# COM 301 Midterm Exam, 10.11.2022

Name: .....

Sciper: .....

## Please wait for instructions before opening this document

- This is a **closed book** exam. Books, notes, and electronic devices are not allowed.

**Multiple choice questions:**

- Multiple-choice questions can have multiple correct answers. You need to mark *all* answers that are correct, and *only those* that are correct to receive the point.
- To mark a correct answer, make a mark *inside* the box corresponding to your answer. Outside marks will not be graded
- Use a black or blue pen to mark your answers. Pencils are not allowed.

**Open text questions:**

- Please write your answers in the corresponding text boxes.
- Do not write more than the lines specified in the box. **Any text outside of the boxes will be ignored**.
- Do not tick the grading boxes of the 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** |
|---|---|---|---|---|---|---|
| | | | | | | / **6 pts** |

| **Open text questions** | **Parts** | | **Total** |
|---|---|---|---|
| **Hiding the Horcruxes** | | | / **2 pts** |
| **Battle Night** | | | / **2 pts** |
| **NovemberFest** | | | / **2 pts** |
| **Geletram** | | | / **2 pts** |
| **Crazy Love** | | | / **2 pts** |
| **Life at the Vortex** | | | / **2 pts** |
| **Total** | | | / **18 pts** |

**Question 1** **[Security Principles]** Rob accidentally downloaded a malware that leverages ambient authority. That malware uploaded all Rob's files (both on their laptop and accessible as shared folders) to a cloud. The company discovers later that during the same leak, documents in other departments, that Rob was not working on, also got leaked due to the malware. Which security principle(s) were incorrectly applied by the company's system administrators that manage the shared folders and allowed the full leak ?

- ☐ Fail-Safe Default
- ☐ Least Privilege
- ☐ Psychological Acceptability
- ☐ Separation of Privilege

**Question 2** **[Access Control]** Which of the following are true about Access Control Lists?

- ☐ They associate permissions to subjects.
- ☐ It is easy and efficient to determine a given user's permissions on all files.
- ☐ They associate permissions to objects.
- ☐ It is easy and efficient to revoke rights by resource.

**Question 3** **[Access Control]** MAC stands for Mandatory Access control in this question with levels secret $<$ top secret. Which of the following statements are true?

- ☐ A system designed using MAC automatically follows the least privilege principle.
- ☐ MAC and DAC cannot coexist within the same system.
- ☐ BLP does not guarantee that top secret information cannot be accessed by the lowest clearance subjects.
- ☐ In MAC, owners can delegate access to a document to any user.

**Question 4** **[Symmetric Cryptography]** In symmetric cryptography, there are two types of ciphers: stream ciphers and block ciphers. Block ciphers have different modes of operation. Which of the following statements are true?

- ☐ When using a block cipher in ECB mode, the encryption of a block does not include information from any other block.
- ☐ CTR mode is not secure if the nonce is reused under two different keys.
- ☐ When using a stream cipher, both the key and the initialization vector (IV) must be kept secret.
- ☐ CBC mode is not secure if the IV is reused under the same key.

**Question 5** **[Cryptography]** Which of the following statements are true?

- ☐ **Encrypt(key, m) = c**, where **c** is a random string, is not a valid form of encryption that provides confidentiality.
- ☐ All encryption schemes guarantee that the risk that an adversary without the secret key can read the plaintext is 0.
- ☐ Applying twice a hash function, i.e., **hash(hash(m))** is less secure than applying it only once.
- ☐ In digital signatures, the secret key is used to verify the signature given a message.

**Question 6** **[Authentication]** Which of the following statements are true?

- ☐ Authentication is a process that determines whether a subject has permission to use a resource or access a file.
- ☐ Encrypting the channel prevents replay attacks during a network-based authentication process.
- ☐ Storing a salted hash instead of a password does not prevent brute-force attacks.
- ☐ In biometrics-based systems, a low rate of false positives is always more important than a low rate of false negatives.

**[Hiding the Horcruxes]** The Dark Lord Voldemort has created seven distinct horcruxes that he wishes to protect from being discovered. He decides to conceal each of the seven horcruxes in seven distinct vaults whose security mechanisms are only known to Voldemort himself. He selects his seven most loyal followers. He locks each horcrux in a vault and gives the key to one of these trusted followers. Then, the dark lord personally takes the vaults to seven hidden locations across the world. The trusted followers keep the key entrusted to them.

**Question 7** Among the following security principles, name two which hold in this system. Justify your answer.

- fail-safe default
- complete mediation
- open design
- separation of privilege
- least privilege

☐ **0** ☐ **0.5** ☐ **1** ☐ **1.5** ☐ **2**

.....

.....

.....

.....

**[Battle Night]** Zwolf is organizing a dance battle night at the Student Party Room. Zwolf uses a server to maintain all the files that are related to the battle. The server relies on Linux access control for the files.
People can only choose to be a participating dancer or a spectator, not both. To join the dance battle, a dancer needs to talk to Zwolf: *"I want to participate in the battle."* Zwolf creates an account for the dancer. To watch the battle, a spectator needs to talk to Zwolf: *"I want to watch the battle."* Zwolf creates an account for the spectator and assigns it to the group "Spectators".
There are three kinds of files on the server:

1. One profile per dancer, `profile_`*`XXX`*`.txt`, where *`XXX`* is a unique identifier for the dancer. This profile is created and owned by the dancer *XXX*. It contains the dancer's personal information (e.g., name, dance style) and should be seen and filled by the dancer. All dancers should be able to read each other's profiles.

2. A python script `dancers_summary.py` that reads through all the dancers' profiles and outputs a list of their names with their dance styles (to the file `list_dancers.txt`). This script is owned by Zwolf. Only Zwolf can modify this script and run it.

3. The list of dancers with their dance styles `list_dancers.txt` that everyone can consult to follow the battle night.

There are three permissions:

`r` read the content of a file

`w` write into the file

`x` execute a file

**Question 8** Zwolf asks you to help them establish the access control policy to these files without *"overprivileged"* subjects.

| **Permissions** | **User** | **Group** | **File name** |
|---|---|---|---|
| `-__________` | `Dancer`*`XXX`* | `Spectators` | `profile_`*`XXX`*`.txt` |
| `-__________` | `Zwolf` | `Spectators` | `dancers_summary.py` |
| `-__________` | `Zwolf` | `Spectators` | `list_dancers.txt` |

*Please, complete the permissions in the table above and justify your answer in the box below.*

☐ **0** ☐ **0.5** ☐ **1** ☐ **1.5** ☐ **2**

.....

.....

.....

.....

**[NovemberFest]** You work at the company *NovemberFest* as a beer creator. *NovemberFest* primarily organizes beer related events, where they present their newest beers, and each of those beers receives a score from beer tasters. *NovemberFest* manages access to the secret beer recipes and the scores from tasters using a **BIBA** access control policy. The scores have a high integrity level, and recipes have a low integrity level. As a beer creator, you are a low integrity subject. The beer tasters are high integrity subjects.

**Question 9** You create a new beer in collaboration with Dr. Paps. The resulting beer is not really good, and you're worried you might lose your job because of that. Can you change the score your beer received? If yes, explain how, and if not, justify.

☐**0** ☐**0.5** ☐**1**

.....

.....

.....

**Question 10** What you feared happened: the CEO of *NovemberFest* learns of your poor performance, and fires you from *NovemberFest*.

To make sure that there are no quarrels among the local companies, the *Lausanne Breweries & Brewery Events Association* designs the following classes of conflicts of interest according to the Chinese Wall model:

**COI1** = {NovemberFest, DecemberFest}

**COI2** = {Dr. Paps, GP, Bunéleuse, Black Frontier}

Following this policy, which companies (other than *NovemberFest*) can you apply to for a new job? Justify.

☐**0** ☐**0.5** ☐**1**

.....

.....

**[Geletram]** Alice uses the *Geletram* application to send messages to Bob. Alice and Bob share a secret symmetric key **K**. This key **K** is also known by *Geletram*.
For each message **msg** Alice wants to send to Bob through *Geletram*, *Geletram* does the following:
It generates a fresh symmetric key $\mathbf{K_{Geletram}}$,
It sends $\mathbf{packet = \{c = Encrypt(K, msg), m = MAC(K_{Geletram}, c), K_{Geletram}\}}$ to Bob's *Geletram* to be decoded, where **Encrypt** is a symmetric encryption scheme, and **MAC** stands for *Message Authentication Code*.
Eve is an adversary that controls the channel in between Alice's *Geletram* and Bob's, i.e., Eve can read and modify any packet before it reaches Bob's *Geletram*.

**Question 11** Does *Geletram* provide confidentiality and integrity of the message **msg** with respect to Eve? If yes, justify why. If not, explain why and propose a fix.

☐ **0** ☐ **0.5** ☐ **1** ☐ **1.5** ☐ **2**

.....

.....

.....

.....

**[Crazy Love]** You are crazy in love with your partner and you send each other a lot of messages everyday. As a security freak, you would like to achieve both confidentiality and integrity of your communication. Your partner proposes to use asymmetric encryption for confidentiality and a hash function for integrity. The scheme goes as follows:

1. Each of you two generates an asymmetric key pair, i.e., you have **(pk1, sk1)** , your partner has **(pk2, sk2)**.
2. You both publish your public key, i.e., you publish **pk1**, your partner publishes **pk2**.
3. You both agree to use a public hash function **H**.
4. When you send a message m to your partner, you do:

**Encrypt(pk2, m) || H(m)**

Assuming the asymmetric encryption **Encrypt()** is secure and the secret keys **sk1**, **sk2** are not leaked to the adversary:

**Question 12** If an adversary seeing the ciphertext **Encrypt(pk2, m) || H(m)** can recover the original message **m**, which of the security properties of the hash function **H** is broken? Justify your answer. ☐**0** ☐**0.5** ☐**1**

.....

.....

**Question 13** If the hash function **H** is collision resistant, pre-image resistant, and 2nd pre-image resistant, can your partner be sure that the message **m** was sent by you? Justify your answer. ☐**0** ☐**0.5** ☐**1**

.....

.....

**[Life at the Vortex]** You live at the Vortex and your low-cost wireless speaker is controlled by a mobile app. The communication between the app and the speaker is unencrypted (e.g. home WiFi). The app and the speaker have a pre-shared key **K** (setup by pressing a special button on the device) that has not been compromised. To send commands, the app sends the following message, which can be successfully decrypted by the device.

**AES256(k=K, m="cmd:" || CMDS)** with **CMDS = ["on" | "off" | "up" | "down"]**

Where || denotes concatenation, e.g. **m="cmd:on"** or **m="cmd:up"**, etc...

Your neighbor at the Vortex is annoyed about the noise.
Justify and state all your assumptions.

**Question 14** Identify a vulnerability and describe an attack that allows the neighbor to shutdown the speaker as soon as you turn it on. Note that denial-of-service attacks are prohibited in the Vortex to minimize wave interference. ☐**0** ☐**0.5** ☐**1**

.....

.....

.....

.....

**Question 15** Describe how the speaker manufacturer can improve the protocol to prevent this attack.
☐**0** ☐**0.5** ☐**1**

.....

.....

.....

.....