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, Tuesday 20 October 2009, 14.00-18.00

Examiner: Professor Erland Jonsson, Ph. 031-772 1698, email: erland.jonsson@chalmers.se

Teacher available during exam: Magnus Almgren, Ph. 031-772 1702.

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. Authentication

a) Define what is meant by authentication.

b) A basic authentication procedure consists of a number of steps and a number of involved parties and entities. Describe this procedure in principle. Name important entities etc and explain their function. Discuss potential problems and attack vulnerability for each of them. “What can go wrong”?

c) There are three (or possibly four) fundamentally different qualities used to perform authentication. Name these and give examples. (10p)

2. UNIX Security

A security consultant has been asked to improve the security of a UNIX system. In a public directory that most users on the system can access, she runs the following command:

```
> ls -al
-rwxr-xr-x 1 root root   18721 2009-10-13 21:56 prg1
-rws---r-x 1 root root   21872 2009-10-13 21:06 prg2
```

Which program do you suggest her to concentrate her efforts on? Explain in detail why. (4p)

3. Cryptography

In the course, we discussed symmetric and asymmetric (public-key) cryptography. For brevity, we will abbreviate them as SC and AC. For each of the following statements, state if you agree with it and explain your reasoning. Note: we will *not* accept only yes/no answers.

a) Asymmetric cryptography (AC) is in general faster than symmetric cryptography (SC).
b) Key management is more manageable with AC compared to SC.
c) Non repudiation can easily be achieved with SC.
d) When receiving a message encrypted with an asymmetric algorithm, you know that if you can successfully decrypt the message, no one has tampered with the message and it comes from the stated sender.
e) *Signing* a message will protect its confidentiality.
f) PGP is a symmetric system.
g) To protect the confidentiality of a very sensitive document, one should use RSA instead of AES if the key length is 256 bit. (7p)

4. Database security

What is SQL injection? What is accomplished with it? Describe what makes SQL injection possible (in principle) and how to protect against it. (3p)

5. Miscellaneous questions

Give a short (i.e. less than ca 20 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. (8p)

a) What a covert channel? How is it used? Are there different kinds?
b) What is Man-in-the-middle-attack? What is achieved by it?
c) What is the context, goal and basic principle of the Clark-Wilson security policy?
d) Operating system security is largely based on *separation*. Describe available types and how they are used.

6. Common Criteria (CC)

a) What is the purpose and use of the "Common Criteria"?
b) Describe the meaning of and use of the concepts "protection profile" and "security target".
c) There are three types of evaluation in the CC: PP evaluation, ST evaluation and TOE evaluation. Describe briefly these three types. (8p)

7. 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})

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*"
Hint: *The Security Level (L,C) dominates (L',C') if and only if L'≤L and C'⊆C.*

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}) (10p)

8. A basic system model of security and its implications for risk.

a) The course has suggested a system model of computer security. The model describes the three basic security aspects ("CIA") in relation to the system and its environment. Draw a simple figure that describes the model, and give an explanation of it. The explanation must clarify the relation between attacks on the system and possible resulting failures. (6p)
b) Give a definition and short explanation of risk. (2p)
c) Give an extended definition of risk that fits into the system model above. (2p)