Information page for written examinations at Linköping University

Examination date	2018-08-24
Room (1)	TER2(10)
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	Ulf Kargén
Contact number during the exam time	013-285876
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
2018-08-24
14-18

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) Which of the information security attributes Confidentiality, Integrity, and Availability is the *Biba* model designed to uphold? Briefly motivate. (2 points)

b) Assume that an attacker has managed to install a bus snooping device in a computer system, which allows him/her to continuously read all data flowing on the memory buses. Explain why Intel SGX could be used to mitigate such an attack, while a software-only memory encryption scheme could not. Clearly motivate your answer based on the technical characteristics of Intel SGX. (2 points)

c) Explain the concept of *sealing* in the context of TCG and TPMs. (2 points)

d) For each of the two secure design principles *Economy of mechanism* and *Fail-safe defaults*, 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. (4 points)

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

a) One way of achieving authentication is via something that you know, such as passwords or PINs. Which are the two other primary ways of achieving authentication? State at least one example for each way! (2 points)

b) Insider attacks on biometric systems can be performed in different ways. Describe what constitutes collusion and coercion and how these differ from each other. (2 points)

c) Design cycle of biometric systems and the nature of the application in which the biometric system will be used (4 points): Describe what is meant by
   i. Cooperative versus non-cooperative users
   ii. Overt/covert deployment of the application.

3. Network security (10 points)

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

b) What are DDoS attacks, how those are implemented, using which mechanisms for TCP? Draw a picture to illustrate a typical scenario. (4 points)

c) IPSec (4 points)

   i. IPsec ESP 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. 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 ***none*** of these commands will fail due to insufficient privileges. List all the users who have the SELECT privilege after the execution of last of these commands. (1 point)
(you only need to list the users; 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 Alice
REVOKE SELECT, INSERT, DELETE ON Student FROM 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*. Moreover, assume two users, Alice and Bob, where Alice has the clearance for security class *Confidential* and Bob has the clearance for security class *Secret*. Under the Bell-LaPadula model, which security class may table *Y* have such that both Alice and Bob would be allowed to copy data from table *Y* into table *X*?
If multiple security classes are possible, list every one of them. On the other hand, if there is no solution (i.e., no security class makes it possible for both Alice and Bob to do the copy), then say so. (1 point)
(you only need to list the security class(es); there is no need for providing an explanation).

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. Notice that this external data is incomplete; that is, we do not have the weight of Dave (as indicated by the question marks in table *E*). What value (i.e., number) for the weight of Dave would have to be in table *E* instead of the question marks such that the attributes {*Weight*, *Postal Code*} are a quasi-identifier of table *T*? (1 point)
(you only need to write down the number; there is no need for providing an explanation).

T

Age	**Weight**	**Postal Code**	**Disease**
19	70	311	Cold
19	71	291	Flu
18	72	183	Flu
18	72	291	Arthritis

E

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

d) Assuming that the attributes {*Weight*, *Postal Code*} are the only quasi-identifier of the aforementioned table *T* (see question c above),
Assuming that the only quasi-identifier of the aforementioned table *T* (see question c above) is {*Weight*, *Postal Code*}, anonymize the table to make it 2-anonymous but not 3-anonymous. To answer this question do not write any text but simply draw an anonymized version of the table. (2 points)

e) Assume a table with data about employees of a company including their salaries. Assume furthermore that the company has only three levels of salary: 40.000 SEK, 45.000 SEK, and 50.000 SEK; i.e., the salary of every employee is one of these amounts. Note, however, that there may be times in which all employees are in the same of these salary levels (i.e., they may all earn either 40.000 SEK, 45.000 SEK, or 50.000 SEK).
For each of the following two statistical queries, what is the sensitivity Δq of the query? (1 point)
(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: What is the difference between the number of employees who have the highest salary level and the number of employees who have the lowest salary level?

Q2: What is the minimum salary among the salaries that employees have at the moment?