LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

# Home exam
# TDDD17 Information Security
# 2020-10-29

**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)**<br>Students admitted **2019 or earlier** | 20 | 25 | 28 |
| Points required **TEN3 (2 hp)**<br>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) Many modern programs, such as PDF readers and web browsers, utilize sandboxing to reduce the attack surface of software exploits. The complex rendering logic executes with minimum privileges, while privileged operations are mediated and carried out by a much smaller software component. This design embodies two of Saltzer and Schroeder' secure design principles. Name these two principles, and explain how they are applied in the above context of software sandboxing. (3 points)

b) An *arbitrary code execution vulnerability* is a flaw in a piece of software that allows an attacker to "trick" a running program into executing (arbitrary) code supplied by the attacker. Consider an arbitrary code execution vulnerability in the following two kinds of software:

   i. A system service running with superuser privileges
   ii. A device driver

   Which of the two cases has the biggest potential impact on security? Clearly motivate your answer. (2 points)

c) Contrast the traditional security ring architecture with that of ARM TrustZone. Give an example scenario where TrustZone would provide a security benefit over the security ring architecture. (3 points)

## 2. Defense against Malware (8 points)

a) Explain the difference between *signatures* and *heuristics* in antivirus products. (2 points)

b) Generally, neither signatures or heuristics in antivirus products are effective for detecting *advanced persistent threats*. Explain why. (2 points)

c) Consider the problem of classifying binaries as either benign or (potentially) malicious. In the course, we discussed two types of *supervised* machine learning for this task. What are those called, and which of them would be most suited for detecting advanced persistent threats? Motivate your answer. (2 points)

d) In contrast to PC malware defense, mobile malware defense is typically more focused on detecting malicious apps when they are uploaded to an app store, rather than detecting malware directly on the client. Explain why. (2 points)

## 3. Network Security (10 points)

a) Describe what “air-gaps” are and how those are useful for network security. Are those good/practical to have and what can breach those? (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 and justify your answer. (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 ?
Provide a brief explanation for your answer. Moreover, 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 377. 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. Provide a brief explanation/justification of your answer. (1 point)

T

| **Age** | **Weight** | **Postal Code** | **Disease** |
|---|---|---|---|
| 21 | 70 | 311 | Arthritis |
| 21 | 71 | 377 | Cold |
| 20 | 72 | 483 | Flu |
| 20 | 72 | 377 | Arthritis |

E

| **Name** | **Age** | **Weight** |
|---|---|---|
| Dave | 21 | 71 |
| Gustav | 21 | 71 |
| Sven | 20 | 70 |
| Bob | 20 | 72 |

d) In which case(s) can a table be 5-anonymous but not 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 draw the table and describe why it is a neighbor. (1 point)

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 20 until the age of 30. Then, for each of the following two statistical queries, what is the sensitivity $\Delta q$ of the query?

In addition to providing the two numbers (sensitivity of Q1 and sensitivity of Q2), provide a brief justification for these numbers. (1 point)

Q1: How many members of age 25 does the organization have?

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