+1/1/60+

EPFL

Ens: Prof. Thomas Bourgeat, Dr. Theresa Stadler
COM-301 - Midterm Exam - XX
06.11.2025
45 minutes
Room : INF 1

1

Extra 1

SCIPER : **999981**

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.
- Students can only have **one A4 cheatsheet recto-verso**.
- **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.
- Only write on the lines in the box.
  - **Text outside the boxes will be ignored**.
  - **You are not allowed to add lines or write between the lines.**
  - All answer lines **EXCEEDING the allowed number of lines** will **NOT be graded**.
- 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 write 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!

Parts	**Questions**		**Total**
Security principles: SecretCakes			/ **4 pts**
Mandatory Access Control: VUCH			/ **4 pts**
Cryptography: PinkBike			/ **4 pts**
Total			/ **12 pts**

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

Security principles: SecretCakes *[4 points]*

The cake company *SecretCakes* has gained a lot of popularity recently because of their new cake recipe. Alice, the CEO of *SecretCakes*, wants to make sure that this recipe remains secret. Only Alice and her daughter, who helped her develop the recipe, should have full access to the recipe. Alice thus decides to store the recipe document on the last floor of *SecretCakes*'s headquarters and puts in place the following system:

- There is one single staircase in the headquarters building that connects the ground floor to all other floors. At every floor, there is a locked door between the staircase and that floor.
- Each *SecretCakes* employee, Alice and her daughter included, has a company card. To access a floor, employees present their personal card to a card reader installed at the door going from the staircase to that floor.
- There is a list of employees that are not allowed access associated with each floor. When an employee presents their card to a card reader, the card reader checks if the employee is on this list, and if not, unlocks the door.
- Every time a new employee is hired, the list of unauthorized employees for each floor is updated.

Questions continue on the next page.

Question 1

Describe a security property that Alice wishes to maintain in relation to the system. Identify the assets and principals included in the security property that you described. *[2 points]*

☐0 ☐0.5 ☐1 ☐1.5 ☐2 *Do not write here.*

.....

.....

.....

.....

Question 2

From the following list of security principles, **choose two** principles that Alice's system **does not follow**. Justify your answer. *[2 points]*

Least common mechanism | Fail-safe default | Economy of mechanism | Complete mediation

☐0 ☐0.5 ☐1 ☐1.5 ☐2 *Do not write here.*

.....

.....

.....

.....

.....

.....

Mandatory Access Control: VUCH *[4 points]*

You have been hired as a security engineer to audit the digital transformation of the *VUCH* hospital. The *VUCH* management wants to deploy state-of-the-art Large Language Models (LLMs) to improve the hospital's operations. The hospital has two departments with different activities: **Medical (M)** and **Patient Management (P)**. Each department has separate directories in the VUCH server. `/data/medical` for files by the Medical department and `/data/patients` for the Patient Management department. Doctors must be able to read both medical and patient data files. Secretaries can read and write patient data files.
VUCH's IT team has installed two LLMs each with a specific task to perform:

- ***pGPT***: An LLM to match doctors to patients and schedule visits. *pGPT* takes patient data files as input and writes its output to a file called `schedule.txt` stored in `/data/patients`. Secretaries access the scheduled visits and notify patients and doctors.
- ***mGPT***: An LLM to predict a medical diagnosis. *mGPT* takes as input a patient's medical data files and the matching of doctors to patients from `schedule.txt` and writes its output to a file called `diagnosis.txt` stored in `/data/medical`. Doctors can edit the diagnosis later on.

Questions continue on the next page.

Question 3

Your task is to create a Mandatory Access Control policy to ensure the confidentiality of all data stored on *VUCH*'s servers.

What is the Mandatory Access Control model most suited for your task: **BLP** or **BIBA**? Justify your choice with respect to the security properties requested by *VUCH*. In your model, list the minimal set of access levels and categories required. *[2 points]*

☐0 ☐0.5 ☐1 ☐1.5 ☐2 *Do not write here.*

.....

.....

List of access levels: .....

List of categories: .....

Question 4

List principals and objects in this system. For each principal and object, set the access level and categories. Your choices must respect the least privilege principle. *[2 points]*

☐0 ☐0.5 ☐1 ☐1.5 ☐2 *Do not write here.*

Principals	**Objects**
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....

Cryptography: PinkBike *[4 points]*

The bike rental company PinkBike has a fleet of bikes stationed in the city. People with a valid PinkBike subscription can unlock a bike at a station, ride the bike around town, and drop it off and lock it again at the same PinkBike station. When a user wants to unlock a bike, they tap their PinkBike card on the bike. The bike reads the subscription number from the card and sends the following message to the PinkBike server:

$$\texttt{PKE.Enc}_{\texttt{pk\_PinkBike}}\texttt{(id\_bike || sub\_num)}, \texttt{MAC}_{\texttt{k\_MAC}}\texttt{(id\_bike)}, \texttt{Hash(sub\_num)}$$

Where:

- `PKE.Enc` is a public-key encryption function secure against chosen-plaintext attacks (CPA).
- `MAC` is a deterministic message authentication scheme.
- `Hash` is a pre-image resistant hash function.
- `||` denotes concatenation.
- `pk_PinkBike` is PinkBike's public key for `PKE.Enc`, which is hard-coded into bikes and known publicly.
- `k_MAC` is a symmetric key pre-shared between the PinkBike server and all bikes, known to no one else.
- `sub_num` is a user's subscription number, which is a random 32-bit number. A user's subscription number should remain private to the user and the PinkBike server.
- `id_bike` is the id of a bike which is printed on the frame of each bike.

Eve is an adversary who does not have a valid PinkBike subscription. Eve is eavesdropping near a bike station and can intercept any network traffic between bikes and the PinkBike server. Eve can drop any message between the bike and the PinkBike server and send arbitrary messages to any bike and the PinkBike server. Eve is physically at the bike station and can thus observe who unlocks which bikes. PinkBike's code is open-source and Eve knows the format of the message and the algorithms used.

Questions continue on the next page.

Question 5

Alice taps her PinkBike card to unlock a bike at the station that Eve is monitoring. This triggers a message from the bike to the PinkBike servers. Can Eve learn Alice's subscription number?

If yes, describe an attack that enables Eve to learn Alice's subscription number and explain why it is successful.
If not, specify which properties of `PKE`, `MAC`, and `Hash` prevent Eve from learning Alice's subscription number. *[2 points]*

☐0 ☐0.5 ☐1 ☐1.5 ☐2 *Do not write here.*

.....

.....

.....

.....

Question 6

Eve has been eavesdropping at the station for a while and has seen every bike getting rented at least once. Later, Alice taps her PinkBike card to unlock a bike at the station. Alice successfully unlocks the bike and drives away. Eve wants to rent another bike than the one Alice just rented, but without paying herself.

Suppose Eve has learned Alice's subscription number. Is Eve able to rent any bike at the station (other than the one that Alice just rented) such that the ride is billed to Alice's subscription?

If yes, describe an attack. If not, explain why such an attack is not possible. *[2 points]*

☐0 ☐0.5 ☐1 ☐1.5 ☐2 *Do not write here.*

.....

.....

.....

.....