+1/1/60+

EPFL

Ens: Prof. Carmela Troncoso
COM-301 - Final Exam - MA
01.02.2024
3 hours
Room : STCC

123

Student 1

SCIPER : **999000**

Do not turn the page before the start of the exam. This document is double-sided, has 5 pages, the last ones possibly blank. Do not unstaple.

- Place your student card on your table.
- Students can only have **two A4 handwritten cheatsheets 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.
- For the **multiple choice** questions, there is only **one** correct answer:
  - +1 point if your answer is correct,
  - 0 points if you give no answer or the answer is invalid (see below). We consider more than one answer as invalid,
  - −0.25 points if your answer is incorrect.
- 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**. 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.

Respectez les consignes suivantes | Read these guidelines | Beachten Sie bitte die unten stehenden Richtlinien		
choisir une réponse | select an answer Antwort auswählen	ne PAS choisir une réponse | NOT select an answer NICHT Antwort auswählen	Corriger une réponse | Correct an answer Antwort korrigieren
ce qu'il ne faut **PAS** faire | what should **NOT** be done | was man **NICHT** tun sollte		

First part: Multiple Choice Questions

For each question, mark the box corresponding to the correct answer (see the cover page for correct marking). Invalid marking will not be counted. Each question has **exactly one** correct answer.

Question 1 : Authentication
Assume Barbie and Ken have established a secure TLS connection. They use this connection for the following authentication exchange in which Barbie uses her password `'Il0veP1nk'` to prove her identity to Ken:

```
Barbie -- (Barbie, 'I want to login') --> Ken
Barbie <-- Hash(Ken) -- Ken
Barbie -- Enc('Il0veP1nk'|Hash(Ken), k) --> Ken
```

- `Hash()` is a secure cryptographic hash function that is second pre-image resistant.
- `str1|str2` is the concatenation of two strings `str1` and `str2`.
- `Enc(m,k)` is the symmetric encryption of message m with key k that Barbie and Ken have securely exchanged before.
- `'-->'` indicates communication via the secure TLS connection.

Which of the following statements is correct?

- ☐ This authentication exchange is secure against replay attacks because Barbie and Ken use a secure TLS channel.
- ☐ This authentication exchange is secure against replay attacks because `Hash(Ken)` is second pre-image resistant.
- ☐ This authentication exchange is not secure against replay attacks because `Hash(Ken)` is not collision resistant.
- ☐ This authentication exchange is not secure against replay attacks because Barbie has chosen a weak password that is easily guessable.

Question 2 : Network
A professor decides that the final exams of their course must be taken online. To ensure fairness, all students must sit in the same classroom during the exam and connect to the server hosting the exam questions using the classroom LAN. The teaching team creates a website with the exam questions and hosts it on the only lab server with IP `107.18.90.101` that all students in the course have interacted with in the past. The teaching team hears that some lazy students who have not studied want to stop the exam from happening through a denial of service (DoS) attack. To reduce the risk of a successful DoS attack, the teaching team keeps the domain name of the exam hidden until the start of the exam.

Which of the following statements is incorrect?

- ☐ Keeping the domain name secret prevents the lazy students from launching a DNS hijacking-based Denial of Service attack.
- ☐ Keeping the domain name secret cannot prevent the lazy students from launching a Denial of Service attack on the classroom LAN gateway.
- ☐ Keeping the domain name secret prevents the lazy students from launching a DNS poisoning-based Denial of Service attack.
- ☐ Keeping the domain name secret cannot prevent the lazy students from using a ping message with a spoofed origin IP address to launch a distributed Denial of Service attack.

Question 3 : Cryptography
During the TLS handshake, the client can propose to the server two methods to decide on the session key k that will be used for encryption:

(a) **Key transport** in which the client will generate a fresh symmetric session key k and send it to the server encrypted with the server's public key pk. Thus, only the server can decrypt the session key with the server's secret key sk. The session key k is deleted at the end of the session.

(b) **Key exchange** in which client and server will exchange cryptographic material to derive a fresh symmetric session key k only known to them to be used during the session. The session key k is deleted at the end of the session.

- k is a symmetric session key known to both sender and client
- pk is the public key of the server known to everyone
- sk is the secret key of the server known only to the server

Which of the following statements is correct?

☐ Only key transport provides forward secrecy because only the server knows sk that enables to decrypt the session key k.

☐ Only key exchange provides forward secrecy because there is no long-term secret involved in the process to decide on the session key k.

☐ None of the options provide forward secrecy because the session key k is deleted at the end of the session.

☐ Both options provide forward secrecy because in both cases the session key k is freshly generated at the start of each session.

Question 4 : Software
Oppenheimer's team wrote a program that can answer queries about statistics on the atomic bombs in storage, e.g., how many atomic bombs are currently in status `'ready to launch'`. The members of the Oppenheimer team ask queries to this program from the lab computer. The team worries that if one of the team members is a spy they could exploit potential bugs in the program to perform a code injection attack to maliciously trigger the launch of a bomb from the lab computer.

Which mitigation guarantees that such an attack cannot be launched?

☐ Implement data execution prevention through the X^W policy on the lab computer.

☐ Use mutation-based fuzzing on the program before loading it to the lab computer.

☐ Add a canary to the stack of the lab computer.

☐ Implement address space layout randomization at the OS level on the lab computer.

Question 5 : Access Control
Which of the following statements is correct?

☐ BIBA's goal of maintaining integrity is consistent with ensuring that information from low clearance levels is available to authorised users with high clearance.

☐ Encrypting part of a message so that the ciphertext can only be decrypted by the intended receiver is an example of a covert channel.

☐ Capabilities are more efficient than access control lists to remove access rights to a particular object.

☐ In role-based access control, increasing the number of roles of a principal can never reduce the number of permissions of this principal.

Question 6 : Web Security

Maurice uses a browser on his personal computer to answer complaints from clients. On the complaints website `bigCorp.org/complaints`, each complaint is reachable at `bigCorp.org/complaints/<complaint-id>` and contains a description text box and a button "View Screenshot". This button redirects Maurice to a **media server** chosen by the writer of the complaint that hosts an image of the problem that they encountered. The URL of this image is not visible on the complaints webpage.
Maurice uses the same web browser to fill out assignments on Foodle, and chat on FreeChat.com. Both Foodle and FreeChat use a session cookie stored in the browser for authentication.

Given his setup and the actions he has to perform to review complaints, which of the following attacks is Maurice vulnerable to?

- ☐ Cross-site scripting; because when returning a webpage to Maurice, the media servers might have `src` URLs that trigger malicious server-side scripts to track him.
- ☐ Cross-site scripting; because malicious media servers might add JavaScript code to the "FreeChat.com" tab to send messages to Maurice's friends using the existing session cookie.
- ☐ Cross-site request forgery; because clients might give any URL for the "View Screenshot" button including `foodle.com/user/set-password?pwd=pwned`, which uses existing session cookies for authentication, to change Maurice's password for Foodle.
- ☐ Cross-site request forgery; because malicious media servers might include JavaScript in the displayed webpage to hijack Maurice's Foodle tab and drop him from his courses.

Question 7 : Malware

You receive an envelope which contains a USB flash drive and a note "Connect it to a computer and open the files". Which of the following is the best way to minimize the risks caused by malware that could be on the flash drive?

- ☐ Connect the flash drive to two computers connected to the Internet such that you can compare the effect of opening the files to learn if there is malware.
- ☐ Connect the flash drive to a computer disconnected from the Internet, open the files in a sandbox and scan for any virus using a signature-based antivirus program. If there is no matched signature, connect the computer to the Internet, re-attach the flash drive, and open the files outside the sandbox.
- ☐ Connect the flash drive to a new computer that is still in factory state and not connected to the Internet or other devices, and open the files.
- ☐ Connect the flash drive to a computer connected to the Internet that has just been updated to install the latest patches for all installed programs, and open the files.

Question 8 : Network Security
Which of the following statements is true?

- ☐ If a user visits “vaud.ch” through a VPN, they are more likely to be able to access the page during a Denial of Service attack targeted against the “vaud.ch” server than users not using a VPN.
- ☐ The establishment of session keys using the Diffie-Hellman protocol does not prevent man-in-the-middle attacks.
- ☐ A stateful firewall can block HTTPS packets based on its payload.
- ☐ Using static hard-coded ARP tables stored on the communicating devices to determine mappings from MAC to IP addresses does not defend against ARP spoofing.

Second Part: Open Questions

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

Cryptography: Star Wars *[2 points]*

Baby Yoda and Obi Wan want to play the "yes or no" game: Obi Wan asks a question, and Baby Yoda must answer yes or no. For example, Obi Wan would ask "Are you really 50 years old?" and Baby Yoda would answer "Yes". Since Baby Yoda does not want any third party to learn his age or any potentially sensitive information Obi Wan may ask about, they decide to use encryption.
While Obi Wan's questions are sent in clear, Baby Yoda encrypts his answers using Obi Wan's public encryption key. Baby Yoda additionally uses a signature scheme to sign his answers with his private signature key. The protocol for one question works as follows:

```
Obi Wan -- (''Are you really 50 years old?'')  --> Baby Yoda
Obi Wan <-- (Enc(''Yes'', pk_ow), Sig(''Yes'', sk_by)) -- Baby Yoda
```

Note: Assume that both the signature scheme `Sig(message, secret_key)` *and the encryption scheme* `Enc(message, public_key)` *do not have vulnerabilities (example: the encryption scheme is non-deterministic, and it is not possible to forge a signature without the secret key); and that Baby Yoda and Obi Wan have made their public keys available to everyone on a public bulletin board.*

Question 9

How could an adversary eavesdropping on the conversation recover Baby Yoda's plaintext answers? *[1 point]*

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

.....

.....

.....

Question 10

Can the adversary that has recovered Baby Yoda's plaintext answers ("Yes"/"No") use this information to recover any of the secret keys, i.e., `sk_by` or `sk_ob`? If yes, explain how. If not, explain why not. *[1 point]*

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

.....

.....

.....

Web Security: Quizzle *[3 points]*

Mario and Luigi need to take a web security exam on "Quizzle" to graduate. They must take the exam in a computer lab from the university, but can use their own laptop. Luigi didn't study well. Mario, who knows Quizzle's source code from an internship, offered to cheat and impersonate Luigi.
Quizzle has the following security mechanisms:

(a) **CSRF protection:** Quizzle keeps a database table called *csrfs*. Each row contains a `csrf_token` and `started_at` (date/time when the student started the exam). The `csrf_token` is embedded in the student's webpage as a **hidden text box** (not visible to the user). The `csrf_token` is refreshed by Quizzle every time the student moves to a different question, or reloads the page.

(b) **Session Cookie:** Quizzle keeps a database table called *sessions*. Each row contains a student `student_id` (the CAMIPRO number), and a `session_id`, generated when a logged-in student enters the exam webpage to add their answers. The `session_id` is stored as a cookie in the student's browser. The `session_id` is generated only once and does not change throughout the exam.

Every time the student writes an answer, their browser sends to the Quizzle server a request containing the question ID, the answer, the CSRF token, and the `session_id` cookie to Quizzle. After validating the request, Quizzle stores the answer in an answers database table in the row containing the student ID and question ID.

Quizzle uses the following code to process the request:

```
1  def save_answer(csrf_token, session_id, question_id, answer):
2
3      # check that the csrf token exists
4      started_at = sql.read(f"SELECT started_at FROM csrfs
5                              WHERE csrf_token = '{csrf_token}'")
6
7      # if started_at is None -> the csrf_token does not exist
8      if started_at is None:
9          return {"student": None, "is_success": False}
10
11     # check the session cookie exists
12     student_id = sql.read(f"SELECT student_id FROM sessions
13                              WHERE session_id = '{session_id}'")
14
15     # if student_id is none, the session does not exist
16     if student_id is None:
17         return {"student": None, "is_success": False}
18
19     # store answer and check if saved correctly
20     db_answer = sql.write(
21     f"  UPDATE answers SET answer='{answer}'
22           WHERE student_id = '{student_id}'
23           AND question_id = '{question_id}';
24         SELECT answer FROM answers
25           WHERE student_id = '{student_id}'
26           AND question_id = '{question_id}'
27        ")
28
29     if db_answer != answer:
30         # some error in saving happened. Ideally
31         # it should never happen
32     return {"student": student_id, "is_success": False}
33
34     # return the response
35     return {"student": student_id", "is_success": True}
```

Notes:

- Prior to the exam, we assume that the login of students to Quizzle is secure. i.e. before accessing the course page, and arriving at the "start exam" button.
- All communications between Quizzle and students happen through TLS.

- `sql.read` does not allow to alter the database tables.
- `sql.write` allows to change the database tables.
- We assume that the answers table is pre-filled with empty answers for all students and questions.

Relevant information about SQL query syntax:

- `SQL SELECT`: returns a list of values chosen FROM the table WHERE the conditions mentioned apply. For our purposes, if only one value exist, it is returned directly (not in a list).
- `SQL UPDATE`: Updates the table by SETTING a value WHERE the conditions mentioned apply. The command returns nothing.
- We can concatenate multiple independent SQL queries with a semicolon (`;`), e.g. lines 21-26. Only the result of the last query is returned. This is useful to do multiple operations at once.

Question 11

Point out a vulnerability in the `save_answer` function that can be exploited by a student. Describe a defence against it. *[1 point]*

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

.....

.....

.....

Question 12

Describe why we need both a `csrf_token` and a session cookie? Are the checks in `save_answer` sufficient to guarantee only authorized students interacts with Quizzle? If not, suggest a change to the system. *[1 point]*

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

.....

.....

.....

.....

Question 13

Given your answers above, construct an attack that allows Mario to impersonate Luigi from his opened exam page using only a script he injects at the start of Mario's exam. (i.e. without opening another browser tab). *[1 point]*

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

.....

.....

.....

.....

.....

Network Security: FELP *[3 points]*

Alice and Bob work at FELP Research Institute on similar topics and their offices are in the same building. Bob is very jealous of Alice's great publications and tries to get access to Alice's internet traffic in order to observe her research progress. They use the same institutional Wi-Fi network, protected with WPA2 password authentication (the `password` is known both to Bob and Alice).

Question 14

Propose a man-in-the-middle attack which Bob can do in order to read Alice's traffic. How can Alice detect this attack? Justify your answer. *[1 point]*

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

.....

.....

.....

.....

Bob notices that Alice visits VCRP 2024 conference website `https://openreview.net/vcrp2024`, and since he wants to submit a paper to the same conference, he decides to prevent Alice from publishing.

Question 15

Is it possible to mislead Alice by informing her about the "new deadline" on a tempered conference webpage? (information about the deadlines is stored in `https://openreview.net/vcrp2024/index.html`, which is available publicly without user authentication). If not possible, explain why. If possible, describe the attack. *[1 point]*

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

.....

.....

.....

.....

Question 16

Is it possible to block Alice's access to the conference webpage from the Wi-Fi network? If not possible, explain why. If possible, describe the attack. *[1 point]*

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

.....

.....

.....

.....

Privacy: P2PM *[2 points]*

George, a British exchange student at the University of Prague, wants to send a message to Franz, another student at the university, that lives in the same student dormitory as George. George and Franz have installed P2PM, a peer-to-peer messaging application that allows them to send messages to each other without an intermediary server. To increase privacy, they configure P2PM to send messages over the Tor network.

Question 17

Agree or disagree with the following statement. Justify your answer. *[1 point]*
Statement: If the Tor path that George's Tor client selects goes through onion routers in Poland, Slovakia, and then Austria, the internet service provider of George's student dormitory cannot learn whether George is sending messages to Franz.

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

.....

.....

.....

.....

Question 18

After his return to Britain, George wants to keep in touch with Franz and sends him another message via P2PM-over-Tor. Agree or disagree with the following statement. Justify your answer. *[1 point]*
Statement: If the path that George's Tor client selects from George in Britain to Franz in the Czech Republic goes through onion routers in Belgium, France, and then Germany, an internet service provider in Russia cannot execute a successful attack to observe that George is sending a message to Franz.

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

.....

.....

.....

.....

Software Security: Token Server *[2 points]*

You are adding a new COM-301 programming assignment called "hw7". For that purpose, you implement a token generator program.

The intended functionality of this program is to generate a token for each student. The token is generated using a seed (which is computed from a hash of the student's unique SCIPER and the assignment ID) and a secret key (which is only known to the grading server). If students get access to this key, they would be able to compute the token of any of the course assignments without doing them.

The code on the next page implements the token generator (omitting code parts irrelevant to the question)

```
char part_token[8], seed[8], key[24];
char output[32];
int index_number;
bool correct_SCIPER_registered = false;
bool submit_assignmentID_in_time = false;
bool no_plagiarism = false;

void checks(char SCIPER_to_check[6], char assignmentID_to_check[3]){
    // this function reads a database of submission records and runs three checks
    // 1. if the input SCIPER is on the list of registered COM-301 students, set correct_SCIPER_registered = true;
    // 2. if the assignment is submitted in time, set submit_assignmentID_in_time = true;
    // 3. if there is no plagiarism detected for this student, set no_plagiarism = true;
    ...
}

void get_seed_and_key(char SCIPER[6], char assignmentID[3]){
    // this function computes a seed for an assignment of a student and  reads a secret key from the grading server
    // the seed is computed by taking 8 chars from hash(SCIPER+assignmentID)
    // after running this function, the seed and the key are stored in output[32]
    ...
}
void generate_token_per_part(char seed[8], char key[24], char part_token[8]){
    // generate a part of the token and store in part_token[8]
    ...
}
void reseed(char SCIPER[6], char assignmentID[3]){
    get_seed_and_key(SCIPER, assignmentID); // obtain seed and the key and store in output[32]
    memcpy(seed, output, 8); // copy the first 8 bytes of output[32] into seed[8]
    index_number = 8;
    memcpy(key, &output[index_number], 24); // copy the next 24 bytes of output[32] into key[24]
    index_number = 32;
}
void generate_token(char SCIPER[6], char assignmentID[3]){
    index_number = 0;
    reseed(SCIPER, assignmentID);
    // generate a token part-by-part using the same seed and key, then concatenate all parts to form the complete token
    for (; index_number <= 31; index_number += 8){
        generate_token_per_part(seed, key, part_token);
        memcpy(&output[index_number], part_token, 8); // copy the generated part_token [8] to output[32]
    }
    printf("Here is the token just generated:\n");
    printf("%.32s\n", output);
}
int main(int argc, char* argv[]) {
    if (argc != 3){
        printf("The number of arguments is wrong! You must pass the student's SCIPER and assignment ID!");
        return -1;
    }
    checks(argv[1], argv[2]);
    if (correct_SCIPER_registered && submit_assignmentID_in_time && no_plagiarism){
        generate_token(argv[1], argv[2]);
    }else{
        printf("Checks failed! No token!");
        return -1;
    }
    return 0;
}
```

Question 19

Since grading is a very sensitive task, you want to test your program.You decide to run a fuzzer on the main function. However, you find that the fuzzer explores a very limited part of the program, even though it has been running for quite some time. Explain why this is the case, and justify your explanation with an example between line 44 and line 57. *[1 point]*

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

.....

.....

.....

.....

Question 20

To test the functionality of the infrastructure for this new assignment, you register yourself as a student, finish the programming assignment, and get a token `"66a908f9HEUpl8RLBtK65Q2oGxFAOjKe"`. Suddenly you realise that students can extract the key from just looking at this token! What is the key? And why using a fuzzer does not help you identify this unwanted incident? *[1 point]*

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

.....

.....

.....

.....

Authentication and Access Control: Startstuff *[2 points]*

The start-up Startstuff has experienced a series of unauthorised accesses to secret documents about unlaunched products. Startstuff learns that these documents were leaked to competing companies, who launched the products before them.

Startstuff uses the Bell-LaPadula (BLP) model with clearance levels: TOP SECRET > CLASSIFIED > PUBLIC to ensure confidentiality. Documents requiring high secrecy (such as documents about unlaunched products) are only accessible to employees with TOP SECRET clearance.

The leaked documents could only be accessed through a script `access_script.sh` which is a TOP SECRET level file in the BLP model. `access_script.sh` can only be executed by employees with TOP SECRET clearance and is executed as follows:

`access_script.sh` *<DOCUMENT_NAME> <OPERATION>*

where *DOCUMENT_NAME* specifies the name of the document and *OPERATION* specifies either READ or WRITE operations on an existing document. The script returns an error if (i) the *DOCUMENT_NAME* or *OPERATION* is invalid, or (ii) the employee trying to execute the script does not have TOP SECRET clearance. Assume there is no declassification of documents.

Startstuff discovers that the documents about unlaunched products were leaked to their competitors by an employee with PUBLIC clearance.

Question 21

Describe an attack in which a TOP SECRET clearance employee leaked the documents about unlaunched products to the PUBLIC clearance employee using a covert channel. Clearly describe the covert channel and justify why this channel is covert. *[1 point]*

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

.....

.....

.....

.....

Question 22

Describe an attack in which the malicious PUBLIC clearance employee directly gained access to the TOP SECRET documents about unlaunched products without the involvement of a TOP SECRET clearance employee. *[1 point]*

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

.....

.....

.....

.....

+2/1/43+

EPFL

2

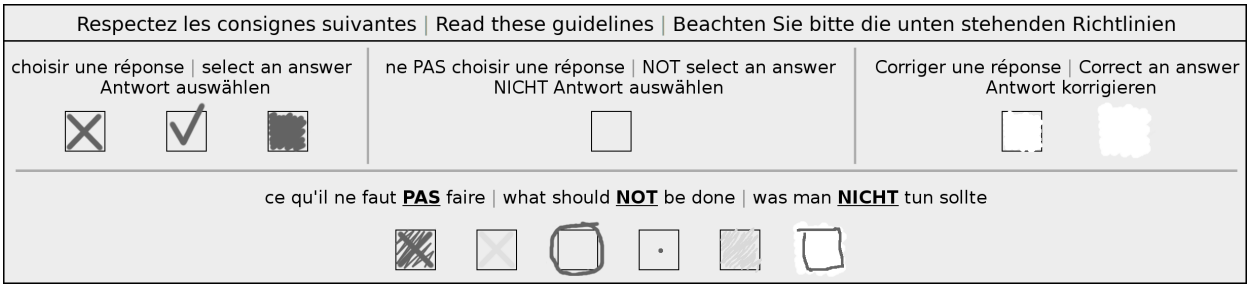
Ens: Prof. Carmela Troncoso
COM-301 - Final Exam - MT
01.02.2024
3 hours

Student 2

SCIPER : **999001**

Do not turn the page before the start of the exam. This document is double-sided, has 5 pages, the last ones possibly blank. Do not unstaple.

- Place your student card on your table.
- Students can only have **two A4 handwritten cheatsheets 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.
- For the **multiple choice** questions, there is only **one** correct answer:
  - +1 point if your answer is correct,
  - 0 points if you give no answer or the answer is invalid (see below). We consider more than one answer as invalid,
  - −0.25 points if your answer is incorrect.
- 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**. 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.



First part: Multiple Choice Questions

For each question, mark the box corresponding to the correct answer (see the cover page for correct marking). Invalid marking will not be counted. Each question has **exactly one** correct answer.

Question 1 : Authentication
Assume Barbie and Ken have established a secure TLS connection. They use this connection for the following authentication exchange in which Barbie uses her password `'Il0veP1nk'` to prove her identity to Ken:

```
Barbie -- (Barbie, 'I want to login') --> Ken
Barbie <-- Hash(Ken) -- Ken
Barbie -- Enc('Il0veP1nk'|Hash(Ken), k) --> Ken
```

- `Hash()` is a secure cryptographic hash function that is second pre-image resistant.
- `str1|str2` is the concatenation of two strings `str1` and `str2`.
- `Enc(m,k)` is the symmetric encryption of message m with key k that Barbie and Ken have securely exchanged before.
- `'-->'` indicates communication via the secure TLS connection.

Which of the following statements is correct?

- ☐ This authentication exchange is not secure against replay attacks because `Hash(Ken)` is not collision resistant.
- ☐ This authentication exchange is secure against replay attacks because `Hash(Ken)` is second pre-image resistant.
- ☐ This authentication exchange is not secure against replay attacks because Barbie has chosen a weak password that is easily guessable.
- ☐ This authentication exchange is secure against replay attacks because Barbie and Ken use a secure TLS channel.

Question 2 : Network
A professor decides that the final exams of their course must be taken online. To ensure fairness, all students must sit in the same classroom during the exam and connect to the server hosting the exam questions using the classroom LAN. The teaching team creates a website with the exam questions and hosts it on the only lab server with IP `107.18.90.101` that all students in the course have interacted with in the past. The teaching team hears that some lazy students who have not studied want to stop the exam from happening through a denial of service (DoS) attack. To reduce the risk of a successful DoS attack, the teaching team keeps the domain name of the exam hidden until the start of the exam.

Which of the following statements is incorrect?

- ☐ Keeping the domain name secret cannot prevent the lazy students from launching a Denial of Service attack on the classroom LAN gateway.
- ☐ Keeping the domain name secret prevents the lazy students from launching a DNS hijacking-based Denial of Service attack.
- ☐ Keeping the domain name secret prevents the lazy students from launching a DNS poisoning-based Denial of Service attack.
- ☐ Keeping the domain name secret cannot prevent the lazy students from using a ping message with a spoofed origin IP address to launch a distributed Denial of Service attack.

Question 3 : Cryptography
During the TLS handshake, the client can propose to the server two methods to decide on the session key k that will be used for encryption:

(a) **Key transport** in which the client will generate a fresh symmetric session key k and send it to the server encrypted with the server's public key pk. Thus, only the server can decrypt the session key with the server's secret key sk. The session key k is deleted at the end of the session.

(b) **Key exchange** in which client and server will exchange cryptographic material to derive a fresh symmetric session key k only known to them to be used during the session. The session key k is deleted at the end of the session.

- k is a symmetric session key known to both sender and client
- pk is the public key of the server known to everyone
- sk is the secret key of the server known only to the server

Which of the following statements is correct?

☐ None of the options provide forward secrecy because the session key k is deleted at the end of the session.

☐ Both options provide forward secrecy because in both cases the session key k is freshly generated at the start of each session.

☐ Only key transport provides forward secrecy because only the server knows sk that enables to decrypt the session key k.

☐ Only key exchange provides forward secrecy because there is no long-term secret involved in the process to decide on the session key k.

Question 4 : Software
Oppenheimer's team wrote a program that can answer queries about statistics on the atomic bombs in storage, e.g., how many atomic bombs are currently in status `'ready to launch'`. The members of the Oppenheimer team ask queries to this program from the lab computer. The team worries that if one of the team members is a spy they could exploit potential bugs in the program to perform a code injection attack to maliciously trigger the launch of a bomb from the lab computer.

Which mitigation guarantees that such an attack cannot be launched?

☐ Use mutation-based fuzzing on the program before loading it to the lab computer.

☐ Implement data execution prevention through the X^W policy on the lab computer.

☐ Add a canary to the stack of the lab computer.

☐ Implement address space layout randomization at the OS level on the lab computer.

Question 5 : Access Control
Which of the following statements is correct?

☐ In role-based access control, increasing the number of roles of a principal can never reduce the number of permissions of this principal.

☐ BIBA's goal of maintaining integrity is consistent with ensuring that information from low clearance levels is available to authorised users with high clearance.

☐ Encrypting part of a message so that the ciphertext can only be decrypted by the intended receiver is an example of a covert channel.

☐ Capabilities are more efficient than access control lists to remove access rights to a particular object.

Question 6 : Web Security

Maurice uses a browser on his personal computer to answer complaints from clients. On the complaints website `bigCorp.org/complaints`, each complaint is reachable at `bigCorp.org/complaints/<complaint-id>` and contains a description text box and a button "View Screenshot". This button redirects Maurice to a **media server** chosen by the writer of the complaint that hosts an image of the problem that they encountered. The URL of this image is not visible on the complaints webpage.
Maurice uses the same web browser to fill out assignments on Foodle, and chat on FreeChat.com. Both Foodle and FreeChat use a session cookie stored in the browser for authentication.

Given his setup and the actions he has to perform to review complaints, which of the following attacks is Maurice vulnerable to?

- ☐ Cross-site scripting; because when returning a webpage to Maurice, the media servers might have `src` URLs that trigger malicious server-side scripts to track him.
- ☐ Cross-site scripting; because malicious media servers might add JavaScript code to the "FreeChat.com" tab to send messages to Maurice's friends using the existing session cookie.
- ☐ Cross-site request forgery; because clients might give any URL for the "View Screenshot" button including `foodle.com/user/set-password?pwd=pwned`, which uses existing session cookies for authentication, to change Maurice's password for Foodle.
- ☐ Cross-site request forgery; because malicious media servers might include JavaScript in the displayed webpage to hijack Maurice's Foodle tab and drop him from his courses.

Question 7 : Malware

You receive an envelope which contains a USB flash drive and a note "Connect it to a computer and open the files". Which of the following is the best way to minimize the risks caused by malware that could be on the flash drive?

- ☐ Connect the flash drive to two computers connected to the Internet such that you can compare the effect of opening the files to learn if there is malware.
- ☐ Connect the flash drive to a new computer that is still in factory state and not connected to the Internet or other devices, and open the files.
- ☐ Connect the flash drive to a computer disconnected from the Internet, open the files in a sandbox and scan for any virus using a signature-based antivirus program. If there is no matched signature, connect the computer to the Internet, re-attach the flash drive, and open the files outside the sandbox.
- ☐ Connect the flash drive to a computer connected to the Internet that has just been updated to install the latest patches for all installed programs, and open the files.

Question 8 : Network Security
Which of the following statements is true?

- ☐ Using static hard-coded ARP tables stored on the communicating devices to determine mappings from MAC to IP addresses does not defend against ARP spoofing.
- ☐ The establishment of session keys using the Diffie-Hellman protocol does not prevent man-in-the-middle attacks.
- ☐ If a user visits "vaud.ch" through a VPN, they are more likely to be able to access the page during a Denial of Service attack targeted against the "vaud.ch" server than users not using a VPN.
- ☐ A stateful firewall can block HTTPS packets based on its payload.

Second Part: Open Questions

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

Cryptography: Star Wars *[2 points]*

Baby Yoda and Obi Wan want to play the "yes or no" game: Obi Wan asks a question, and Baby Yoda must answer yes or no. For example, Obi Wan would ask "Are you really 50 years old?" and Baby Yoda would answer "Yes". Since Baby Yoda does not want any third party to learn his age or any potentially sensitive information Obi Wan may ask about, they decide to use encryption.
While Obi Wan's questions are sent in clear, Baby Yoda encrypts his answers using Obi Wan's public encryption key. Baby Yoda additionally uses a signature scheme to sign his answers with his private signature key. The protocol for one question works as follows:

```
Obi Wan -- (''Are you really 50 years old?'')  --> Baby Yoda
Obi Wan <-- (Enc(''Yes'', pk_ow), Sig(''Yes'', sk_by)) -- Baby Yoda
```

Note: Assume that both the signature scheme `Sig(message, secret_key)` *and the encryption scheme* `Enc(message, public_key)` *do not have vulnerabilities (example: the encryption scheme is non-deterministic, and it is not possible to forge a signature without the secret key); and that Baby Yoda and Obi Wan have made their public keys available to everyone on a public bulletin board.*

Question 9

How could an adversary eavesdropping on the conversation recover Baby Yoda's plaintext answers? *[1 point]*

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

.....

.....

.....

Question 10

Can the adversary that has recovered Baby Yoda's plaintext answers ("Yes"/"No") use this information to recover any of the secret keys, i.e., `sk_by` or `sk_ob`? If yes, explain how. If not, explain why not. *[1 point]*

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

.....

.....

.....

Web Security: Quizzle *[3 points]*

Mario and Luigi need to take a web security exam on "Quizzle" to graduate. They must take the exam in a computer lab from the university, but can use their own laptop. Luigi didn't study well. Mario, who knows Quizzle's source code from an internship, offered to cheat and impersonate Luigi.
Quizzle has the following security mechanisms:

(a) **CSRF protection:** Quizzle keeps a database table called *csrfs*. Each row contains a `csrf_token` and `started_at` (date/time when the student started the exam). The `csrf_token` is embedded in the student's webpage as a **hidden text box** (not visible to the user). The `csrf_token` is refreshed by Quizzle every time the student moves to a different question, or reloads the page.

(b) **Session Cookie:** Quizzle keeps a database table called *sessions*. Each row contains a student `student_id` (the CAMIPRO number), and a `session_id`, generated when a logged-in student enters the exam webpage to add their answers. The `session_id` is stored as a cookie in the student's browser. The `session_id` is generated only once and does not change throughout the exam.

Every time the student writes an answer, their browser sends to the Quizzle server a request containing the question ID, the answer, the CSRF token, and the `session_id` cookie to Quizzle. After validating the request, Quizzle stores the answer in an answers database table in the row containing the student ID and question ID.

Quizzle uses the following code to process the request:

```
1  def save_answer(csrf_token, session_id, question_id, answer):
2
3      # check that the csrf token exists
4      started_at = sql.read(f"SELECT started_at FROM csrfs
5                              WHERE csrf_token = '{csrf_token}'")
6
7      # if started_at is None -> the csrf_token does not exist
8      if started_at is None:
9          return {"student": None, "is_success": False}
10
11     # check the session cookie exists
12     student_id = sql.read(f"SELECT student_id FROM sessions
13                              WHERE session_id = '{session_id}'")
14
15     # if student_id is none, the session does not exist
16     if student_id is None:
17         return {"student": None, "is_success": False}
18
19     # store answer and check if saved correctly
20     db_answer = sql.write(
21     f"  UPDATE answers SET answer='{answer}'
22           WHERE student_id = '{student_id}'
23           AND question_id = '{question_id}';
24         SELECT answer FROM answers
25           WHERE student_id = '{student_id}'
26           AND question_id = '{question_id}'
27        ")
28
29     if db_answer != answer:
30         # some error in saving happened. Ideally
31         # it should never happen
32     return {"student": student_id, "is_success": False}
33
34     # return the response
35     return {"student": student_id", "is_success": True}
```

Notes:

- Prior to the exam, we assume that the login of students to Quizzle is secure. i.e. before accessing the course page, and arriving at the "start exam" button.
- All communications between Quizzle and students happen through TLS.

- `sql.read` does not allow to alter the database tables.
- `sql.write` allows to change the database tables.
- We assume that the answers table is pre-filled with empty answers for all students and questions.

Relevant information about SQL query syntax:

- `SQL SELECT`: returns a list of values chosen FROM the table WHERE the conditions mentioned apply. For our purposes, if only one value exist, it is returned directly (not in a list).
- `SQL UPDATE`: Updates the table by SETTING a value WHERE the conditions mentioned apply. The command returns nothing.
- We can concatenate multiple independent SQL queries with a semicolon (`;`), e.g. lines 21-26. Only the result of the last query is returned. This is useful to do multiple operations at once.

Question 11

Point out a vulnerability in the `save_answer` function that can be exploited by a student. Describe a defence against it. *[1 point]*

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

.....

.....

.....

Question 12

Describe why we need both a `csrf_token` and a session cookie? Are the checks in `save_answer` sufficient to guarantee only authorized students interacts with Quizzle? If not, suggest a change to the system. *[1 point]*

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

.....

.....

.....

.....

Question 13

Given your answers above, construct an attack that allows Mario to impersonate Luigi from his opened exam page using only a script he injects at the start of Mario's exam. (i.e. without opening another browser tab). *[1 point]*

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

.....

.....

.....

.....

.....

Network Security: FELP *[3 points]*

Alice and Bob work at FELP Research Institute on similar topics and their offices are in the same building. Bob is very jealous of Alice's great publications and tries to get access to Alice's internet traffic in order to observe her research progress. They use the same institutional Wi-Fi network, protected with WPA2 password authentication (the `password` is known both to Bob and Alice).

Question 14

Propose a man-in-the-middle attack which Bob can do in order to read Alice's traffic. How can Alice detect this attack? Justify your answer. *[1 point]*

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

.....

.....

.....

.....

Bob notices that Alice visits VCRP 2024 conference website `https://openreview.net/vcrp2024`, and since he wants to submit a paper to the same conference, he decides to prevent Alice from publishing.

Question 15

Is it possible to mislead Alice by informing her about the "new deadline" on a tempered conference webpage? (information about the deadlines is stored in `https://openreview.net/vcrp2024/index.html`, which is available publicly without user authentication). If not possible, explain why. If possible, describe the attack. *[1 point]*

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

.....

.....

.....

.....

Question 16

Is it possible to block Alice's access to the conference webpage from the Wi-Fi network? If not possible, explain why. If possible, describe the attack. *[1 point]*

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

.....

.....

.....

.....

Privacy: P2PM *[2 points]*

George, a British exchange student at the University of Prague, wants to send a message to Franz, another student at the university, that lives in the same student dormitory as George. George and Franz have installed P2PM, a peer-to-peer messaging application that allows them to send messages to each other without an intermediary server. To increase privacy, they configure P2PM to send messages over the Tor network.

Question 17

Agree or disagree with the following statement. Justify your answer. *[1 point]*
Statement: If the Tor path that George's Tor client selects goes through onion routers in Poland, Slovakia, and then Austria, the internet service provider of George's student dormitory cannot learn whether George is sending messages to Franz.

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

.....

.....

.....

.....

Question 18

After his return to Britain, George wants to keep in touch with Franz and sends him another message via P2PM-over-Tor. Agree or disagree with the following statement. Justify your answer. *[1 point]*
Statement: If the path that George's Tor client selects from George in Britain to Franz in the Czech Republic goes through onion routers in Belgium, France, and then Germany, an internet service provider in Russia cannot execute a successful attack to observe that George is sending a message to Franz.

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

.....

.....

.....

.....

Software Security: Token Server *[2 points]*

You are adding a new COM-301 programming assignment called "hw7". For that purpose, you implement a token generator program.

The intended functionality of this program is to generate a token for each student. The token is generated using a seed (which is computed from a hash of the student's unique SCIPER and the assignment ID) and a secret key (which is only known to the grading server). If students get access to this key, they would be able to compute the token of any of the course assignments without doing them.

The code on the next page implements the token generator (omitting code parts irrelevant to the question)

```
char part_token[8], seed[8], key[24];
char output[32];
int index_number;
bool correct_SCIPER_registered = false;
bool submit_assignmentID_in_time = false;
bool no_plagiarism = false;

void checks(char SCIPER_to_check[6], char assignmentID_to_check[3]){
    // this function reads a database of submission records and runs three checks
    // 1. if the input SCIPER is on the list of registered COM-301 students, set correct_SCIPER_registered = true;
    // 2. if the assignment is submitted in time, set submit_assignmentID_in_time = true;
    // 3. if there is no plagiarism detected for this student, set no_plagiarism = true;
    ...
}

void get_seed_and_key(char SCIPER[6], char assignmentID[3]){
    // this function computes a seed for an assignment of a student and  reads a secret key from the grading server
    // the seed is computed by taking 8 chars from hash(SCIPER+assignmentID)
    // after running this function, the seed and the key are stored in output[32]
    ...
}
void generate_token_per_part(char seed[8], char key[24], char part_token[8]){
    // generate a part of the token and store in part_token[8]
    ...
}
void reseed(char SCIPER[6], char assignmentID[3]){
    get_seed_and_key(SCIPER, assignmentID); // obtain seed and the key and store in output[32]
    memcpy(seed, output, 8); // copy the first 8 bytes of output[32] into seed[8]
    index_number = 8;
    memcpy(key, &output[index_number], 24); // copy the next 24 bytes of output[32] into key[24]
    index_number = 32;
}
void generate_token(char SCIPER[6], char assignmentID[3]){
    index_number = 0;
    reseed(SCIPER, assignmentID);
    // generate a token part-by-part using the same seed and key, then concatenate all parts to form the complete token
    for (; index_number <= 31; index_number += 8){
        generate_token_per_part(seed, key, part_token);
        memcpy(&output[index_number], part_token, 8); // copy the generated part_token [8] to output[32]
    }
    printf("Here is the token just generated:\n");
    printf("%.32s\n", output);
}
int main(int argc, char* argv[]) {
    if (argc != 3){
        printf("The number of arguments is wrong! You must pass the student's SCIPER and assignment ID!");
        return -1;
    }
    checks(argv[1], argv[2]);
    if (correct_SCIPER_registered && submit_assignmentID_in_time && no_plagiarism){
        generate_token(argv[1], argv[2]);
    }else{
        printf("Checks failed! No token!");
        return -1;
    }
    return 0;
}
```

Question 19

Since grading is a very sensitive task, you want to test your program.You decide to run a fuzzer on the main function. However, you find that the fuzzer explores a very limited part of the program, even though it has been running for quite some time. Explain why this is the case, and justify your explanation with an example between line 44 and line 57. *[1 point]*

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

.....

.....

.....

.....

Question 20

To test the functionality of the infrastructure for this new assignment, you register yourself as a student, finish the programming assignment, and get a token `"66a908f9HEUpl8RLBtK65Q2oGxFAOjKe"`. Suddenly you realise that students can extract the key from just looking at this token! What is the key? And why using a fuzzer does not help you identify this unwanted incident? *[1 point]*

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

.....

.....

.....

.....

Authentication and Access Control: Startstuff *[2 points]*

The start-up Startstuff has experienced a series of unauthorised accesses to secret documents about unlaunched products. Startstuff learns that these documents were leaked to competing companies, who launched the products before them.

Startstuff uses the Bell-LaPadula (BLP) model with clearance levels: TOP SECRET > CLASSIFIED > PUBLIC to ensure confidentiality. Documents requiring high secrecy (such as documents about unlaunched products) are only accessible to employees with TOP SECRET clearance.

The leaked documents could only be accessed through a script `access_script.sh` which is a TOP SECRET level file in the BLP model. `access_script.sh` can only be executed by employees with TOP SECRET clearance and is executed as follows:

`access_script.sh` *<DOCUMENT_NAME> <OPERATION>*

where *DOCUMENT_NAME* specifies the name of the document and *OPERATION* specifies either READ or WRITE operations on an existing document. The script returns an error if (i) the *DOCUMENT_NAME* or *OPERATION* is invalid, or (ii) the employee trying to execute the script does not have TOP SECRET clearance. Assume there is no declassification of documents.

Startstuff discovers that the documents about unlaunched products were leaked to their competitors by an employee with PUBLIC clearance.

Question 21

Describe an attack in which a TOP SECRET clearance employee leaked the documents about unlaunched products to the PUBLIC clearance employee using a covert channel. Clearly describe the covert channel and justify why this channel is covert. *[1 point]*

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

.....

.....

.....

.....

Question 22

Describe an attack in which the malicious PUBLIC clearance employee directly gained access to the TOP SECRET documents about unlaunched products without the involvement of a TOP SECRET clearance employee. *[1 point]*

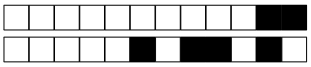
☐ **0** ☐ **0.25** ☐ **0.5** ☐ **0.75** ☐ **1** *Do not write here.*

.....

.....

.....

.....



+3/1/26+

EPFL

Ens: Prof. Carmela Troncoso
COM-301 - Final Exam - SV
01.02.2024
3 hours

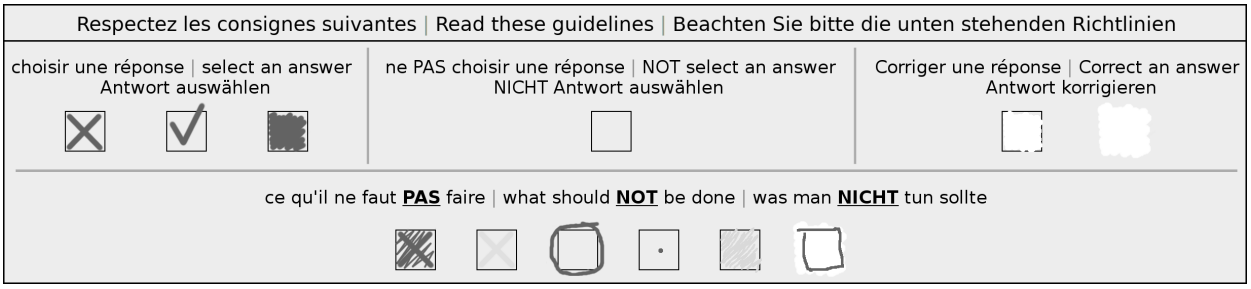
3

Student 3

SCIPER : **999002**

Do not turn the page before the start of the exam. This document is double-sided, has 5 pages, the last ones possibly blank. Do not unstaple.

- Place your student card on your table.
- Students can only have **two A4 handwritten cheatsheets 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.
- For the **multiple choice** questions, there is only **one** correct answer:
  - +1 point if your answer is correct,
  - 0 points if you give no answer or the answer is invalid (see below). We consider more than one answer as invalid,
  - −0.25 points if your answer is incorrect.
- 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**. 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.



First part: Multiple Choice Questions

For each question, mark the box corresponding to the correct answer (see the cover page for correct marking). Invalid marking will not be counted. Each question has **exactly one** correct answer.

Question 1 : Authentication
Assume Barbie and Ken have established a secure TLS connection. They use this connection for the following authentication exchange in which Barbie uses her password `'Il0veP1nk'` to prove her identity to Ken:

```
Barbie -- (Barbie, 'I want to login') --> Ken
Barbie <-- Hash(Ken) -- Ken
Barbie -- Enc('Il0veP1nk'|Hash(Ken), k) --> Ken
```

- `Hash()` is a secure cryptographic hash function that is second pre-image resistant.
- `str1|str2` is the concatenation of two strings `str1` and `str2`.
- `Enc(m,k)` is the symmetric encryption of message m with key k that Barbie and Ken have securely exchanged before.
- `'-->'` indicates communication via the secure TLS connection.

Which of the following statements is correct?

- ☐ This authentication exchange is not secure against replay attacks because Barbie has chosen a weak password that is easily guessable.
- ☐ This authentication exchange is secure against replay attacks because Barbie and Ken use a secure TLS channel.
- ☐ This authentication exchange is not secure against replay attacks because `Hash(Ken)` is not collision resistant.
- ☐ This authentication exchange is secure against replay attacks because `Hash(Ken)` is second pre-image resistant.

Question 2 : Network
A professor decides that the final exams of their course must be taken online. To ensure fairness, all students must sit in the same classroom during the exam and connect to the server hosting the exam questions using the classroom LAN. The teaching team creates a website with the exam questions and hosts it on the only lab server with IP `107.18.90.101` that all students in the course have interacted with in the past. The teaching team hears that some lazy students who have not studied want to stop the exam from happening through a denial of service (DoS) attack. To reduce the risk of a successful DoS attack, the teaching team keeps the domain name of the exam hidden until the start of the exam.

Which of the following statements is incorrect?

- ☐ Keeping the domain name secret cannot prevent the lazy students from using a ping message with a spoofed origin IP address to launch a distributed Denial of Service attack.
- ☐ Keeping the domain name secret prevents the lazy students from launching a DNS hijacking-based Denial of Service attack.
- ☐ Keeping the domain name secret cannot prevent the lazy students from launching a Denial of Service attack on the classroom LAN gateway.
- ☐ Keeping the domain name secret prevents the lazy students from launching a DNS poisoning-based Denial of Service attack.

Question 3 : Cryptography
During the TLS handshake, the client can propose to the server two methods to decide on the session key k that will be used for encryption:

(a) **Key transport** in which the client will generate a fresh symmetric session key k and send it to the server encrypted with the server's public key pk. Thus, only the server can decrypt the session key with the server's secret key sk. The session key k is deleted at the end of the session.

(b) **Key exchange** in which client and server will exchange cryptographic material to derive a fresh symmetric session key k only known to them to be used during the session. The session key k is deleted at the end of the session.

- k is a symmetric session key known to both sender and client
- pk is the public key of the server known to everyone
- sk is the secret key of the server known only to the server

Which of the following statements is correct?

☐ Only key transport provides forward secrecy because only the server knows sk that enables to decrypt the session key k.

☐ Both options provide forward secrecy because in both cases the session key k is freshly generated at the start of each session.

☐ Only key exchange provides forward secrecy because there is no long-term secret involved in the process to decide on the session key k.

☐ None of the options provide forward secrecy because the session key k is deleted at the end of the session.

Question 4 : Software
Oppenheimer's team wrote a program that can answer queries about statistics on the atomic bombs in storage, e.g., how many atomic bombs are currently in status `'ready to launch'`. The members of the Oppenheimer team ask queries to this program from the lab computer. The team worries that if one of the team members is a spy they could exploit potential bugs in the program to perform a code injection attack to maliciously trigger the launch of a bomb from the lab computer.

Which mitigation guarantees that such an attack cannot be launched?

☐ Use mutation-based fuzzing on the program before loading it to the lab computer.

☐ Add a canary to the stack of the lab computer.

☐ Implement data execution prevention through the X^W policy on the lab computer.

☐ Implement address space layout randomization at the OS level on the lab computer.

Question 5 : Access Control
Which of the following statements is correct?

☐ In role-based access control, increasing the number of roles of a principal can never reduce the number of permissions of this principal.

☐ Capabilities are more efficient than access control lists to remove access rights to a particular object.

☐ BIBA's goal of maintaining integrity is consistent with ensuring that information from low clearance levels is available to authorised users with high clearance.

☐ Encrypting part of a message so that the ciphertext can only be decrypted by the intended receiver is an example of a covert channel.

Question 6 : Web Security

Maurice uses a browser on his personal computer to answer complaints from clients. On the complaints website `bigCorp.org/complaints`, each complaint is reachable at `bigCorp.org/complaints/<complaint-id>` and contains a description text box and a button "View Screenshot". This button redirects Maurice to a **media server** chosen by the writer of the complaint that hosts an image of the problem that they encountered. The URL of this image is not visible on the complaints webpage.
Maurice uses the same web browser to fill out assignments on Foodle, and chat on FreeChat.com. Both Foodle and FreeChat use a session cookie stored in the browser for authentication.

Given his setup and the actions he has to perform to review complaints, which of the following attacks is Maurice vulnerable to?

- ☐ Cross-site scripting; because when returning a webpage to Maurice, the media servers might have `src` URLs that trigger malicious server-side scripts to track him.
- ☐ Cross-site scripting; because malicious media servers might add JavaScript code to the "FreeChat.com" tab to send messages to Maurice's friends using the existing session cookie.
- ☐ Cross-site request forgery; because clients might give any URL for the "View Screenshot" button including `foodle.com/user/set-password?pwd=pwned`, which uses existing session cookies for authentication, to change Maurice's password for Foodle.
- ☐ Cross-site request forgery; because malicious media servers might include JavaScript in the displayed webpage to hijack Maurice's Foodle tab and drop him from his courses.

Question 7 : Malware

You receive an envelope which contains a USB flash drive and a note "Connect it to a computer and open the files". Which of the following is the best way to minimize the risks caused by malware that could be on the flash drive?

- ☐ Connect the flash drive to two computers connected to the Internet such that you can compare the effect of opening the files to learn if there is malware.
- ☐ Connect the flash drive to a computer connected to the Internet that has just been updated to install the latest patches for all installed programs, and open the files.
- ☐ Connect the flash drive to a computer disconnected from the Internet, open the files in a sandbox and scan for any virus using a signature-based antivirus program. If there is no matched signature, connect the computer to the Internet, re-attach the flash drive, and open the files outside the sandbox.
- ☐ Connect the flash drive to a new computer that is still in factory state and not connected to the Internet or other devices, and open the files.

Question 8 : Network Security
Which of the following statements is true?

- ☐ A stateful firewall can block HTTPS packets based on its payload.
- ☐ Using static hard-coded ARP tables stored on the communicating devices to determine mappings from MAC to IP addresses does not defend against ARP spoofing.
- ☐ The establishment of session keys using the Diffie-Hellman protocol does not prevent man-in-the-middle attacks.
- ☐ If a user visits "vaud.ch" through a VPN, they are more likely to be able to access the page during a Denial of Service attack targeted against the "vaud.ch" server than users not using a VPN.

Second Part: Open Questions

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

Cryptography: Star Wars *[2 points]*

Baby Yoda and Obi Wan want to play the "yes or no" game: Obi Wan asks a question, and Baby Yoda must answer yes or no. For example, Obi Wan would ask "Are you really 50 years old?" and Baby Yoda would answer "Yes". Since Baby Yoda does not want any third party to learn his age or any potentially sensitive information Obi Wan may ask about, they decide to use encryption.
While Obi Wan's questions are sent in clear, Baby Yoda encrypts his answers using Obi Wan's public encryption key. Baby Yoda additionally uses a signature scheme to sign his answers with his private signature key. The protocol for one question works as follows:

```
Obi Wan -- (''Are you really 50 years old?'')  --> Baby Yoda
Obi Wan <-- (Enc(''Yes'', pk_ow), Sig(''Yes'', sk_by)) -- Baby Yoda
```

Note: Assume that both the signature scheme `Sig(message, secret_key)` *and the encryption scheme* `Enc(message, public_key)` *do not have vulnerabilities (example: the encryption scheme is non-deterministic, and it is not possible to forge a signature without the secret key); and that Baby Yoda and Obi Wan have made their public keys available to everyone on a public bulletin board.*

Question 9

How could an adversary eavesdropping on the conversation recover Baby Yoda's plaintext answers? *[1 point]*

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

.....

.....

.....

Question 10

Can the adversary that has recovered Baby Yoda's plaintext answers ("Yes"/"No") use this information to recover any of the secret keys, i.e., `sk_by` or `sk_ob`? If yes, explain how. If not, explain why not. *[1 point]*

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

.....

.....

.....

Web Security: Quizzle *[3 points]*

Mario and Luigi need to take a web security exam on "Quizzle" to graduate. They must take the exam in a computer lab from the university, but can use their own laptop. Luigi didn't study well. Mario, who knows Quizzle's source code from an internship, offered to cheat and impersonate Luigi.
Quizzle has the following security mechanisms:

(a) **CSRF protection:** Quizzle keeps a database table called *csrfs*. Each row contains a `csrf_token` and `started_at` (date/time when the student started the exam). The `csrf_token` is embedded in the student's webpage as a **hidden text box** (not visible to the user). The `csrf_token` is refreshed by Quizzle every time the student moves to a different question, or reloads the page.

(b) **Session Cookie:** Quizzle keeps a database table called *sessions*. Each row contains a student `student_id` (the CAMIPRO number), and a `session_id`, generated when a logged-in student enters the exam webpage to add their answers. The `session_id` is stored as a cookie in the student's browser. The `session_id` is generated only once and does not change throughout the exam.

Every time the student writes an answer, their browser sends to the Quizzle server a request containing the question ID, the answer, the CSRF token, and the `session_id` cookie to Quizzle. After validating the request, Quizzle stores the answer in an answers database table in the row containing the student ID and question ID.

Quizzle uses the following code to process the request:

```
1  def save_answer(csrf_token, session_id, question_id, answer):
2
3      # check that the csrf token exists
4      started_at = sql.read(f"SELECT started_at FROM csrfs
5                              WHERE csrf_token = '{csrf_token}'")
6
7      # if started_at is None -> the csrf_token does not exist
8      if started_at is None:
9          return {"student": None, "is_success": False}
10
11     # check the session cookie exists
12     student_id = sql.read(f"SELECT student_id FROM sessions
13                              WHERE session_id = '{session_id}'")
14
15     # if student_id is none, the session does not exist
16     if student_id is None:
17         return {"student": None, "is_success": False}
18
19     # store answer and check if saved correctly
20     db_answer = sql.write(
21     f"  UPDATE answers SET answer='{answer}'
22           WHERE student_id = '{student_id}'
23           AND question_id = '{question_id}';
24         SELECT answer FROM answers
25           WHERE student_id = '{student_id}'
26           AND question_id = '{question_id}'
27        ")
28
29     if db_answer != answer:
30         # some error in saving happened. Ideally
31         # it should never happen
32     return {"student": student_id, "is_success": False}
33
34     # return the response
35     return {"student": student_id", "is_success": True}
```

Notes:

- Prior to the exam, we assume that the login of students to Quizzle is secure. i.e. before accessing the course page, and arriving at the "start exam" button.
- All communications between Quizzle and students happen through TLS.

- `sql.read` does not allow to alter the database tables.
- `sql.write` allows to change the database tables.
- We assume that the answers table is pre-filled with empty answers for all students and questions.

Relevant information about SQL query syntax:

- `SQL SELECT`: returns a list of values chosen FROM the table WHERE the conditions mentioned apply. For our purposes, if only one value exist, it is returned directly (not in a list).
- `SQL UPDATE`: Updates the table by SETTING a value WHERE the conditions mentioned apply. The command returns nothing.
- We can concatenate multiple independent SQL queries with a semicolon (`;`), e.g. lines 21-26. Only the result of the last query is returned. This is useful to do multiple operations at once.

Question 11

Point out a vulnerability in the `save_answer` function that can be exploited by a student. Describe a defence against it. *[1 point]*

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

.....

.....

.....

Question 12

Describe why we need both a `csrf_token` and a session cookie? Are the checks in `save_answer` sufficient to guarantee only authorized students interacts with Quizzle? If not, suggest a change to the system. *[1 point]*

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

.....

.....

.....

.....

Question 13

Given your answers above, construct an attack that allows Mario to impersonate Luigi from his opened exam page using only a script he injects at the start of Mario's exam. (i.e. without opening another browser tab). *[1 point]*

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

.....

.....

.....

.....

.....

Network Security: FELP *[3 points]*

Alice and Bob work at FELP Research Institute on similar topics and their offices are in the same building. Bob is very jealous of Alice's great publications and tries to get access to Alice's internet traffic in order to observe her research progress. They use the same institutional Wi-Fi network, protected with WPA2 password authentication (the `password` is known both to Bob and Alice).

Question 14

Propose a man-in-the-middle attack which Bob can do in order to read Alice's traffic. How can Alice detect this attack? Justify your answer. *[1 point]*

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

.....

.....

.....

.....

Bob notices that Alice visits VCRP 2024 conference website `https://openreview.net/vcrp2024`, and since he wants to submit a paper to the same conference, he decides to prevent Alice from publishing.

Question 15

Is it possible to mislead Alice by informing her about the "new deadline" on a tempered conference webpage? (information about the deadlines is stored in `https://openreview.net/vcrp2024/index.html`, which is available publicly without user authentication). If not possible, explain why. If possible, describe the attack. *[1 point]*

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

.....

.....

.....

.....

Question 16

Is it possible to block Alice's access to the conference webpage from the Wi-Fi network? If not possible, explain why. If possible, describe the attack. *[1 point]*

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

.....

.....

.....

.....

Privacy: P2PM *[2 points]*

George, a British exchange student at the University of Prague, wants to send a message to Franz, another student at the university, that lives in the same student dormitory as George. George and Franz have installed P2PM, a peer-to-peer messaging application that allows them to send messages to each other without an intermediary server. To increase privacy, they configure P2PM to send messages over the Tor network.

Question 17

Agree or disagree with the following statement. Justify your answer. *[1 point]*
Statement: If the Tor path that George's Tor client selects goes through onion routers in Poland, Slovakia, and then Austria, the internet service provider of George's student dormitory cannot learn whether George is sending messages to Franz.

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

.....

.....

.....

.....

Question 18

After his return to Britain, George wants to keep in touch with Franz and sends him another message via P2PM-over-Tor. Agree or disagree with the following statement. Justify your answer. *[1 point]*
Statement: If the path that George's Tor client selects from George in Britain to Franz in the Czech Republic goes through onion routers in Belgium, France, and then Germany, an internet service provider in Russia cannot execute a successful attack to observe that George is sending a message to Franz.

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

.....

.....

.....

.....

Software Security: Token Server *[2 points]*

You are adding a new COM-301 programming assignment called "hw7". For that purpose, you implement a token generator program.

The intended functionality of this program is to generate a token for each student. The token is generated using a seed (which is computed from a hash of the student's unique SCIPER and the assignment ID) and a secret key (which is only known to the grading server). If students get access to this key, they would be able to compute the token of any of the course assignments without doing them.

The code on the next page implements the token generator (omitting code parts irrelevant to the question)

```
char part_token[8], seed[8], key[24];
char output[32];
int index_number;
bool correct_SCIPER_registered = false;
bool submit_assignmentID_in_time = false;
bool no_plagiarism = false;

void checks(char SCIPER_to_check[6], char assignmentID_to_check[3]){
    // this function reads a database of submission records and runs three checks
    // 1. if the input SCIPER is on the list of registered COM-301 students, set correct_SCIPER_registered = true;
    // 2. if the assignment is submitted in time, set submit_assignmentID_in_time = true;
    // 3. if there is no plagiarism detected for this student, set no_plagiarism = true;
    ...
}

void get_seed_and_key(char SCIPER[6], char assignmentID[3]){
    // this function computes a seed for an assignment of a student and  reads a secret key from the grading server
    // the seed is computed by taking 8 chars from hash(SCIPER+assignmentID)
    // after running this function, the seed and the key are stored in output[32]
    ...
}
void generate_token_per_part(char seed[8], char key[24], char part_token[8]){
    // generate a part of the token and store in part_token[8]
    ...
}
void reseed(char SCIPER[6], char assignmentID[3]){
    get_seed_and_key(SCIPER, assignmentID); // obtain seed and the key and store in output[32]
    memcpy(seed, output, 8); // copy the first 8 bytes of output[32] into seed[8]
    index_number = 8;
    memcpy(key, &output[index_number], 24); // copy the next 24 bytes of output[32] into key[24]
    index_number = 32;
}
void generate_token(char SCIPER[6], char assignmentID[3]){
    index_number = 0;
    reseed(SCIPER, assignmentID);
    // generate a token part-by-part using the same seed and key, then concatenate all  parts to form the complete token
    for (; index_number <= 31; index_number += 8){
        generate_token_per_part(seed, key, part_token);
        memcpy(&output[index_number], part_token, 8); // copy the generated part_token [8] to output[32]
    }
    printf("Here is the token just generated:\n");
    printf("%.32s\n", output);
}
int main(int argc, char* argv[]) {
    if (argc != 3){
        printf("The number of arguments is wrong! You must pass the student's SCIPER and assignment ID!");
        return -1;
    }
    checks(argv[1], argv[2]);
    if (correct_SCIPER_registered && submit_assignmentID_in_time && no_plagiarism){
        generate_token(argv[1], argv[2]);
    }else{
        printf("Checks failed! No token!");
        return -1;
    }
    return 0;
}
```

Question 19

Since grading is a very sensitive task, you want to test your program.You decide to run a fuzzer on the main function. However, you find that the fuzzer explores a very limited part of the program, even though it has been running for quite some time. Explain why this is the case, and justify your explanation with an example between line 44 and line 57. *[1 point]*

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

.....

.....

.....

.....

Question 20

To test the functionality of the infrastructure for this new assignment, you register yourself as a student, finish the programming assignment, and get a token `"66a908f9HEUpl8RLBtK65Q2oGxFAOjKe"`. Suddenly you realise that students can extract the key from just looking at this token! What is the key? And why using a fuzzer does not help you identify this unwanted incident? *[1 point]*

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

.....

.....

.....

.....

Authentication and Access Control: Startstuff *[2 points]*

The start-up Startstuff has experienced a series of unauthorised accesses to secret documents about unlaunched products. Startstuff learns that these documents were leaked to competing companies, who launched the products before them.

Startstuff uses the Bell-LaPadula (BLP) model with clearance levels: TOP SECRET > CLASSIFIED > PUBLIC to ensure confidentiality. Documents requiring high secrecy (such as documents about unlaunched products) are only accessible to employees with TOP SECRET clearance.

The leaked documents could only be accessed through a script `access_script.sh` which is a TOP SECRET level file in the BLP model. `access_script.sh` can only be executed by employees with TOP SECRET clearance and is executed as follows:

`access_script.sh` *<DOCUMENT_NAME> <OPERATION>*

where *DOCUMENT_NAME* specifies the name of the document and *OPERATION* specifies either READ or WRITE operations on an existing document. The script returns an error if (i) the *DOCUMENT_NAME* or *OPERATION* is invalid, or (ii) the employee trying to execute the script does not have TOP SECRET clearance. Assume there is no declassification of documents.

Startstuff discovers that the documents about unlaunched products were leaked to their competitors by an employee with PUBLIC clearance.

Question 21

Describe an attack in which a TOP SECRET clearance employee leaked the documents about unlaunched products to the PUBLIC clearance employee using a covert channel. Clearly describe the covert channel and justify why this channel is covert. *[1 point]*

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

.....

.....

.....

.....

Question 22

Describe an attack in which the malicious PUBLIC clearance employee directly gained access to the TOP SECRET documents about unlaunched products without the involvement of a TOP SECRET clearance employee. *[1 point]*

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

.....

.....

.....

.....