5

LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

# Written exam
# TDDD17 Information Security
# 2015-08-21
# 14-18

**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** Which of the information security attributes Confidentiality, Integrity, and Availability is the Bell-La Padula model designed to uphold? Briefly motivate.

**D1** In the lectures, the 8 secure design principles of Saltzer and Schroeder was presented. From these, pick *three* of your own choosing, and for each one:

- Describe the principle in about one sentence.
- Describe the motivation behind the principle.
- Give a practical example of the principle.

## Identification and authentication, Biometric user authentication

**G2** Define segmentation and enhancement in relation to feature extraction!

**D2** Attacks at the template database: Discuss the problem of leakage of biometric template information and why this constitutes a serious problem in biometric systems!

## Network security

**G3** Explain what a SYN flood attack attempts to achieve and how it works.

**D3**

a) What are trust relationships? How can they be modelled, and what can the model help to achieve?

b) There are several ways the E-box of a NIDS system can be attacked. Pick one that we have discussed in this course and explain in detail how the attack is performed, why it theoretically could work, and what the consequences are of a successful attack.

c) What is the role of the SPD in IPsec?

## Risk analysis

**G4** A risk table is created in step 2 of CORAS. Draw an example of a risk table, and then answer the following questions: who participates in creating it, what does it contain, and what is its purpose?

**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** Three types of physical intrusion alarms were discussed in this course. Name them and briefly explain what they are (no more than 30 words each).

**D5**

a) Name and briefly explain four types of alternative processing sites. Make sure to describe the contrasts between the types.

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) During the project scope and planning phase of BCP, it is important to have team members with a variety of expertise. Excluding the person responsible for the BCP process, what five other areas should be represented? Name the areas and give an example of who belongs to the area.