COM 301 Midterm Exam, 08.11.2023

Name: .....

Sciper: .....

Please wait for instructions before opening this document

- This is a **closed book** exam. Books, notes, and electronic devices are not allowed. Students can only have one A4 handwritten cheatsheet recto-verso.

Multiple choice questions:

- Multiple-choice questions have *one* correct answer. If you mark the correct answer, you get one point. If you mark an incorrect answer, 0.25 points will be subtracted. If you mark no answer, you will get zero points.
- To mark your answer, make a mark *inside* the corresponding box. Marks outside a box will be ignored.
- Use a black or blue pen to mark your answers. Pencils are not allowed.

Open text questions:

- Write your answers in black or blue pen in the corresponding text boxes. Pencil will be ignored.
- 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.

Questions

- The supervisors will not answer any questions regarding the content of the exam questions

Reserved for grading, please leave blank!

Multiple choice questions						**Total**
						/ **7 pts**

Open text questions	**Parts**			**Total**
Fast Thesis Pitch				/ **2 pts**
Interviewing Journalists				/ **2 pts**
Fred Discussion				/ **2 pts**
Secure Accounting				/ **3 pts**
FELP authentication				/ **2 pts**
Total				/ **18 pts**

Question 1 **[Access Control]** You want to book a room in the BC building but find that it is already booked. You contact EPFL maintenance from a corridor phone to report a water leak in the room. To be on the safe side, the maintenance team cancels all bookings in the room and puts it in maintenance status. After discovering that there was actually no leak, the maintenance team reopens the room for bookings. Quickly, you manage to book the room before anyone else.
Which of the following is true?

- ☐ There is no confused deputy because everyone has an equal opportunity to book the room once the booking reopens.
- ☐ There is a confused deputy problem because the maintenance team wrongly believes there is a leak.
- ☐ There is no confused deputy problem because the maintenance team has the right to cancel all bookings.
- ☐ There is a confused deputy problem because the maintenance team cancels all bookings.

Question 2 **[Applied Cryptography]** You download a sketchy version of Microsoft Office from an untrusted website. To check that the download corresponds to the true software, you look at the checksum (hash) of the Microsoft Office program from the official Microsoft website. Then you compute the hash of the software you downloaded and compare it to the official checksum.
What property must the hash function have for you to be sure that you just downloaded the correct version of Office and not a modified version that could contain malware?

- ☐ The hash function used to compute the checksum of the Office program must be preimage resistant.
- ☐ The hash function used to compute the checksum of the Office program must be slow to compute.
- ☐ The hash function used to compute the checksum of the Office program must be collision resistant.
- ☐ The hash function used to compute the checksum of the Office program must have second preimage resistance.

Question 3 **[Authentication]** Which of the following statements is correct?

- ☐ In password-based authentication, storing salts in the clear leads to offline brute-force attacks.
- ☐ For password storage, a fast hash function is more secure against offline brute-force attacks than a slow hash function.
- ☐ For a 6-digit password that only contains numbers (1 000 000 eligible passwords), the probability of a user manually choosing "000000" as their password is $p = \frac{1}{1\,000\,000}$.
- ☐ Having the server sign the challenge used to prevent replay attacks in password-based authentication would not increase security against these attacks.

Question 4 **[Security Principles]** After listening to the COM-301 lecture on Security Principles, you are enthusiastic about analysing the security of systems you use every day and to what extent they fulfil the eight main principles. You start by analysing the PubliBike system in which a registered user can rent a bike at a fixed hourly rate through a mobile application.
Which of the following statements is correct?

- ☐ The fact that I have to pay for every bike rental after I have returned it to a docking station satisfies the complete mediation principle.
- ☐ The fact that bikes are locked unless a user enters a valid code to unlock a bike satisfies the fail-safe defaults principle.
- ☐ The fact that anyone can download the mobile application from the app store satisfies the open design principle.
- ☐ The fact that payment occurs after a bike rental satisfies the economy of mechanism principle.

Question 5 **[Access Control]** A group of psychology `researchers` plan to study group dynamics. They set up an experiment where `volunteers` need to solve a puzzle together and write their progress in a file `puzzle/updates.log`. `Researchers` hire "`spies`" to hide among the `volunteers` to cause tension in the group and disrupt their progress. To avoid being discovered, `spies` do the same activities as the `volunteers`. To keep the experiment unbiased, `researchers` should not communicate with `volunteers` nor `spies`.
At the end of the experiment, the `spies` write their observations regarding group dynamics to a separate file `dynamics/observations.log`. These observations must be kept secret from `volunteers`. In the end, `researchers` analyse `puzzle/updates.log` and `dynamics/observations.log` to generate their `report.txt` that must not be shared with `spies` nor `volunteers`.

Assuming that
(1) for Bell-LaPadula model the ordering of classes is (TOP SECRET > SECRET > CONFIDENTIAL > UNCLASSIFIED),
(2) for BIBA, the ordering is (HIGH INTEGRITY > LOW INTEGRITY),
(3) "Puzzle" and "Dynamics" are categories;
which of the following options is a good choice to ensure that all accesses happen according to the rules?

- ☐ **BIBA**
  Subjects: `researchers`: HIGH INTEGRITY, `spies`: HIGH INTEGRITY, `volunteers`: LOW INTEGRITY
  Objects: `report.txt`: HIGH INTEGRITY, `dynamics/observations.log`: LOW INTEGRITY, `puzzle/updates.log`: LOW INTEGRITY
- ☐ **Bell-LaPadula**
  Subjects: `researchers`: (TOP SECRET, {Puzzle, Dynamics}), `spies`: (UNCLASSIFIED, {Puzzle, Dynamics}), `volunteers`: (UNCLASSIFIED, {Puzzle})
  Objects: `report.txt`: (TOP SECRET, {Puzzle, Dynamics}), `dynamics/observations.log`: (SECRET, {Dynamics}), `puzzle/updates.log`: (UNCLASSIFIED, {Puzzle})
- ☐ **Bell-LaPadula**
  Subjects: `researchers`: (SECRET, {Puzzle, Dynamics}), `spies`: (SECRET , {Puzzle, Dynamics}), `volunteers` (UNCLASSIFIED, {Puzzle, Dynamics})
  Objects: `report.txt` (TOP SECRET, {Puzzle, Dynamics}), `dynamics/observations.log` (SECRET, {Dynamics}), `puzzle/updates.log` (SECRET, {Puzzle})
- ☐ **Bell-LaPadula**
  Subjects: `researchers`: (TOP SECRET, { }), `spies`: (SECRET, {Dynamics}), `volunteers`: (UNCLASSIFIED, {Puzzle})
  Objects: `report.txt` (TOP SECRET, { }), `dynamics/observations.log` (SECRET, {Dynamics}), `puzzle/updates.log` (SECRET, {Puzzle})

Question 6 **[Applied Cryptography]** Assuming that:
`m` is a message,
`Enc` denotes a symmetric encryption scheme,
`MAC` a message authentication scheme,
`K1` and `K2` are two symmetric keys,
and that Roberta and Gustave have securely pre-shared the keys `K1` and `K2` before.

Which of the options below would allow Roberta to send messages to Gustave while ensuring the confidentiality and integrity of the exchange?

- ☐ `Enc(K1, m), MAC(K1, m)`
- ☐ `Enc(K1, m), MAC(K2, m)`
- ☐ `MAC(K2, Enc(K1, m))`
- ☐ `Enc(K1, m), MAC(K2, Enc(K1, m))`

Question 7 **[Authentication]** Which of the following statements is correct?

- ☐ A token-based authentication system is only secure if the seed is kept secret.
- ☐ Biometric templates cannot be compromised.
- ☐ AES-128 cannot be used in a token-based authentication mechanism.
- ☐ A signature on a credit card is an example of biometrics.

[Fast Thesis Pitch] EPFL is hosting a "Fast Thesis Pitch" competition where students get a chance to pitch their thesis within 3 minutes. The winners are awarded cash prizes.
The organisers want attendees to the competition to vote to decide the winners. The organisers gather two student volunteers to develop a voting application. Each attendee may vote for multiple presenters, but should only vote once for a single presenter.
They develop an application and make the code available to the public. The application contains a simple form in which attendees can write the name of their preferred presenter. Since this is a time-sensitive event, to keep things fast, the attendees don't need to create an account for voting, i.e., there is no authentication. The backend of the application collects all the submissions and dumps them into a Microsoft Excel sheet. At the end of the event, the votes for each presenter are counted, and the 10 presenters with the most votes are declared winners.
The organisers are worried that the voting application has vulnerabilities that allow attendees to boost their friends' votes. Lacking background in computer science, the volunteer students contact you to review their application. You start your analysis by checking if the application follows the security principles.

Question 8 Name two security principles followed by this application. Justify your answer.

☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

.....

Question 9 Name two security principles **not** followed by this application. Justify your answer.

☐0 ☐0.25 ☐0.5 ☐0.75 ☐1

.....

.....

.....

.....

.....

[Investigative Journalists] Nova, a security researcher, is working on the digital safety of investigative journalists. To understand their security and privacy needs, Nova plans to organize group interviews with several journalists.
Each journalist has two different affiliations. One affiliation is their employer: a journalist can be employed by a newspaper (e.g., Zurich Times, Lausanne Journal) or have no employee (freelancer). Newspapers compete against each other. A journalist's second affiliation is with a journalist organization (e.g., JournalismForever, TrueReporters, and Write4World). These organizations are not for profit, and hence, do not compete with each other.
Nova plans to interview the following five journalists:

- *Journalist 1 (J1)*: working for Zurich Times, affiliated with TrueReporters
- *Journalist 2 (J2)*: working for Lausanne Journal, affiliated with Write4World
- *Journalist 3 (J3)*: previously worked for Zurich Times, now retired, but still affiliated with TrueReporters
- Journalist 4 (J4): works as a freelance journalist, affiliated with JournalismForever
- *Journalist 5 (J5)*: working for Lausanne Journal, previously affiliated with Write4World

Question 10 Nova wants to avoid that the group interviews cause any conflicts of interest for the journalist and asks you to help with forming the interview groups. Assign the journalists into interview groups, minimizing the number of interviews Nova has to conduct. Justify your answer, explaining what security considerations led you to propose the assignment.

☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

.....

Question 11 After conducting a group interview, Nova must give all interviewed journalists in this group the opportunity to review and modify the collected data.
For a journalist `Jx` in an interview of `GroupJ`, the collected data include:

- A text file that contains background information of the journalist `Jx`: `bg-info-Jx.txt`
- An audio recording of the interview of `GroupJ`: `audio-GroupJ.mp4`
- A text transcription of the audio recording of the interview of `GroupJ`: `transcription-GroupJ.txt`
- A script that takes as input (1) an audio recording (2) a text file and prints the difference between a direct transcribing of this audio recording and the input text file: `difference-audio-text.sh`

Each journalist should be able to review and modify their own background information and their group's transcription. All journalists in group `GroupJ` should be able to run the script with inputs `audio-GroupJ.mp4` with `transcription-GroupJ.txt` to see what has been modified.
Assuming that:

- Nova is using a UNIX system,
- Nova themselves is the `nova` user belonging to the group `Researcher`,
- Journalist `Jx` is a user belonging to their interview group `GroupJ`,

assign the minimal permissions that are needed for this scenario:

Permissions	User	Group	File name
`-__________`	`Jx`	`GroupJ`	`bg-info-Jx.txt`
`-__________`	`nova`	`Researcher`	`audio-GroupJ.mp4`
`-__________`	`nova`	`GroupJ`	`transcription-GroupJ.txt`
`-__________`	`nova`	`GroupJ`	`difference-audio-text.sh`

Complete the permissions in the table above and justify your answer in the box below.

☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

.....

[Fred Discussion] After graduating from EPFL, Fred decides to build an online discussion platform. On Fred Discussion, users have one out of two roles: Students and Teachers.

1. Students can write and edit their own posts. Students can read, like, and respond to posts of all other users.

2. Teachers can write and edit their own posts. Teachers can read, respond to, edit, and delete posts of students. Teachers can read and respond to posts of other teachers.

Fred wants to use a cryptographic hash function H() to ensure that if a teacher edits the post of a student, the student can provide evidence that their post has been edited. To do so, for every post p Fred Discussion computes its hash h=H(p), publishes it alongside the post, and sends a copy of the post and its hash to the author of the post. If a post gets edited, Fred Discussion computes the hash of the edited post h'=H(p'), updates the post and its hash, and sends a copy of the updated post and its hash to the original author of the post.

Question 12 What is the minimum set of security properties the hash function H() needs to have to achieve Fred's goal? Justify your answer and describe how students would use the hashes h and h' to show that a post has been edited. ☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

.....

Question 13 What is the minimum set of security properties the hash function needs to have if Fred in addition wants to ensure students can not write posts that they later edit but claim otherwise? Justify your answer and describe how teachers would use the hashes h and h' to show that a post has been edited. ☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

.....

[Secure Accounting] You set up a business on campus: LAYD. Through LAYD, users can order lollipops and get them delivered to their desks. LAYD employees take the lollipops to the users. Upon delivery, employees register in their LAYD app how many lollipops they gave to users. At the end of the day, every employee's app sends the following message to the LAYD central server to communicate the number of lollipops L this employee has delivered:

$$\mathbf{Enc(k_1, L),\ MAC(k_1, L),\ MAC(k_2,\ Enc(k_1, L)),\ Sig(PK_{server}, L)}$$

For each of the statements below, say if they are true or false. Justify your answer.

Notation:

- **L** – number of lollipops delivered by the employee
- $\mathbf{k_1}$ - symmetric key freshly generated by the app before sending the message
- $\mathbf{k_2}$ - symmetric key generated by the app when installed on employees' phones and securely shared with the central server at that point
- $\mathbf{PK_{server}}$ - asymmetric public key of the LAYD server
- Enc($\mathbf{k}, \mathbf{m}$) - symmetric encryption of a message m with the symmetric key k
- MAC($\mathbf{k}, \mathbf{m}$) - message authentication code of message m with the symmetric key k
- Sig($\mathbf{PK}, \mathbf{m}$) - signature on message m using the public key PK

Question 14 *Statement 1*: the server can compute the total number of lollipops delivered by all employees at the end of the day. ☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

Question 15 *Statement 2*: the server can be sure that the lollipop counts are sent by an LAYD app.

☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

Question 16 *Statement 3*: whether the server can or cannot prove to a third party that the lollipop counts were sent by LAYD apps depends on the secrecy of the asymmetric secret key of the server, i.e., if has been leaked or not.

☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

[FELP Authentication] FELP is a research institute with a cautious security department. In the past, internal FELP services used a password-based authentication system with passwords chosen by users. After a leak of a large password database, FELP wants to update their authentication system. They consider two options:

1. Force all FELP employees to change their password every 6 months. Every employee chooses their new password, constrained to the same rules as in the previous system: It should contain at least 10 characters, include at least one number and one special symbol, and they cannot reuse the old password.

2. Generate and issue new passwords to all employees once. The new passwords are generated at random so that they contain 10 characters and include at least one number and one special symbol.

Question 17 Assuming that a potential adversary has access to the database of leaked passwords mentioned above, list one advantage and one disadvantage for both approaches.

☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1**

.....

.....

.....

.....

.....

Question 18 After some internal discussions, the FELP security department decides that any password-based solution is insufficient and should be replaced by a biometric-based authentication. Fortunately, FELP has a good quality ID-like photo for every employee from when they obtained their PROMICA card, an access card issued to every employee at the start of their employment. To get access to FELP online services, employees need to turn on their laptop camera, take a photo, and send it to the server. The server computes the template and compares it to the PROMICA database and if it is a match it allows access to the service. Otherwise, access is denied. Write one security argument for why the new solution improves the system, and one why it may degrade security. ☐**0** ☐**0.25** ☐**0.5** ☐**0.75** ☐**1**

.....

.....

.....

.....

.....