7

WIRELESS LANS II

# Homework

First Name:

Last Name:

***Note the requirements in Thought Questions 7-4 and 7-5.***

# The TJX Breach

1. a) What was the attackers’ first step in breaking into TJX and other companies?

**b) Why do you think TJX failed to upgrade to stronger security than WEP? (This question requires your reasoned opinion. There may be more than one consideration.)**

c) How was the TJX break-in an international crime?

# 802.11i WLAN Security

## Drive-By Hackers

**2. How can a drive-by hacker defeat a site’s border firewall?**

## The 802.11i WLAN Security Standard

3. **a) What cryptographic protections does 802.11i provide**?

b**) How is this protection limited**?

**c) Distinguish between link security and end-to-end security**.

**d) What does the Wi-Fi Alliance call 802.11i**?

**e) When offered the choice when you are configuring a wireless access point, which WLAN security standard should you choose**?

## 802.11i Stages

4 a) For what use scenario was 802.11i PSK mode created?

b) For what use scenario was 802.11i’s 802.111X mode created?

**c) Does the choice of initial authentication mode change how other phases of 802.11i work**?

## Pre-Shared Key (PSK) Initial Authentication Mode in 802.11i

5 a) For what use scenario was 802.11i PSK mode created?

b) What must a user know to authenticate his or her device to the access point?

**c) In what ways is the pairwise session key the user receives after authentication different from the PSK**?

**d) What three operational security threats must PSK users consider**?

**e) Why is this risk probably acceptable for the PSK use scenario? (The answer is not in the text.**)

f) How long must passphrases be in order to generate strong pre-shared keys?

## 802.111X Mode Operation

6 a) Contrast the use scenarios for initial authentication in PSK mode and 802.111X mode.

**b) Which initial authentication mode or modes of 802.11i authentication use(s) a central authentication server**?

**c) What does the Wi-Fi Alliance call 802.11i initial authentication mode**?

d) In 802.111X operation, what device acts as the authenticator in Ethernet?

e**) What device acts as the authenticator in Wi-Fi**?

7. **a) Why does 802.111X mode in Wi-Fi need additional security between the authenticator and the host**?

b**) How does 802.11i provide this additional security**?

8 a**) What initial authentication mode does 802.11i use? (Yes, this is a trick question**.)

b) **Which mode is used for message-by-message encryption, authentication, and message integrity? (Another trick question**!)

# Beyond 802.11i Security

## Rogue Access Points

9 **a) Who creates a rogue access point**?

b) Why are they dangerous?

## Evil Twin Access Points and Virtual Private Networks (VPNs)

10 a) What kind of physical device is an evil twin access point?

**b) What does the evil twin do after initial association when the client transmits to the legitimate access point**?

**c) Distinguish between evil twin access points and rogue access points. (The answer is not explicitly in the text.**)

**d) How are VPNs able to defeat evil twin attacks**?

# 802.11 Wi-Fi Wireless LAN Management

## Access Point Placement

11 a) Describe the process by which access point locations are determined.

**b) When must firms do site surveys to give users good service**?

## Centralized Management

12 a) How might a security administrators use SNMP Get commands to access points?

**b) How does centralized management provide for the detection of rogue access points**?

c) Comment on the cost of central access point management.

# ~~Box: Expressing Power Ratios in Decibels~~

~~13 a) The power level at 10 meters is 100 mW.~~

~~At 20 meters, it is 5 mW.~~

~~How many dB has it lost?~~

~~b) Compared to an omnidirectional antenna, a dish antenna quadruples radiated power.~~

~~How much is this change in decibels?~~

~~c) Compute the decibel value for a power ratio of 17:1.~~

~~d) Of 1:33.~~

~~14 a) Fill in the missing values in Figure 7-18.~~

~~Approximate, without using Excel, the decibels for a ratio for b) 8:1.~~

~~c) 9:1.~~

~~d) 110:1.~~

~~e) 1:7.~~

~~f) 1:90.~~

# Peer-to-Peer Protocols for The Internet of Things (IoT)

15 **Compare the relative advantages and disadvantages of high-speed Bluetooth and NFC**.

## Wi-Fi Direct

16 Compare normal Wi-Fi and Wi-Fi Direct.

## Bluetooth

17 a) What is a PAN? (Do not just spell out the abbreviation.)

**b) Compare the relative benefits of classic Bluetooth and high-speed Bluetooth**.

**c) Why would you not want to use high-speed Bluetooth all the time**?

d) What is the benefit of low-energy Bluetooth for device design?

18 **a) What does it mean that Bluetooth uses one-to-one operation**?

b**) Is this still true if a master communicates with four slaves**?

c) Can a Bluetooth master have multiple slaves?

**d) Can a Bluetooth slave have two masters**?

**e) Can a Bluetooth device be both a master and a slave simultaneously**?

19 **a) Why would it be nice if Wi-Fi offered a basic printing profile**?

b) What Bluetooth profile would you use for a game joystick?

20 a) Must two Bluetooth devices pair each time they meet?

b**) When must they pair afterward**?

## Near Field Communication (NFC)

21 a) When two devices communicate using NFC, how close do they have to be?

b) How does near-field communication differ from normal radio communication?

**c) Passive RFID chips have no batteries. How can they transmit when queried**?

d) What is the state of NFC standards?

# Conclusion

## End of Chapter Questions

Thought Questions

~~7-1 (If you read the box on expressing power ratios in decibels) a) If you are told that a signal has attenuated by 20 dB, about how much has it attenuated?~~

~~b) What would you say about attenuation if you were told that a signal has attenuated by 19 dB?~~

~~You do not have access to a calculator or computer.~~

~~You must approximate.~~

~~c) What would you say about attenuation if you were told that a signal has attenuated by 7 dB?~~

7-2 Answer the following in terms of the security principles you learned in Chapter 4.

a) List the security principles in Chapter 4.

b) What principle do rogue access points compromise?

c) What principle does the danger of giving out PSK keys to people who are not authorized to have them represent?

d) What principle does having both 802.11i and centralized security management represent?

e) What principle is exemplified by rogue access points?

7-3 Create a policy for 802.11 Wi-Fi security in your wireless network at home.

This is not a trivial task.

Do not just jot down a few notes.

*Make it a document for people in your home to read, not something for your teacher to read.*

7-4 Create a policy for 802.11 Wi-Fi security in a wireless network in a five-person company with a one-access point WLAN.

**This is a big task.**

Do not just jot down a few notes.

***Make it a document for people in your firm to read*, *not something for your teacher to read. If you do not, you will get a zero for this homework assignment. Begin with a preamble on the risks that are involved. State each policy element, following it with a statement why each policy element is necessary****.*

7-5 Create a policy for 802.11 Wi-Fi security in a wireless network in a 500-employee company with a 47-access point WLAN.

**This is a big task.**

Do not just jot down a few notes.

*Make it a document for people in your firm to read, not something for your teacher to read.*

***Make it a document for people in your firm to read*, *not something for your teacher to read. If you do not, you will get a zero for this homework assignment. Begin with a preamble on the risks that are involved. State each policy element, following it with a statement why each policy element is necessary****.*

7-6 a) A firm that has a building that is a long line has 10 access points. About how many will it need if the space between access points is cut in half?

b) A firm has a building with a square floor plan. It has 100 access points. About how many will it need if the space between access points is cut in half?

c) A firm has a building that is a cube. It has 100 access points. About how many will it need if the space between access points is cut in half?

d) A firm has a building that is a cube. It has 100 access points. About how many will it need if the distance between access points is increased by 20%?

7-7 People with NFC devices are often told to physically bump their device against the reader. What do you think is the value of this practice?

Perspective Questions

7-8 What was the most surprising thing you learned in this chapter?

7-9 What was the most difficult part of this chapter for you?