Information page for written examinations at Linköping University

Examination date	2016-06-07
Room (2)	R36 R37
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
2016-06-07
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) In the context of the Trusted Computing Group (TCG) architecture, what is a *Core Root of Trust for Measurement* (CRTM)? Answer in a few sentences. (1 point)

b) Explain the term *Measurement* in the context of TCG. Explain with figures and text how it works, the core hardware and/or software components involved, and what it is used for. (3 points)

c) An *arbitrary code execution vulnerability* is a flaw in a piece of software that allows an attacker to "trick" a running program into executing (arbitrary) code supplied by the attacker. Consider an arbitrary code execution vulnerability in the following two kinds of software:

   i. A system service running with superuser privileges
   ii. A device driver

   Which of the two cases has the biggest potential impact on security? Clearly motivate your answer. (2 points)

d) Consider the two security technologies below. For each of the two cases in (c), explain why or why not each technology could be used to mitigate the effects of an arbitrary code execution attack. (4 points)

   i. SELinux
   ii. ARM TrustZone

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

a) Describe the main difference between identification and identity verification related to information collected from the template database! (2 points)

b) Feature extraction module: Describe briefly what segmentation and enhancement is! (2 points)

c) Design cycle of biometric systems: Briefly describe four of the main challenges related to collecting biometric data and how to handle these. (4 points)

3. Network security (10 points)

a) Name two mechanisms typically employed to implement perimeter defense. (2 points)

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

c) Network intrusion detection systems generally consist of four boxes. Explain two different attacks that target the E-box. For each one of the attacks explain how the attack is performed, why it theoretically could work, and what the consequences are of a successful attack. (4 points)

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

a) Explain, with an example, how attack trees are created. (2 points)

b) Explain and compare the two concepts *electronic vaulting* and *remote mirroring*. (2 points)

c) Name the four steps of BCP. (2 points)