

NATIONAL UNIVERSITY OF SINGAPORE

CS2107 — INTRODUCTION TO INFORMATION SECURITY

(Semester 1: AY 2017/18)

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 **EIGHTEEN** 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	20		
Q4	20		
Total	60		

1. [10 marks] (Terminologies): The following ten security-related descriptions are obtained from the Web. Fill in the blanks *on this question paper* with the most appropriate terminology from the list given below. Put only one choice per question, and you can write either the terminology 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 | (16) Privilege escalation |
| (2) Integrity | (17) Side-channel attack |
| (3) Availability | (18) Covert channel |
| (4) Authenticity | (19) Zero-day vulnerability |
| | (20) Typo squatting |
| (5) Public key | (21) Click fraud |
| (6) Private key | (22) Social engineering |
| (7) Digital signature | (23) Phishing |
| (8) MAC | |
| | (24) Fuzzing |
| (9) Format string vulnerability | (25) Kerckhoffs' principle |
| (10) Buffer overflow | (26) Mandatory access control |
| (11) Integer overflow | (27) Discretionary access control |
| (12) XSS | (28) Intermediate access control |
| (13) CSRF | (29) Role-based access control |
| (14) SQL injection | (30) Protection rings |
| (15) Clickjacking | |

- (i) Mirai is malware that turns networked devices running Linux into remotely controlled bots, which can be used as part of a botnet in large-scale network attacks. The Mirai botnet has been used in some of the largest and most disruptive DDoS attacks, which affect the of, among others, computer security journalist Brian Krebs's website and DNS provider Dyn.
- (ii) Uber has sued an advertising British firm Fetch Media for . Uber said that Fetch Media, that ran Uber ads on some websites, claimed credit for app downloads even when customers didn't click on an ad first.
- (iii) An attacker registered for the domain name "www.dbsbank.com", and then set up a maliciously-spoofed DBS bank website. The attacker was hoping that some Internet users would visit the website and mistakenly believe that they visit the website of DBS bank. This is an example of a/an attack.

- (iv) In 2016, a game machine at a resort in Iowa printed a prize ticket of \$42,949,672.76. The resort refused to pay this amount calling it a malfunction, using in their defense that the machine clearly stated that the maximum payout was \$10,000, so any prize higher than that had to be the result of a/an [redacted]. The Iowa Supreme Court ruled in favor of the resort.
- (v) [redacted] attacks are becoming a more common attack method used by hackers. These attacks take advantage of the trust a website has for a user's input and browser. The victims are tricked into performing a specific action they are not intending to do on a legitimate website, where they are authenticated to.
- (vi) A malware called Trojan.Bachosens opens backdoors on compromised computers and siphons out information. It utilizes [redacted] over DNS, ICMP and HTTP protocols to link with a command-and-control server.
- (vii) [redacted] is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions, or for finding potential memory leaks.
- (viii) A/an [redacted] discovered by security researchers are purchased by a wide variety of parties, including militaries, intelligence agencies, software vendors, and cybercriminals. Their intentions also vary widely: some buyers want to fix and defend software, others want to mount offensive cyber operations.
- (ix) Kubernetes (K8s), which was originally designed by Google and then donated to the Cloud Native Computing Foundation, is an open-source system for automating deployment, scaling, and management of containerized applications. The recent Kubernetes 1.8 improves its security by using [redacted], which links users and entity roles with the required level of access to a given component.
- (x) MiFare Crypto 1 is a stream cipher used in London's Oyster card, Netherland's OV-Chipcard, and in numerous wireless access control and ticketing systems worldwide. Researchers were able to recover this algorithm by reverse engineering. The encryption uses a 48-bit key, which could be recovered in seconds on a PC given a known IV (from one single encryption). The card manufacturer failed to apply [redacted].

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

(i) In the context of an insecure channel, we can say that a message that has been modified in transit means that it no longer comes from its original source. From this argument, we can draw a conclusion that:

- (a) data-origin authenticity implies data integrity
- (b) data integrity implies data-origin authenticity
- (c) data confidentiality implies data integrity
- (d) data integrity implies data confidentiality
- (e) data confidentiality implies data-origin authenticity

(ii) 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 first rule of the monastery above (R_1) 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

(iii) In Facebook, a user who creates a post can determine who can view the post, namely either: public, all friends, specific friends, or private (only the user). This is an example of a/an _____.

- (a) mandatory access control
- (b) discretionary access control
- (c) role based access control
- (d) protection rings
- (e) least privilege principle

- (iv) Suppose you are assigned a task to harden the Web server `www.companyxyz.com` of Company XYZ, and assume that you are given an access to the company network. Now you want to perform the following steps:

S_1 : Find out the IP addresses of the Web server and associated DNS server.

S_2 : Check that the Web server is alive.

S_3 : Find out all open ports in the server besides HTTP/HTTPS.

What is the most suitable UNIX/Linux tool chain (in the required order) that you should run to complete the sequence of tasks above?

- | | |
|---------------------------------------|--|
| (a) <code>ping, nslookup, nmap</code> | (d) <code>nslookup, ping, nmap</code> |
| (b) <code>nmap, nslookup, ping</code> | (e) <code>nslookup, nmap, wireshark</code> |
| (c) <code>nmap, ping, nslookup</code> | |

- (v) _____ protocol secures applications at the IP layer as well as all IP-based application traffic.

- | | |
|-------------|-----------|
| (a) HTTPS | (d) IPSec |
| (b) DNSSEC | (e) WPA2 |
| (c) TLS/SSL | |

(Note: The following 5 questions summarize different Web attacks by distinguishing them. The term *server* below means either Web server or its associated database server.)

- (vi) Which Web attack below is a case whereby a client attacks a server?

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

- (vii) Which Web attack below is a case whereby a server attacks a client?

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

(viii) Which Web attack below is a case whereby a client attacks another client by exploiting the victim client's trust of an involved server?

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

(ix) Which Web attack below is a case whereby a client attacks another client by exploiting an involved server's trust of the victim client?

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

(x) Which Web attack below is a case whereby the relaying network attacks a client?

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

3. [20 marks] (Short Questions): Answer Questions (ii) and (iii) in 1–3 sentences, or by using a concise diagram.

(i) [6 marks] (Cryptographic Techniques and Services)

In the module, you have learnt various cryptographic techniques, which include:

Hash (H)	Block cipher (BC)
MAC (M)	Stream cipher (SC)
Digital signature (DS)	Public-key cipher (PKC)

Assign the techniques listed above into the applicable cell(s) in the table below. Note that one technique may be able to provide *more than one* cryptographic services. You can just write down the letter shorthand of a listed technique, i.e. H for Hash, below. (Note: You can presume that block cipher refers to as a secret-key based technique.)

Cryptographic Service	Relevant Secret-Key Technique(s)	Relevant Public-Key Technique(S)
Confidentiality (with high diffusion)		
Confidentiality (with low diffusion)		
Integrity		
Authenticity		
Non-repudiation		

(ii) [6 marks] (Cryptography: Secret-Key Cryptography)

Wikipedia says that the Caesar/shift cipher is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some (fixed number of) positions down the alphabet. For example, with a right shift of 3, A would be replaced by D, B would become E, and so on. By first transforming the 26 letters and the space character (' ') into numbers according to the scheme $A \rightarrow 0, B \rightarrow 1, \dots, Z \rightarrow 25, _ \rightarrow 26$, the encryption of letter x by a shift n can be mathematically described as:

$$E_n(x) = (x + n) \bmod 27.$$

- (a) (1 mark) What is the key space size of the Caesar/shift cipher including a “trivial encryption” where each letter x is mapped into itself?

- (b) (2 mark) The Vigenere cipher improves the Caesar cipher by employing a series of interwoven Caesar ciphers based on the letters of a (repeating) key. Suppose the plaintext is: ATTACKATDAWN, and the key is ABCDABCDABCD. The ciphertext then becomes: AUVDCLCWDBYQ. Notice that the letter T at the second and third positions are encrypted differently into U and V, respectively. Suppose the employed key length is k , what is the key space size of the Vigenere cipher including a “trivial encryption”?

- (c) (1 mark) Is the Vigenere cipher still easily broken under the known-ciphertext attack scenario?

- (d) (2 marks). Consider the ciphertext-only attack scenario. Suppose you know the used key length k , say 8. Given a long ciphertext, how can you possibly recover the plaintext? Explain your method clearly and sufficiently.

- (iii) [8 marks] **(Cryptography: Mode-of-Operation)** Let us consider the Cipher Block Chaining (CBC) mode-of-operation, which is commonly used to encrypt a plaintext longer than a block. In CBC, each plaintext block is XOR-ed with the previous ciphertext block before being encrypted. An IV is used in encrypting the first plaintext block. Mathematically, the encryption can be expressed as follows:

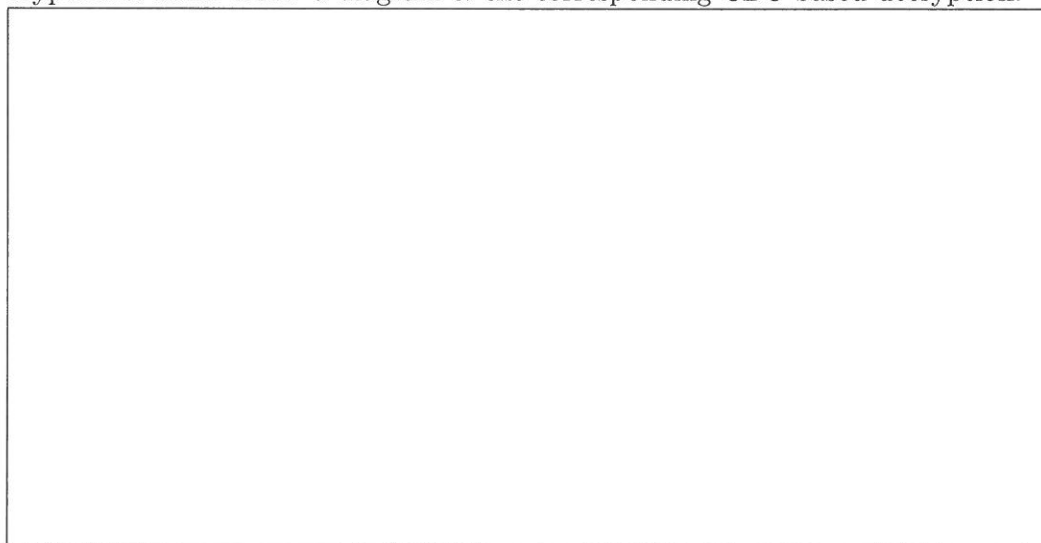
Given a n -block plaintext message $x_1, x_2, x_3, \dots, x_n$ and a secret key K ,

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

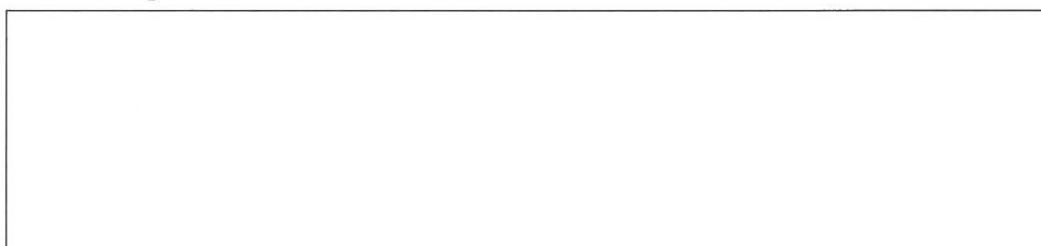
$$y_0 = IV;$$

$$y_k = Enc_K(x_k \oplus y_{k-1}), \text{ for } k = 1, 2, 3, \dots, n.$$

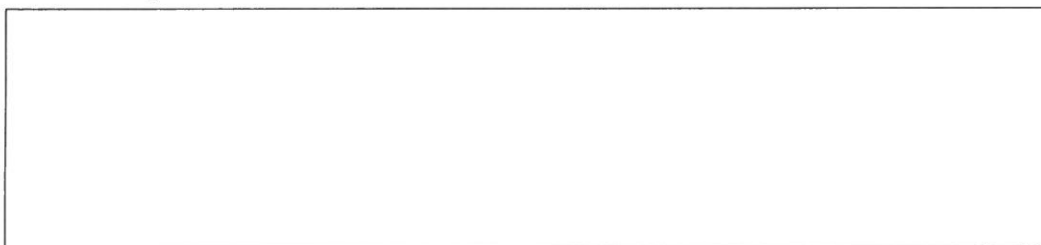
- (a) (2 marks) Your lecture notes show a diagram depicting how a CBC-based encryption is done. Draw a diagram of the corresponding CBC-based decryption.



- (b) (1 mark) How is decryption affected if the *first* ciphertext block y_0 is removed from the ciphertext?



- (c) (1 mark) How is decryption affected if the *last* ciphertext block y_n is removed from the ciphertext?



- (d) (1 mark) How is decryption affected if there is a single-bit flip error in the *first* ciphertext block y_0 ? Which ciphertext blocks will be corrupted?

- (e) (3 marks) Suppose we already have the encryption of a message x as above. Now, we want to add a particular plaintext block x_0 at the beginning of the message x , so that the extended plaintext becomes $x_0, x_1, x_2, \dots, x_n$. Given an existing ciphertext $y_0, y_1, y_2, \dots, y_n$ and x_0 , a legitimate user who knows the key K can efficiently achieve this by just inserting a ciphertext block y_{-1} at the beginning of the ciphertext, and produce the extended ciphertext $y_{-1}, y_0, y_1, \dots, y_n$. Show how the user should set y_{-1} , which is the new IV in the extended ciphertext.

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

(i) [10 marks] (Firewall Design)

Consider the firewall scenario and design in Tutorial 6, whose solution is posted in IVLE. For your reference, the solution is given below.

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

DMZ: Web-server, Email-server, Lab, Lab-printers.

Internal: Teachers, Teacher-printers, SQL-server.

Firewall F_1 :

<i>source IP</i>	<i>dest IP</i>	<i>source port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>
Web-server	*	HTTP	*	OUT	Allow
*	Web-server	*	HTTP	IN	Allow
Email-server	*	SMTP	*	OUT	Allow
*	Email-server	*	SMTP	IN	Allow
Lab	*	*	HTTP	OUT	Allow
*	Lab	HTTP	*	IN	Allow
Teachers	*	*	HTTP	OUT	Allow
*	Teachers	HTTP	*	IN	Allow
*	*	*	*	*	Block

Firewall F_2 :

<i>source IP</i>	<i>dest IP</i>	<i>source port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>
SQL-server	Web-server	SQL	*	OUT	Allow
Web-server	SQL-server	*	SQL	IN	Allow
Teachers	*	*	HTTP	OUT	Allow
*	Teachers	HTTP	*	IN	Allow
Teachers	Email-server	*	SMTP	OUT	Allow
Email-server	Teachers	SMTP	*	IN	Allow
*	*	*	*	*	Block

- (a) (2 marks) Suppose you also want to allow **Lab** and **Teachers** to access any HTTPS servers on the Internet. Put new rules to be inserted at (the top of) F_1 (Note: the pre-defined port number of HTTPS can be written as HTTPS):

<i>source IP</i>	<i>dest IP</i>	<i>source port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>

- (b) (1 mark) Also put new rules to be inserted at (the top of) F_2 :

<i>source IP</i>	<i>dest IP</i>	<i>source port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>

- (c) (1 mark) Suppose now you can afford a 3-firewall setting to further strengthen the school's network. You want to remove **Lab** and **Lab-printers** from DMZ, which is still a rather unsafe network zone, into an independent network segment. Describe your new network partitioning. (Assume that F_1 is the outer/public-facing firewall and F_3 is your innermost firewall.)

- (d) (2 marks) Write down the rules for F_1 in your new 3-firewall setting, assuming that you allow **Lab** and **Teachers** to access only HTTP and SMTP as in Tutorial 6 (Note: you are allowed to cite the difference from the rules for firewall $F_1/F_2/F_3$ in the previous 2-firewall setting given above):

<i>source IP</i>	<i>dest IP</i>	<i>source port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>

- (e) (2 marks) Write down the rules for F_2 in your new 3-firewall setting (Note: you are allowed to cite the difference from the rules for firewall $F_1/F_2/F_3$ in the previous 2-firewall setting given above):

<i>source IP</i>	<i>dest IP</i>	<i>source port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>

(f) (2 marks) Write down the rules for F_3 in your new 3-firewall setting

(Note: you are allowed to cite the difference from the rules for firewall $F_1/F_2/F_3$ in the previous 2-firewall setting given above):

<i>source IP</i>	<i>dest IP</i>	<i>source port</i>	<i>dest port</i>	<i>direction</i>	<i>action</i>

(ii) [5 marks] (Secure Programming)

Consider the following C program snippet.

```
1  void copy_function(char *input)
2  {
3      unsigned char buffer[31];
4      unsigned char input_length = strlen(input);

5      if (input_length <= 30)
6      {
7          strcpy(buffer, input);
8          printf("The supplied argument is %s.\n", buffer);
9      }
10     else
11     {
12         printf("Your supplied argument is too long!\n");
13     }
14 }

15 int main(int argc, char *argv[])
16 {
17     if (argc == 2)
18         copy_function(argv[1]);
19     else
20         printf("Please supply one argument with length at most 30 characters.\n");

21     return 0;
22 }
```

- (a) (3 marks) The above program is vulnerable. Describe the vulnerability, and its input instance (in particular the length of the supplied first argument).

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

(iii) [5 marks] (Authentication and network protocol)

Bob developed a one-time password system for authentication to UNIX-like OSs. He wanted to efficiently derive a one-time password for each session of user U , based on the user's master password P_U . Because each session password is used only once, they are useless to password sniffers. The k -th one-time password is derived by recursively applying a one-way hash function $h()$ to P_U , i.e. $p_k = h^k(P_U)$, for $k = 1, 2, \dots, n$.

The authentication protocol works as follows.

Initial set-up: User U memorizes P_U .

User U and a host H set U 's initial status to $(U, n, h^n(P_U))$.

Current state: The current password entry of U in H is $(U, c, h^c(P_U))$, with $1 \leq c \leq n$.

User's next authentication:

1. $U \rightarrow H: U$
2. $H \rightarrow U: c$, "Your next one-time password:"
3. $U \rightarrow H: p_{c-1} = h^{c-1}(P_U)$
4. H checks the kept entry $(U, c, h^c(P_U))$, and grants access if $h(p_{c-1}) = h^c(P_U)$.

Then H updates U 's current password entry to $(U, c-1, h^{c-1}(P_U))$.

Notice that a password sniffer who obtains $h^c(P_U)$, with $1 \leq c \leq n$, cannot derive the next one-time password $p_{c-1} = h^{c-1}(P_U)$ as $h()$ is a strong one-way hash function. Can Mallory, an *active attacker* who acts as a man-in-the-middle between U and H , gain the knowledge of U 's next session password and perhaps also authenticate herself to H ? If so, describe how Mallory can accomplish that.

This page is intentionally left blank.

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

— End-Of-Paper —