請勿攜去
Not to be taken away

香 港 中 文 大 學
The Chinese University of Hong Kong

二０一八至一九年度下學期科目考試
Course Examination 2nd Term, 2018-19

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

時間　2　小時　0　分鐘
Time allowed : 2 hours 0 minutes

學號　　座號
Student I.D. No. : ..... Seat No. : .....

Notes to All Students:

1. You need to complete all questions **(Total Marks = 120).**
2. Please write down your answers to the answer book.
3. Please write down your name and student ID on both question paper and answer book.

Part I -- Multiple Choices

Please select out all answers for each question in order to get full four marks. Any wrong answer will lead to zero mark. Any missing answer will lead to two marks.

Multiple-Choice questions not to be provided.

P.1 – P.3

Part II True or False

For each statement, please first answer whether it is true or false. For False statement, please also explain why it is wrong (For True statement, explanation is not required). Missing explanations will lead to one mark only. Each question carries four marks.

True-False questions not to be provided.

Part III Short Question and Answers

Please answer each question accurately and concisely.

1. Here is a variant of one-time pad encryption algorithm. Let c be cipher text, m be plaintext, k be the encryption key, and $c_0 = m_0 \oplus k_0$, $c_1 = m_1 \oplus k_1$, ... $c_n = m_n \oplus k_n$, where $\oplus$ is XOR operation, $k_2 = k_1 \oplus k_0$, $k_3 = k_2 \oplus k_1$... $k_n = k_{n-1} \oplus k_{n-2}$, and k_0, k_1 are generated by a secure random number generator. Is this encryption algorithm secure or insecure? Please explain why if you think it is insecure. [10']

2. Why attackers usually choose the SUID programs as the target to launch attacks like buffer overflow? [5']

3. Why is TCP protocol vulnerable to hijacking attack? Please list your reasons and give one mitigation solution. [3'+3']

4. Please explain the strengths and weaknesses of the following firewall deployment scenarios in defending servers, desktop machines against network threats. [4'+4']
   A) Only a firewall at the network perimeter.
   B) One firewall on every end-host machine.

5. Suppose Alice had developed a program called ***Agent*** that can run as a privileged system service and provide some interfaces to other external client processes (e.g., another user-space application). With such interfaces, a client processes can request the ***Agent*** program to take photos or record audios, even though that client process does not have the permission to access those camera and microphone resources. Will ***Agent*** cause any potential security risk? What risk? And how to modify the ***Agent*** program to mitigate the potential risk? [5'+5']

6. Answer following questions about authentication and passwords
   A) Password is a common but imperfect authentication method. Could you give two examples on how vendors/websites enhance the password authentication process? [4']
   B) Besides password, fingerprint is another popular authentication method. What are the possible strength and weakness of using fingerprints to authenticate users? (2'+3')

C) Users' passwords should be kept securely in a server database. One common practice is to add a "salt" to the origin password and then do the hash. What is "salt"? How can it improve authentication security? (2'+3')

7. What is difference between authentication and authorization? [4']

8. Please answer following questions related to Cross-Site Scripting (XSS) and cross-site request forgery (CSRF) attacks.

   A) Explain the differences between XSS and CSRF. [4']

   B) What is the fundamental reason for a web site being vulnerable to XSS attack? How to defense against it effectively? [2'+4']

9. Could you give a real world example of applying security principle "Isolation"? Please also explain how the "isolation" principle can improve the system security. [2'+3']

- End -