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 (DIT641 for GU), Tuesday 19 October 2010, 14.00-18.00

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 $\leq$ grade 3 < 38 p $\leq$ grade 4 < 46 p $\leq$ grade 5 (EDA263)

30 p $\leq$ pass < 46 p $\leq$ pass with distinction (DIT641)

1. Access control

Explain the three concepts of Mandatory Access Control, Discretionary Access Control and Role Based Access Control. For Role-Based Access control discuss the usage, advantages and role assignment procedure. (8p)

2. Viruses and bots

a) In many cases the word "virus" is used as synonymous with "malware". However, there is a more exact definition of a virus and its characteristics. Give this definition.
b) A computer virus consists of three functional parts. Name and describe those parts.
c) A virus typically goes through four operational phases during its lifetime. Name and describe these phases.
d) There are at least two types of viruses that are especially designed to avoid detection. Name these types and explain how they accomplish their goal.
e) Explain the function and usage of a zombie, a bot and a botnet. (10p)

3. Clark-Wilson Security Policy

Clark and Wilson proposed a commercial security policy for what they called "well-formed transactions". In which context can this policy be used and what is the purpose of it? The policy is defined in terms of an "access triple". Give and explain this triple. Also give an illustrating example of the use of this model by means of a block diagram. (8p)

4. Common Criteria (CC)

a) Explain the meaning of and use of the concepts TOE, PP and ST?
b) There are three types of evaluation in the CC: PP evaluation, ST evaluation and TOE evaluation. Describe briefly these three types.
c) Explain the CC concepts component, package and EAL?
d) Assume a system has passed a CC evaluation. What can you say about the security of this system? Discuss and motivate your answer. (8p)

5. Security metrics

The course has suggested a system model of computer security based on the inputs to and outputs from the system. Draw a simple figure that describes the model, and give an explanation of it and its relation to security and dependability attributes. Define and explain security and dependability metrics that are based on the model. (10p)

6. Hard disk erasure

Data remanence is the residual representation of data on e.g. a hard disk. The data may remain even if attempts have been made to remove them. Explain why this data remanence may be a problem? Describe four basically different methods to remove data on hard disks and discuss what the result will be? (10p)

7. Miscellaneous questions

Explain briefly the following terms:. (6p)

a) link encryption
b) query analysis
c) reference monitor
d) key escrow
e) demilitarized zone
f) diffusion (wrt cryptos)