5

LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

# Written exam
# TDDD17 Information Security
# 2015-03-16
# 8-12

**Permissible aids**
English dictionary (printed, NOT electronic)

**Teacher on duty**
Marcus Bendtsen, 0733-140708

**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 may answer at most 3 general questions and 3 in-depth questions.* You may answer both the general and the in-depth question for *at most one topic*. If you answer more than 3 general or 3 in-depth questions, we will randomly discard excess answers. If you answer both questions for more than one topic, we will randomly discard answers for all but one of the affected topics.

Students who have completed one or both of the optional labs in 2015 will get bonus points on the exam. Each completed lab gives 2 bonus *in-depth points*. Note that you must still fulfil the minimum requirement for points from general questions to pass the exam (see below).

You may answer in Swedish or English.

**Grading**
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 or lab bonus points. The exam grading depends on the total number of accumulated points.

The following grading scale is preliminary and might be adjusted during grading.

| **Grade** | C (3) | B (4) | A (5) |
|---|---|---|---|
| **Points required** | 12 | 17 | 21 |

## System Security

**G1** If the password file `/etc/passwd` cannot be read on a UNIX system, e.g. due to a disk problem, typically no users can log in anymore. Which secure design principle is this an example of? In a more general context, *briefly* motivate the rationale for this design principle.

**D1** a) What is a *cold boot attack*? Give a short example of such an attack.

b) For the respective technologies *ARM TrustZone* and *Intel SGX*, explain if they are effective at preventing cold boot attacks. Briefly explain the relevant details of each technology to motivate your answer.

## Identification and authentication, Biometric user authentication

**G2** What are the three basic methods of person recognition? What is the main advantage of using biometric recognition?

**D2** State at least three ways of providing multibiometrics. State at least three qualities multibiometrics is expected to provide. Make a short discussion (approximately one handwritten page) regarding how the stated ways may achieve the stated qualities.

## Network security

**G3** In this course we have discussed two mechanisms used to handle perimeter defense when designing networks. Name these mechanisms.

**D3** a) IPsec can work in two modes, name these modes and draw figures showing what the IP-packets look like when processed in these two modes.

b) What functions do the security policy database and the security association database provide in IPsec? Explain and draw figures showing examples of entries in these databases.

## Risk analysis

**G4** Explain the general process used to create attack trees.

**D4** Explain the ISRAM risk analysis method. It should be clear from your explanation what is done in each step, which equations/tables are used, and you should give examples of the output from each step. In order to structure your response, come up with a simple scenario where you can apply ISRAM and then explain the method by applying it to this scenario. (It is not necessary that your risk analysis is complete, only that every step is carefully explained and exemplified).

## Business continuity planning, Disaster recovery planning, Physical security

**G5** Explain two main characteristics of electronic vaulting.

**D5**

a) When a third party is contracted to develop software, a risk that the third party ceases to exist occurs (e.g. through bankruptcy). In this course we discussed two mechanisms that mitigate the consequence of this risk, explain these two mechanisms.

b) Explain how ALE values are calculated. Make sure that you explain each factor, and when possible, break down the factor to its individual components and explain these as well.

c) Explain two mechanisms that can be applied in order to mitigate risks due to emanation of signals (e.g. wireless, radio, etc.).