UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2013/2014

COURSE NAME	:	COMPUTER SECURITY
COURSE CODE	:	BIT 31303
PROGRAMME	:	3 BIT
EXAMINATION DATE	:	JUNE 2014
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **SEVEN (7)** PAGES

Q1 (a) Classify each of the following as a violation of **confidentiality** (C), OR **integrity** (I), OR **availability** (A), OR of some combination thereof:

(i) Adham installs keylogger program and hijacks Adra's Facebook session. He reads Hasan's messages to Adra and sends a response.

(3 marks)

(ii) Judika using Jack The Ripper tool to crack Julie's computer password. He then log in as Julie and set a new password in her word document.

(3 marks)

(iii) Sinchan posts a message on fsktm facebook's group, a popular social networking site, asking student to claim free voucher at freeticket.org website starting 12am tomorrow.

(3 marks)

(iv) Karl pretends to be Kareem, from human resources department at his company. He calls Information Technology Center (ITC) and ask for Kareem's password. He then logs in as Kareem and upgrade his working grade from DS45 to DS52.

(3 marks)

(v) Mimiloma forge Kikilala's signature on house agreement. He then issues fake cheque to the house developer.

(3 marks)

(b) Consider the following C code:

```
/* Information about the current CD. */
struct cd {
 int numtracks; /*The number of tracks on this disc.*/
 int tracklen[16]; /*The length of each track on the disc*/
 void  (*notify)(struct  cd  *);  /*Call  this  when  the  CD  info
changes*/};

struct cd *curcd = makestructcd();

/* Update the length of track number 'track'. */
void update_cdinfo(int track, int newtracklen)
{
 if (track > 16)
 return;
 curcd->tracklen[track] = newtracklen;
(curcd->notify)(curcd);
}
```

Figure Q1(b)

Assume that `makestructcd()` allocates and initializes a `struct cd`. The attacker can arrange for `update_cdinfo()` to be called with whatever values of track and `newtracklen` he likes.

(i) What is the security vulnerability in this code?

(2 marks)

(ii) Determine how could an attacker exploit this vulnerability to trigger the execution of malicious code?

(3 marks)

Q2 (a) Suppose we have the following network nodes A, B, C and D in **Figure Q2(a)**.

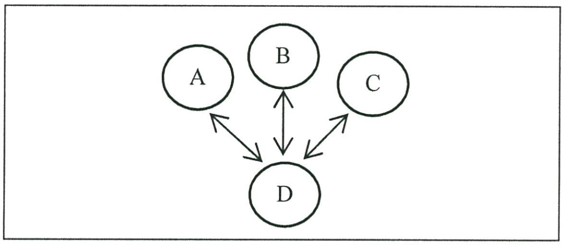

Figure Q2(a)

(i) How many key(s) do we have to generate such that A, B and C can communicate with D in a bidirectional secure way using a symmetric encryption algorithm?

(2 marks)

(ii) Replace the symmetric encryption algorithm with the public key system. How many public key(s) do we have to generate such that A, B and C can communicate with D in a bidirectional secure way?

(2 marks)

(iii) Discuss **ONE (1)** difference between block cipher and stream cipher.

(2 marks)

(b) Consider a Vernam Cipher with the following scenario letter encodings:

letter	A	E	I	M	O	R	T	V
encoding	000	001	010	011	100	101	110	111

Assume that a message (M) = MOVIE is Vernam encrypted into ciphertext (C) = RTOMO ; C=M ⊗ K where ⊗ shows XOR operation. Determine the encryption key, K by providing details of your cryptanalysis.

(5 marks)

(c) Encrypt the message:

```
Life is like riding a bicycle
```

using the following algorithms:

(i) Caesar Cipher (use shift by 3)

(5 marks)

(ii) Caesar Cipher (use key = ”alberteinstein”)

(5 marks)

(iii) Vigenere Cipher (use key=”alberteinstein”)

(5 marks)

Q3 (a) SQL injection is a technique often used to attack data driven applications. This is done by including portions of SQL statements in an entry field in an attempt to get the website to pass a newly formed fraudulent SQL command to the database. Explain how intrusion prevention (IPS), query-level access controls and event correlation can be combined to effectively combat SQL injection.

(8 marks)

(b) Discuss **THREE (3)** roles of the Database Administrator (DBA) with respect to security?

(5 marks)

(c) Demonstrate the use of an audit trail, with special reference to a database system.

(7 marks)

(d) Consider the following scenarios:

Company A:
Gemilang Sdn Bhd is a big corporate with 10 branches accessing its corporate server farm located at its headquarters in Parit Raja.

Company B:
Bindu Sdn Bhd, a small company with 100 employees is running its own web server for marketing purposes.

Propose suitable firewall topologies for each company.

(6 marks)

Q4 (a) Ramlee received fraud email claimed from Maybank regarding his account profile as shown in **Figure Q4(a)**.

```
From         : Maybank <ssl.secure@maybank2u.com.my>
Reply-to     : marketing@keystoneridge.com
Date         : Wednesday, 15 April, 2014 12:00 PM
To           : p.ramlee@gmail.com
Subject      : Customer Status Update
Attachment   : maybank.zip
--------------------------------------------------------
Dear Customer,
It has come to our notice that your account profile has not
been validate since we upgrade our server. To avoid account
suspension, kindly log on to our website below to validate
your profile.
Log On
We are sorry for any convenience this may cause. Thank you
for choosing us.

Mybank2u
```

Figure Q4(a)

Analyze **Figure Q4(a)** and outline **FOUR (4)** reasons why this email is categorized as fraud email.

(8 marks)

(b) Describe **THREE (3)** important practices that could avoid virus infection through online application.

(6 marks)

(c) Illustrate the concept of social engineering with **ONE (1)** example.

(4 marks)

(d) COMBI Bank hires you as a Computer Security officer to design a secure solution for their Internet banking. The Internet banking has the following requirement:

- A customer should be authenticated by some other method than using password to log in to the Internet banking. The authentication technique using only password is not enough.

(i) Discuss **TWO (2)** methods that should be good solutions for authenticating the internet banking. Explain how the method is used for authentication.

(4 marks)

(ii) Outline **THREE (3)** good security practices that are important to protect your password.

(6 marks)

- END OF QUESTION –

FINAL EXAMINATION

SEMESTER/SESSION: SEM II/2013/2014 PROGRAMME : 3 BIT
COURSE NAME : COMPUTER SECURITY COURSE CODE: BIT 31303

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FIGURE Q2(c)(iii)