Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2019-03-21
Sal (1)	U1(31)
Tid	14-18
Utb. kod	TDDD17
Modul	TEN2
Utb. kodnamn/benämning **Modulnamn/benämning**	Informationssäkerhet, fk En skriftlig tentamen
Institution	IDA
Antal uppgifter som ingår i tentamen	4
Jour/Kursansvarig Ange vem som besöker salen	Ulf Kargén
Telefon under skrivtiden	013-285876
Besöker salen ca klockan	15:00, 17:00
Kursadministratör/kontaktperson (namn + tfnr + mailaddress)	Madeleine Häger-Dahlqvist, 013-282360, madeleine.hager.dahlqvist@liu.se
Tillåtna hjälpmedel	Dictionary (printed, not electronic)
Övrigt	Preliminary grading: C(3): 20 points, B(4): 26 points, A(5): 30 points
Antal exemplar i påsen	

LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2019-03-21
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) With the traditional access control mechanism used in Unix/Linux, one can assign read/write/execute permissions to owner/group/others. What access control scheme is this an example of? What characterizes this method for access control? (1 points)

b) SELinux and Apparmor are both examples of another type of access control scheme. What is the name of this scheme, and what characterizes it? Give one pro and one con of this type of access control, compared to the traditional one in question a). (2 points)

c) Explain in a sentence or two what sets *rootkits* apart from "regular" malware. (1 point)

d) A common rootkit technique is to load a malicious device driver. Explain the purpose of this and how it helps the rootkit achieve its goals. (1 point)

e) Consider the case where an attacker is able to compromise the BIOS/firmware, boot loader, or OS kernel. Compare how this would impact the security provided by respectively Intel SGX and ARM TrustZone. Briefly motivate your answer based on technical characteristics of the two systems. (2 points)

f) Pick **three** of Saltzer and Schroeder's secure design principles. For *each* of the three principles, name the principle and describe it in a sentence or two. (3 points)

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

a) There are three basic methods of person recognition. Something the user knows, such as passwords, are the first basic method. What are the two other basic methods of person recognition? Give an example for each basic method (in the same way as passwords are an example of something the user knows)! (2 points)

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

c) State at least two ways of providing multibiometrics. State at least two qualities multibiometrics is expected to provide. Make a short discussion regarding how the stated ways may achieve the stated qualities. (4 points)

3. Network security (10 points)

a) What are Advanced Persistent Threats (APT) and how those are different from Hacktivism? (2 points)

b) What are common issues with DNS from security viewpoint? What is the role of DNSSEC? Draw a picture to show a DNSSEC recursive query. (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. (4 points)

4. Database Security and Privacy (6 points)

a) Assume user Bob 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 the last of these commands. (You only need to list the users; there is no need for providing an explanation/justification). (1 point)

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

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

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

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

# statement 5, issued by user Alice
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 Bob
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 Alice;
```

b) Consider the following security classes and the following multilevel relation:

TopSecrect (*T*) > *Secret* (*S*) > *Confidential* (*C*) > *Unclassified* (*U*)

Employee

Name		**Salary**		**JobPerformance**	
Eva	S	70.000	T	Fair	T
Gustav	U	45.000	S	Fair	C
Dave	U	55.000	S	Fair	U
Alicia	U	71.000	C	Good	C

For this relation, the following SQL query returns the number of tuples (rows) in which the value of the JobPerformance attribute is the string "Fair".

SELECT COUNT(*) FROM Employee WHERE JobPerformance="Fair";

Remember that in a multilevel relation not every value is visible to every user. Instead, which values a user can see depends on the security clearance of the user. Now, under the Bell-LaPadula model, for which security class would user Alice need to have clearance such that for her the given query returns the number 2 ?
If multiple security classes are possible as an answer, list every one of them. On the other hand, if there is no solution (i.e., no matter which clearance Alice has, for her the query would always return a number different from 2), then say so. (You only need to list the security class(es); there is no need for providing an explanation). (1 point)

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*? (You only need to write down the number; there is no need for providing an explanation). (1 point)

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) Remember that the simplest form of statistical queries are queries that return just a single number. Hence, an example would be a query such as the following: "What is the average salary of all the employees in the database?" Now, 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. Give an example of a simple statistical query over this university database such that the sensitivity Δq of that query is 1. (It is sufficient to write down this query simply as a question in plain English; i.e., there is no need to write an SQL statement here.) (1 point)