COM-301 : Computer Security
MIDTERM - 25th October
Group A

Lastname: **Firstname:** **SCIPER:**

The exam must be completed with a PEN that is BLUE or BLACK. Pencil will not be corrected (the question will count as 0).

For the short answers, please be careful with the calligraphy.

No book, calculator, phone, or laptop are allowed during the exam.

	Correct (+2 pts each correct)	Wrong (-1pts each wrong)
Question 1 (30pts)		

	Correct (+5 pts each correct)	Wrong (-2pts each wrong)
Question 2 (40pts)		

	3.1	3.2	3.3	3.4
Question 3 (30pts)				

Total	

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]
		Eliminating buffer overflows would completely prevent the problem of trojans.
		Some viruses add their code to that of existing executables residing on disk.
		Virus can spread to systems even if they have no Internet connectivity.
		If following the open design principle a developer publishes the source code of a program, we can be sure that the executable version will not have backdoors.
		An advantage of signature-based detection over anomaly detection is the reduced number of false positives.

TRUE	FALSE	**Cryptography and Authentication:** [10pts]
		Digital signatures use public-key cryptography to provide both integrity and authentication.
		If we chain hash computations (e.g, h = Hash(Hash(Hash(message))) the value h is more second pre-image resistant than the Hash() function itself.
		Computing a hash for a data item using a cryptographic hash function such as SHA-1 requires possession of the correct secret key.
		A secure stream cipher is a good choice to encrypt a TV channel that is broadcasted live.
		Computing the plaintext MAC and then encrypting both plaintext and MAC (MAC-then-Encrypt) ensures that you can check the integrity of the ciphertext.

TRUE	FALSE	**Principles and basics:** [10pts]
		A vulnerability is the result of an attack.
		Having two security controls to provide access always provides better security regardless of how they are combined.
		If I have two critical services running in my system the good choice is to run them in separate processors even if that means having to keep two processors safe.
		Making sure that at least two users are required to run any functionality in the system ensures that the least privilege principle is fulfilled.
		If a program hits a bug, the best is to rewind the last actions and try again with a different random input.

Question 2: <u>Circle</u> the correct answer
[40pts] [+5 per correct answer, -2 per wrong answer]

Only responses with one valid answer will be corrected!

C) **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 Malware: Once it has infected a machine the BadAss worm sends itself to all of the addresses in the Address Book of the user. This may cause…

A) A Denial of Service on the BadAss worm
B) A Denial of Service on the computers of the infected users' contacts
C) A Denial of Service on the Internet
D) Nothing happens, the BadAss worm is very innocuous!

2.2 Memory safety - The following program:

```
void test( char *array, char *input) {
      char buf[30];
      input = array;
      char *ptr = &buf[20];
      ptr = ptr + 3;
      printf(input);
      free(input);
      *ptr = 1000;
}
```

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

2.3 Insecure Interaction Between Components - Performing good sanitization of users' input:

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, this is not a sufficient countermeasure against these attacks

2.4 Security testing - Take the following code:

```
int example(bool b1, bool b2) {
      int a = 0;
      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

2.5 Trusted computing - Attestation is a property:

A) That ensures that data can only be accessed using the dedicated interface
B) That ensures that the code inside the device is the expected code
C) That enables to store keys outside the device
D) That ensures no side channel exists

2.6 Trusted computing - A Hardware Secure Module:

A) Is a secure standalone device
B) Is a function to store keys
C) It is a secure enclave
D) It is a protected region of the memory where code runs securely

2.7 Mitigations - A stack canary protects against code injection:

A) Always
B) Only if control flow cannot be hijacked
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 Microsoft, and LG, and you are ready for a new assignment. According to the policy you can work with:

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

Lastname: **Firstname:** **SCIPER:**

Question 3: Answer the question in at most THREE lines [30 pts]

1. Agree or disagree and <u>justify</u>: ***"A One Time Pad is the best choice to transmit a secret document of 1Mb because we know it provides perfect secrecy"*** **[5 pts]**

2. Agree or disagree and <u>justify</u>: "Is it a good idea to secure your password database by encrypting each password using symmetric encryption. For example, for each password store Enc(k, password|salt), where k is a symmetric key." [5 pts]

3. Which properties (one or more) does this exchange achieve: [10pts]

Bob sends to Alice: Enc(PK_{Alice},k), Enc(PK_{Bob},k), AES(k,M)

PK_{Alice}= Public key of Alice
PK_{Bob}= Public key of Bob
AES(sk,data)= Symmetric-key encryption of data using AES-256 in CBC mode, with the key sk
Enc(pk,data) = Public-key encryption of data with the key pk
k = symmetric key
M = message

[Hint: the possible properties are Confidentiality, Integrity, Authentication, and Non-Repudiation]

4. A commitment scheme is a cryptographic primitive that allows one to commit to a chosen value (i.e., one cannot change it later in time) while keeping it hidden from others, with the ability to reveal the committed value later. A possible implementation of commitments is a hash function. To commit to the value 89, one provides Hash(89).

Imagine a case in which the professor commits to Joe Doe's score, imagine 60, in COM-301 and sends the commitment to central services. Since Joe is not happy with the score, he would like to convince the central services that the score was higher.

When the professor chooses the hash function, what property/properties is needed to make sure that Joe Doe will not succeed. (Justify)

[Hint: the possible properties are pre-image resistance, second-preimage resistance, collision resistance. There is no need to write their definitions, just the justification]