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 12 January 2010, 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. 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. Give an example of a library function in C that will make your program vulnerable to buffer overflows. Please discuss at least one automatic approach to defend against this type of vulnerability, an approach that does not depend on the programmer's skill in writing correct code. (8p)

2. Security Mechanisms

There are many available security methods and mechanisms that work in different ways and with different focuses. Describe the three security mechanisms listed below from a security point of view, e. g. how and to what extent they improve security. Also discuss possible drawbacks:

a) a Biometric Authentication mechanism
b) an Intrusion Detection mechanism
c) a Virus scanner with response functionality
Also describe the fundamental functional differences between them. (8p)

3. Chinese Wall security policy

Assume that you are head of division in a successful consultancy company. The company has the following customers: Air France (airlines), Volvo (cars), Swedbank (banks), SAAB (cars), Finnair (airlines), Nordea (banks) and Lufthansa (airlines). The company has recently implemented the Chinese Wall security policy.

a) What is accomplished by this policy? What does it imply for the company (and you) and for the customers?
b) Name and describe the three abstraction levels in the Chinese Wall security policy.
c) Draw a figure to show how the seven companies above would be represented according to this policy? Mark the abstraction levels in the figure (if appropriate).
d) You have two people working for you, Adam and Carol. They are trying to access data in the order given below (1-8). Please specify whether the access is allowed (OK) or denied (No) and give the reasons for denial (if any).
1. Adam tries to access data from Finnair.
2. Adam tries to access data from Lufthansa.
3. Carol tries to access data from Lufthansa.
4. Adam tries to access data from SAAB.
5. Carol tries to access data from SAAB.
6. Adam tries to access data from Nordea.
7. Adam tries to access data from Volvo.
8. Adam tries to access data from Swedbank.
e) When making the budget for the coming years, you want to reduce your personell cost. What is the minimum number of people you need in order to serve all the customers above? Please explain why. (8p)

4. Database security

A serious problem in a database is if a failure occurs while data.is being modified.

a) Clarify why this is a specific problem.
b) There is a method to avoid the effects of such a failure and perform updating in a robust and secure way. Name and describe this method. (8p)

5. Intrusion tolerance

a) What is the idea and goal of intrusion tolerance?
b) The course has covered an intrusion tolerance method (called FRS) aimed for secure archiving.
Describe this method and the benefits of it. Draw a block diagram and explain how it works. Discuss potential flaws and objections that could be raised against the method. (8p)

6. Key Escrow Systems

a) What is meant by a key escrow system? What is the idea and potential benefit behind it?
b) Discuss extensively the problems with the implementation of a large-scale key escrow infrastructure, in particular from an organisational perspective. Give examples! (10p)

7. 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? (10p)