NATIONAL UNIVERSITY OF SINGAPORE

CS2107 — INTRODUCTION TO INFORMATION SECURITY

(Semester 2: AY 2014/15)

Time Allowed: 2 Hours

INSTRUCTIONS TO STUDENTS

1. Please write your Student Number only. Do not write your name.
2. This assessment paper contains **FIVE** questions and comprises **ELEVEN** 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	15		
Q2	25		
Q3	20		
Q4	20		
Q5	20		
Total	100		

1. **[15 marks]** (Terminologies) The following descriptions are obtained from the web. Fill in the blanks with the most appropriate terminologies from the following list. Only one answer per blank. Some choices may appear more than once in the answer. You can either write the terminology or its number in the blank. (Ignore grammar rules on plural forms).

(1) black hat
(2) white hat
(3) black list
(4) white list
(5) zero-day vulnerability
(6) vulnerability
(7) exploit
(8) CVE
(9) revocation list
(10) root certificate
(11) certificate
(12) Extended Validated Certificate
(13) signature
(14) canery
(15) integrity
(16) confidentiality
(17) non-repudiation
(18) availability
(19) discretionary access control
(20) role-based access control
(21) mandatory access control
(22) mnemonic method
(23) maximum likelihood
(24) Kerckoffs's principle
(25) obscurity
(26) least privilege
(27) side-channel attack
(28) honeynet
(29) trapdoor function
(30) bait-and-switch

(a) Buffer overflow is an attack on the memory _____ .

(b) The hardware key-logger captures the keystrokes, and thus compromise _____ .

(c) Signature scheme uses PKC whereas mac uses symmetric key. Hence, signature is able to ensure _____ while mac can't.

(d) Superfish admits installing _____ as so to be the man-in-the-middle between the browser and the web-server even under the secure HTTPS connection.

(e) Your web browser will display a green address bar when visiting a web site that has been secured by a valid _____ .

(f) Some hackers are criminals and use their computer skills to harm or damage computer systems. These people are called _____ hackers.

(g) A _____ refers to a flaw in the software which is unknown to the manufacturers. This security hole could be exploited by hackers before the vendor becomes aware and rushes to fix it, and thus giving this name.

(h) _____ is a list of information security flaws that aims to provide common names for publicly known cyber security issues. The goal is to make it easier to share data across separate tools, repositories, and services with a "common enumeration."

(i) A _____ is a register of those that are being provided a particular privilege, service, mobility, access or recognition. Those in it will be accepted, approved or recognized.

(j) A basic rule of cryptography is to use published, public, algorithms and protocols; there should be no secrecy in the algorithm. This is generally known as _____ .

(k) The attack uses the power consumed by the chip to derive the secret key. This is an example of _____ .

(l) The user selects a phrase and extracts a letter of each word in the phrase (e.g. Titwclhediml for "This is the worst car I have ever driven in my life'). This is known as the _____ .

(m) A _____ contains intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security.

(n) Under _____ , the subject can transfer authenticated objects or information access to other users.

(o) The algorithm of RC4 was initially not made public, and thus security was achieved partially by _____ .

2. **[25 marks]**

(a) Alice was connected to the Internet via a hotel free wifi, which was open and not protected by WEP nor WPA. Alice logged-in to IVLE and uploaded her CS2107 report. Recall that IVLE only accepts HTTPS. Bob was another hotel guest and was also enrolled in CS2107. Mark a cross "×" beside the items which can be obtained or completed by Bob,

i. ☐ The fact that Alice visited IVLE;
ii. ☐ Alice's IVLE password;
iii. ☐ Alice's ip-address;
iv. ☐ Alice's mac address;
v. ☐ IVLE's private key;
vi. ☐ IVLE's certificate;
vii. ☐ The TLS/SSL session key;
viii. ☐ Alice's report;
ix. ☐ DNS attack (the "basic type of DNS attack" as described in lecture 5 slide 22 to 26.)

(b) Consider another guest Charles. Charles carried out a few additional steps: connected to Internet via the hotel's wifi; connected to IVLE via an *anonymous proxy*; uploaded the encrypted report. Similarly, mark a cross "x" beside the items which can be obtained/performed by Bob.

i. ☐ The fact that Charles visited IVLE;
ii. ☐ Charles's ip address;
iii. ☐ Charles's mac address;
iv. ☐ Charles's report.

Here is an description of anonymous proxy from the web. "*An anonymous proxy provides a service that attempts to make activity on the Internet untraceable. It is a proxy server that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.*"

(c) Dave is another guest, and he carried out these steps: encrypted the report using a tool in Acrobat Reader; connected to Internet via the hotel's wifi; sent the encryption password to the lecturer through email; logged-in to IVLE and uploaded the encrypted report. Describe a scenario where Dave's extra precaution provides more security than Alice's procedures (i.e. describe a scenario whereby an attack on Alice is possible but not on Dave).

3. **[20 marks]** A musical fountain B and a console C are connected by a wireless communication channel. Both B and C share a 256-bit key k. All transmitted messages are encrypted. That is, if m is the message, the ciphertext $AES_k(m)$ will be sent wirelessly.

   The fountain can be controlled by a set of 2^{24} valid instructions, and each instruction is represented using 4 bytes. An instruction can be sent from C to B over the wireless channel. If the fountain receives an invalid instruction, the instruction will be discarded; otherwise the instruction will be carried out. Note that the delicate equipments in the fountain can be damaged by executing inappropriate instructions.

   Explain why this system is not secure. In particular, explain why an attacker who sends random ciphertexts over the wireless channel can inflict damages.

   An updated version of the communication system includes integrity check by adding a SHA3 digest. The message m (in particular the 4-byte instruction) is concatenated with its digest $SHA3(m)$. Hence, $AES_k(m \| SHA3(m))$ will be sent wirelessly. The AES is configured as a stream cipher. That is, based on the key k and the initial value, the encryption scheme generates a pseudo random sequence, and then "xor" the sequence with $m \| SHA3(m)$.

   Explain why the updated version can prevent the above-mentioned attack.

This updated version is also not secure. Suppose an attacker has obtained the ciphertext $c_0 = AES_k(m_0 \| SHA3(m_0))$ and knows the instruction m_0, the attacker can construct the ciphertext $c_1 = AES_k(m_1 \| SHA3(m_1))$ where m_1 can be any instruction chosen by the attacker. Explain how the attacker can compute c_1.

A revised version uses AES under the CBC mode, instead of the stream cipher mode. Give an attack on the revised version.

4. **[20 marks]**

(a) The school is planning to re-configure the lab's door access systems. Two options are being considered:

(A) To gain access, a student has to tap his/her student's card, and then enters password.

(B) To gain access, a student has to tap his/her student's card, and then has his/her fingerprint scanned.

Give the two main advantages of option (A) over option (B).

Give the two main advantages of option (B) over option (A).

(b) The school is also considering incorporating two-factor authentication into IVLE. The two factors are the password, and the biometric fingerprint. Hence, every user's laptop must be equipped with a fingerprint scanner. To login, the user has to key in the usual username and password, follows by having the fingerprint scanned. You strongly object and argue that, (1) password guessing attacks can side-step the "who you are" factor and essentially bring the process back to single-factor authentication, and (2) it can be less "secure" than the original password authentication due an additional security concern.

Explain more on the attack in (1).

Give the additional security concern in (2).

5. **[20 marks]**

(a) Consider the permission and ownership of the following Unix files.

```
-rwx---r-x   1 alice   year1 10 Mar 10 01:00 program1
-rwx---r-x   1 bob     staff 10 Mar 10 01:00 program2
-rws---r-x   1 bob     staff 10 Mar 10 01:00 program3
-rw-------   1 bob     staff 10 Mar 10 01:00 data.txt
```

Suppose `alice` executes `program2`, who would be the real UID of the process?

Who would be the effective UID?

Does this process has permission to read `data.txt`?

Suppose `alice` executes `program3`, who would be the real UID of the process?

Who would be the effective UID?

Does this process has permission to read `data.txt`?

Does Unix file system adopt access control list or capability?

(b) We know that `strcpy()` is not safe because there is no bound checking. The following segment attempts to perform the check. In this program, `a` is an array whose size is 20. The string `b` is provided by the potentially malicious user. The variable `reserve` indicates the number of cells to be reserved in array `a`. To prevent buffer overflow, the program checks that the length of `b` is well below 20 before copying it to `a`.

```
{ unsigned char total, reserve;      // each is a 8-bit unsigned integer
  reserve=10;

  total =  reserve + strlen (b);     // strlen(b) returns the length of b
  if (total < 20) { strcpy ( a, b);} // copy string b into a
}
```

Explain why the above is still vulnerable, and describe the choices of `b` such that buffer overflow will occur.

— End-Of-Paper —