浙江大学 20 18 - 20 19 学年 春 学期

《信息安全原理》课程期末考试试卷

课程号：21190850，开课学院：计算机学院、软件学院

考试试卷：A 卷（请在选定项上打 √）

考试形式：闭卷（请在选定项上打 √）

考试日期：2019 年 4 月 17 日，考试时间：90 分钟

诚信考试，沉着应考，杜绝违纪。

考生姓名：_____学号：_____所属院系：_____

题序	一	二	三	四	五	六	七	八	总 分
得分									
评卷人									

一、填空题（每空 1 分，共计 10 分）

The packet type in IPSEC providing both confidential and authentication service is _____(1)_____, there are two operating mode called _____(2)_____ mode and tunnel mode when using it.

To add a digital signature using RSA, we usually use _____(3)_____ to do preprocessing first, then use RSA to complete the actual signing process. To produce a signature, the sender should use its _____(4)_____ to sign, while the receiver or a third party can use _____(5)_____ of the sender to verify the signature.

The four elements of information security are _____(6)_____, integrity, availability and authenticity.

The one-way function which Diffie-Hillman algorithm based on is_____(7)_____. In terms of encryption, the main advantages of Public-Key algorithm compared with Private-Key algorithm are _____(8)_____

In TLS/SSL protocols, SSL Record protocol consists of the following steps: _____(9)_____, compressing (optional), _____(10)_____, encryption, adding SSL record header.

二、单项选择题（每题 2 分，共计 20 分）

(1) Which of the following is **not** included in the three elements of access control ? ( )

A. The subject

B. The object

C. The access permission

D. The operation

(2) About spam emails, which of the following is correct? ( )

A. The proportion of spam is about 10% among all emails currently.

B. Technical means is the only way to deal with spam.

C. Sending spam emails is just for fun for hackers.

D. Spam emails can not be completely prohibited through technical means.

(3) For authorization, the **wrong** statement of the following comments is ? ( )

A. In RBAC model, roles and user groups are the same.

B. Principle of Least Privilege is a core principle of security access control.

C. Authorization is on the premise of the identity authentication.

D. Authorization includes three main functions: assigning permissions, recycling permissions and checking permissions.

(4) For mandatory access control, which of the following is correct? ( )

A. Bell-Lapadula principle contains two properties: no write down, no read up.

B. Bell-Lapadula principle is to ensure the integrity.

C. Mandatory access control may not be more secure than role-based access control and discretionary access control.

D. Trojan horse can happen even if mandatory access control model is properly applied.

(5) For password based authentication, which of the following is **wrong** ? ( )

A. Using password salt can avoid dictionary attacks.

B. Passwords stored in the system should be one-way hashed, rather than storing plaintext password.

C. Password could be stolen due to various reasons, such as the server being compromised, using a machine with Trojan or the network communication being sniffed, etc.

D. Password authentication and biometric authentication (such as Fingerprint and Iris, etc.) methods have their own advantages; both cannot be completely replaced yet.

(6) Now, which algorithm is secure for military use? ( )

A. DES

B. MD5

C. SHA-0

D. AES

(7) About IPSEC protocol, which of the following is correct? ( )

A. Both AH and ESP headers support data integrity verification.

B. An IPSEC packet can have both AH and ESP headers.

C. Tunnel mode can only be used in IPV6, IPV4 only supports transport mode.

D. A duplex connection use a security association SA to conduct security parameters management.

(8) The core feature of Rootkit is? ( )

A. Self-propagating

B. Execute malicious codes.

C. Hiding.

D. Spread spams.

(9) Botnet is usually <u>not</u> used to do? ( )

A. Steal passwords.

B. Spam and Click Fraud.

C. Release new worms and new vulnerabilities.

D. Distributed Denial of Service Attack.

(10) For virus, which of the following is correct? ( )

A. A virus may have a lot of mutations.

B. Virus is a standalone program.

C. We can detect all viruses by inspecting the signature of viruses.

D. Any virus will not infect my computer if Anti-Virus software is installed.

三、判断题（每题 2 分，共计 20 分）

(1) An insider conducts most attacks.

(2) Hackers are just geeks who are out to show that they can break into networks.

(3) Frequency analysis attack of the classic ciphers cannot be used to attack Chinese plaintext ciphers.

(4) Public-key encryption algorithm is safer than symmetric key encryption algorithm.

(5) The encryption process of 3DES algorithm uses three different keys, conducting the DES encryption algorithm three times. Assume the plain text is P, then the cipher text $C = E_{K3}(E_{K2}(E_{K1}(P)))$.

(6) The DES algorithm is based on the Feistel structure, and the AES is not.

(7) Using public-key encryption algorithm, the senders encrypts the plaint text with their own private-key, the recipients decrypts the cipher text with the senders' public-key.

(8) For the mandatory access control, its security is certainly higher than discretionary access control and role-based access control; even the configuration is not properly done.

(9) The Thompson Compiler Trojan cannot be removed even we recompile the compiler.

(10) As long as we pay attention to the format of the URL and its authority, network phishing can be avoided.

四、问答题（每题 8 分，共计 40 分）

(1) Please briefly describe the Kerckhoffs' principle and its impaction on the history of encryption.

(2) Please briefly describe the Diffie-Hellman algorithm and its Man-in-The-Middle Attack.

(3) Please briefly describe the differences of digital signature and message authentication code

MAC, and give out the process of conducting long text digital signature/verification and the process of message authentication code/verification (Both painting and text description are needed).

(4) Please briefly describe the concept of mandatory access control and concept of covert channels in mandatory access control (by example).

(5) Please briefly describe the principles of TCP SYN Flooding Attacks, and describe the principles of the SYN cookies to against TCP SYN Flooding Attacks (Both painting and text description are needed).

五、应用题（每题 10 分，共计 10 分）

Please recall the four assignments of this course and answer the following questions.

1. Please describe the general contents of our four assignments.
2. Please list three difficulties and your solutions during completing these assignments.
3. What have you gained through completing these assignments, please gives out three main points.