LiTH, Linköpings tekniska högskola
IDA, Institutionen för datavetenskap
Nahid Shahmehri

Written exam

TDDD17 Information Security

2008-06-02

This exam is **only** for the students who are registered for **TDDD17**.

There is a separate exam for TDDC03 Information Security.

Make sure you have the right exam!

Permissible aids

Dictionary (printed, NOT electronic)

Teacher on duty

David Byers, 0708-282821

Instructions

There are 5 general questions and 5 in-depth questions. The general questions are from G1 to G5, and the in-depth questions are from D1 to D5. The questions are grouped pair-wise under their corresponding topic.

You have to answer at most 3 general questions and 3 in-depth questions. You must answer at least one of the questions for each topic. A correct answer for a general question gives you 2 points, and a correct answer for an in-depth question gives you 6 points. To pass the exam you need to accumulate at least 3 points from general questions and 9 points from in-depth questions. The exam grading depends on the total number of accumulated points.

Attention

If you answer more than 3 (general) + 3 (in-depth) questions we will randomly choose 3 + 3 answers for correcting the exam, while the rest of the answers will be discarded.

Hardware and Operating System Security

G1 Describe the purpose of tamper evidence, tamper resistance, and tamper response for hardware. Give one example for each category, and one attack it protects against.

D1 In the lecture it was shown how different protection mechanisms are applied to memory. Explain which of these mechanisms can be used for process protection in a multiprogramming environment and which one not. Detail why this is so, and name example of such implementation.

File System Security and Trusted Computing

G2 Given a physical hard disk, it can be accessed via hardware, its character and block devices, its mount point, and e.g. administrative programs on a UNIX workstation. Describe how you make sure access control gets enforced for each of these possible access paths.

D2 Explain how Operational and Life-Cycle Assurance (according to common criteria) help increasing trust into a system.

Identification and Authentication

G3 Typical tokens can be smart cards or RFID devices. The book chapter used as literature for this part of the course treats mainly attacks on smart cards, while the slides mention some additional types of attack. Which typical attacks are equally valid for both normal contact smart cards and for RFID chips? Which attacks differ, and in what way, i. e. which attacks are more easy in one of the two cases and why is it more easy?

D3 D: The paper on fingerprints, which is the main part of the course literature on biometrics, contains explanations of several statistical properties of biometric systems in addition to the usual FAR and FRR. Most of them were not explained during the lectures, but hey are still part of the course. Explain what the following measures are:

FAR=FMR

FRR=FNMR

EER

ZeroFNMR

ZeroFMR

FTE

FTC

FTM

Network Security

G4 WPA is an interim security solution for IEEE 802.11 networks. Briefly explain at least one security weakness in WPA, as it is commonly deployed, and how that weakness can be exploited in practice.

D4 WPA is an interim security solution for IEEE 802.11 networks. Name at least two important design constraints (other than security) that influenced the design of WPA. WPA includes a set of algorithms known as TKIP, which address weaknesses in WEP. Explain the various algorithms, the weaknesses in WEP they are meant to address, and how they accomplish this goal.

Risk Analysis, Business Continuity Planning, Physical Security

G5 What can an attacker learn from the Google query:
site:microsoft.com -www.microsoft.com?
What is the difference between hazard analysis and risk analysis?

D5 Sketch (a) a HAZOP-diagram and (b) an event tree diagram for systemic failures that can occur in a room with a bath tub, shower or wash basin. Consider risks of water overflow only. What do you gain by a HAZOP-diagram? What do you gain by an event tree? Describe shortly the differences.