COM-301 : Computer Security
FINAL - 1st February 2019

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

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO

The exam must be completed with a BLUE or BLACK PEN. Pencil will not be corrected (a question answered only in pencil will count as 0).

Please be careful with the calligraphy. Illegible answers will count as 0.

The minimum score per question is 0 points. Very wrong statements inside a response will cancel any correct statement, and the full subquestion will count as 0.

Unless stated otherwise ALL questions require justification.

Books, calculators, phones, and laptops are NOT allowed during the exam.

	Correct (+1 pts each correct)	Wrong (-0.5 pts each wrong)
Question 1 (15 pts)		

	Correct (+2 pts each correct)	Wrong (-1pts each wrong)
Question 2 (18 pts)		

	3.1 (4 pts)	3.2 (5 pts)	3.3 (8 pts)	3.4 (9 pts)
Question 3 (26 pts)				

	4.1 (12 pts)	4.2 (8 pts)
Question 4 (20 pts)		

	5.1 (7 pts)	5.2 (7 pts)	5.3 (7 pts)
Question 5 (21 pts)			

TOTAL	

GUIDELINES TO RESPOND TO QUESTIONS 1 AND 2

 **Selecting an answer**  **Cancelling an answer**

You can only change your mind to cancel an answer. Once an answer has been canceled you cannot "uncancel" it.
To leave a question unanswered either do not circle any option or cancel all the answers. Ambiguous answers will be considered wrong. If in doubt, ask a TA.

There is ONLY ONE correct response per question. Responses with more than one circled answer will be considered wrong!

The questions do NOT require justification, any justification will be disregarded.

Question 1: Circle the correct answer
[15 pts] [+1 per correct answer; -0.5 per wrong answer]

1.1. Malware. [5 pts]

1.1.1. Eliminating buffer overflows would completely prevent the problem of backdoors.

A) True
B) False

1.1.2. An example of ransomware is a malware that threatens to destroy a computer's content unless the owner pays an economical compensation.

A) True
B) False

1.1.3. Only expert hackers can use malware to do malicious actions.

A) True
B) False

1.1.4. Viruses can spread to systems even if they have no Internet connectivity.

A) True
B) False

1.1.5. A star topology with one command and control station connected to all bots enables perfect control over the bots. Therefore it is a robust choice to configure a botnet.

A) True
B) False

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

1.2. Privacy. [5 pts]

1.2.1. A service provider offering easy default privacy preferences for users does not guarantee that the users' privacy is protected from the service provider.

A) True
B) False

1.2.2. Having privacy when using digital services is important for individuals, but not for corporations or governments.

A) True
B) False

1.2.3. Encrypting communications is enough to provide privacy with respect to an adversary that can observe all Internet traffic.

A) True
B) False

1.2.4. In order to provide anonymity against a state adversary it is necessary that the first and last nodes in a Tor path are owned by different people in different countries.

A) True
B) False

1.2.5. Attribute based credentials allow users to authenticate in a manner such that they are unlinkable across contexts.

A) True
B) False

1.3. Principles and basics. [5 pts]

1.3.1. The adversary's capabilities to attack a system are called vulnerabilities.

A) True
B) False

1.3.2. To comply with the principle of open design a company can release the binary code for the piece of software they sell.

A) True
B) False

1.3.3. The Trusted Computing Base (TCB) is made up of all of the elements in the system on which the security policy relies.

A) True
B) False

1.3.4. Following the least privilege principle implies that principals should only be given access to assets on a need-to-know basis.

A) True
B) False

1.3.5. When making a security argument about a system the threat model is not relevant.

A) True
B) False

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

Question 2: <u>Circle</u> the correct answer
[18 pts] [+2 per correct answer, -1 per wrong answer]

2.1 Security policies. Consider a university which uses classification labels:

```
student < professor < dean < president
```

for its documents. The process of upgrading a document from student to president is called:

A) Declassification
B) BIBA
C) Bell La Padula
D) Sanitization

2.2 Authentication. When designing a password-based authentication system, which of the following mechanisms should you use to mitigate the impact of offline attacks when the adversary gets access to the database:

A) Requiring knowledge of a nonce (random number) that has just been sent to the authenticating principal before accepting a password
B) Concatenating a salt with the password before hashing
C) Using a fast hash function
D) Storing the hash of the password beside a hash of a random salt

2.3 Trusted computing. Tamper resistance, which ensures that a secure device cannot be physically opened, is a very important property to ensure:

A) Attestation
B) Isolation
C) Integrity
D) Sanitization

2.4 Malware. A honeypot is a computer which, on purpose, has vulnerabilities that can be exploited remotely so that it gets attacked. This is useful for:

A) Better understanding how malware, in particular botnets, work
B) Stopping worms from spreading
C) Amplifying the effect of viruses
D) Separating the intranet from the demilitarized zone

2.5 Access control. Consider the following program, owned by Alice, that raises an alarm whenever the temperature in a room is too low.

```
void alarm(int degrees, int hot) {
  if (degrees < 17) {
    file = open("logalarm.txt","a"); // open temperature log in append mode
    write("Freezing at %d degrees \n", degrees,file);  // log temperature
    close(file);                     // close messages log
  } else {
    hot += 1;                        // increase the count of hot days
  }
  exit;
}
```

Which of the following permission configurations will allow Bob to correctly execute the function alarm while assuring Alice that the alarm log cannot be tampered.

A)
```
-rwx--x--x   Alice Alice+Bob alarm
-rwxrw----   Alice Alice+Bob logalarm
```

B)
```
-rws--x--x   Alice Alice+Bob alarm
-rwx-w----   Alice Alice+Bob logalarm
```

C)
```
-rws--x--x   Alice Alice+Bob alarm
-rwxr-----   Alice Alice+Bob logalarm
```

D)
```
-rwx-w---x   Alice Alice+Bob alarm
-rw-r-x---   Alice Alice+Bob logalarm
```

2.6 Network security. Deep packet inspection is a firewall filtering technique that:

A) Inspects each packet header in isolation and rejects/allows depending on certain rules
B) Works equally well when traffic is sent in the clear, and when traffic is sent encrypted
C) Inspects the content of the packets and rejects/allows depending on certain rules
D) Never works

2.7 Software security. Data execution prevention (DEP):

A) Ensures that a memory page that can be read from cannot be executed
B) Ensures that a memory page that can be written to cannot be executed
C) Ensures that the stack canary is not modified
D) Is a well known fuzzing technique

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

2.8 Network Security. The lack of security mechanisms in network protocols enables adversaries to change the origin of packets. This in turn enables:

A) Rerouting packets by changing the cost of routes in the BGP protocol
B) DNS hijacking attacks in which an adversary changes the content of a DNS response
C) Providing fake MAC addresses in response to an ARP request to bootstrap a man in the middle attack
D) The creation of VPNs that provide confidentiality and integrity for packets traversing the Internet

2.9 Access Control. Consider a system in which Alice can read and write to the file `xxx.sys`, can read the file `yyy.sys`, and can execute the file `zzz.sys`. Bob can read and write to `yyy.sys`, and cannot access `zzz.sys` or `xxx.sys`. Charlie can execute `yyy.sys`, can write and read `xxx.sys` and only write `zzz.sys`.

The Access Control List for this system would be:

A) xxx.sys = {Alice={read,write}, Bob={}, Charlie={read,write}}
yyy.sys = {Alice={read}, Bob={read,write}, Charlie={execute}}
zzz.sys = {Alice={execute}, Bob={}, Charlie={write}}

B) Alice = {xxx.sys={read,write},yyy.sys={read},zzz.sys={execute}}
Bob = {yyy.sys={read,write}}
Charlie = {xxx.sys={read,write},yyy.sys={execute},zzz.sys={write}}

C) xxx.sys = {Alice={read,write},Bob={read},Charlie={execute}}
yyy.sys = {Bob={read,write}}
zzz.sys = {Alice={read,write},Bob={execute},Charlie={write}}

D) None of the above

GUIDELINES TO RESPOND TO QUESTION 3

Answer each question in at most 3 lines.

No matter the size of the letters or the margins on the side, every time the text changes lines, we will consider it a new line. If in doubt, ask a TA.

Each extra line (4th line or beyond) will result in a reduction of 0.5 points.

Question 3: Provide a short answer to the following questions [26 pts]

3.1. Biometrics. Agree or disagree and justify: "When configuring biometrics to be used as an authentication function to secure payments it is important that there is a low false positive rate even if there are many false negatives[1] " [4 pts]

3.2. Security policies. Suppose you work for a company that implements a Bell La Padula policy to protect highly sensitive documents. For this purpose this company installs a computer called `SecureWorld` in a separate room where only two employees: the Big Boss and John Honestson, can access. Documents are uploaded to `SecureWorld` by writing them to a USB stick and giving this USB stick to John Honestson. John is forbidden to retrieve any document from the machine or USB and reproduce it outside of `SecureWorld`'s room or reveal its contents. As his family name indicates, John honestly follows this rule.

You want to go to Aruba this summer. Thus, you are very interested in knowing when the Employee evaluation that will trigger the yearly bonus is uploaded to `SecureWorld` so that you can start making your bookings. You promise John to bring him some very nice Swiss chocolate if he reveals to you when the file is installed, even if he does not tell you the content. As this does not make him break the no-retrieving-no-revealing-content rule, John agrees.

a) You and John need to come up with a way for John to communicate to you when the file is uploaded without the Big Boss, or any other employee of the company, realizing that this message is being sent. What is this type of secret communication called? (No justification, just the name) [2 pts]

[1] A false positive happens when a wrong input is considered correct
A false negative happens when a right input is considered wrong

b) Suggest one adequate way to implement the secret communication, i.e., a good way for John to let you know that the Employees evaluation has been uploaded to `SecureWorld` without anybody noticing he is communicating with you. Before publishing the yearly bonus, Big Boss puts every employee under 24/7 surveillance, so you need to exchange this message under the watchful eye of Big Boss. There is no need for the secret communication mechanism to use a computer, although it can. Justify your answer [3 pts]

3.3. Applied Cryptography Given this exchange

Bob sends to Alice: $Enc(PK_{Alice},k1)$, $Enc(PK_{Bob},k2)$, $AES(k1,M)$, $MAC(k2,M)$

PK_{Alice}= Public key of Alice, SK_{Alice}= Secret key of Alice
PK_{Bob}= Public key of Bob, SK_{Bob}= Secret key of Bob
AES(k,data)= Symmetric-key encryption of data using AES-256, with the key k
MAC(k,data) = Message Authentication Code of data using key k
Enc(pk,data) = Public-key encryption of data with the key pk
k = symmetric key
M = message

Circle the correct answer: "*Yes*", "*No*", or "*Broken"* (select Broken when the described exchange requires a step that Alice or Bob cannot execute). Justification is required.

a) This combination ensures that Mallory, who is eavesdropping on the exchange, cannot read the message M. [2 pts]

"*Yes*" "*No*" "*Broken*"

b) This combination ensures that Alice can detect if the message has been modified by Mallory. [2 pts]

"*Yes*" "*No*" "*Broken*"

c) Does the exchange enable Alice to authenticate Bob as the sender of the message? If yes, explain which of the elements in the exchange provides this property. If not explain what needs to be added. [2 pts]

"*Yes*" "*No*" "*Broken*"

d) If Bob signs the message by computing Alice's signature $Sig(SK_{Alice}, M)$, would the integrity of the message be preserved with respect to Mallory? [2 pts]

"*Yes*" "*No*" "*Broken*"

3.4 Trusted computing. You are the new Chief Security Officer at SecurityMatters, a new startup that aims to build a personalized "vault" for users so that they can store a backup of their passwords for other sites.

Imagine that the first round of financing has gone very well and the company has gotten 1M CHF. Since you have money, you want to build a hardware-based solution.

a) What hardware would you install in your servers if you want to make sure that you will not be able to see the passwords even if you wanted to? (Just name, no need to justify) [2 pts]

b) To communicate with their vaults in a secure way, naturally your customers need to use cryptographic means. Thus, you create an application that they can install on their laptops or smartphones that can interact with the secure vault. What is the minimal cryptographic material that this application needs to know to be able to set up a secure channel with the secure vault? Justify. [3 pts]

c) Naturally, your customers want to make sure that they are actually speaking with the vault, and that the vault is operating correctly. Name the property that allows the vault to prove that it is operating as expected and briefly explain how it works. [4 pts]

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

GUIDELINES TO RESPOND TO THE REMAINING QUESTIONS

There is no limit to the number of lines you may write to respond to the questions below. Note, however, that the space given is sufficient to justify the answers correctly.

Question 4: Software security. Consider the code below and answer the questions [20 pts]

```
1: /* Copy the first k characters of src into dst from the n-th
2: character in dst on */
3: void copycat (char *dst , char *src, int k , int n )   {
4:    for ( int i = 0 ; i < k ; i++) [2] {
5:       dst[i + n] = src[i] ;
6:    }
7: printf (dst)
8: }
```

4.1 The instruction in line 5 allows an adversary to attack this function. Explain two possible attacks that exploit the vulnerabilities exposed by this bad programming (there are more than two attacks, just pick two). For each attack provide a modification to the code to solve it (modify or add lines of code). [12pts]

a) First attack

How the attack works [3pts]:

How can it be avoided [3pts]:

[2] This is a for loop that, starting with i=0, on each pass increases i in one (i=i+1). It is executed again and again while i is smaller than k. When i>=k the loop is not executed anymore.

a) Second attack

How the attack works [3pts]:

How can it be avoided [3pts]:

4.2 Line 7 contains another vulnerability. Explain how this vulnerability can be exploited and modify the line to avoid these problems. [8pts]

How the attack works [4pts]:

How can it be avoided [4pts]:

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

Question 5: Network security. There is a new Internet service `RankAProf` in which students can give ratings to their professors and provide comments on the lectures. To promote honesty, the website publishes the comments anonymously.

To add a rating or a comment, a student needs to visit `www.rankaprof.com`, which is hosted in the US, from her browser and log in. When the user is logged in, the server opens a session and keeps adding ratings and comments to a temporary list. Only when the student clicks “Publish” is the list added to the database and deleted.

Answer the following questions.

5.1 EPFL sees that some professors get very bad ratings and wants to know which students are giving these ratings in order to talk to them and understand how to improve. [7 pts]

a) How can the EPFL system administrators identify which computers are used to access the website from the campus network? [3 pts]

b) Of the technologies we have studied in class, which would help students avoid the monitoring from the system administrators? If no technology would help, explain why. [4 pts]

5.2 A professor with bad ratings wants to identify which students are writing negative comments on `RankAProf`. Since he is not an EPFL system administrator, he cannot inspect the packets. Thus, he wishes to man in the middle the communication. Explain one way of becoming a man in the middle and propose a countermeasure to avoid this attack. [7 pts]

a) Attack. Concretely identify where in the network the professor must be to deploy this attack and describe how it works (only one attack is needed, select your favourite) [3 pts]

b) Defense. Explain a protocol from the ones seen in class that prevents the attack you propose in **a)**. Explain how it defeats the attack. [4 pts]

5.3 Because the students have taken COM-301 and are using all the protections learned in the course, the professor cannot monitor or hijack the connections. Therefore, the professor decides to directly take the `RankAProf` website down. Explain one way to perform a Denial of Service attack and propose a countermeasure to avoid this attack. [7pts]

a) Attack. Concretely identify where in the network the professor must be to deploy this attack and describe how it works (only one attack is needed, select your favourite) [3 pts]

b) Defense. Explain how to prevent the attack you propose in **a)**. [4 pts]