Information page for written examinations at Linköping University

Examination date	2018-06-04
Room (2)	U10(12) U11(9)
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	Ulf Kargén
Contact number during the exam time	013-285876
Visit to the examination room approximately	09:30, 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
2018-06-04
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) Explain in general terms what a DMA attack is. (1 point)

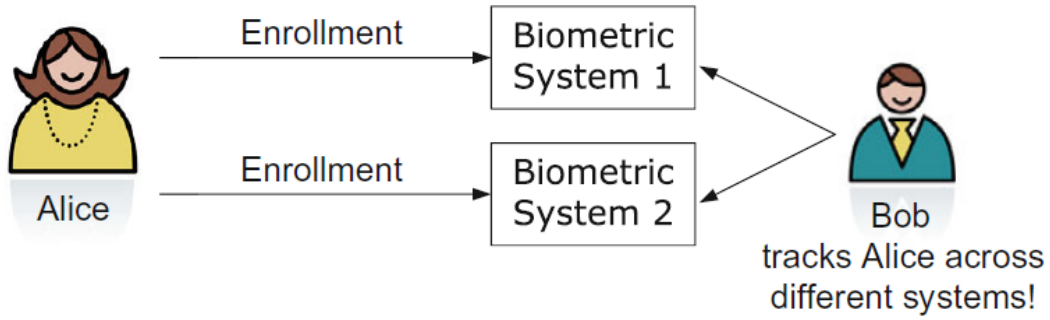
b) Provided that a DMA attack is possible on a given system, could *Intel SGX* be used to mitigate such an attack? Explain why or why not. (1 point)

c) For each of the two secure design principles *Fail-safe defaults* and *Separation of privilege*, state what the principle says, briefly summarize the motivation for the principle (as given by Saltzer and Schroeder), and give an example of an existing system/technology/situation where the principle is applied. (The example does not need to be computer-related.) (4 points)

d) Explain how a TPM can be used together with hard drive encryption, so that the hard drive can only be decrypted if the system software has not been tampered with. Your explanation should include all the important hardware and software components involved, and relevant technical features of the TPM. (4 points)

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

a) What type of security threat does the figure below describe? What are the effect for legitimate users of this security threat and what aspect of security is violated? (2 points)



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

c) When evaluating biometric systems, in which ways are error rates and return on investment of importance? (4 points)

3. Network security (10 points)

a) Suppose you are in charge of securing a new enterprise corporate network. List the main principles you will apply. (2 points)

b) Describe main principles used in cellular network security (2G/3G/4G). What has changed from generations to generation? What are common attacks attempted in cellular systems? (4 points)

c) Suppose you are running an Intrusion Detection System over IPv4 traffic. (4 points)

What kind of packet fields (e.g. destination IP address) you can use for traffic analysis (i.e., those are not encrypted) if the flow is using

i. TLS 1.2

ii. IPsec transport mode ESP

iii. IPsec tunnel mode AH

4. Database Security and Privacy (6 points)

a) Assume user Alice creates a table *Student(Name, PN, Age)* and, thereafter, the following 12 SQL commands are issued in the given order by the given users. Note that some of these commands will fail due to insufficient privileges. Identify all those commands that fail. (You only need to list the statement number of the statements that fail; there is no need for providing an explanation/justification).

```
# 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 Bob
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 of security classes:

TopSecrect > *Secret* > *Confidential* > *Unclassified*

Suppose we have two tables, *X* and *Y*, where *X* has security class *Confidential* and *Y* has security class *Unclassified*. If user Bob wants to copy data from table *Y* into table *X*, which security class would he need a clearance for to be allowed such a copying under the Bell-LaPadula model. If multiple security classes would be possible, list every one of them. If there is no solution (i.e., no clearance would make it possible to do the copy), then say so. (You only need to list the security class(es); there is no need for providing an explanation/justification).

c) Consider the following two tables, *E* and *T*. Suppose attribute *Disease* in table *T* is a sensitive attribute and *Age*, *Weight*, and *Postal Code* are not sensitive, and table *E* represents some external data about *all* persons in the postal code area 291. Given this external data, list *all* quasi-identifiers of table *T*. Notice that there might be multiple different quasi-identifiers; if this is the case, you have to list all of them.
(You only need to list the quasi-identifier(s); there is no need for providing an explanation/justification).

T

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

E

Name	**Age**	**Weight**
Sven	19	71
Gustav	19	71
Bob	18	70
Dave	18	72

d) In which case(s) can a table be 5-anonymous but not 4-anonymous?

e) Recall that the definition of differential privacy is based on a notion of neighboring databases. Consider a database D that consists only of the aforementioned table T (see question c above), and assume another database D' that contains a similar table T. What could this table T in D' look like if databases D and D' are neighbors? To answer this question do not write any text but simply draw the table.

f) Assume a table with data about members of an organization including their ages. Assume furthermore that persons can be a member of the organization only from the age of 30 until the age of 60. Then, for each of the following two statistical queries, what is the sensitivity Δq of the query?
(You only need to provide the two numbers: sensitivity of Q1 and sensitivity of Q2; there is no need for providing an explanation/justification).

Q1: How many members of age 30 does the organization have?

Q2: What is the age of the oldest member of the organization?