NATIONAL UNIVERSITY OF SINGAPORE

CS2107 — INTRODUCTION TO INFORMATION SECURITY

(Semester 2: AY 2017/18)

Time Allowed: 2 Hours

INSTRUCTIONS TO STUDENTS

1. Write your Student Number only. Do not write your name.
2. This assessment paper contains **FIVE** questions and comprises **FIFTEEN** printed pages.
3. Answer **ALL** questions.
4. Write your answer within the given box in each question.
5. This is an Open Book assessment.

Student Number: ☐☐☐☐☐☐☐☐☐

Question	Full Marks	Marks	Remark
Q1	20		
Q2	15		
Q3	15		
Q4	15		
Q5	15		
Total	80		

Q1. **[20 marks] Multiple Choice Question.** Most of the following descriptions are obtained from the public domain, e.g. wiki, blogger, standards, etc. Give the most appropriate choice. *Mark your answers on the provided answer sheet.*

(1) During your job interview, the interviewer mentioned "SOC level-2". The interviewer was probably referring to:

a. The area outsides SR1 in School of Computing.

b. Design decision on system-on-a-chip security

c. Second level security analysis guided by separation-of-concerns principle.

d. Higher level tasks in a security operating center.

(2) Eve, unlike the malicious Mallory, is a passive attacker who can only _____ messages.

a. replay

b. sniff

c. spoof

d. drop

(3) _____ works by enslaving IoT devices to form a massive connected network. The devices are then used to deluge websites with requests, overloading the sites and effectively taking them offline.

a. Mirai

b. Superflish

c. Heartbleed

d. WannaCry

(4) Suppose an organization decides to have 256-bit key for symmetric key. To achieve equivalent security, what would be the size of the hash digest?

a. 128

b. 256

c. 384

d. 512

(5) A(n) _____ is a hole or flaw in a software program for which there is no patch or fix yet, usually because such flaw is still unknown to the software vendor.

a. CVE
b. privilege escalation
c. zero-day vulnerability
d. exposure

(6) Which of the following statements on collision is most appropriate?

i. It is believed that SHA3 does not have collision and thus is collision-resistant.
ii. For any message, there is another message having the same SHA1 digest and thus SHA1 is not collision resistant.
iii. There are infinite number of collisions in SHA3, but none have been found yet.
iv. Collision of MD5 can be efficiently found and thus pre-image can be easily computed.

(7) In our product, the AES key is only known to the communicating entities, and all messages will be encrypted before leaving each entity. Hence, our product achieves _____.

a. end-to-end encryption
b. forward secrecy
c. perfect secrecy
d. semantic security

(8) A _____ refers to potentially harmful software code that is installed on a person's computer without the user needing to first accept or even be made aware of the software installation.

a. zero-day vulnerability
b. drive-by download
c. malware
d. backdoor

(9) _____ are attacks on systems that use the same protocol in both directions. The attacker spoofs the victim's IP address and sends a request for information to servers known to respond to that type of request. The server answers the request and sends the response to the victim's IP address.

a. Renegotiation attacks
b. Name resolution attacks
c. Reflection attacks
d. Man-in-the-middle

(10) A _____ can perhaps best be defined as any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms.

a. side-channel attack
b. amplification attack
c. XSS
d. TOCTOU

(11) Alice was using the free open (i.e. without protection such as WPA) wifi in a cafe to login into IVLE (over https) and read news in `http://www.bbc.com`. Bob was also in the cafe sitting in the far corner. Bob could obtain:

a. Alice's IVLE password and information in answer (b).
b. The fact that Alice visited IVLE and information in (c).
c. The fact that Alice visited `http://www.bbc.com`.
d. None of the above.

(12) Alice was using her home wifi (protected by WPA2), and login into IVLE (over https) and read news in `http://www.bbc.com`. Bob was a neighbour next door. Bob could obtain:

a. Alice's IVLE password and information in answer (b).
b. The fact that Alice visited IVLE and information in (c).
c. The fact that Alice visited `http://www.bbc.com`.
d. None of the above.

(13) **(Access Control)** Two organizations A and B classify documents into two types: *sensitive* and *non-sensitive*, and employees into two classes: *trusted* and *untrusted*. Organization A adopts Bell-LaPadula, whereas organization B adopts Biba in controlling who can read/write which documents. In which organization a trusted employee is permitted to write to a sensitive documents?

a. Both A and B.
b. A only.
c. B only.
d. None.

(14) Consider the same setting in question (13). In which organization an untrusted employee is permitted to read a sensitive documents?

a. Both A and B.
b. A only.
c. B only.
d. None.

(15) Consider the same setting in question (13). In which organization a trusted employee is permitted to write to a non-sensitive documents?

a. Both A and B.
b. A only.
c. B only.
d. None.

(16) Consider the same setting in the previous question (13). In which organization a untrusted employee is permitted to write to a sensitive documents?

a. Both A and B.
b. A only.
c. B only.
d. None.

(17) **(Access Control)** Consider the permission and ownership of the following Unix files.

```
-rwx---r-x   1 root    staff 10 Mar 10 01:00 p1
-rws---r-x   1 bob     year1 10 Mar 10 01:00 p2
-rw-------   1 bob     year1 10 Mar 10 01:00 d1.txt
-rw-------   1 root    staff 10 Mar 10 01:00 d2.txt
```

Suppose user `alice` executes `p1`, the respective real UID and effective UID of the process is:

a. `root`, `root`
b. `root`, `alice`
c. `alice`, `root`
d. `alice`, `alice`

(18) Referring to question (17). Suppose user `alice` executes `p1`, the process has read permission to the following file(s):

a. `d1.txt` and `d2.txt`
b. `d1.txt` only
c. `d2.txt` only
d. none.

(19) Referring to question (17). Suppose user `alice` executes `p2`, the respective real UID and effective UID of the process is:

a. `bob`, `bob`
b. `bob`, `alice`
c. `alice`, `bob`
d. `alice`, `alice`

(20) Referring to question (17). Suppose user `alice` executes `p2`, the process has read permission to the following file(s):

a. `d1.txt` and `d2.txt`
b. `d1.txt` only
c. `d2.txt` only
d. none.

This page is intentionally left blank.

Q2. **[15 marks]** A question was posted in the public forum **Stack Overflow**: "*What is the difference between hashing a password (using SHA3 with salt) and encrypting it (using AES-CBC mode with random IV)? Which way is recommended for password file protection?*" You want to post an answer.

(a) (5 marks) Consider the method that uses encryption. Suppose the user has entered a password p and the stored ciphertext is c, describe the verification process. What is the main difference from the hashing method?

(b) (1 mark) State which method (either hashing or encryption) is recommended.

(c) (4 marks) Give one strong reason to support your recommendation (if more than one are given, only the first one will be marked).

(d) (5 marks) A user posted this answer: "*You should use both, i.e. first hash and then encrypt.*" This answer received mixed comments from the community, with some supported it and some rejected it. You want to support it. Give one scenario where performing both is more secure than using only the method you recommended.

Q3. **[15 marks]** Consider the setting in the Multiple Choice Question Q1(11). Here, Alice was diligent in making sure that the url displayed in the browser was correct.

(a) (6 marks) Bob's had setup a web-server with ip address 11.22.33.44. Describe how Bob could mislead Alice to this web-server although Alice's intention is to visit `http://www.bbc.com`. (Hint: DNS).

(b) (3 marks) Explain why the above attack would not work on IVLE.

(c) (6 marks) In addition, Bob knew that Alice's Lenovo laptop still had Superfish root certificate installed. Of course, Bob was very familiar with the Superfish attack and had all published information on the attack, such as the public key, private keys involved. Describe how Bob could steal Alice's IVLE password.

Q4. **[15 marks]** (Secure Programming) Bob is implementing a mobile cashless payment system. The following steps are carried out to complete a transaction: (1) The customer uses the mobile phone to scan the Merchant's 2D barcode which carries a message m. (2) The mobile phone displays m and prompts the user. (3) If the customer clicks the "ok" button, the amount of money indicated in m will be transferred to the merchant.

The message m should be one of the two forms:

"`Cash $`x`.`y` only`ø" or "`Free`ø"

where x and y are sequences of numeric characters, and 'ø' represents the null character (i.e. value 0). For e.g. m can be "`Cash $1302.30 only`ø". Below is the C program snippet that performs the transaction.

```
L1:    unsigned char m [100];
L2:    unsigned char s [200];
L3:    unsigned int x,y;

L4:    READ_QRCODE(m); //read a 100-byte sequence from 2D barcode and store them in m.
L5:    x= E_DOLLAR(m); //extract x from m.
L6:    y= E_CENTS (m); //extract y from m.

L7:    strcpy (s, m);
L8:    strcat (s, "  :)");
L9:    DISPLAY (s);   // display the message on mobile phone.

L10:   if (x> 300)
L11:      {    HANDLE_ERROR(x);}  // No transfer of more than $300 allowed
L12:   else if (CONFIRM())         // true if user clicks on the ok button.
L13:      {    TRANSFER (  100*x+y );}       // transfer (100*x+y) cents to merchant
```

Remarks:

i. Routines with capitalised names (e.g. `TRANSFER()`) are correctly and securely implemented.

ii. The 2D barcode's payload is a 100-byte sequence where each byte can be of any value (including non-printable ASCII).

iii. The routine `E_DOLLAR (m)` searches for the first occurrence of the character '`$`' in `m`, and then converts subsequent consecutive numeric characters into an integer. If there is no occurrence of '`$`' or no succeeding numeric character, value 0 is returned. Similarly, the routine `E_CENTS (m)` searches for the first occurrence of the character '`.`' in `m`, and returns the succeeding integer. It also returns 0 if there is no occurrence of '`.`' or no succeeding numeric character. E.g. when `m` is `asdfeea$123.051asdf`, then x is 123 in L5 and y is 51 in L6.

Describe how to display a maliciously crafted 2D barcode to achieve the following.

(a) (5 marks) Potentially crash the process. Which line in the program snippet causes this vulnerability?

(b) (5 marks) The mobile phone displays "`Free :)`", and yet if the user clicks on "ok", $1.50 will be transferred to the merchant.

(c) (5 marks) The message displayed indicates an amount less than $500 (or even free), but if the user clicks "ok", $500 will be transferred to the merchant.

Q5. **[15 marks]** Bob implemented a single-signed-on web-based grading system for CS2107. After the lecturer has logged-in, an authentication token will be stored as cookie. The cookie is of the format:

userid : **ddmmyy** : **hhss** : **s**

where **ddmmyy** and **hhss** is the date and time of last login session, and s is the SHA3 digest of the string **userid** : **ddmmyy** : **hhss**. E.g. a cookie could be

```
Alice:030418:1400:dkdowkdhfuwADksdjusijehs
```

The token will also be stored in the server. Subsequently, for any http(s) request sent by the lecturer, the authentication token will be automatically sent as cookie. The server accepts if the cookie matches the stored token.

(a) (5 marks) Explain why the above authentication is insecure.

(b) (4 marks) Give a way to fix the problem in the previous question.

(c) (6 marks) When the lecturer wants to modify the grade of a student, say changing Bob's grade to 55, the following request will be sent.

```
https://cs2107.com/modify?lecturer=Alice&student=Bob&grade=55
```

Consider the secure system that has been fixed in question 4(b). Bob wants to maliciously change his grade to 100. Suggest a method to achieve that.

— End-Of-Paper —