請勿攜去
Not to be taken away





# 香 港 中 文 大 學

## The Chinese University of Hong Kong

二 0 一七至一八年度上學期科目考試

Course Examination 1st Term, 2017-18

科目編號及名稱
Course Code & Title : IERG4130 Introduction to Cyber Security

時間
Time allowed : 3 小時 hours 00 分鐘 minutes

學號
Student I.D. No. : .....

座號
Seat No. : .....

Answer ALL the Questions in Section I, and 4 out of 6 in Section II.
The questions carry a total of 100 marks.
Each question of the same section carries the same marks.
Put your answers on the answer-book.
Make your answers precise and concise.

**Use of Electronic Calculators:** "The calculator:

(a) should be self-contained, silent, battery-operated and pocket-sized; and
(b) should have numeral-display facilities only; and
(c) should be used only for the purpose of calculation.

It is the candidate's responsibility to ensure that the calculator operates satisfactorily and the candidate must record the name and type of calculator on the front page of the examination scripts."

**Special Note:**
Each candidate is allowed to bring ONE A4-sized sheet with notes on both sides into the examination venue.

**Section I (total of 36 marks)**

True-False questions not to be provided.

## Section II (64 marks, choose 4 out of 6, mark your choices on the cover)

### *Q1. Network Security (16 marks in total)*

Identification field in IP datagram uniquely identifies a datagram. Usually, the value is incremented by one for every packet sent. Fragments of the same datagram will have the same identification value. This allows the receiver to determine which fragment belongs to which datagram.

Host 4130 implements the identification field in IP datagram as follows. It maintains a single counter that is incremented by one for every packet sent. The value of the counter is embedded in each outgoing packet. Suppose host 4130 responds to ICMP ping requests.

(a) [2 marks] Suppose you can exchange packets with host 4130, how can you test if 4130 sent a packet to others within a certain time?

(b) [6 marks] Suppose you want to test whether a victim host V accepts connection to port *n* without revealing your IP to V. Explain how to use host 4130 to achieve this.
Hint: Recall the following facts about TCP:

- A host that receives a SYN packet to an open port *n* sends back a SYN/ACK response to the source IP.
- A host that receives a SYN packet to a closed port *n* sends back a RST packet to the source IP.
- A host that receives a SYN/ACK packet that it is not expecting sends back a RST packet to the source IP.
- A host that receives a RST packet sends back no response.

(c) [4 marks] Suppose an attacker sends ICMP packets to an IP broadcast address. How would host 4130 respond if it receives those packets? What is the goal of the attacker in doing this?

(d) [4 marks] Suggest two different ways to prevent the attacks from happening as mentioned in (b) and (c) respectively. Briefly Explain.

***Q2. Network Defense (16 marks in total)***

(a) [4 marks] In SSL, the client uses public key encryption to encrypt a (symmetric) session key for further communications. Name one advantage of such approach. Explain it briefly.

(b) [4 marks] Describe a scenario that we should use transport Mode of IPsec over tunnel Mode. Explain it briefly.

(c) [4 marks] Describe an attack that can be prevented by a stateful firewall but not a stateless firewall. Explain it briefly.

(d) [4 marks] What is zero-day attack? Which kind of firewall, anomaly-based or signature-based, is more likely to discover such attack? Why?

***Q3. Key Exchange Protocol (16 marks in total)***

Alice and Bob want to come up with a symmetric key for a communication session between them. Suppose Eve is able to observe and modify the traffic between Alice and Bob.

Suppose Alice and Bob decided to use Needham–Schroeder protocol.

(a) [4 marks] Who are Alice and Bob trusting? What can go wrong if the trust assumption does not hold?

(b) [4 marks] Can Eve learn the symmetric key between Alice and Bob? If yes, suggest a way to prevent this. If not, state what prevents this. Briefly explain.

Suppose Alice and Bob decided to use Diffie-Hellman Key Exchange protocol.

(c) [4 marks] Can Eve learn the symmetric key that Alice and Bob eventually obtained from Diffie-Hellman Key Exchange protocol? If yes, suggest a way to prevent this. If not, state what prevents this. Briefly explain.

(d) [4 marks] Suppose Eve is a weaker attacker such that she cannot modify the traffic, can Eve learn the symmetric key between Alice and Bob? If yes, suggest a way to prevent this. If not, state what prevents this. Briefly explain.

***Q4. Public Key Cryptography (16 marks in total)***

Alice has generated an RSA public key by first choosing two prime numbers $p$ = 101 and $q$ = 151. She computes $N = 101 \times 151$, and chooses $e$ = 6043. The public key is set as $(e, N)$.

(a) [2 marks] Show that $d$ = 3907 can be used as the decryption key $dk$.

(b) [6 marks] Given a ciphertext $c$ = 4130, find the corresponding message $m$ with steps. (Hint: You may use the Chinese Remainder Theorem to speed it up.)

Suppose $g$ is a generator of a cyclic group with prime order $q$.
Consider the following signature system:
KeyGen: random pick $x, y$, set $h = g^x$, $u = g^y$, output $sk = (x, y)$ and $pk = (g, h, u)$
Sign($sk$, $m$): output $s$ such that $u = g^m h^s$
Verify($pk$, $m$, $s$): output accept if $u = g^m h^s$ and reject otherwise.

(c) [4 marks] Show how to find $s$ using $sk$ in the signing algorithm.

(d) [4 marks] Show that with the signatures on two different messages $m$ and $m'$, one can recover $sk$.

***Q5. Symmetric Key Cryptography (16 marks in total)***

Suppose an attacker has a Double-DES ciphertext $c = \text{Enc}_{k2}(\text{Enc}_{k1}(m))$ and the corresponding message $m$.

(a) [4 marks] Describe how can the attacker recover $k1$ and $k2$ by the naïve brute-force attack. What is the time and space complexity of the attack?

(b) [4 marks] Describe how can the attacker recover $k1$ and $k2$ using meet-in-the middle attack. What is the time and space complexity of the attack?

We use AES encryption (Enc($k$, $m$), Dec($k$, $c$)) and a secure hash function h to construct a probabilistic MAC scheme (PSign, PVerify) as follows:

Psign($sk$, $m$):
1. Pick a random string $r$ having the same length as $sk$;
2. Output $s$ = (h($r$), Enc(h($m$), $r \oplus sk$))

(c) [4 marks] Write down the verification algorithm PVerify($sk$, $m$, $s$) such that an adversary cannot forge on a message without seeing any valid MAC.

(d) [4 marks] Suppose you are provided with an oracle machine that given $m$, returns a valid probabilistic MAC on $m$ which we call $s$. You are an attacker who can use this machine ONCE only. Show probabilistic MAC is insecure by giving a valid MAC $s'$ for a new message $m' \neq m$.

***Q6. Authentication Mechanisms (16 marks in total)***

Consider the following variant of UNIX password system: replace the original password file with a publicly readable file called /etc/encpw. An entry in the file for user A consists of the user's identifier $id_A$ and the encrypted password $c_A$ = AES.Enc(KeyDer($p_A$), $p_A$), where KeyDer() is a key derivation function which outputs an AES secret key when given a password, and $p_A$ is the user's login password.

(a) [2 marks] The system needs to verify that $p_A$ was correctly supplied. Explain the procedure.

(b) [6 marks] Assuming all the cryptographic algorithms are publicly known, is the above variant more secure than the typical UNIX password system? Give two reasons to justify your answer.

You want to screen-lock your smartphone such that only you can unlock it and use the apps in it.

(c) [4 marks] Describe two possible "non-secret-based" locking mechanisms which do not require any memorization. For each of those, describe the corresponding attack.

(d) [4 marks] You lent your smartphone to your friend for a few minutes. Later, you found that your friend can also unlock your smartphone (either by recalling your secret, or passing one of the authentication mechanisms in (c)). Describe one way that your friend has possibly done in those few minutes. Briefly explain how the attack is possible. Remember to state which one of the underlying authentication mechanism you assumed in answering this question, secret-based or non-secret-based.

- End -