NATIONAL UNIVERSITY OF SINGAPORE

CS2107 — INTRODUCTION TO INFORMATION SECURITY

(Semester 1: AY2018/19)

Time Allowed: 2 Hours

INSTRUCTIONS TO STUDENTS

1. Please write your Student Number only. Do not write your name.
2. This assessment paper contains **FOUR** questions and comprises **SIXTEEN** printed pages.
3. Answer **ALL** questions.
4. Write your answer within the given box in each question on this question paper.
5. This is an **OPEN BOOK** assessment.
6. You may use NUS APPROVED CALCULATORS.
   Nonetheless, you should be able to work out the answers without using a calculator.

Student Number: — — — — — — — — —

This portion is for examiner's use only:

Question	Full Marks	Marks	Remarks
Q1	10		
Q2	10		
Q3	10		
Q4	20		
Total	50		

1. **[10 marks] (Terminology):** The following ten security-related descriptions are obtained from the Web. Fill in the blanks ***on this question paper*** with the **most** appropriate term from the list given below. Put only **one choice** per question, and you can write either the term or its number in the blank. Note that some choices *may appear more than once* in this part. You may ignore any grammatical rules on plural forms.

(1) Confidentiality
(2) Integrity
(3) Availability
(4) Authenticity

(5) Public key
(6) Private key
(7) Digital signature
(8) MAC

(9) Format string vulnerability
(10) Buffer overflow
(11) Integer overflow
(12) XSS
(13) CSRF
(14) SQL injection
(15) Clickjacking

(16) Privilege escalation
(17) Side-channel attack
(18) Covert channel
(19) Zero-day vulnerability
(20) Typo squatting
(21) Click fraud
(22) Social engineering
(23) Phishing

(24) Fuzzing
(25) Kerckhoffs' principle
(26) Mandatory access control
(27) Discretionary access control
(28) Intermediate access control
(29) Role-based access control
(30) Protection rings

(i) Petya is a family of ransomware discovered in 2016, which targets Microsoft Windows-based systems. It infects the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system. Otherwise, the _____ of the user's data is affected.

(ii) In an event where a user or process is able to obtain a higher level of access than a system administrator or system developer intended, we thus can say that there is a/an _____.

(iii) A/an _____ occurs when a person, automated script, or computer program imitates a legitimate user of a web browser, clicking on a online advertisement without having an actual interest in the target of the ad's link.

(iv) Ariane 5's first test flight failed, with the rocket self-destructing 37 seconds after launch because of a malfunction in the control software. The malfunction was due to a data conversion issue, where a 64-bit floating point value was represented by a 16-bit signed integer. The software's programmer(s) failed to consider the danger of _____, which cost the company ~$370 million.

(v) An attacker can exploit a/an _____ in a C program that calls `printf()` function, among others, to illegally display data from the call stack in memory.

(vi) _____ is a type of injection attack, in which an end-user attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

(vii) The Biba and Bell-LaPadula models can be used to enforce access control in government and military applications, where data integrity and confidentiality are of utmost importance. They are two examples of _____, where the users in the applications cannot override or modify the enforced policies, either accidentally or intentionally.

(viii) _____ attacks data-driven web applications, where the involved back-end database servers are targeted by a malicious web user.

(ix) American fuzzy lop uses _____ technique for testing software by providing randomly-generated inputs, searching for those inputs which cause the program to crash. It employs genetic algorithms in order to efficiently increase code coverage of the test cases. So far it helped in detection of significant software bugs in dozens of major free software projects.

(x) Some CPUs support a feature called NX ("No eXecute") or XD ("eXecute Disabled") bit, which in conjunction with software, can be used to mark pages of data (such as those containing the stack and the heap) as readable and writable but not executable. This feature can thus help mitigate _____ attacks.

2. **[10 marks] (Multiple Choice Questions):** Choose the **best** answer, and circle/cross the corresponding *letter choice* on this **paper**. No mark is deducted for wrong answers.

The first 4 (four) questions refer to this given scenario.

Alice used her laptop to connect to a WiFi service provided by a cafe. The WiFi access was protected by WPA2. As a regular customer, Alice knew the WiFi password, which is a strong password. The cafe owner Mallory set the password, and had a full control of the WiFi router. As such, Mallory could listen, fabricate, or block packets that went through the WiFi. Bob was another customer in the cafe, but did not know the WiFi password.

On her browser, Alice typed the URL of a bank site `https://www.securebank.com`, and then logged into it. The bank employed 2-factor authentication in protecting an account access, where a password and a one-time PIN (OTP) sent via SMS were verified. It turned out that Alice's browser also had an active malicious browser extension, which could illegally capture all Alice inputs to the browser.

(i) Who knew the fact that Alice visited `www.securebank.com`?

(a) Bob only
(b) Mallory only
(c) The browser extension only
(d) Bob and Mallory only
(e) Mallory and the browser extension only

(ii) Who knew Alice's typed and sent bank username and password?

(a) Bob only
(b) Mallory only
(c) The browser extension only
(d) Bob and Mallory only
(e) Mallory and the browser extension only

(iii) Who knew the private key of the `www.securebank.com` web server?

(a) Bob only
(b) Mallory only
(c) The browser extension only
(d) The web server only
(e) Alice only

(iv) Subsequently, who could impersonate Alice and illegally access Alice's account?

(a) Mallory only
(b) The browser extension only
(c) Bob and Mallory only
(d) Mallory and the browser extension only
(e) None of Bob, Mallory and the browser extension

(v) Which of the following statements is *incorrect* with regard to access control:

(a) ACL has an issue in getting an overview of the objects that a particular subject has access rights to

(b) Capabilities has an issue in getting an overview of the subjects who have access rights to a particular object

(c) Access control matrix can be very large, and thus difficult to manage

(d) Intermediate control is employed to provide a more fine-grained access control than those provided by ACL and capabilities

(e) UNIX/Linux file permission adopts a group-based intermediate control

(vi) In your holiday to Himalaya, you discover a monastery where the monks have defined the following rules that you, as the commoner, must abide by:

R_1: A monk may write a prayer book that can be read by commoners, but not one to be read by a high priest.

R_2: A monk may read a book written by the high priest, but may not read down to a pamphlet/note written by a commoner.

Conceptually, the second rule of the monastery above (i.e. R_2) implements:

(a) No read-up rule of Bell-LaPadula

(b) No write-down rule of Bell-LaPadula

(c) No write-up rule of Biba

(d) No read-down rule of Biba

(e) None of the above

(vii) Suppose you know that Bob, on your hub-based local area network, is about to connect to a remote server using the insecure telnet protocol. You want to capture Bob's username and password, which are sent in clear by his telnet client. Subsequently, you also want to find out all open ports on the server besides telnet. What are the most suitable tools (in the required order) that you should run?

(a) `ping`, `nmap`

(b) `nslookup`, `nmap`

(c) `Wireshark`, `nmap`

(d) `Wireshark`, `nslookup`

(e) `nmap`, `traceroute`

(viii) Which type of firewall should you deploy at your company network's gateway so that the `HTTP referer` header field can be removed from all outbound HTTP request packets due to privacy concerns:

(a) (Traditional) packet filter

(b) Stateful-inspection (packet filter)

(c) HTTP proxy

(d) Personal firewall

(e) 2-firewall setting

(ix) Which web attack below requires its victim web user to first log in and authenticate himself/herself with an involved web server?

(a) XSS
(b) CSRF
(c) SQL injection
(d) drive-by download
(e) proxy re-encryption

(x) Which software security technique below can help detect if a stack-based buffer overflow has occurred, so that the program execution can be subsequently aborted?

(a) canary
(b) memory randomization
(c) ASLR
(d) input filtering
(e) patching

3. **[10 marks] (Short Answer Questions):** Answer the questions below in 1–3 sentences, or by using a concise diagram.

   (i) **[4 marks] (UNIX/Linux Access Control)**
   As a newly-assigned system administrator in your company, you are given the root account of a server host. On the server, you notice the following suspicious file under the `/usr/games/` folder:

   ```
   -rwsr-xrwx 1 root root 17435 Nov 20 15:25 pacman
   ```

   (a) (1 mark) When a normal (non-root) local user Bob with UID=1800 executes the file, what will be the process' real UID and effective UID?

   (b) (1 mark) When Bob invokes the executable file, can the process read the following file if the executable indeed performs a reading operation on the file?

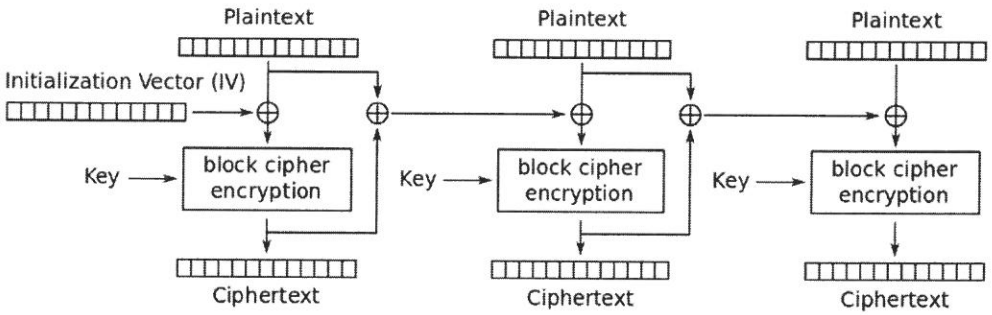
   ```
   -rw-r----- 1 hr staff 9678 Nov 15 19:51 /company/hr/employeedata
   ```

   Explain why or why not.

   (c) (2 marks) Give two commands, in both symbolic mode and octal mode notations, that can clear the setuid bit and change the file permission into: `-rwxr-xr-x`.

(ii) **[6 marks] (Cryptography: Mode-of-Operation)** Let us consider the *Propagating Cipher Block Chaining* (PCBC) mode-of-operation, whish is designed to cause small changes in the ciphertext to propagate indefinitely when decrypting, as well as when encrypting.

In PCBC mode, each block of plaintext is XOR-ed with both the previous plaintext block and the previous ciphertext block before being encrypted. An initialization vector (IV) is used in the first block, which is then added before the first ciphertext block. The mode can be diagrammatically depicted as follows.



Mathematically, the encryption can be expressed as follows:

Given a n-block plaintext message $x_1, x_2, x_3, \ldots, x_n$ and a secret key K,

PCBC outputs $(n+1)$-block ciphertext message $y_0, y_1, y_2, \ldots, y_n$, where:

$y_0 = IV$;

$y_i = Enc_K(x_i \oplus x_{i-1} \oplus y_{k-1})$, for $i = 1, 2, 3, \ldots, n$;

$x_0 \oplus y_0 = IV$.

(a) (2 marks) Draw a diagram of the corresponding PCBC-based decryption.

(b) (1 mark) How is decryption affected if the IV is missing from the ciphertext? Explain which plaintext block(s) that can be recovered correctly, and which one(s) that cannot be recovered?

(c) (1 mark) How is decryption affected if there is a single-bit flip error in the ciphertext block y_8? Explain which plaintext block(s) that can be recovered correctly, and which one(s) that cannot be recovered?

(d) (1 mark) Can the encryption processes of different blocks belonging to a plaintext run in parallel? Explain briefly why or why not.

(e) (1 mark) How about the decryption of a ciphertext's different blocks? Can it run in parallel? Explain briefly why or why not.

4. **[20 marks] (Scenario-based Questions):**

   (i) **[8 marks] (Firewall Design)**

   Suppose you, as a network administrator, want to deploy a 2-firewall setting to protect your company's network. The machines in your company's network include:

   - `Web-server`: the company's Web server;
   - `Email-server`: the company's email server;
   - `Internal`: all internal hosts.

   In your DMZ, you want to put both `Web-server` and `Email-server`, which should be accessible from the Internet as well as `Internal`:

   - `Web-server` accepts both `HTTP` and `HTTPS` traffic;
   - `Email-server` accepts `SMTP` traffic.

   As commonly found, you want to allow your `Internal` to have `HTTP` and `HTTPS` traffic with any hosts on the Internet. Additionally, your `Internal` can have `DNS` traffic with `ISP-DNS-server`, which is hosted by your ISP. All other traffic *must be blocked.*

   Similar to your tutorial, you can set up the following network partitioning:

   `Internal` $\leftarrow$ (IN) F_2 (OUT) $\rightarrow$ DMZ $\leftarrow$ (IN) F_1 (OUT) $\rightarrow$ Internet

   (a) (4 marks) Please list the rules at the front-end/outer firewall F_1:

source IP	*dest IP*	*source port*	*dest port*	*direction*	*action*

(b) (4 marks) Also specify the rules at the back-end/inner firewall F_2:

source IP	*dest IP*	*source port*	*dest port*	*direction*	*action*

(ii) **[6 marks] (Secure Programming)**
Consider the following C program.

```
1   #include <stdio.h>
2   #include <string.h>

3   void safe_copy(char *input) {
4       unsigned char s;
5       char buf[81];

6       s = strlen(input);
7       if (s > 80) {
8           strncpy(buf, input, 80);
9           buf[80] = '\0';
10      }
11      else
12          strcpy(buf, input);

13      printf("After the safe copy, the content of buf is: %s\n", buf);
14  }

15  int main(int argc, char *argv[]){
16      if (argc < 2) {
17          printf("Please supply a string with at most 80 characters.\n");
18          return -1;
19      }
20      safe_copy(argv[1]);
21      return 0;
22  }
```

(a) (2 marks) Is the program above safe if the length of the supplied first argument is at most 80? Explain why or why not.

(b) (2 marks) Is the program above vulnerable? If so, describe the vulnerability, and instances of the supplied first argument input that will cause the issue.

(c) (2 marks) Which line(s) of code in the program above should you modify in order to make the program free from the vulnerability? Write the replacement line(s) as well.

(iii) **[6 marks] (Network Protocol)**

A company uses a public-key encryption based protocol to allow for a message acknowledgment among its internal users. Suppose $E_{Pb_X}()$ denotes a public-key encryption operation using the public-key of entity X. The message acknowledgment protocol of message m that is sent from A to B works as follows:

1. $A \rightarrow B$: A, B, $E_{Pb_B}(m)$
2. B : decrypts $E_{Pb_B}(m)$ using its private key to recover m
3. $B \rightarrow A$: B, A, $E_{Pb_A}(m)$
4. A : decrypts $E_{Pb_A}(m)$ using its private key;
   and if m is recovered, it concludes that B has received m

That is, A first sends the message m encrypted using the public key of B, together with the two parties' identities (i.e. A and B). Subsequently, B decrypts the encrypted message to recover m. It then acknowledges the received m by sending it encrypted using A's public key, together with the message sender and receiver identities in reverse order, in Step 3.

(a) (3 marks) Suppose C is an employee in the company, who also has a valid public/private key pair. Suppose it can listen to the communication channel used, and also send message(s). The protocol above is insecure. Show how C can listen to an (encrypted) message that is sent and acknowledged by two parties A and B, and then launch an attack to recover the message m.

(b) (3 marks) Suggest how you can prevent the attack described in part (a) by modifying the format of the message to be encrypted in Steps 1 and 3. You can use the notation || to denote a string concatenation operation. Also explain briefly how your improved protocol can prevent the attack.

BLANK PAGE

(You can use this page if you need more space to write down your answers)

— END OF PAPER —