+1/1/60+

**Ens: Prof. Edouard Bugnion**
**COM-301 - Final Exam - XX**
**13.01.2025**
**2 hours 45 minutes**
**Room : PO 01**

# Extra 1

SCIPER : **999991**

**Do not turn the page before the start of the exam. This document is double-sided, has 11 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 |
|---|---|---|---|---|---|
| Network Security | | | | | / 4 pts |
| Software Security | | | | | / 3 pts |
| Privacy | | | | | / 2 pts |
| Web Security | | | | | / 2 pts |
| Malware | | | | | / 3 pts |
| Authentication and Cryptography | | | | | / 3 pts |
| Total | | | | | / 17 pts |

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

**General Note:** *they* is a gender-neutral third-person pronoun. In this exam, *they/their* can refer to a singular individual, for example Charlie in the Privacy question.

## Network Security *[4 points]*

Paul works at the national Internet Service Provider. He wants new challenges, so he is applying for a job at Peach, a cutting-edge IT company in the country where Paul works. Paul has photos from night outings on a website called `http://seehowiparty.com`, for which the server has not enabled TLS. Paul does not want Peach's Human Resources department to see these photos, so he wants to prevent them from accessing the website.
Assume that Paul cannot join the Peach local network. Also assume that Paul wants to be able to show his photos in `seehowiparty` to his friends, that Paul needs Human Resources employees to be able to have normal internet access to services to process his application, and that Paul does not want to be caught launching an attack.

### Question 1

Propose an attack that Paul could launch to ensure that nobody within the Peach network can access the `seehowiparty` website. Explain what capabilities (what knowledge and what accesses) enable Paul to carry such an attack. *[1 point]*

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

.....

.....

.....

### Question 2

Would using DNS over HTTPS (DoH) protect the HR team at Peach from the attack Paul is launching? Justify. *[1 point]*

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

.....

.....

.....

**Question 3**

If `seehowiparty.com` would activate access via HTTPS, would this protect the team at Peach from the attack? Justify. *[1 point]*

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

.....

.....

.....

**Question 4**

If the HR department connects to the `seehowiparty.com` server through an IPSEC tunnel, would this protect the team at Peach from the attack? Justify. *[1 point]*

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

.....

.....

.....

## Software Security *[3 points]*

Consider the following code:

```
1  int64_t f(int64_t a, int64_t b) {
2      int64_t* y[10];
3      int64_t x[100]; // array of 64-bit numbers
4      initialize_y(y); // Fills y of valid pointers
5      initialize_x(x, y); // Initializes x with respect to y
6      if ((a < 0) || (a > 100)) {
7          return 0;
8      };
9      x[a] = b;
10     return *(y[0]);
11 }
12
13 void main() {
14       ...
15       printf("%dld", f(a, b));
16       ...
17 }
```

Assume that there is no optimization or mitigation activated on the computer running the code. As a reminder, the stack pointer grows towards the lower addresses.

### Question 5

Find a line in the code above that contains a vulnerability. Justify. *[1 point]*

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

.....

.....

### Question 6

Find values a and b such that `main()` leads to the leakage of a secret value stored at memory address `0xff1234ff`. Justify. *[1 point]*

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

a = .....; b = .....; .....

.....

.....

.....

**Question 7**

Would activating (1) stack canaries, (2) W∧X (write `XOR` execute, also known as Data Execution Prevention), or (3) ASLR mitigate the attack? For each mitigation, answer yes or no and justify. *[1 point]*

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

.....

.....

.....

.....

## Privacy *[2 points]*

Meta has a very strict confidentiality policy for employees working in the innovation department. Charlie, who works in the innovation department, is too excited about the latest project and wants to tell the details to their friend Brown, working at a newspaper so that Brown will have the first article on the topic. Since WhatsApp (operated by Meta) is end-to-end encrypted (the encryption algorithm and the app are considered secure by security experts ), Charlie uses it to tell Brown about the research. As the day of the release of the project to the public gets closer, the number of messages Charlie and Brown exchange increases substantially. The day before the public release, a news website where Brown is known to contribute to leaks the information. Then, Charlie gets called by their superior and asked whether they had leaked information to a journalist.

**Question 8**

Explain why Meta had a suspicion that they should ask Charlie about the leak. *[1 point]*

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

.....

.....

.....

**Question 9**

Based on your previous answer, if Charlie would have installed a Tor client on both their phone and Brown's so that any WhatsApp connection from the phones to a server would be made via Tor, would Meta have suspected Charlie? *[1 point]*

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

.....

.....

.....

## Web Security *[2 points]*

Suppose the ISAcademia website would run the code below in their server, executed when the following URL is called (with example parameter values):

`isa.epfl.ch/addGrade.php?username=Bugnion&course=com301&sciper=123123&grade=5`

```
1  <?php
2
3  // initiate the session to validate sessions
4   session_start();
5
6   if (! session_is_registered($_GET['username' ])) {  // if the session is invalid
7   echo "invalid session detected!";
8   // Redirect user to  isa.epfl.ch/login  so they can log in the page to access the
       service
9   [...]
10  exit;}
11
12
13
14 echo '<div class="header"> Welcome, Prof. ' . $_GET['username' ]. '</div>';
15
16 $student = findStudentInDB($_GET['sciper'])
17
18
19
20 // set grade for student
21  setGrade($student, $_GET[ 'course'], $_GET['grade'])
22
23  echo "Your grade has been set.";
24
25 ?>
```

A professor has seen this code and observes that a Cross Site Request Forgery (CSRF) attack is possible. Thus, they decide that they will wipe their cookies cache after every visit to ISA.

### Question 10

Explain why the attack is possible and whether the action of the professor would protect him from this attack. *[1 point]*

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

.....

.....

.....

After the professor tells the IT department about the issue with the CSRF attack, the engineers fix it. Then, one of the engineers says that they should also eliminate line 14, because this line can also be exploited.

**Question 11**

Agree or disagree with the engineer. If you agree, explain which attack this line enables, provide an example of what the adversary would need to write to exploit it (no need to have executable code), and explain why your proposal would result in an exploit. If you disagree, explain why this line cannot be misused by an adversary. *[1 point]*

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

.....

.....

.....

.....

## Malware *[3 points]*

Alex, a student at FELP, found out their laptop is infected with malware. Alex remembers about the time they found a USB stick in the COM-301 classroom and plugged it in their laptop. They think the malware may have entered their laptop from the USB key.

**Question 12**

Propose something Alex could have done to reduce the risk of malware infection when plugging the USB stick. *[1 point]*

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

.....

.....

**Question 13**

The FLEP IT Team observes unusual packets being sent from Alex's laptop to other FLEP employees' laptops. Given this behavior, which type of malware of the ones seen in the lecture can it be (provide only one). Justify. *[1 point]*

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

.....

.....

**Question 14**

The IT team plans to install a personal firewall on each student's laptop to block incoming/outgoing connections from applications unknown by the IT team. Would this measure help protect against the type of malware identified in Question 13? *[1 point]*

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

.....

.....

## Authentication and Cryptography *[3 points]*

Your company has recently introduced two-factor authentication. This new feature enables the VPN service used to connect to the corporate network. Assume that the VPN uses a token-based 2FA in which the token and the server use the following scheme to compute a challenge sent to the server to complete the authentication:

```
IV = SHA256(k || time)
challenge = get_last6digits(Enc(k, IV, time))
```

where:

- `SHA256` is a secure hash function. It takes an arbitrary-length string and outputs a 256-bit hash value fulfilling preimage, second-preimage and collision resistance;
- `x||y` denotes the concatenation of strings `x` and `y`;
- `k` is a 256-bit cryptographic key unique for each user.
- `time` is a string representing the number of 30-second epochs since 1970 (using time in UNIX format), which is assumed to be synchronized between token and server;
- `Enc(k, IV, m)` is a symmetric encryption scheme such as `AES256`, which, given a 256-bit key `k` and an initialization vector `IV`, returns the encryption of `m` under that key and `IV`;
- `get_last6digits(n)` returns the last 6 digits of `n`.

**Question 15**

When connecting to the VPN, will the user:

(a) always enter the same 6-digit number,

(b) enter the same 6-digit number often, or

(c) enter the same 6-digit number with small probability.

Justify. *[1 point]*

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

.....

.....

**Question 16**

Assume that in the scheme above, the function used to produce the IV is changed to

`XORHash(k, time) = (k XOR pad(time)) % 2`$^{256}$

where:

- `k` is a 256-bit cryptographic key, as before;
- `pad` is a function that adds zeros to time until it has the same length as `k`;
- `%` denotes the modulus operation, and in this case `x % 2`$^{256}$ is equivalent to selecting the last 256 bits of `x`.

Does this change introduce any vulnerability that did not exist in the version that uses SHA256? Justify. *[1 point]*

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

.....

.....

**Question 17**

The `SHA256`-based fulfills preimage, second-preimage and collision resistance. Is it the case for the `XORHash` function? For each property, if yes justify, and if not provide a counter example. *[1 point]*

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

**collision resistance:**

.....

$2^{nd}$ **preimage resistance:**

.....

**preimage resistance:**

.....