Example exam questions - VT2022

The exam consists of twenty-five (25) multiple or single choice questions (single choice will be indicated), fifteen (15) true/false questions and two (2) essay questions.

Below are only some example questions.

Part A Multiple/Single choice questions

1. Which of the following algorithms are not based on block cipher?

a) RC4

b) DES

c) Cesar

d) Fortezza

e) IDEA

2. Public-key cryptography algorithms can be used for______

a) checking integrity, providing confidentiality, providing non-repudiation

b) digital signatures, encryption/decryption, key exchange

c) access control, authentication, accountability

d) calculating hash, calculating sequence number, calculating message digest

3. Many hackers make use of buffer overflow in the system software to perform attacks. The most efficient method to overcome this type of vulnerability is ____. (Select one!)

a) to install a firewall

b) to install an intrusion detection system

c) to update the system software using a new patch

d) to install the up-to-date anti-virus software in the system

e) none of above

4. A proper installed and configured firewall in a company’s wireless network can prevent _________.

a) the company’s data traffic from being eavesdropped

b) the people inside the company from visiting unneeded websites outside the company

c) the people in adversary companies from visiting the company’s servers

d) the data traffic with internal addresses from entering the company’s network

e) none of above

5. Among the following protocols, _____ is not a secure protocol.

a) SSL

b) ICMP

c) HTTPS

d) VPN

e) ARP

6. When HTTPS is used, _____ is not encrypted.

a) URL of the requested document

b) Contents of HTTP payload

c) Contents of TCP header

d) HTML documents

e) SSL record header

7. If a message is authenticated, it means that __________.

a) the message has not been altered

b) the message source is authentic

c) the message is encrypted and confidential

d) a MAC (message authentication code) is attached in the message

Part B Ture or False

1. Kerberos is server that can authenticate a client to access services provided by the Kerberos server.

2. The digital signature of a message can be used to verify the sequence of the message.

3. Connection-oriented integrity service should assure that messages are received with no insertion, reordering and replays.

4. Passive attack is difficult to detect and active attack difficult to prevent.

Part C Essay

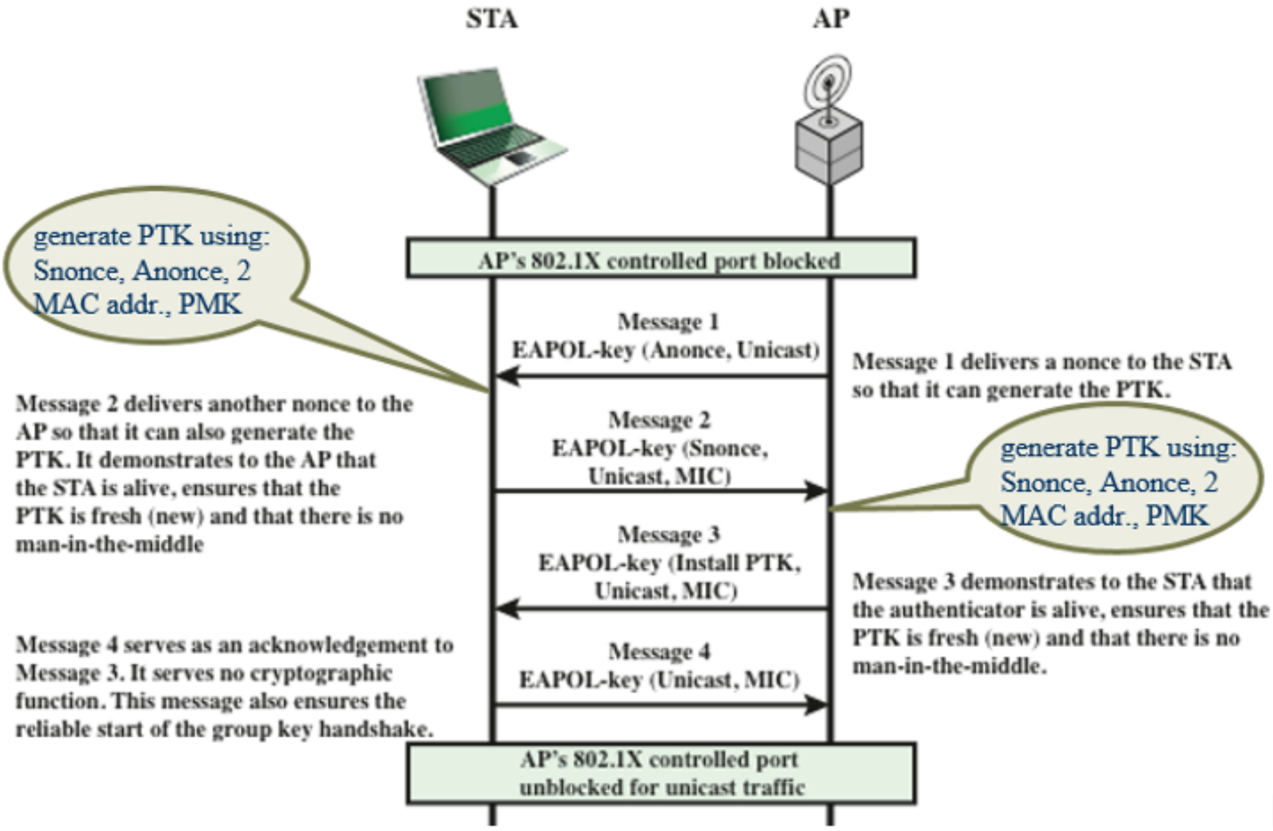
1. Recall the four-way handshake (i.e., Message 1 to Message 4 shown in the figure below) in the key management phase of IEEE 802.11i for Wireless LAN security.

a) Explain the functions or purposes of the four-way handshake.

b) What are the functions of PTK (Pairwise Transient Key)? How to understand “the PTK can be ensured to be fresh and no man-in-the-middle” by using Message 2 and Message 3?

c) STA (the supplicant) accepts retransmissions of

Message 3, even after it has sent a Message 4. Suppose there is an attacker between STA and AP (i.e., man-in-the-middle), who triggers retransmissions of Message 3 by preventing Message 4 from arriving at the AP (the authenticator). Analyze and reason what may happen and what results can be caused in this case.


STA
AP
generate PTK using: Snonce, Anonce, 2 MAC addr., PMK
AP's 802.1X controlled port blocked
Message 1 EAPOL-key (Anonce, Unicast)
Message 1 delivers a nonce to the STA so that it can generate the PTK.
Message 2 delivers another nonce to the AP so that it can also generate the PTK. It demonstrates to the AP that the STA is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle
Message 2 EAPOL-key (Snonce, Unicast, MIC)
generate PTK using: Snonce, Anonce, 2 MAC addr., PMK
Message 3 EAPOL-key (Install PTK, Unicast, MIC)
Message 3 demonstrates to the STA that the authenticator is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle.
Message 4 serves as an acknowledgement to Message 3. It serves no cryptographic function. This message also ensures the reliable start of the group key handshake.
Message 4 EAPOL-key (Unicast, MIC)
AP's 802.1X controlled port unblocked for unicast traffic

2. A company provides data services based on web. It has a local network connecting some servers and employees' working computers. Suppose you are invited to design a network-based intrusion detection system (IDS) for the company.

a) Specify an IDS approach and describe the functional units, the functions of each unit, and the possible tools in your designed system.

b) Illustrate the IDS you designed with a figure (indicating the functional units you designed), indicating where in the networks it will be located.

c) Give an example attack on the company’s network and explain how your designed IDS system works.

Last modified: Monday, 14 February 2022, 10:37