+1/1/60+

COM-301 Midterm #1

24 October 2019

Identification
Please encode your SCIPER on the right (one digit per column), and write your first and last names below.

First Name and Last Name:

.....

.....

☐**0**	☐**0**	☐**0**	☐**0**	☐**0**	☐**0**
☐**1**	☐**1**	☐**1**	☐**1**	☐**1**	☐**1**
☐**2**	☐**2**	☐**2**	☐**2**	☐**2**	☐**2**
☐**3**	☐**3**	☐**3**	☐**3**	☐**3**	☐**3**
☐**4**	☐**4**	☐**4**	☐**4**	☐**4**	☐**4**
☐**5**	☐**5**	☐**5**	☐**5**	☐**5**	☐**5**
☐**6**	☐**6**	☐**6**	☐**6**	☐**6**	☐**6**
☐**7**	☐**7**	☐**7**	☐**7**	☐**7**	☐**7**
☐**8**	☐**8**	☐**8**	☐**8**	☐**8**	☐**8**
☐**9**	☐**9**	☐**9**	☐**9**	☐**9**	☐**9**

INSTRUCTIONS
The exam must be completed with a PEN that is BLUE or BLACK. Pencil will not be corrected (the question will count as 0).
No book, calculator, phone, or laptop are allowed during the exam

Part 1: Multiple-choice questions
Please mark the correct answer by filling the corresponding square.
There is **only one** correct answer per question.
Correct answer gets +1. Incorrect answer gets -0.5. No answer gets 0. Incoherent answers (for example, multiple marked answers) get -0.5.
Use white-out fluid to erase an answer (other deletions get -0.5).

Question 1 **[Authentication]** The use of salts to store passwords prevents brute force attacks by:

- ☐ Requiring the adversary to guess the salt besides the password
- ☐ Avoiding replay attacks
- ☐ Strengthening the pre-image resistance of the hash function
- ☐ Forcing the adversary to repeat the computations for every salt

Question 2 **[Security Policies]** To protect both the integrity and the confidentiality of the assets in your system, you decide to establish policies following both BIBA and BLP security models setting the same integrity and confidentiality security levels. As a result:

- ☐ All subjects can read files on security levels that dominate them
- ☐ Subjects can read and write only within their own security level
- ☐ Subjects can read only within their own security level
- ☐ No subject can read or edit any files

Question 3 **[Access control]** What problem is easier to solve with capabilities than with access control lists.

- ☐ Permission updates for a file
- ☐ Confused deputy problem
- ☐ Revocation of rights for all users on one file
- ☐ Change of permissions for one user on one file

Question 4 **[Security principles]** To secure the entrance to an intimate concert of One Direction, the organizers decide that the best way to control the fans is to only open one door to the venue and hire one big, strong, guard to check the tickets. However, the guard has a cold and from time to time, he needs to sneeze several times. During this time, fans without a ticket slip in. This mechanism is obviously not good and does not follow many principles; but which one does it follow?

- ☐ Separation of Privilege
- ☐ Fail-safe default
- ☐ Economy of mechanism
- ☐ Least common mechanism

Question 5 **[Security policies]** Suppose you work for a company with a Chinese Wall security policy with clients in the following conflict classes:

- Google, Mozilla, Safari
- Aldi, Coop, Migros
- Quicksilver, Carhartt
- Lenovo, HP

You have previously worked on cases for Coop, and Quicksilver, and you are ready for a new assignment. According to the policy the largest set of companies you can work with is:

- ☐ Google, Mozilla, Safari, Coop, Quicksilver, Lenovo, HP
- ☐ Google, Mozilla, Safari, Aldi, Coop, Migros
- ☐ Google, Mozilla, Safari, Lenovo, HP
- ☐ Google, Aldi, Quicksilver, Lenovo

Question 6 **[UNIX permissions]** A small shop owner is building a new accounting log as follows:

- Creates an account log `Accounts`, of which she is the owner (her login is `shopowner`
- Creates one user per employee, and assigns all of these to the group `employees`.
- Creates a program `Recorder` to append the content of the cash register in the at the end of the day.

The shop owner is very worried that her employees are stealing from her, so she does not want them to have the capability to tamper with the log other than using `Recorder`. Which of the following permission configurations would you recommend to the owner:

☐
```
-rwx-wx--x shopowner employees Accounts
-rwsrwx-wx shopowner employees Recorder
```

☐
```
-rwxrw---- shopowner employees Accounts
-rwxr-x--x shopowner employees Recorder
```

☐
```
-rw-r----- shopowner employees Accounts
-rws--x--x shopowner employees Recorder
```

☐
```
-r-x--x--x shopowner employees Accounts
-r-s-----x shopowner employees Recorder
```

Question 7 **[Cryptography]** A friend of yours is organizing a mystery dinner in which he emails a long character story and a role to each participant. After attending Com-301, each participant generated a key pair and sent the public key to the organizer so that he can encrypt his mails. For the first night, the organizer wants to ensure that everyone received their email correctly. He asked participants to prove they received their email correctly, in a way that, if somebody intercepts the reply, they cannot learn the role. However, he forgot to give them his public key, so they cannot encrypt their reply. What primitive would you recommend that the participants use?

☐ A stream cipher

☐ A hash function with pre-image resistance

☐ An asymmetric cipher combined with Diffie Hellman

☐ A hash function with collision resistance

Part2: Short answer questions: Please write your answer only within the lines provided (not more than 3 lines unless specified). Anything over the specified number of lines will not considered. Answers are graded on a scale of 0 to 4.
Please mind your calligraphy, undecipherable text will not be graded.

Question 8 **[Access control]** Alice can read the file `xxx.sys`, can write on the file `yyy.sys`, and cannot access the file `zzz.sys`. Bob can read and write to `yyy.sys`, and cannot access `xxx.sys`, but can execute `xxx.sys`. Charlie can execute `yyy.sys`, can write and read `xxx.sys` and only write on `zzz.sys`. Create the access control matrix based on this scenario.
Exceptionally you get an extra line to build the matrix ☐**0** ☐**1** ☐**2** ☐**3** ☐**4**

.....

.....

.....

.....

Question 9 **[Security principles]** Write one security principle that is preserved and one that is not preserved by the following mechanism (Justify your answer):
A firewall router that inspects every connection and stops connections from known insecure protocols (e.g., telnet) and let the rest pass. ☐**0** ☐**1** ☐**2** ☐**3** ☐**4**

.....

.....

.....

Question 10 **[Cipher configuration]** Is the following pseudocode for a function to encrypt movies a secure use of a stream cipher? Justify your answer.

```
var iv = "bestidever"

def EncryptMovie(movie):
    key = GenerateSecureRandomKey() // generates a truly random key
    secureKeyTransfer(key) // securely sends the key to the
                           // recipient
    EncryptedMovie = Salsa20(key,iv,movie) // uses Salsa20 stream
                                           // cipher
    return(EncryptedMovie)
```

☐0 ☐1 ☐2 ☐3 ☐4

.....

.....

.....

Question 11 **[Cryptography]** Alice sends to Bob the following message: $Enc(PK\_Bob, k), Enc(k, m), MAC(k, m)$ where
- $Enc(key, x)$ is the symmetric encryption of x under the key key,
- $Enc(PK\_y, x)$ is the asymmetric encryption of x under the public key of y,
- $MAC(key, x)$ is the Message Authentication Code of x under the key key.

When Bob receives this message, can he be sure of the integrity of the message m sent by Alice? (Justify)

☐0 ☐1 ☐2 ☐3 ☐4

.....

.....

.....

Question 12 **[Security policies]** A professor asks a TA to upload the previous year's final exam *without answers* to Moodle. The TA has been bribed by this years students and has put a small mark in the pdf besides the correct answers in the multi-choice questions. What do we call this way of passing information? How should the professor check the exam pdf to avoid this problem? ☐0 ☐1 ☐2 ☐3 ☐4

. . . . . .

. . . . . .

. . . . . .

Question 13 **[Security principles]** The TAs deploy a service to check homework cheating. Initially, this service runs on port 15. Then, a student runs a Denial of Service on this port. To avoid these attacks, the TAs decide to use a random port in [10-15]. Is this a good strategy? Justify. ☐0 ☐1 ☐2 ☐3 ☐4

. . . . . .

. . . . . .

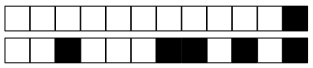
. . . . . .

Question 14 **[Authentication]** Cersei and Jamie meet secretly every week in the crypt. To make sure that they are each other, before opening the door they have a protocol in which:
1) Jamie knocks a particular sequence (toc, toc, toctoc)
2) Cersei replies with anothe sequence (toctoc, toc, toctoc)
3) Jamie replies with just (toc).
Is this safe against an eavesdropping Tyrion hidden behind the bushes? If yes, justify. If not, explain how to fix it. ☐**0** ☐**1** ☐**2** ☐**3** ☐**4**

.....

.....

.....



Question 15 [UNIX permissions] Alice is a TA in a human science course given by Prof. Bob. Bob has developed a program to help with the grading and asked Alice to configure the access control. Alice does not know anything about UNIX permission, so she forwarded system requirements to you and asked you to describe users and file permission.

Users:
1) Each student gets his own account. You just need to define one user as 'student', and Alice will handle the rest.
2) Alice and Charlie are TAs.
3) Bob is the professor.
4) Alice, Bob, and Charlie are considered as 'teaching staff'.

Files:
1) All grades are stored in 'grades.csv'.
2) TAs' duties is written in 'ta.txt'.
3) 'grader.exe' is a program which updates grades.

Requirements:
1) Students are only allowed to read grades.
2) Teaching staff should be able to run and maintain the grader.
3) TAs should be able to read TAs' duties, but only Bob should be able to modify it.
4) Bob should still be able to access every file after TAs' graduate. (University deletes TAs' accounts after graduation)

☐**0** ☐**1** ☐**2** ☐**3** ☐**4**

.....

.....

.....