Information page for written examinations at Linköping University

Examination date	2019-09-07
Room (1)	TER1(5)
Time	8-12
Edu. code	TDDD17
Module	TEN2
Edu. code name **Module 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	Ulf Kargén
Contact number during the exam time	013-285876
Visit to the examination room approximately	Available via phone.
Name and contact details to the course administrator (name + phone nr + mail)	Annelie Almquist, 013-282934, annelie.almquist@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
2019-09-07
8-12

Permissible aids
English dictionary (printed, NOT electronic)

Teacher on duty
Ulf Kargén, 013-285876

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.

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) 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)

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) Pick **two** of Saltzer and Schroeder's secure design principles, and for each of the two, name and describe the principle and give a practical example of where it is applied. (4 points)

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

a) Define briefly segmentation and enhancement in relation to feature extraction! (2 points)

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

c) Multibiometrics: What are the main general advantages of multibiometrics? State at least two different ways of providing multibiometrics! (4 points)

3. Network security (10 points)

a) Describe what "air-gaps" are and how those are useful for network security. Are those good/practical to have and what can breach those? (2 points)

b) List as many attacks typical for wireless networks as you can. Can you rely on typical coverage range of wireless networks as a security measure? (4 points)

c) Much of Internet security, especially e-commerce, is based on TLS/SSL. (4 points) What is the difference between those two?

   i. What are certificates, how are those used and validated, what are possible problems?

   ii. Describe, in two sentences each, five basic attacks prevented by proper use of TLS/SSL

4. Database Security and Privacy (6 points)

a) Assume user Alice creates a table *Student(Name, PN, Age)* and, thereafter, the following SQL commands are issued in the given order by the given users. Note that statements 10 and 12 will fail due to insufficient privileges. Now, *describe the strategy/algorithm* that you would apply to check for each command in such a sequence whether the corresponding user has sufficient privileges to execute the command or not. (2 points)

```
# statement 1, issued by user Alice
GRANT SELECT, INSERT, DELETE ON Student TO Bob, Charlie WITH GRANT
OPTION;

# statement 2, issued by user Alice
INSERT INTO Student VALUES ("Bob", 319, 21);

# statement 3, issued by user Alice
GRANT SELECT ON Student TO Eve;

# statement 4, issued by user Bob
SELECT Name FROM Student;

# statement 5, issued by user Bob
GRANT SELECT ON Student TO Eve, Charlie WITH GRANT OPTION;

# statement 6, issued by user Eve
GRANT SELECT ON Student TO Charlie;

# statement 7, issued by user Alice
REVOKE SELECT ON Student FROM Charlie;

# statement 8, issued by user Charlie
SELECT PN FROM Student;
```

statement 9, issued by user Alice
REVOKE SELECT, INSERT, DELETE ON Student FROM Bob;

statement 10, issued by user Charlie
GRANT SELECT ON Student TO Dave;

statement 11, issued by user Eve
SELECT PN FROM Student;

statement 12, issued by user Charlie
SELECT PN FROM Student WHERE Name="Bob";

b) Consider the following table *T*. Assuming that the only quasi-identifier of this table is {*Weight*, *Postal Code*}, anonymize the table to make it 3-anonymous. To answer this question do not write any text but simply draw an anonymized version of the table. (1 point)

T

Age	**Weight**	**Postal Code**	**Disease**
19	70	311	Cold
19	71	291	Flu
18	72	483	Flu
18	72	291	Arthritis

c) Assume a privacy-preserving query mechanism M_Q for some database query Q. Specify the property that M_Q needs to have such that we can say M_Q provides ε-differential privacy. (2 points)

d) Assume a university database with exam grades of students, where the possible grades that can be achieved are 0 (for fail), 3, 4, or 5. What is the sensitivity Δq of the following query? (1 point)

What is the difference in the number of students who got the highest grade (5) compared to students who got the second-highest grade (4)?

(You only need to provide the sensitivity value; there is no need for providing an explanation/justification).