+1/1/60+

COM-301 Midterm #2

28 November 2019

Identification
Please encode your SCIPER on the right (one digit per column), and write your first and last name 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).
Books, calculators, phones, and laptops are **not** allowed during the exam.

Part 1: Multiple-choice questions
Mark the correct answer by *completely* filling in the corresponding square (■).
There is **only one** correct answer per question.
Each correct answer earns +1 point. Incorrect answers have a penalty of -0.5 points each. No answer neither adds nor subtracts points. Multiple marked answers are considered incorrect and will result in -0.5 points.
Use white-out fluid to change (delete) an answer (other deletions yield -0.5).
Read the answers carefully, the template may split the answers across columns.

Question 1 **[Network Security]** Border Gateway Protocol (BGP) hijacking is a suitable attack to:

- ☐ Redirect traffic by guessing sequence numbers
- ☐ Redirect traffic by changing correspondences between IP addresses and domain names
- ☐ Redirect traffic from machines within the same LAN as the victim
- ☐ Redirect traffic to routers under the adversary's control without being on the same network as the victim

Question 2 **[Attacks]** To do a cross site scripting attack it is essential that:

- ☐ Cookies hold authentication information
- ☐ It is possible to abuse the privileges of a confused deputy
- ☐ There is a web form to feed Javascript code to the server
- ☐ The input received by the server is not correctly sanitized

Question 3 **[Password security]** The goal of hashing algorithms designed to hash passwords is to:

- ☐ Slow down offline hash computations
- ☐ Increase pre-image resistance
- ☐ Increase collision resistance
- ☐ Prevent the hashing of passwords without a salt

Question 4 **[Authentication]** The token-based authentication mechanism seen in the class, which authenticate users using something that they have, require:

- ☐ That the token knows the public key of the verification server
- ☐ That both token and verification server use the same hash function
- ☐ That the token and the verification server share a key
- ☐ That tokens delete their key after each verification

Question 5 **[Software Security]** The main role of stack canaries is to:

- ☐ Prevent adversaries from writing on the stack
- ☐ Sanitize the return address of any function
- ☐ Detect unauthorized overwrites in the stack
- ☐ Avoid uncontrolled format strings

Question 6 **[Applied cryptography]** A MAC is a good choice to provide integrity:

- ☐ Only when the symmetric key is encrypted with a public key
- ☐ When conversation partners have a pre-shared symmetric key
- ☐ Only when the symmetric key is signed
- ☐ Any time a message is encrypted with a symmetric key

Question 7 **[Security Principles]** In order to access a football match, the supporters of New Team must authenticate to a server using their club card. The supporters of the rival team, Toho, know this and flood the server with authentication requests so that the server cannot handle New Team fans' authentication requests, and the New Team has to play without support. What security principle was not respected?

- ☐ Least common mechanism
- ☐ Least privilege
- ☐ Fail-safe defaults
- ☐ Open design

Question 8 **[Attacks]** Which of the following countermeasures is a good choice to avoid Cross Site Request Forgery attacks:

- ☐ Only authorize actions after the authentication step
- ☐ Sanitize the cookies before they are processed
- ☐ Not execute anything received from the user
- ☐ Verify the origin of the information

Part2: Short answer questions: Write your answer using *only* the lines provided. Anything beyond the specified number of lines will not be considered for grading. Answers are graded on a scale from 0 to 4.
Please mind your calligraphy; undecipherable responses will not be graded.

Question 9 **[Software Security]** Gru has written the code below to manage the bonuses of minions that participate in evil missions. This function receives an identifier for a minion and then prompts the minion to provide the name of the mission they participated in. Gru asks for your help debugging the function.
Identify two lines that contain unsafe code that may lead to a memory safety error. For those two lines i) explain the vulnerability, and ii) explain whether a Minion can exploit this vulnerability to increase their bonus even when their mission did not succeed.

Assume that Minions are good teammates and will never steal a bonus from another Minion by providing others' successful mission names.

```
int bonus[100] =  { 0 };                    /* array of 100 integers initialized to 0 */

char successDB(char* mission) {

    /* function that returns 0 for failed missions */
    /* and 1 for successful missions */
    /* if the mission does not exist, it crashes */

}

1: int AddMission(int minionID) {
2:      char success;                       /* mission name */
3:      char mission[30];                   /* one byte: 1 if mission succeeds, 0 otherwise */
4:
5:      gets(mission);                      /* reads mission name from keyboard */
6:      success = successDB(mission);       /* checks in the DB the success of the mission */
7:
8:      if (success == 1) { bonus[minionID] += 1 }; /* if mission succeeded, increase bonus */
9:
10:     return 0;
11: }
```

☐0 ☐1 ☐2 ☐3 ☐4

. . . . . .

. . . . . .

. . . . . .

. . . . . .

Question 10 **[Applied cryptography]** A group of security researchers traveling to Fakeland learn that, upon arrival at the airport, Fakeland's border authorities will require their laptops for inspection. Fakeland authorities are famous for installing spying software during the inspection, so the researchers decide to take a snapshot of the laptops' state to make sure that they can detect changes. For this purpose they plan to hash the content of the laptops' hard drive and write this hash on a paper. This way when they receive their laptops back, they can compute the hash of the content again and compare it to the value in their notes.

What property or properties must the hash function have in order to prove that no new software was installed (by comparing the hash on the piece of paper with the hash computed after crossing the border)? (Justify your answer)

☐0 ☐1 ☐2 ☐3 ☐4

.....

.....

.....

.....

Question 11 **[Biometrics]** Agree or disagree with the following statement and justify your answer: "When configuring biometrics to be used as an authentication function to secure access to students' exams grades, it is important that the system has a low false negative rate even if the system finds many false positives".

☐0 ☐1 ☐2 ☐3 ☐4

.....

.....

.....

.....

[Software security] The startup `NewHeaven` hires you to help them develop secure software.

Question 12 The main product at `NewHeaven` has roughly ten thousand line of code. Propose a technique that they can use to find as many vulnerabilities as possible. Explain how they should measure their success. (Justify your answer).

☐0 ☐1 ☐2 ☐3 ☐4

.....

.....

.....

.....

Question 13 The `NewHeaven` developers tell you that in their server, they sometimes need to execute code that is provided as a parameter in a function. But they tell you that this is safe because the server implements Data Execution Prevention. Is this correct? (Justify your answer).

☐0 ☐1 ☐2 ☐3 ☐4

.....

.....

.....

.....

[Network Security] The IT team at the EPFL library is worried because they have seen Malicious Student hanging around. They fear that Malicious is attacking other students' connections.
Agree or disagree with the following statements. Justify your answer. If Malicious Student can launch an attack or break a property, describe how.

Question 14 If students visit `com301.epfl.ch` obtaining the IP address of the server using DNSSEC and submit their homework to the server using HTTPS (HTTP over TLS), Malicious Student cannot know which page the students are visiting. ☐**0** ☐**1** ☐**2** ☐**3** ☐**4**

.....

.....

.....

.....

Question 15 The confidentiality of the students' homework is guaranteed if they obtain the IP address of the `com301.epfl.ch` server using DNSSEC and then submit their homework to the server using HTTP. ☐**0** ☐**1** ☐**2** ☐**3** ☐**4**

.....

.....

.....

.....

Question 16 If the server `com301.epfl.ch` is in the library's Local Area Network, and the students submit their homework using HTTP, then Malicious Student cannot launch a man in the middle attack. ☐**0** ☐**1** ☐**2** ☐**3** ☐**4**

. . . . . .

. . . . . .

. . . . . .

. . . . . .