

## Exam Report: 5.10.8 Practice Questions

Date: 1/21/2020 12:58:23 pm  
Time Spent: 22:05

Candidate: Garsteck, Matthew  
Login: mGarsteck

## Overall Performance

Your Score: 60%



View results by: ☐ Objective Analysis ☒ Individual Responses

## Individual Responses

## ▼ Question 1:

Incorrect

Which of the following specifications identify security that can be added to wireless networks? (Select two.)

➡ ☐ 802.11i

➡ ☒ 802.1x

☐ 802.11a

☐ 802.2

☐ 802.3

☐ 802.5

## Explanation

802.11i defines security for wireless networks. Standards described in 802.11i have been implemented in Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). 802.1x is an authentication protocol that can be used on wireless networks. Use of 802.1x on a wireless network is described in the 802.11i specifications.

802.11a is a wireless standard that describes how wireless communications work. However, the standard does not include security considerations. 802.2 defines standards for data link layer communications. 802.3 is Ethernet, and 802.5 is token ring.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_01]

## ▼ Question 2:

Correct

Which of the following wireless security methods uses a common shared key configured on the wireless access point and all wireless clients?

☐ WPA Enterprise and WPA2 Enterprise

☐ WEP, WPA Personal, WPA Enterprise, WPA2 Personal, and WPA2 Enterprise

☐ WPA Personal and WPA2 Enterprise

➡ ☒ WEP, WPA Personal, and WPA2 Personal

## Explanation

Shared key authentication can be used with WEP, WPA, and WPA2. Shared key authentication used with WPA and WPA2 is often called WPA Personal or WPA2 Personal.

WPA Enterprise and WPA2 Enterprise use 802.1x for authentication. 802.1x authentication uses user names and passwords, certificates, or devices, such as smart cards, to authenticate wireless clients.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_02]

### ▼ Question 3: Correct

Which of the following offers the **weakest** form of encryption for an 802.11 wireless network?

- ☐ WAP
- ☐ WPA
-  ☒ WEP
- ☐ WPA2

## Explanation

Wired Equivalent Privacy (WEP) has the weakest encryption for 802.11 wireless networks. WEP uses a shared key for the encryption key. This key is easily captured and broken. The only encryption worse than WEP is no encryption at all.

WPA2 uses AES for encryption and offers the strongest encryption. WPA uses TKIP for encryption. WAP is an acronym for wireless access point. WAP also stands for wireless application protocol, which is used with mobile devices, such as PDAs and smart phones.


## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_03]

### ▼ Question 4: Correct

What encryption method is used by WPA for wireless networks?

- ☐ AES
- ☐ 802.1x
-  ☒ TKIP
- ☐ IPsec
- ☐ WEP

## Explanation

WPA uses TKIP for encryption. TKIP uses rotating encryption keys for added security over WEP.

AES encryption is used with WPA2. WEP is a security method for wireless networks that provides encryption through the use of a shared encryption key (the WEP key).

IPsec is an encryption method that is used for VPN tunneling. While it can be used on a wireless network, it is used in addition to encryption provided by either WEP, WPA, or WPA2. 802.1x is an authentication method for wired and wireless networks.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_04]

### ▼ Question 5: Correct

Which of the following features are supplied by WPA2 on a wireless network?

- ☐ Network identification
- ☐ Centralized access point for clients

- ☐ Client connection refusal based on MAC address
- ☐ Traffic filtering based on packet characteristics

➡ ☒ Encryption

## Explanation

Wi-Fi Protected Access (WPA) provides encryption and user authentication for wireless networks.

MAC address filtering allows or rejects client connections based on the hardware address. The SSID is the network name or identifier. A wireless access point (called an AP or WAP) is the central connection point for wireless clients. A firewall allows or rejects packets based on packet characteristics (such as address, port, or protocol type).

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_06]

### ▼ Question 6: Incorrect

You need to configure a wireless network. You want to use WPA2 Enterprise. Which of the following components will be part of your design? (Select two.)

- ➡ ☒ AES encryption
- ➡ ☐ 802.1x
- ☐ WEP encryption
- ☒ ~~TKIP encryption~~
- ☐ Open authentication
- ☐ Preshared keys

## Explanation

To configure WPA2 Enterprise, you will need a RADIUS server to support 802.1x authentication. WPA2 uses AES for encryption.

WPA2-PSK, also called WPA2 Personal, uses pre-shared keys for authentication. WPA uses TKIP for encryption.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_08]

### ▼ Question 7: Incorrect

You need to implement a wireless network link between two buildings on a college campus. A wired network has already been implemented within each building. The buildings are 100 meters apart.

What type of wireless antennae should you use on each side of the link? (Select two.)

- ➡ ☐ Parabolic
- ➡ ☒ High-gain
- ☐ Normal-gain
- ☒ ~~Directional~~
- ☐ Omnidirectional

## Explanation

You should use *high-gain parabolic* antennae on each side of the link. A high-gain antenna usually has a gain rating of 12 dBi or higher. A parabolic antenna uses a parabolic-shaped reflector dish. It is highly directional, concentrating the radio waves transmitted from the sender into a very narrow beam. When the receiver uses a parabolic antenna, it can only receive a signal from one specific direction. It supports very high-gain radio signals that can be transmitted over long distances, but it requires a clear line of sight (LOS) between the sender and the receiver.

A *normal-gain* antenna usually has a gain rating between 2 and 9 dBi. An *omnidirectional* antenna radiates and absorbs signals equally in every direction around the antenna. Because it spreads its gain in a 360-degree pattern, the overall range of an omnidirectional antenna is typically much less than that of a directional antenna. A *directional* antenna focuses its radiation and absorption of signals in a specific direction. However, they typically have a much shorter range than a parabolic antenna.

## References


LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_09]

### ▼ Question 8: Incorrect

You need to configure the wireless network card to connect to your network at work. The connection should use a user name and password for authentication with AES encryption.

What should you do?

-  ☐ Configure the connection to use WPA2-Enterprise.
- ☒ ~~Configure the connection to use WPA2 Personal.~~
- ☐ Configure the connection to use WPA-Personal.
- ☐ Configure the connection to use WPA-Enterprise.

## Explanation

Select WPA2-Enterprise for the wireless connection. WPA2 is required to support AES encryption. An Enterprise configuration (using either WPA or WPA2) authenticates using user names, passwords, and 802.1x authentication. A RADIUS server is required for using 802.1x.

A Personal (or PSK) configuration uses a pre-shared key for authentication. All clients are configured using the same pre-shared key. WPA uses TKIP for encryption.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_13]

### ▼ Question 9: Correct

Match the wireless networking security standard on the left to its associated characteristics on the right. Each standard can be used more than once.

Short initialization vector makes key vulnerable.

 WEP

Uses AES for encryption.

 WPA2

Uses RC4 for encryption.

 WEP

Uses TKIP for encryption.

 WPA

Uses CBC-MAC for data integrity.





Uses CCMP for key rotation.



## Explanation

WEP is an optional component of the 802.11 specifications. It was deployed in 1997. WEP:

- Uses Rivest Cipher 4 (RC4) with a 40-bit key and 24-bit initialization vector (IV) for encryption.
- Uses CRC-32 for data integrity applied to the data only (not the header).
- Supports open, shared key, and (recently) 802.1x authentication.
- Requires that keys be manually configured on each device.
- Uses a short initialization that allows hackers to easily crack the key.

WPA was deployed in 2003 as an intermediate measure to take the place of WEP while a fully secured system (802.11i) was prepared. WPA:

- Uses temporal key integrity protocol (TKIP) for encryption.
- Uses the message integrity check (MIC) algorithm for data integrity applied to both the data and the header.
- Supports both pre-shared key (referred to as WPA-PSK or WPA Personal) and 802.1x (referred to as WPA Enterprise) authentication.
- Can typically be implemented in WEP-capable devices through a software/firmware update.

WPA2 was deployed in 2005. It resolves the weaknesses inherent in WEP and is intended to replace both WEP and WPA. WPA2:

- Uses cipher block chaining message authentication code (CBC-MAC) for data integrity applied to both the data and the header.
- Uses advanced encryption standard(AES) with a 128-bit key and a 48-bit initialization vector for encryption. It is similar to and more secure than TKIP, but requires special hardware for performing encryption.
- Supports both pre-shared key (referred to as WPA2-PSK or WPA2 Personal) and 802.1x (referred to as WPA2 Enterprise) authentication.
- Provides dynamic key generation and rotation through the CCMP protocol.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_14]

### ▼ Question 10: Correct

Which of the following are typically used for encrypting data on a wireless network? (Select two.)

☐ Diffie-Hellman

☐ ElGamal

☐ MD-5

➡ ☒ TKIP

➡ ☒ AES

## Explanation

TKIP and AES are used for encrypting data. TKIP is used with WPA wireless standards, while AES is used with WPA2 and other encryption applications.

ElGamal and Diffie-Hellman are asymmetric encryption methods. They are both used for key exchange and digital signatures. MD-5 is a hashing algorithm.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_15]

**Question 11:****Incorrect**

You want to connect a laptop computer running Windows to a wireless network.

The wireless network uses multiple access points and WPA2-Personal. You want to use the strongest authentication and encryption possible. SSID broadcast has been disabled.

What should you do?

- ➡ ☐ Configure the connection with a pre-shared key and AES encryption.
- ☒ ~~Configure the connection to use 802.1x authentication and AES encryption.~~
- ☐ Configure the connection with a pre-shared key and TKIP encryption.
- ☐ Configure the connection to use 802.1x authentication and TKIP encryption.

**Explanation**

To connect to the wireless network using WPA2-Personal, you will need to use a pre-shared key for authentication. AES encryption is supported by WPA2 and is the strongest encryption method.

WPA and WPA2 designations that include Personal or PSK use a pre-shared key for authentication. Methods that include Enterprise use a RADIUS server for authentication and 802.1x authentication with user names and passwords.

**References**

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_17]

**Question 12:****Correct**

Which of the following is used on a wireless network to identify the network name?

- ➡ ☒ SSID
- ☐ Subnet mask
- ☐ MAC address
- ☐ IP address

**Explanation**

Wireless devices use the SSID to identify the network name. All devices on a wireless network use the same SSID.

The MAC address is a unique physical device address. The IP address is a logical address that includes both the logical network and the logical device address. The subnet mask is used with the IP address to identify the network portion of the IP address.

**References**

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_18]

**Question 13:****Incorrect**

Which of the following are true about Wi-Fi Protected Access 2 (WPA2)? (Select two.)

- ☐ WPA2 uses RC4 for encryption and CRC-32 for data integrity.
- ➡ ☒ WPA2 uses AES for encryption and CBC-MAC for data integrity.
- ☒ ~~Upgrading from a network using WEP can usually be done through a firmware upgrade.~~
- ➡ ☐ Upgrading from a network using WEP typically requires installing new hardware.
- ☐ WPA2 uses RC4 for encryption and MIC for data integrity.

## Explanation

Wi-Fi Protected Access 2 (WPA2) uses advanced encryption standard (AES) for encryption and cipher block chaining message authentication code (CBC-MAC) for data integrity. Because of the processor-intensive nature of AES, new hardware is typically required when upgrading from a wireless network that currently uses WEP.

Wired Equivalent Privacy (WEP) uses RC4 for encryption and CRC-32 for data integrity. Wi-Fi Protected Access (WPA) uses RC4 for encryption and MIC for data integrity. Typically, you can implement WPA through a firmware update.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_19]

### ▼ Question 14: Correct

WiMAX is an implementation of which IEEE committee?

- ☐ 802.1x
- ☐ 802.11a
- ☐ 802.11b
- ☐ 802.11g
- ☐ 802.11i
- ☐ 802.15

➡ ☒ 802.16

## Explanation

WiMAX is an implementation of the 802.16 specifications for metropolitan wireless area networks.

802.1x is an authentication method. 802.11a/b/g are wireless local area networking standards. 802.11i is the security standards for wireless networks, WPA2 being the implementation of the 802.11i standards. 802.15 contains the specifications for personal wireless area networks, Bluetooth being the most common implementation.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_20]

### ▼ Question 15: Correct

You have a small wireless network that uses multiple access points. The network uses WPA and broadcasts the SSID. WPA2 is not supported by the wireless access points.

You want to connect a laptop computer to the wireless network. Which of the following parameters will you need to configure on the laptop? (Select two.)

- ☐ AES encryption
- ☐ Channel
- ➡ ☒ Pre-shared key
- ➡ ☒ TKIP encryption
- ☐ BSSID

## Explanation

To connect to the wireless network using WPA, you will need to use a pre-shared key and TKIP encryption. Using a pre-shared key with WPA is known as WPA-PSK or WPA Personal.

AES encryption is used by WPA2. The channel is automatically detected by the client. The basic service set identifier (BSSID) is a 48-bit value that identifies an AP in an infrastructure network or a STP in an ad hoc network. The client automatically reads this and uses it to keep track of APs when roaming between cells.

## References

LabSim for Security Pro, Section 5.10.

[All Questions SecPro2017\_v6.exm WIRELESS\_OVRW\_22]