Information page for written examinations at Linköping University

Examination date	2016-03-16
Room (1)	T2
Time	8-12
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	09:00, 11:00
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
2016-03-16
8-12

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) Back in the days of Windows XP, it was common for home PC users to always run with full Administrator privileges due to compatibility reasons. Which of Saltzer and Schroeder's 8 design principles does this violate? Also explain how this practice can significantly increase the consequences of an attack against vulnerable software running on the PC, e.g. a web browser. (2 points)

b) In response to the above problem, Microsoft added a mechanism called User Account Control (UAC) in Windows Vista. UAC would show a popup when a program attempted to perform a privileged action, requiring user confirmation. However, due to the annoying frequency of popups, users often disabled UAC altogether. Relate this to another of the 8 design principles. (1 points)

c) Assume that an attacker has managed to get arbitrary code to execute on a system with full superuser privileges. The attacker's code attempts to install a rootkit in the form of a malicious device driver, to get permanent stealthy access to the system. Is it possible to prevent the installation of malicious drivers using a software-only solution in the kernel? If yes, briefly outline how this mechanism would work. If no, explain why, and briefly explain what would be needed to prevent the attack (using techniques mentioned in the course). (*Note*: Assume that execution of attacker code with superuser privileges cannot be prevented.) (3 points)

d) Assume instead that an attacker has managed to reprogram the firmware of the main hard drive, and inserted malicious code that can manipulate data as it is being loaded from the drive. Is a software-only mechanism sufficient to detect this? If yes, briefly outline how this mechanism would work. If no, explain why, and briefly explain what would be needed to detect or prevent the attack (using techniques mentioned in the course). (4 points)

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

a) Define identification vs identity verification. (2 points)

b) What makes permanence an important quality when choosing a biometric trait? (2 points)

c) Identify and describe four advantages of multibiometrics. (4 points)

3. Network security (10 points)

a) Explain how firewalking is done in practice and what it hopes to achieve. (2 points)

b) In the lectures, four challenges were discussed in relation to configuring and using network intrusion detection systems. Explain these four challenges. (4 points)

c) Security associations (SA), security policy databases (SPD) and security association database (SAD) are three integral parts of IPsec. Explain what they are, what they contain and how they work together. Your answer should be detailed, should include examples of entries in the SPD and SAD, and it should be clear how the three combine to make IPsec work. (4 points)

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

a) What are the deliverables of the third step of CORAS? (2 points)

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. (2 points)

c) Which are the three elements required for a fire to ignite and burn? For each element, give an example of how it can be removed, thereby suppressing the fire. (2 points)