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

# Written exam

# TDDD17 Information Security

# 2008-08-15

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** In the lecture you have heard the words “administrator”–“ordinary user” and “user mode”–“kernel mode”. Describe briefly what these expressions mean. Is there a connection between them? If yes, which? How are the two expressions connected to the security of a system?

**D1** Given a solution like the iButton, you are requested to add additional tamper response mechanisms to protect extremely high-value secrets (e.g. PGP keys for your spy network). Name two environment variables that you could protect against, and how you would respond to invalid changes. Why is the iButton not the right platform for extremely high-value secrets? How would you package them instead?

## File System Security and Trusted Computing

**G2** File system access control depends both on the logical data structures on disk, and on the operating system interpreting them. Explain what this means (by e.g. looking at MSDOS vs. UNIX, and FAT vs. EXT3 or NTFS).

**D2** Systems with a higher assurance level have both information flowing in the system, and labels associated with that information, flowing over separate channels. These labels contain security level/classification information. What are the security benefits of this separation of information and labels? Describe what validation mechanisms you would implement in the kernel to prevent unauthorized Inter-process Communication?

## Identification and Authentication

**G3** Explain two statistical traps:

Suppose that there are $x=m^n$ possible passwords in a system, where n is the maximum number of characters in a password and m is the number of characters in the set of allowed characters. Then x/2 is not a good estimate of the expected number of guesses that is needed for an experienced attacker to guess the password of a given user. Why?

The FRR can be very different from the average number of false rejections that a given user experiences during repeated authentication attempts. Why?

**D3** One of the required properties of a biometric identifier is permanence over time. Fingerprints are supposed to have very good permanence. But actually accidents, like cuts can violate this. Use your knowledge of how fingerprint details are scanned, stored and analysed to discuss how systems could perhaps be designed to recognize such damages and cancel for their effects in the analysis! Also consider the problem of dirt on fingers or readers, and try to estimate if sophisticated readers could be able to distinguish between the effect of small specs of dirt and fingerprint characteristics!

## Network Security

**G4** Briefly explain what a trust relationship is and why trust relationships are an important concept in network security.

**D4** AUSCERT defines the term "security domain" as "a network of computer systems that share a specified security level through a common element".
Explain why security domains are such an important concept when designing secure computer networks. Explain how security domains relate to security mechanisms. Explain why overlapping security domains could be a problem from a security point of view. Give at least two real world examples of security domains.

## Risk Analysis, Business Continuity Planning, Physical Security

**G5** Define hazard analysis. What is it? When is it useful? What does it “not” address?

Define business continuity planning. What is it? When is it useful? What does it “not” address?

**D5** Describe shortly the steps of a risk analysis you would perform for analyzing the security of a website where customers can buy items by credit card.

Describe shortly the steps of business continuity planning for a company that maintains a website where customers can buy items by credit card.