請勿攜去
Not to be taken away

香 港 中 文 大 學

The Chinese University of Hong Kong

二 0 一六至一七年度上學期科目考試

Course Examination 1st Term, 2016-17

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

時間 小時 分鐘
Time allowed : 2 hours 30 minutes

學號 座號
Student I.D. No. : ..... 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 (T) or False (F) with reasoning: 3 marks per question, no penalty for incorrect answer. However, in order to get ANY credit for each question, you need to justify your answer with a brief explanation, no matter you answered T or F.

True-False questions not to be provided.

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

Q1. MAC and Signature (16 marks in total)

Let the initial vector $IV = c_{-1} = 0$ and an underlying block cipher be (Enc, Dec). We use CFB residue to be the message authentication code (MAC) for a multiple-block message $M = (m_0, m_1, ..., m_n)$ as follows: $c_i = \text{Enc}(sk, c_{i-1}) \oplus m_i$, and outputs the last ciphertext block c_n as the resulting tag τ.

(a) [4 marks] Suppose you are provided with an "oracle machine" that given M, returns a valid CFB-residue tag τ for M. You can use this machine ONCE only. Show CFB-residue is insecure by giving a valid tag τ' for a new message M' ≠ M.

(b) [4 marks] Suggest a fix to this CFB residue.

Consider the textbook RSA signature scheme. Given $p = 101$, $q = 199$, $N = 20099$, $e = 679$, $pk = (e, N)$.

(c) [1 mark] Show that the value of the signing key $sk = d = 8719$.

(d) [1 mark] Show that $p^{-1} \bmod q \equiv 67 \bmod q$.

(e) [6 marks] The signature σ of a message m is computed as $\sigma = m^d \bmod N$. Note that d is usually a large number so we usually use the Chinese Remainder Theorem to speed it up. Given $m = 15012$, find its signature σ with steps.

Q2. Password Hashing (16 marks in total)

When storing a password p for user u, a website randomly generates a string (called a salt) s, and saves the tuple $(u, s, r = H(p||s))$, where H is a cryptographic hash function and || denotes the string concatenation operation.

(a) [2 marks] When user u tries to log in with a password p^*, how does the web server verify the password?

(b) [2 marks] Which kind of attack can salt s help to defend against?

(c) [2 marks] A tester said that the storage is encrypted so salting is unnecessary. But the security architect insists to keep it. What is the security principle behind?

Consider $H^*(x) = g^x \bmod q$, where q is a large prime and g is a generator of $\mathbb{Z}_q^*$.

(d) [3 marks] Given H^* and an image $h = H^*(x)$ for a random x, is it hard to find y such that $H(y) = h$? Justify your answer. State any assumption you have made.

(e) [3 marks] Given H^*, is it hard to find x and y such that $H^*(x) = H^*(y)$? Justify your answer.

(f) [4 marks] Is H^* a suitable choice for the website's password hashing scheme? Justify your answer in terms of efficiency and security.

Q3. Needham-Schroeder Protocol (16 marks in total)

Alice (A) and Bob (B) use Needham–Schroeder protocol to come up with a symmetric key for a communication session between them with the help of a trusted server (S).

Recall the details of Needham–Schroeder protocol are as follows:

1. $A \rightarrow S: A, B, N_1$
2. $S \rightarrow A: \mathrm{Enc}_{K_{AS}}(N_1, B, K_{AB}, \mathrm{Enc}_{K_{BS}}(K_{AB}, A))$
3. $A \rightarrow B: \mathrm{Enc}_{K_{BS}}(K_{AB}, A), \mathrm{Enc}_{K_{AB}}(N_2)$
4. $B \rightarrow A: \mathrm{Enc}_{K_{AB}}(N_2 - 1, N_3)$
5. $A \rightarrow B: \mathrm{Enc}_{K_{AB}}(N_3 - 1)$

Notations:

K_{AS} is a symmetric key known by A and S only

K_{BS} is a symmetric key know by B and S only

K_{AB} is a symmetric key generated by S for this session between A and B

N_1, N_2, N_3 are nonces

(a) [4 marks] What is replay attack? In general, which part(s) of "CIA triad" is(/are) replay attack violating? Explain.

(b) [4 marks] What is nonce? What is the purpose of N_1?

(c) [4 marks] Eve has been monitoring and recording the Needham-Schroeder protocol messages exchanged between Alice and Bob. One day Eve somehow uncovers an old session key (an old K_{AB} value) from a previous protocol exchange. How can Eve leverage all the recoded information and this old key (denoted K'_{AB}) to compromise Bob's security if Bob follows the protocol?

(d) [4 marks] What should be $\boldsymbol{a}$, $\boldsymbol{b}$ and $\boldsymbol{c}$ if we want to fix the vulnerability by replacing steps 1 and 2 of Needham-Schroeder protocol by the 4 steps below? (i.e., after the 4 steps below, the step 3 of the original protocol will be executed.)

1. $A \rightarrow B: A$
2. $B \rightarrow A: \boldsymbol{a}$
3. $A \rightarrow S: A, B, N_1, \boldsymbol{b}$
4. $S \rightarrow A: \mathrm{Enc}_{K_{AS}}(N_1, B, K_{AB}, \boldsymbol{c})$

Q4. DNS Cache Poisoning Attack (16 marks in total)

Suppose a client, a server, and an attacker are connected to a switch.

(a) [4 marks] If the attacker is a passive one, can it sniff the traffic between the client and the server? Explain.

(b) [4 marks] If the attacker is an active one, can it sniff the traffic between the client and the server? Explain.

Consider another attacker who wants to launch DNS cache poisoning attack.

(c) [4 marks] Recall that queryID of a DNS request is a 16-bit value, and the DNS system has implemented source port randomization which contributes 11 bits of entropy. How many packets the attacker needs to send for a successful rate more than half according to the birthday attack strategy? Explain.

(d) [4 marks] Name one cryptographic primitive that can help to address DNS cache poisoning. Explain.

Q5. Denial-of-Service (16 marks in total)

An anti-spam company, GreenMail, uses a vigilante approach to fighting spam. For each spam reported by a GreenMail's user, GreenMail automatically visits the websites advertised by the URLs in the spam messages and leaves complaints on those websites. GreenMail operates on the assumption that as the community grows, the flow of complaints from hundreds of thousands of computers will apply enough pressure on spammers (and their clients) to stop spamming.

After a short while of operation, GreenMail's public website comes under a massive DDoS attack in the form of SYN flood.

(a) [3 marks] Briefly describe the steps to launch a SYN flood attack.

(b) [3 marks] Briefly describe why the steps you described can cause a denial-of-service.

(c) [4 marks] Describe under what situation can GreenMail use a packet-filter firewall to defend itself against the DDoS that uses SYN flood. Also describe what kind of rule the firewall needs to apply.

(d) [3 marks] Explain how the GreenMail service itself could be used to mount a DoS attack.

(e) [3 marks] Briefly describe one approach that victims of the above attack in (d), or a website under DDoS attack in general, could use to defend themselves.

Q6. IPSec (16 marks in total)

Recall that the structures of an IP packet before/after applying IPSec are as follows:

(hdr: header, trlr: trailer, auth: authentication trailer/data)

(a) [3 marks] What are the main functions of Authentication Header (AH), Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE)?

(b) [4 marks] Write down the parts (e.g., TCP hdr, Data) that are encrypted and/or authenticated in transport mode, tunnel mode, when AH and ESP is used respectively.

A corporation establishes gateways GW1 and GW2 at different branches. They enable machines in different branches to communicate securely over the Internet by implementing IPSec at the gateways only. It means that when a machine A inside the first network sends an IP packet to a machine B in the second network, the gateway GW1 intercepts the IP packet in transit and encapsulates it into an IPSec packet. At the other end, GW2 recovers the original IP packet to be routed in the second network to machine B.

(c) [4 marks] Explain why using IPSec is better than SSL in this scenario.

(d) [5 marks] Which of the IPSec modes, tunnel or transport, and AH or ESP, should be used if it was desired that no Internet eavesdroppers should be able to learn about the identities A and B of the communicating parties. Explain briefly.

- End -