國立成功大學

110學年度碩士班招生考試試題

編　號：189

系　所：電腦與通信工程研究所

科　目：資訊安全概論

日　期：0203

節　次：第 1 節

備　註：不可使用計算機

國立成功大學 110 學年度碩士班招生考試試題

系　所：電腦與通訊工程研究所

考試科目：資訊安全概論

考試日期：0203，節次：1

第 1 頁，共 2 頁

※ 考生請注意：本試題不可使用計算機。 請於答案卷(卡)作答，於本試題紙上作答者，不予計分。

1. IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. (20%)
   a. List and briefly describe some applications of IPsec. (10%)
   b. List and briefly describe some benefits of IPsec. (10%)
2. In IEEE 802.1, open system authentication simply consists of two communications, An authentication is requested by the client, which consists the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration. (20%)
   a. What are the benefits of this authentication scheme? (10%)
   b. What are the security vulnerabilities of this authentication scheme? (10%)
3. What are the POP3 and IMAP. (10%)
4. Consider the following threats to Web security and describe how each is countered by a particular feature of TLS. (25%)
   a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm. (3%)
   b. Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full ciphertext to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys). (3%)
   c. Replay Attack: Earlier TLS handshake messages are replayed. (3%)
   d. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client. (3%)
   e. Password Sniffing: Passwords in HTTP or other applications traffic are eavesdropped. (3%)
   f. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data. (3%)
   g. IP Hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts. (3%)
   h. SYN Flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module

typically leaves the "half-open connection" around for a few minutes. Repeated SYN messages can clog the TCP module. (4%)

5. a. Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement. (8%)

   b.Repeat Problem 5.a for a payment gateway system where a user pays for an item using their account via the payment gateway. (7%)

6. a. What are the roles of the public and private key. (5%)

   b.What are three broad categories of applications of public-key cryptosystems? (5%)