

Question 1 For each of the following, cross either TRUE or FALSE

[30pts] [+2 per correct answer ; -1 per wrong answer]

See below how to respond to this question. Any other way of giving a response (including ambiguous marking) will be considered wrong. There won't be any objection for ambiguous marking; if you are in doubt ask a TA.

The question does not require justification, any justification will be disregarded.

TRUE	FALSE	Example topic: [10pts]
		Question that you want to leave unanswered
X		Question that you want to mark as TRUE.
	X	Question that you want to mark as FALSE.
	X	Question where you changed your opinion from TRUE to FALSE
X		Question where you changed your opinion from FALSE to TRUE
		Question where you changed your opinion and you want to leave unanswered

This means that you cannot change your mind 2 times. Please think twice before answering, there is plenty of time to do the exam.

TRUE	FALSE	Malware: [10pts]
	X	Eliminating buffer overflows would completely prevent the problem of Internet worms.
X		Viruses can spread to systems even if they have no Internet connectivity
	X	Some trojans add their code to that of existing executables residing on disk.
	X	If following the open design principle a developer publishes the source code of a program, we can be sure that its executable version will not have backdoors.
X		An advantage of anomaly detection over signature-based detection is the ability to potentially detect novel attacks.

Lastname:

Firstname:

SCIPER:

TRUE	FALSE	Cryptography and Authentication: [10pts]
	X	MACs use public-key cryptography to provide both integrity and non-repudiation.
	X	Computing a hash for an image using a cryptographic hash function such as SHA-256 requires possession of the correct secret key.
X		If we chain hash computations (e.g., $h = \text{Hash}(\text{Hash}(\text{Hash}(\text{message})))$) the value h is not more collision resistant than the $\text{Hash}()$ function itself.
	X	A block cipher in CBC mode is a good choice to encrypt a TV channel that is broadcasted live.
X		Computing the plaintext MAC and then encrypting the plaintext and MAC together (MAC-then-Encrypt) ensures that you can check the integrity of the plaintext.
TRUE	FALSE	Principles and basics: [10pts]
X		A vulnerability is a weakness that can be exploited by an adversary.
	X	Always assigning users the minimum permissions necessary is a good way of following the separation of privilege principle.
X		Having two security controls one after the other provides better security than using the security controls in parallel.
	X	Always assigning users the minimum permissions necessary is a good way of following the separation of privilege principle.
	X	The best idea to keep a system safe is check that no input is trying to do anything malicious before letting any function run.

Question 2: Circle the correct answer (only one!)

[40pts] [+5 per correct answer, -2 per wrong answer]

Only responses with one valid answer will be corrected!

☒ Selecting an answer

☐ Cancelling an answer

This means you can only change your mind once to cancel an answer. You cannot recover the answer. To leave a question unresponded either do not circle any option, or cancel all the answers. Ambiguous answers will be considered wrong. If in doubt, ask a TA.

Please think twice before answering, there is plenty of time to do the exam.

2.1 Memory safety - The following program:

```
void test( char *array, char *input) {  
    char buf[30];  
    input = array;  
    char *ptr = &buf[20];  
    ptr = ptr + 10;  
    printf("%s", input);  
    free(input);  
    *ptr = 30;  
}
```

- A) Contains a temporal memory safety bug
- ☒ B) Contains a spatial memory safety bug
- C) There is no bug, let's run it!
- D) Contains an uncontrolled format string

2.2 Insecure Interaction Between Components - Checking the origin of an HTTP request:

- A) Would defend from Cross-site scripting and Cross-site Request Forgery
- B) Would defend from Cross-site scripting but not Cross-site Request Forgery
- ☒ C) Would defend from Cross-site Request Forgery but not Cross-site scripting
- D) None of the two, this is not a sufficient countermeasure against any attacks

· Lastname:

Firstname:

SCIPER:

2.3 Security testing - Take the following code:

```
int example(bool b1, bool b2) {  
    int a = 1;  
    char c[2];  
    if (!b1) { a -= 1; }  
    if (b2) { a -= 1; }  
    return c[a];  
}
```

Using only one vector (false, true) as input is a good testing strategy because:
[Hint: note that the question asks about the strategy]

- A) It provides full branch coverage
- B) It provides full data coverage
- C) It is not a good strategy. Although it discovers the bug, it provides none of the above
- D) It discovers the bug

2.4 Trusted computing - Isolation is a property: TOPIC NOT ANYMORE IN THE COURSE

- ☒ A) That ensures that data can only be accessed using the dedicated interface
- B) That ensures that code inside the device runs as expected
- C) That ensures the authenticity of the device
- D) That ensures integrity of the data stored in the device

2.5 Malware - The BadAss virus attaches itself to the Chrome browser. Whenever a web requires a login, the browser gets the password stored in windows password manager. The virus steals the user's passwords stored in windows password manager. Who is acting as confused deputy?

- A) The BadAss virus
- ☒ B) Chrome
- C) Windows password manager
- D) This is not a case of confused deputy!

2.6 Trusted computing - A secure enclave: TOPIC NOT ANYMORE IN THE COURSE

- A) Is a function to store keys
- B) Is a standalone device
- C) It is a Hardware Secure Module
- ☒ D) It is a protected region of the memory where code runs securely

2.7 Mitigations - A stack canary protects against control-flow injection:

- A) Always
- B) Only if Data Execution Prevention protects against code injection
- C) Never
- ☒ D) Only if we are sure the value of the canary does not leak

2.8 Chinese Wall policy - Suppose you work for a company with a Chinese Wall security policy with clients in the following conflict classes:

- { Motorola, Huawei, LG }
- { Panasonic, Sony }
- { Credit Suisse, UBS, BCV }
- { Microsoft, Apple }

You have previously worked on cases for Sony, and UBS, and you are ready for a new assignment. According to the policy you can work with:

- ☒ A) Motorola, Huawei, LG, Sony, UBS, Microsoft, Apple
- B) Motorola, Huawei, LG, Microsoft, Apple
- C) Huawei, Panasonic, Apple, Microsoft
- D) Microsoft, Apple, BCV, UBS, Credit Suisse, Sony, Panasonic, LG, Huawei, Motorola