+1/1/60+

Ens: Prof. Edouard Bugnion
COM-301 - Midterm Exam - [redacted]
07.11.2024
2 hours
Room : [redacted]

1

[redacted]

SCIPER : [redacted]

Do not turn the page before the start of the exam. This document is double-sided, has 7 pages, the last ones possibly blank. Do not unstaple.

- Place your student card on your table.
- **No other paper materials** are allowed to be used during the exam.
- Using a **calculator** or any electronic device is not permitted during the exam.
- For the **open text** questions:
  - Only write on the lines in the box. **Text outside the boxes or the lines will be ignored**.
  - Do not tick the grading boxes on top of the text boxes.
  - Please mind your calligraphy; undecipherable responses will not be graded.
- Use a **black or dark blue ballpen** and clearly. Pencil will be ignored. Clearly erase with **correction fluid** if necessary
- The supervisors will not answer any questions regarding the content of the exam questions.

Reserved for grading, please leave blank!

Questions	**Parts**	**Total**
Access Control & Security Principles		**/ 2 pts**
Mandatory Access Control		**/ 2 pts**
Authentication		**/ 3 pts**
Cryptography		**/ 4 pts**
Hash functions		**/ 2 pts**
Total		**/ 13 pts**

Answer inside the box. Your answer must be carefully justified. Leave the grading boxes free : they are reserved for the corrector.

Access Control & Security Principles *[2 points]*

Tropyota is preparing the launch of its new hybrid motor: the Hybris. Before the launch, the plans for the Hybris must only be available to and modifiable by the Design team. Tropyota wants to make sure no competitor can see their new technology and asks for an emergency program to delete the plans from the server if they detect a spy is in the building. This program should be launched by Carla the CEO, who is in the Management team. Assuming that every team has an associated permission group, Dave the designer writes the program and assigns the following permissions:

```
-rwxr-xr-- dave managers program_to_delete_plans
-rw-rw---- dave designers hybris_plans.dwg
```

Question 1

Does this configuration achieve the purpose that Carla can delete the data if she suspects the presence of a spy? Justify. Otherwise, fix it. *[0.5 point]*

☐0 ☐0.25 ☐0.5 *Do not write here.*

.....

.....

_ _ _ _ _ _ _ _ _ dave managers program_to_delete_plans

_ _ _ _ _ _ _ _ _ dave designers hybris_plans.dwg

Question 2

Given the configuration that allows Carla to delete the data if she suspects the presence of a spy, does it fulfill the least privilege principle? Justify. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

.....

.....

Question 3

From this list of principles: fail-safe defaults, complete mediation, separation of privilege, and least common mechanism, name a security principle not followed by Tropyota in their emergency deletion procedure. Justify. *[0.5 points]*

☐0 ☐0.25 ☐0.5 *Do not write here.*

.....

.....

Mandatory Access Control *[2 points]*

The SuperChef studio designed a new season of their cooking competition TV show and is about to start filming. The producers have already finalized the list of weekly challenges, the casting directors have chosen the cast of the season, and the cast members have been given a list of cooking equipment they have to bring to the set.
The studio implements mandatory access control with **Bell-LaPadula (BLP)** with three security levels: `Top Secret > Confidential > Unclassified`. They give the following classifications to objects and principals:

- The Producers have clearance Top Secret. The List Of Challenges of the season are Top Secret.
- The Casting Directors have clearance Confidential. The Cast List is Confidential.
- The Cast Members have clearance Unclassified. The List Of Cooking Equipment is Unclassified.

Question 4

Can a malicious cast member read the list of challenges ahead of the season? Justify. *[1 points]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

.....

.....

.....

Question 5

Assume that a casting director is friends with one cast member. Describe a covert channel that would allow them to send the rest of the cast to their friend before the filming starts. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

.....

.....

.....

Authentication *[3 points]*

At the University of LFPE, the passwords of *gaspar* accounts are stored in a database with the following format:

`gaspar_username, salt || Hash(Hash(gaspar_password), gaspar_password), salt`

Where:

- Hash is a secure hash function.
- salt is a 128-bit random number freshly generated for each line
- `m1 || m2` is the concatenation of `m1` and `m2`.

Question 6

Assume that a student got access to the database. Explain how they can perform a dictionary attack and recover the plain passwords and why such an attack is feasible. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

.....

.....

.....

Question 7

Propose an alternative format to store the passwords of *gaspar* accounts in the database so that if the database leaks, a dictionary attack is not feasible anymore. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

`gaspar_username`, ...

Question 8

Assuming the passwords are stored following your answer in Q3.2 but the size of the salt is now reduced to **2-bits**. Describe the process to recover the plaintext passwords. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

.....

.....

.....

Cryptography *[4 points]*

A research lab wants to conduct a study in which they give sensors to participants to measure their heart rate. The sensor captures this rate every minute. Every hour, the sensor sends the average heart rate over the last 60 minutes to the researchers' server. The sensor's message has the following format:

`Enc(PK_server, (avg_rate, time)), MAC(k, (avg_rate, time)), Hash((avg_rate, time))`

Where:

- `k` is a key shared by all sensors and the server
- `PK_server` is the public key of the server, which is the only one with access to the corresponding secret key
- `Enc(PK,m)` is the encryption of `m` under the public key `PK`
- `MAC(k,m)` is the message authentication code of `m` under the key `k`
- Hash is a secure hash function (fulfills the three security properties seen in the lectures)
- Time is the hour at which the sensor sends the statistic (e.g. 6 pm)

Note: Assume that: (1) the sensors' heart rate measurements are accurate, (2) participants cannot remove the sensor without help from the researchers, (3) it is not possible to extract any key from the sensor or change the software inside, and (4) sensors have perfect connectivity.

Question 9

Can the researchers be sure that no adversary is able to send an arbitrary heartbeat measurement to the server (i.e., any value chosen by an adversary and not already measured by a sensor)? Justify. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

.....

.....

.....

Question 10

Does this scheme provide confidentiality of the average heartbeats measured by the sensors against an adversary who eavesdrops sensors' messages? Justify. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

. . . . . .

. . . . . .

. . . . . .

Question 11

Explain why the researchers cannot be sure that each measurement has been received at most once by the server. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

. . . . . .

. . . . . .

. . . . . .

Question 12

Provide an alternative message format that would allow the researchers to be sure that they receive each message from a sensor at most once. *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

. . . . . .

. . . . . .

Hash functions *[2 points]*

To get around the new privacy protections by browsers that eliminate third-party cookies, *AggreggCo.* is searching for new identifiers that allow them to track users across websites. One approach is to take advantage of the fact that users must provide their email on many occasions (e.g., to log in or to subscribe to a newsletter). To this end, *AggreggCo.* asks websites to add a script that takes users' emails and sends its hash, i.e., `Hash(user_email)`, to *AggreggCo.* Then, *AggreggCo.* can use this hash to construct a profile of each user composed of all the websites the user visits. *AggreggCo* claims that spammers cannot use the hashes to send spam to the users.
For each of the following properties, explain whether the property is necessary or not. Justify.

Question 13

Pre-image resistance: *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

. . . . . .

. . . . . .

Question 14

Second pre-image resistance: *[1 point]*

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1 *Do not write here.*

. . . . . .

. . . . . .