LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

# Home exam
# TDDD17 Information Security
# 2020-06-08

**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)

Imagine that you are tasked with creating a software version of an e-banking token. The security of such token schemes rests on a challenge-response technique, where a shared secret *S* is stored in the token (a standalone physical device) in such a way that *S* can never be retrieved directly. The banking provider is also aware of which *S* is associated with which customer. When logging in to your internet bank, a challenge nonce *C* (i.e., a random number) is displayed at the login site. When inputting *C* in the token, a response *R* is derived from *S* and *C* (e.g., using a cryptographic hash). When submitting *R* at the login site, the banking provider can check if *R* is correct, given the known *S* and provided *C*.

A software-only scheme, where *S* is simply stored in your computer's file system and used by some software, is inherently less secure, since an attacker that manages to install malware on the computer can simply exfiltrate and copy *S* to his or her own computer. A somewhat more secure scheme is to encrypt S with a password that needs to be typed in by the user before computing a response *R*. However, an attacker that manages to install, e.g., a rootkit on the computer can still break this scheme. For example, the password can be captured using a keylogger, or the decrypted *S* can be captured directly by dumping RAM contents.

In this course, we have discussed various hardware extensions to enhance system security. Pick one of the technologies presented in this course, and outline a design for a secure software e-banking token based on this technology. (Of course, the design can also make use of any pre-existing software-based security measure, such as protocols for secure communication.) Your design should describe how *S* can initially be retrieved securely from the provider during setup, and stored in such a way that it cannot be retrieved even if an attacker manages to compromise the OS. (You can assume that the OS is not compromised during initial setup of *S*.) Likewise, you should describe how *R* can be computed in a secure way even if the OS is compromised. You don't need to go into technical details (like exact technical terms), but you should clearly describe which features of the chosen technology that the security of various parts of your design rests upon. Finally, you should also state what the *root of trust* is in your scheme, based on the chosen technology and design.

## 2. Defense against Malware (8 points)

a) Clearly explain why most antivirus engines today employ *emulation*. Your answer should explain which evasion technique emulation mitigates, how this evasion technique works, why it is used by malware authors, and how emulation helps to defeat such evasion attempts. (4 points)

b) It is known that mobile malware is significantly more common for the Android platform than for the iOS platform. Explain why. (1 point)

c) The emergence of *malware creation kits* is one of the reasons why antivirus companies are increasingly using machine learning for malware detection. Explain why. (3 points)

## 3. Network Security (10 points)

The page count stated together with the points for each question is to give you a better idea of the expected scope of the answer. Page counts assume 12pt single-spaced text. For reference, a typical A4 page contains about 500 words when using this text size.

a) Describe what is a DarkNet and which technologies it is using. (2 points, 0.3 pages)

b) What are tradeoffs of using IPSec versus TLS for VPN? (4 points, 0.7 pages)

c) Describe the main principles of designing a secure corporate network. Where in the network and why would you place SCADA devices, DMZ, web and mail servers, wireless APs, remote access, office PCs, printers, file servers, remote clouds? (4 points, 1 page)

## 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 statement 5 will fail due to insufficient privileges.
Describe the strategy/algorithm that you would apply to check for *every* command in such a sequence whether the corresponding user has sufficient privileges to execute the command or not. For simplicity, assume a system in which granting privileges with grant option is not possible. (2 points)

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

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

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

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

# statement 5, issued by user Eve
DELETE FROM Student WHERE Name = "Bob";

# statement 6, issued by user Alice
REVOKE SELECT ON Student FROM Eve;

# statement 7, issued by user Eve
INSERT INTO Student VALUES ("Sven", 481, 23);
```

b) Explain in about two to four sentences why identity disclosure leads to attribute disclosure. (1 point)

c) 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 $\Delta q$ of the following query, and why?

*What is the difference in the number of students who got the highest grade (5) compared to students who got the lowest grade (0)?*

Explain/justify your answer in about five to ten sentences and make sure that your explanation uses the related terminology correctly. (1.5 points)

d) Recall that we talked about three main layers where database encryption may be performed (storage-level encryption, database-level encryption, application-level encryption). Describe how the CryptDB approach fits into this picture (i.e., in which of these layers is it placed?). Justify your answer. (1.5 points)