Information page for written examinations at Linköping University

Examination date	2016-08-19
Room (1)	G34
Time	14-18
Course code	TDDD17
Exam code	TEN2
Course name **Exam name**	Information Security, Second Course (Informationssäkerhet, fk) Written examination (En skriftlig tentamen)
Department	IDA
Number of questions in the examination	4
Teacher responsible/contact person during the exam time	Marcus Bendtsen
Contact number during the exam time	0733-140708
Visit to the examination room approximately	15:00, 17:00
Name and contact details to the course administrator (name + phone nr + mail)	Madeleine Häger-Dahlqvist, 013-282360, madeleine.hager.dahlqvist@liu.se
Equipment permitted	Dictionary (printed, not electronic)
Other important information	Preliminary grading: C(3): 20 points, B(4): 26 points, A(5): 30 points
Number of exams in the bag	

LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2016-08-19
14-18

Permissible aids
English dictionary (printed, NOT electronic)

Teacher on duty
Marcus Bendtsen, 0733-140708

Instructions
There are 4 main questions on the exam. Your grade will depend on the total points you score. The maximum number of points is 34.

Students who have completed both of the labs before their respective soft deadlines in 2016 will get 2 bonus points on the exam.

You may answer in Swedish or English.

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

Grade	C (3)	B (4)	A (5)
Points required	20	26	30

1. System Security (10 points)

a) Full disk encryption can be used to protect sensitive data in case an untrusted party gains physical access to a computer. Many security recommendations state that when disk encryption is used, the computer should be completely powered off when left unattended, rather than just using the screen-lock. In a sentence or two, explain the rationale behind this recommendation. (1 point)

b) Assume that a disk-encrypted computer has been left powered on, but with the screen-lock active. *Name* and *explain* **two** possible attacks mentioned in the course, which could be used to read out the data on the encrypted disk. Assume that the attacker has physical access to the computer. For each attack, briefly explain all steps of the attack. (4 points)

c) Assume that the attacker instead tries to get the confidential data by inserting spyware into the OS boot loader, which sends the (decrypted) confidential data to the attacker the next time the computer is rebooted. Explain how a TPM can be used to prevent disk content from being decrypted if the boot loader has been tampered with.
(5 points)

2. Identification and authentication, Biometric user authentication (8 points)

a) Discuss briefly why liveness is important to detect when measuring biometric traits! (2 points)

b) Describe briefly at least two ways an insider attack on biometric systems may be performed! (2 points)

c) Design cycle of biometric systems: Discuss briefly each of the following challenges related to understanding the nature of the biometric application! (4 points)

i. Cooperative users
ii. Overt/covert deployment
iii. Habituated/Non-habituated users
iv. Attended/Unattended operation

3. Network security (10 points)

a) Which are the three main points that should be considered when designing secure networks? (2 points)

b) Describe in detail the algorithm used when creating a shared secret using Diffie-Hellman key exchange. (4 points)

c) IPSec (4 points)

   i. 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.

   ii. 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.

4. Risk analysis, BCP/DRP and physical security (6 points)

a) 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. (2 points)

b) Name and explain four different ways of conducting training and testing of a disaster recovery plan. (2 points)

c) Explain two mechanisms that can be applied in order to mitigate risks due to emanation of signals (e.g. wireless, radio, etc.). (2 points)