kate}, classified as (Confidential, {Vulnerability})

For each of the following examples, specify **(1) what kind of document access is allowed** (read/write/both/none) and **(2) why that is so**, i.e. in your answer we want you to refer to your answer in (a). For example: "only write access is allowed, read access breaks property X"

b) Aron wants to access D_1, classified as (TS, {Sweden, Malware})
c) Kate wants to access D_2, classified as (C, {Malware})
d) Caleb wants to access D_3, classified as (C, {Vulnerability})
e) Aron wants to access D_4, classified as (C, {Sweden})
f) Kate wants to access, D_5, classified as (S, {Vulnerability})

(7p)

7. Miscellaneous questions

Give a short (i.e. less than ca 10 lines) but exhaustive answer to each of the following questions: (The answer must include not only the function, usage, principle etc, but also the (security) context into which the object of the question would be applicable.)

(13p)

a) How does a DDoS attack differ from a DoS attack? Include an image.
b) Operating system security is largely based on *separation*. Describe available types and how they are used.
c) What is a Man-in-the-middle-attack? What is achieved by it?
d) What is social engineering?
e) Define the false alarm rate often describing an intrusion detection system.
f) What is SQL injection? What is accomplished with it? Describe what makes SQL injection possible (in principle) and how to protect against it.
g) Describe three basically different methods to achieve unauthorized access to a password. Also give a countermeasure for each of them.
h) What is meant by Security Target and Protection Profile? Which is the difference?

i) What is meant by key escrow?
j) Will signing a message protect its confidentiality?
k) Is PGP a symmetric system?
l) Should one use RSA or AES to protect the confidentiality of a very sensitive document, if one knows the largest key length that can be used is 256 bit.
m) In public-key cryptography (as opposed to symmetric cryptography), one has two different keys. Is it possible to use one key as a primary key and the other as a backup if the first key is lost?