LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Home exam
TDDD17 Information Security
2020-08-21

Teacher on duty
Ulf Kargén, ulf.kargen@liu.se, 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 32.

Since the number of credits for the exam have changed from 3 to 2 hp (or ECTS) in 2020, we use two different grading scales depending on which year you were admitted to the course, as shown in the table below. The grading scales are preliminary and might be adjusted during grading.

Grade	C (3)	B (4)	A (5)
Points required **TEN2 (3 hp)** Students admitted **2019 or earlier**	20	25	28
Points required **TEN3 (2 hp)** Students admitted **2020**	16[1]	23	26

Answers should be submitted through Lisam as a single PDF or ASCII text (.txt) document before the end of the exam time. Figures should be integrated into the document and *not* submitted as separate files. If you use PDF format, figures could be drawn either electronically, or by hand and scanned/photographed. If you use plain text format, you can draw ASCII art. To facilitate easier grading, it is preferred that you express formulas, pseudo-code, etc., as electronic text, and not as handwritten figures.

You are allowed to use any aid, but **all kinds of collaboration with others is strictly forbidden**. Also, **copying any part of an answer from another source will be considered plagiarism**. The questions will be checked for plagiarism and sharing of answers between students using Urkund, and any suspected cheating will be reported to the university disciplinary board. **By taking the exam, you solemnly promise to abide by the above rules.**

In the event that you experience technical difficulties with Lisam that prevent you from submitting, it is allowable to submit answers via email. However, this should only be used as a last resort if Lisam for whatever reason would stop functioning.

The home exam will not be anonymous due to the exceptional COVID-19 situation.

Ulf Kargén will be available to answer questions during the exam via email and phone.

[1] And to those of you who would like to point out that 16/20 > 2/3, I say that the number of points you score on the exam is not a linear function of how many hours you studied.

1. System Security (8 points)

a) Consider Saltzer and Schroeder's principle of *Complete mediation*. Name one attack discussed in the course that is possible due to lacking adherence to this principle. Explain how the attack relates to the principle of complete mediation. (2 points)

b) Consider a computer system that must be shared between users that may not entirely trust each other. It can be argued, based on another of Saltzer and Schroeder's design principles, that it is better to give each user a separate virtual machine running on the system, rather than simply creating a regular user account for each user. Which principle, and why? (2 points)

c) For each of the two hardware security extensions below, explain whether it would still be possible to trust a security mechanism based on that extension *if an attacker has managed to compromise the BIOS/Boot ROM of the computer*. (4 points)

   i. ARM TrustZone
   ii. Intel SGX

2. Defense against Malware (8 points)

a) Malware have traditionally been divided into viruses, worms, and trojans. Today, almost all malware are trojans. Explain why. (3 points)

b) Imagine that we are training a machine learning model to detect mobile malware based on the set of Unicode strings extracted from an app. That is, apps are classified as malicious or benign based on the presence or absence of one or several strings. (We here assume that apps are not obfuscated to prevent extraction of strings.) (5 points)

   Explain using a small example:

   i. How overfitting can here lead to false negatives.
   ii. How overfitting can here lead to false positives.

3. Network Security (10 points)

a) There are several different kinds of firewalls. Explain what characterizes the following kinds of firewalls, and briefly discuss the pros and cons of each type. (2 points)
   i. Packet filter
   ii. Stateful firewall
   iii. Application layer firewall

b) Which steps are typically involved on an attack on a system that is not directly accessible to an attacker? For each step, name and briefly explain one security mechanism that could be used to prevent, detect or mitigate that step of the attack. If no mechanism is applicable at one or more of the steps, explain why. (4 points)

c) DNS cache poisoning is a potentially very serious attack. Explain what the consequences of a successful DNS cache poisoning attack could be. Cache poisoning is possible due to a flaw in the DNS protocol. Explain what this flaw is, and propose a way to prevent DNS cache poisoning (at least in practice, in situations where the attacker is unable to examine the DNS query). State what would be required for your solution to be deployed in practice. (4 points)

4. Database Security and Privacy (6 points)

a) Assume that user Alice creates a table *Student(Name, PN, Age)* and, thereafter, the following 9 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 and give a detailed justification of your answer. (1.5 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;

b) Consider the following order 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.

In addition to providing the answer to the question, explain the reasoning based on which you arrived at this answer. (1.5 points)

c) 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

d) Explain the privacy-utility trade off in the context of using the Laplace-based approach to achieve differential privacy. (1 point)

e) 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. Consider the following *histogram query*.

Return a histogram that represents the grade distribution across all TDDD17 exams (i.e., the distribution of the number of students per grade) such that every histogram bucket corresponds to one of the possible grades.

The sensitivity Δq of this query is 1. Explain in about five to ten sentences why that is the case. Make sure that your explanation uses the related terminology correctly. (1 point)