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, Wednesday 29 August 2012, 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.

Grades will be posted before Friday 14 September, 2012.

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. A biological approach to security

The course has suggested that there is a biological analogy to computer security. Describe and explain this analogy. What can be learnt from a security viewpoint? Give examples. (8p)

2. Set-UID programs

a) What is a SUID (set-UID) program? Explain the functionality and intended use of such a program. How does it show that a program is SUID?
b) Explain why and how SUID programs can be a security problem.
c) Define and explain the function of RUID and EUID and their relation to SUID programs.
(6p)

3. 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)

4. Authentication using Kerberos

Below is found a somewhat simplified version of the steps in a Kerberos v.4 authentication procedure. In this, the client C is using the Kerberos authentication server (AS) to access a service from the server V.

(1) **C => AS:** ID_C // ID_{TGS} // TS_1
(2) **AS => C:** $E_{K(C)}$ [K(C,TGS) // ID_{TGS} //TS_2 // $Lifetime_2$ // $Ticket_{TGS}$]

(3) **C => TGS:** ID_V // $Ticket_{TGS}$ // $Authenticator_C$
(4) **TGS => C:** $E_{K(C,TGS)}$ [K(C,V) // ID_V // TS_4 // $Ticket_V$]

(5) **C => V:** $Ticket_V$ // $Authenticator_C$
(6) **V => C:** $E_{K(C,V)}$ [TS_5 + 1]

(7) $Ticket_{TGS}$ = $E_{K(TGS)}$ [K(C,TGS) // ID_C // AD_C // ID_{TGS} // TS_2 // $Lifetime_2$]
(8) $Ticket_V$ = $E_{K(V)}$ [K(C,V) // ID_C // AD_C // ID_V // TS_4 // $Lifetime_4$]
(9) $Authenticator_C$ = $E_{K(C,TGS)}$ [ID_C // AD_C // TS_3]

Describe briefly the following elements in the procedure and explain their function:
a) (2), $E_{K(C)}$
b) (2), K(C,TGS) and (7), K(C,TGS)
c) (2), $Lifetime_2$ and (7), $Lifetime_2$
d) (6), TS_5 + 1
e) (8), $Ticket_V$ and its elements
f) (9), $Authenticator_C$ and its elements (8p)

5. Intrusion detection

a) The function of an intrusion detection system (IDS) can be described by the false alarm rate. Define what is meant by this term. There are (at least) two other terms that describe the basic function of an IDS. Name and give a definition of these. (3p)

b) There is a fundamental reason why the false alarm rate is one of the biggest problem for IDS's, a reason that is generally applicable to many types of systems that have certain characteristics, and not only to IDS's. Describe this problem in some detail and explain why it is applicable to IDS's. Give a numeric example. (7p)

6. Insiders

Give a general and comprehensive discussion of the ”insider” problem in computer security. Which are the insider threats? Different types of insiders? Countermeasures? Relate insider threats to other types of threats. Estimate their importance for system security. (8p)

Note: The answer to this question can be given in many different ways and not everything can be covered. The answer will judged based on the approach taken, i.e. what you select to incorporate in your description and how it is structured and presented.

7. 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.) (12p)

a) What is a covert channel? How is it used? Are there different kinds?

b) What is a Man-in-the-middle-attack? What is achieved by it?

c) Operating system security is largely based on *separation*. Describe available types and how they are used.

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

e) What is defensive programming? What is the purpose and use of it?

f) Describe the Bell-LaPadula model?