LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2019-06-10
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) In a sentence or two, explain the concept *Root of Trust*. (1 point)

b) In a system using Intel SGX, what is the Root of Trust? Explain why. How does this differ from a system using ARM TrustZone? (3 points)

c) 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? Name and explain the principle in a sentence or two. (1 point)

d) 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. Name and explain also that principle in a sentence or two. (1 point)

e) 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)

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

a) What makes permanence an important quality when choosing a biometric trait? (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) Attacks at the user interface: Discuss how impersonation and spoofing may be exploited to breach the security of a biometric system. (4 points)

3. Network security (10 points)

a) What is IP multihoming and how can it affect the security? (2 points)

b) Describe main principles used in cellular network security (2G/3G/4G). What has changed from generation 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) can you 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). (1 point)

```
# 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 security classes and the following multilevel relation:

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

Employee

Name		**Salary**		**JobPerformance**	
Eva	S	70.000	S	Fair	T
Gustav	U	45.000	S	Fair	C
Dave	U	55.000	C	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" and the value of the Salary attribute is greater than 40,000.

SELECT COUNT(*) FROM Employee WHERE JobPerformance="Fair" AND Salary > 40000;

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 Bob need to have clearance such that for him the given query returns the number 1 ?
You only need to list the security class(es); there is no need for providing an explanation. 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 Bob has, for him the query would always return a number different from 1), then say so. (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. 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). (1 point)

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) Assume a table with the four columns *DateOfBirth*, *ZIP*, *Gender*, and *Salary*. Suppose that this table is 5-anonymous. In which case(s) can this table be 4-anonymous? (1 point)

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. (1 point)

f) 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?

What is the average grade of all students with student ID = 1?

(You only need to provide the sensitivity value; there is no need for providing an explanation/justification). (1 point)