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 08 Mars 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 Tuesday 27 Mars, 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. Authentication

a) Define what is meant by authentication.
b) Define what is meant by authorization.
c) Describe the four steps of an authentication procedure.
d) The information used for authentication can be of three (or potentially four) fundamentally different kinds. Describe and exemplify those. (8p)

2. SYN spoofing attack

Please explain the SYN spoofing attack as described in the book. Your answer should discuss the following. (10p)

a) The normal three-way handshake of TCP connection procedure (as a figure).
b) How the attack works (use the figure from a) in your description).
c) What "weakness" of the target computer the attacker is targeting.
d) One key requirement for the attack to work (hint: what happens with RST packets?)
e) One reason why the attacker may choose this attack over a message flooding attack.

3. Cryptography

You are having a discussion with a friend about cryptography. Your friend makes a series of statements. Please tell us how you would respond (True or False). Note that you have to answer with an explanation to get any points.

{Example: *You should not run unknown programs.*
→ True. Reason: they may contain a Trojan horse or other types of malware.} (8p)

a) Public-key encryption is more secure from cryptanalysis than symmetric encryption.
b) Public-key encryption is a general-purpose technique that has made symmetric key encryption obsolete.
c) Key distribution is trivial in public-key encryption. It is enough to go to *any* online database to download a key for direct use.
d) I prefer to use public-key cryptography (to symmetric cryptography), because then I have two different keys. This enables me to use one key as a primary key and the other as a backup.

4. Risk Analysis

a) Give a definition of risk. Also give a simple example of a risk calculation.
b) Describe the overall Risk Assessment Procedure for an IT system's security risks.
c) What kind of trade-off is made as a result of the risk analysis?
d) What is the benefit and usage of this trade-off?
e) Which are the problems and possible draw-backs with the risk analysis procedure and the trade-off? Explain! (10p)

5. Defensive programming

The program on the last page of the exam (vlnPrg.cc) has at least two major security problems. (**Note:** the password is in cleartext for practical reasons. This is not one of the intended problems that we are asking for.)
Answer the following questions after reading the code (and the descriptive comments). (6p)

a) Explain briefly the two problems and how a hacker could exploit them.
b) Explain how the program could be fixed, i.e. give us the pseudocode that replaces lines in the original program (only for the two major problems).
c) The problems within the program has to do with a larger concept. Explain this concept.

6. Common criteria

a) Explain the meaning of the concepts TOE, PP and ST.
b) There are three types of evaluation in the Common Criteria: PP evaluation, ST evaluation and TOE evaluation. Describe those evaluation types briefly and how they are related to each other.
c) Explain the concepts component, package and EAL **(**8p)

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.) (10p)

a) What is a covert channel? How is it used? Are there different types?
b) Operating system security is largely based on *separation*. Describe available types and how they are used.
c) What is a side-channel attack? Give its characteristics and usage.
d) Describe what is meant by the concept "configuration management". Why is it used? Which are the security implications of it?
e) What is meant by computer forensics?