7

WIRELESS LANS II

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

* Explain 802.11i Wi-Fi security.
* Explain why 802.11i security is not enough for WLANs.
* Discuss 802.11 WLAN management.
* Work with decibel representations of power ratios (If you read the box on decibels)
* Compare and contrast peer-to-peer local wireless technologies that will be important for the Internet of Things, including Bluetooth.

# The TJX Breach

TJX Companies, Inc. (TJX) has over 2,500 retail stores in the United States, Canada, England, Ireland, and several other countries. These companies do business under such names as TJ Maxx and Marshalls. In its literature, TJX describes itself as “the leading off-price retailer of apparel and home fashions in the U.S. and worldwide.” With this mission statement, there is strong pressure to minimize costs.

On December 18, 2006, TJX detected “suspicious software” on its computer systems. Four days later, the company informed law enforcement authorities in the United States and Canada. On the 27th, security consultants determined that customer data had been stolen.

The consultants initially determined that the intrusion software had been working for seven months before TJX discovered it. A few weeks later, the consultants discovered that the attackers had also breached the company several times in 2005. All told, the consultants estimated that attackers stole 45.7 million customer records. At the time, this was by far the largest number of personal customer records ever stolen from any company.

The thieves did not steal these records for the thrill of breaking in or to enhance their “cred.” They did it to make fraudulent credit card purchases in the names of the customers whose information they had stolen.

TJX did not tell customers that their data has been stolen for nearly another month. The company said that it had needed time to beef up its security. It also said that law enforcement officials had asked TJX to withhold information to avoid tipping off the data thieves about the investigation. Of course, the delay left the customers ignorant of the danger they faced.

How did the breaches occur? First, the data thieves broke into poorly protected wireless networks in some Florida stores.[[1]](#footnote-1) The breached stores had protected their wireless networks, but they used the vulnerable wired equivalent privacy (WEP) security standard instead of the newer and better 802.11i standard. The attackers could use WEP cracking software widely available on the Internet.

In TJX’s card processing system in Massachusetts, poor firewall protection[[2]](#footnote-2) allowed the data thieves to enter several systems and to install a sniffer that listened to the company’s poorly encrypted traffic passing into and out of the processing center. They soon learned that TJX was retaining some sensitive credit card information that should not have been retained. It was this improperly retained information that the data thieves found most valuable.[[3]](#footnote-3)

Previous data breaches had prompted the major credit card companies to create the Payment Card Industry–Data Security Standard (PCI–DSS) that specified how companies must protect credit card information. Failure to implement PCI–DSS control objectives can result in fines and even the revocation of a company’s ability to accept credit card payments. When the breach occurred, TJX was far behind in its PCI–DSS compliance program. The company complied with only three of the twelve required control objectives. Internal memos revealed that the company knew that it was in violation of the PCI–DSS requirements, particularly with respect to its weak encryption in retail store wireless networks.[[4]](#footnote-4) However, the company deliberately decided not to move rapidly to fix this problem. In November 2005, a staff member noted that “saving money and being PCI compliant is important to us, but equally important is protecting ourselves against intruders. Even though we have some breathing room with PCI, we are still vulnerable with WEP as our security key. It must be a risk we are willing to take for the sake of saving money and hoping we do not get compromised.”

When the staff member noted that “we have some breathing room with PCI,” he was referring to the fact that TJX had been given an extension allowing it to be noncompliant beyond the standard’s specified compliance date.[[5]](#footnote-5) This additional time, ironically, was given after the data breaches had already begun. This extension was dependent upon evaluation of a self-written TJX report on its compliance project. The letter that authorized the extension was sent by a fraud control vice president for Visa. It ended with, “I appreciate your continued support and commitment to safeguarding the payment industry.”

When TJX finally announced the breach, it quickly faced commercial lawsuits and government investigations. TJX was first sued by seven individual banks and bank associations. In December 2007, TJX settled with all but one of these banks, agreeing to pay up to $40.9 million. This would reimburse the banks for the cost of reissuing credit cards and other expenses.

The company also received a large fine from Visa. Actually, Visa could not fine TJX directly, so it had to fine TJX’s merchant bank. (Merchant banks are financial institutions that serve—and should control—retail organizations that accept credit card payments.) The merchant bank passed the fine on to TJX. During the summer of 2007, Visa fined TJX’s merchant bank $880,000 and announced that it would continue to impose fines at $100,000/month until TJX had fixed its security problem. However, after the TJX settlement with the seven banks and banking associations, this fine was to be reduced by an undisclosed amount.

In this battle of corporate giants, consumers came dead last. In 2007, the Federal Trade Commission approved a settlement between TJX and the consumers who had their private information stolen. The FTC required TJX to do security audits every two years for the next 20 years and to report the results of those audits to the FTC.[[6]](#footnote-6) Of course, this did nothing for affected customers. Furthermore, the settlement applied only to the roughly 455,000 victims who had given personally identifiable information when they returned goods without a receipt. Other victims—the vast majority of the victims--only received a small voucher or the opportunity to buy TJX merchandise at sale prices.[[7]](#footnote-7) This settlement was approved.

In 2008, the Department of Justice charged eleven individuals with the break-in and the subsequent use of the stolen information.[[8]](#footnote-8) Three were Americans, and they were jailed rapidly. Two more were in China. The other six lived in Eastern Europe. Although the three Americans conducted the actual data theft, they fenced the stolen information overseas. Two of the American defendants entered plea deals to testify against the alleged ringleader, Albert Gonzalez of Miami, Florida. Gonzalez was sentenced in 2010 to 20 years in prison.

One surprising thing about this indictment was the revelation that these hackers had plundered other companies as well. The attackers had repeated the crime with at least a half dozen other major companies, including OfficeMax, 7-Eleven, Dave & Busters, and Heartland Payment Systems.[[9]](#footnote-9) The Heartland break-in was especially severe because Heartland does credit card payment processing for other firms. Most of these break-ins also began with the exploitation of WEP security.

Test Your Understanding

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?

# Introduction

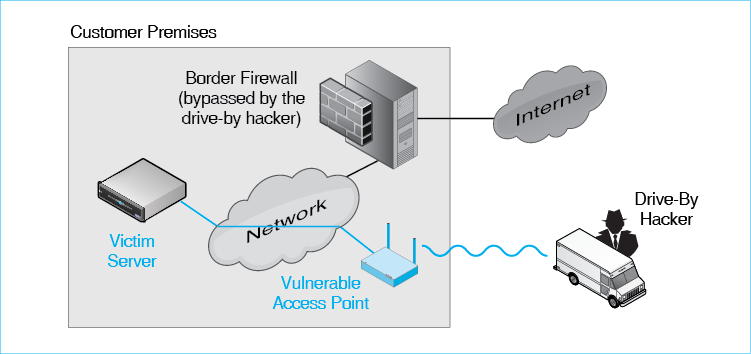
In Chapter 6, we focused on how 802.11 wireless LANs operate. In this chapter, we will look at Wi-Fi security and management. We will then turn to other local wireless technologies.

# 802.11i WLAN Security

## Drive-By Hackers

Figure 7-1 illustrates a typical organizational site. It has a border firewall that scrutinizes traffic going into and out of the site. Within the site, clients connect to the internal network through Wi-Fi access points. Their communication is not filtered by the border firewall.

Figure 7-1: Drive-By Hacking



The figure also shows a drive-by hacker. This adversary is located outside the corporate premises. However, he or she attempts to connect to an access point within the site.[[10]](#footnote-10) If the attempt is successful, then the attacker can communicate with any hosts within the site—without going through the border firewall. The attacker can send attack packets to any host and may be able to intercept conversations within the customer premises. This is exactly what the TJX hackers did.

Companies may mistakenly believe that someone outside their walls will be too far away to communicate with internal access points. However, drive-by hackers use highly directional antennas that allow them to send very strong signals and to receive signals that would be too weak to hear with normal Wi-Fi equipment.

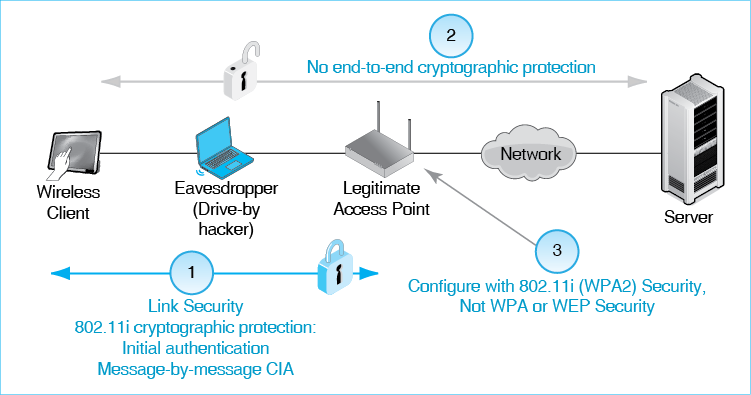
Test Your Understanding

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

## The 802.11i WLAN Security Standard

Realizing the danger of drive-by hackers, the 802.11 Working Group created the 802.11i standard. Figure 7-2 shows that 802.11i provides cryptographic protection between the wireless access point and the wireless host. This protection includes initial authentication plus message-by-message confidentiality, integrity, and authentication (CIA). A drive-by hacker cannot intercept traffic from or send his or her own messages to an access point protected with 802.11i security.[[11]](#footnote-11)

Figure 7-2: Scope of 802.11i Security Protection



Note in the figure that 802.11i protection only provides link security between the wireless client and the wireless access point. It does not provide end-to-end security between the wireless client and the server on the wired LAN (or a server on the Internet). The 802.11i standard has a very limited objective—to protect wireless transmission between the access point and wireless host.

The protection provided by 802.11i only extends between the wireless access point and wireless host.

Although its physical scope is limited, 802.11i protects transmissions within its scope very well. For example, the standard uses the Advanced Encryption Standard (AES) for confidentiality. It also uses strong standards for all other aspects of cryptology.

The 802.11i standard is actually the third standard created to protect communication between wireless clients and access points in 802.11 WLANs. The original standard was wired equivalent privacy (WEP). The 802.11 Working Group created WEP as part of the original 802.11 standard in 1997. Unfortunately, WEP was deeply flawed. As a stop-gap measure, the Wi-Fi Alliance created an interim security standard based on an early draft of 802.11i but using much weaker standards for cryptographic protections than 802.11i called for. The Wi-Fi Alliance called their interim standard Wireless Protected Access (WPA).

Today, there is no reason to use WPA because 802.11i is superior, and using WEP is malpractice at best. However, many wireless access points and wireless routers continue to offer these ancient choices. To add to the confusion, the Wi-Fi Alliance calls the 802.11i standard WPA2, and many wireless access points and wireless routers still use this terminology. All access points and wireless clients today support WPA2 at no extra cost. The only choice today should be to use 802.11i/WPA2.

The choice today should be to use 802.11i/WPA2.

Test Your Understanding

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

The 802.11i standard provides a broad spectrum of security protections. At the beginning of a session between a client and an access point, the two parties exchange information. This normally includes initial authentication, which is distinct from ongoing message-by-message authentication that takes place after the initial handshaking stage. In initial authentication, the wireless client is the supplicant. It must prove its identity to the access point before the access point will allow the client to connect.

When the 802.11 Working Group created the 802.11i standard, it realized that different initial authentication methods would be needed in homes and large enterprises. These two initial authentication methods are shown in Figure 7-3. Note that whatever initial authentication mode, ongoing communication has the same very strong protections, with message-by-message confidentiality, integrity, and authentication. These ongoing protections are extremely strong.

Figure 7-3: Components of 802.11i Security

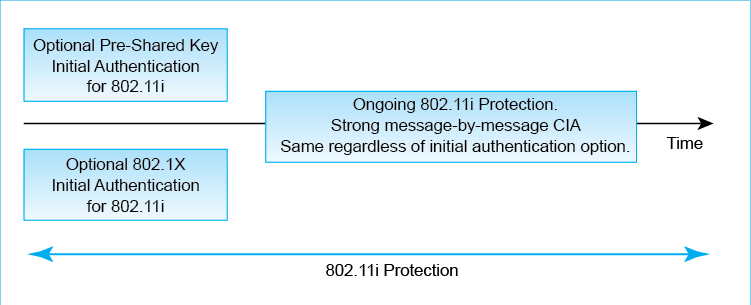


Figure 7-4 shows that these two initial authentication modes are designed for very different environments. 802.1X initial authentication mode was created for corporations with many access points. It is extremely strong but complex to implement. Using 802.1X for initial authentication would be overkill in residences. To use it, you would have to have an authentication server in addition to the other devices in your home! The Ethernet Alliance has rightly dubbed this enterprise mode.

Figure 7-4: 802.11i Modes of Initial Authentication (Study Figure)

|  |  |  |
| --- | --- | --- |
| Mode of 802.11i Initial Authentication | Pre-Shared Key Mode | 802.1X Mode |
| Environment | Home, business with single access point | Companies with multiple access points |
| Uses a Central Authentication Server | No | Yes |
| Authentication Basis | Knowledge of pre-shared key | Credentials on central authentication server |
| Technical Security | Technologically strong, but weak human security can compromise the technological security | Technically extremely strong but can be defeated by rogue access points and evil twin attacks. |
| Operational Threats | Mismanaging the pre-shared key | Rogue access points, evil twin attacks |

The 802.11 Working Group created the simpler Pre-Shared Key (PSK) initial authentication mode for homes. PSK mode is also attractive for small businesses with a single access point. PSK initial authentication mode is a bit weaker than 802.1X initial authentication mode, but it is still strong if implemented properly. The Ethernet Alliance calls this personal mode.

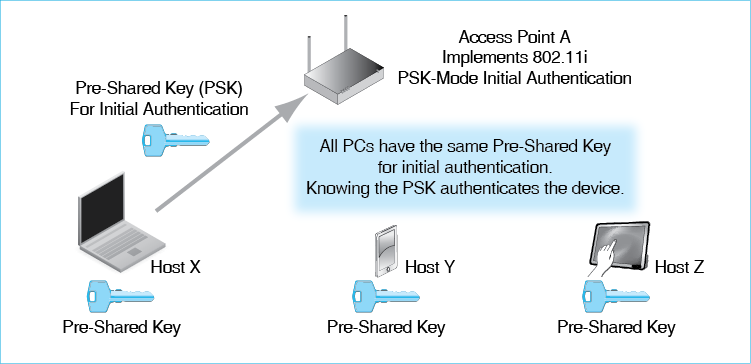
Test Your Understanding

4. a) For what use scenario was 802.11i PSK mode created? b) For what use scenario was 802.11i’s 802.1X 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

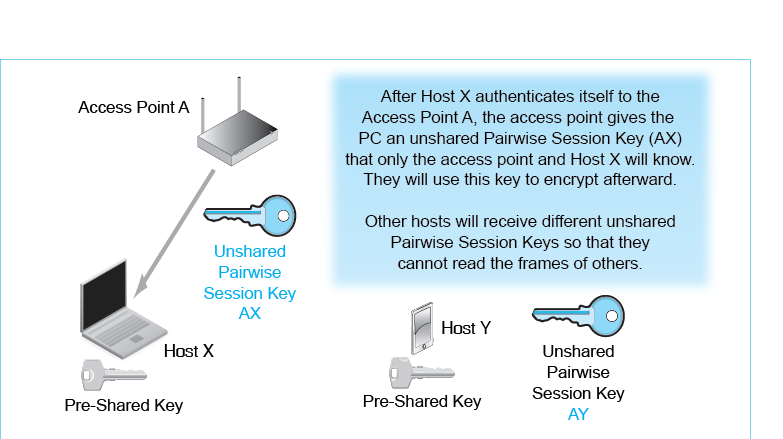
Pre-Shared Session Keys.  Figure 7-5 shows that the access points and wireless hosts need to know the same pre-shared key (PSK) for initial authentication. Demonstrating to the access point that the client knows the PSK authenticates the client to the access point. As the name suggests, all hosts on the single access point have the same pre-shared key to authenticate themselves. In fact, *anyone* who knows the PSK can authenticate himself or herself to the access point.

Figure 7-5: 802.11i Pre-Shared Key (PSK) Initial Authentication Mode



Unshared Pairwise Session Keys. After authentication using the pre-shared key, the wireless access point gives each authenticated device a new unshared pairwise session key to use while communicating with the access point subsequently. Figure 7-6 shows this second key. It is a session key because it will only be used for a single communication session. The next time a client authenticates itself, it will receive a different session key. It is a pairwise key in the sense that each client will have a different session key with the access point. Each client will use its own pairwise session key to encrypt frames sent to the access point. Other clients, not knowing the unshared pair session keys of others, will not be able to read these frames.

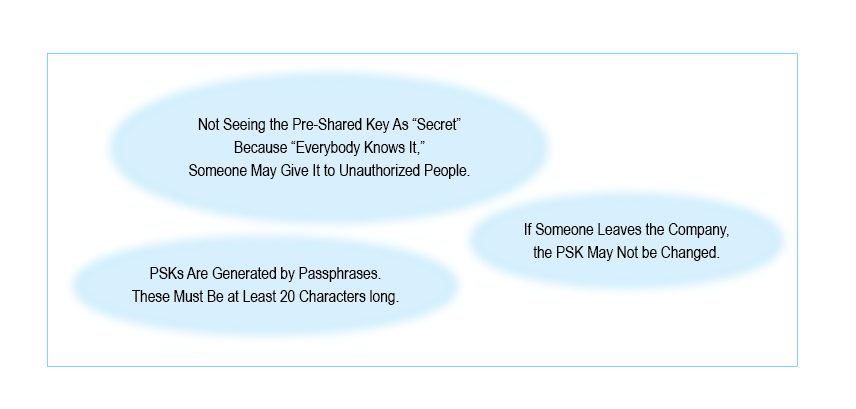
Figure 7-6: Unshared Pairwise Session Key after Initial Authentication



Security Threats in 802.11i PSK Mode. Although 802.11i PSK mode is technically strong, it faces some threats involving how the PSK is managed. Operational (human) security must be equal to the technical security if a residence or small business is to be safe.

One operational security threat is that someone who is not authorized to use the network will be given the pre-shared key. In a home or very small business, there is still the danger that someone, rationalizing that everyone knows the pre-session key, will give it to an unauthorized person. In a residential network, this is even more likely. Some PSK mode access points have a guest account to provide temporary access to outsiders as appropriate.

Figure 7-7: Operational Security Threats in Pre-Shared Key Mode (Study Figure)



If a person leaves a company that uses 802.11i PSK mode, it is important to change the pre-shared key. There is no automated way to do this. It must be changed on all devices that will use the access point. Given the fact that work is involved, it is all too easy to delay doing this.

Another danger is that the household or small business will select a weak passphrase. To create the pre-shared key, the household or company creates a long passphrase, which is much longer than a password. The client or access point enters this passphrase; the system then automatically generates the 64-bit PSK. The passphrase must be at least 20 characters long to generate a strong pre-shared key. If short passphrases are used, 802.11i in PSK mode can be cracked in a few seconds.

In 802.11i pre-shared key mode, the passphrase must be at least 20 characters long to generate a strong pre-shared key.

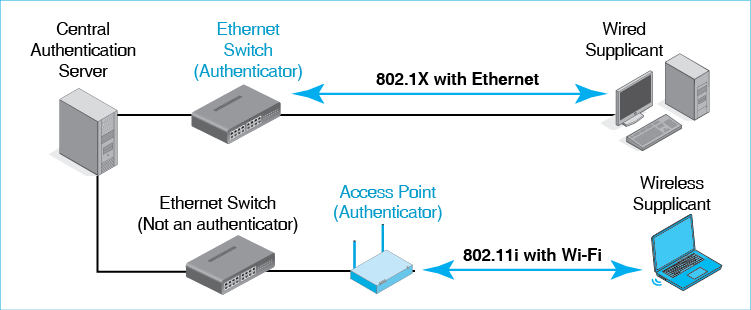
Test Your Understanding

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?

## 802.1X Mode Operation

Again, 802.11i with PSK mode for initial authorization is for homes and for small businesses with a single access point. Large firms with many access points must use a different 802.11i initial authentication mode, 802.1X mode. (The Wi-Fi Alliance calls this mode enterprise mode.) In Chapter 5, we saw that 802.1X was created for initial authentication in Ethernet switched networks. Its goal was to prevent attackers from simply walking into a building and plugging a computer into any wall jack or directly into a switch. Figure 7-8 shows that the Ethernet workgroup switch acts as the authenticator. A computer wishing to access the Ethernet network connects to the authenticator via a UTP connection. A central authentication server checks the supplicant’s credentials and sends an accept/reject decision to the authenticator.

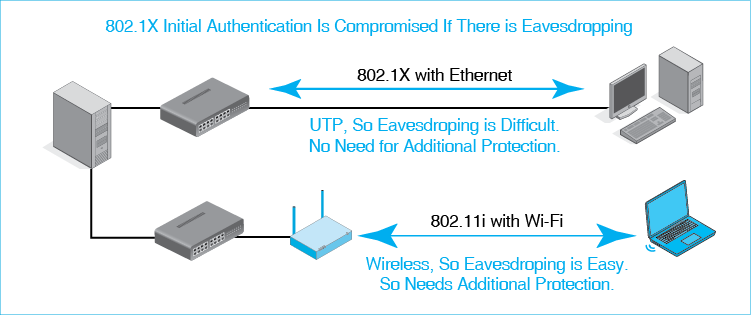
Figure 7-8: 802.11i in 802.1X Mode for Initial Authorization



In Wi-Fi, the 802.1X authenticator is no longer the Ethernet switch; instead is the access point. 802.1X authentication communication takes place between the access point and the wireless supplicant. Authentication messages pass between the client and the central authentication server via the access point.

A vulnerability in 802.1X initial authentication communication is that it is easily compromised if someone can eavesdrop on message exchanges. For Ethernet access, wiretapping is unlikely, so there is no general need to have additional security between the wired host and the workgroup switch to protect 802.1X initial authentication. Consequently, as Figure 7-9 shows, 802.1X offers no protection for the transmission of initial authentication credentials.

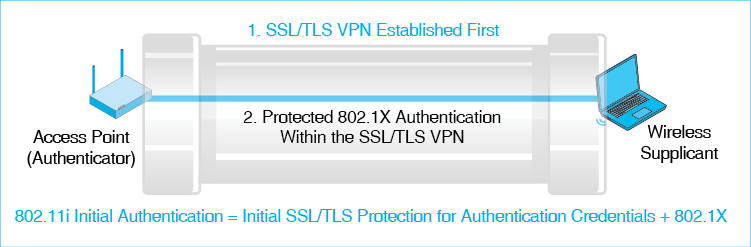
Figure 7-9: The Need for Security in 802.1X Initial Authentication Transmissions



In Wi-Fi, of course, all transmissions between the client and the authenticator are wireless and therefore easy to intercept. This is unacceptable for the transmission of authentication credentials in 802.1X authentication.

To address this problem, the 802.11 Working Group extended the 802.1X standard to work in 802.11i. The extension’s job is to protect authentication exchanges in 802.1X. As Figure 7-10 shows, 802.11i does this by first creating an SSL/TLS virtual private network between the wireless client and the wireless access point. SSL/TLS was selected because it does not require the supplicant or verifier to exchange any secret information during the setup. After the VPN is created, the danger of eavesdropping is eliminated.

Figure 7-10: 802.11i Protection for 802.1X Initial Authentication Communication



Now, 802.1X authentication, which does require the exchange of secret information, takes place safely. This exchange is encrypted for confidentiality by SSL/TLS, so there is no danger of an eavesdropper being able to read credentials during authentication.

Test Your Understanding

6. a) Contrast the use scenarios for initial authentication in PSK mode and 802.1X 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 802.1X operation, what device acts as the authenticator in Ethernet? e) What device acts as the authenticator in Wi-Fi?

7. a) Why does 802.1X 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

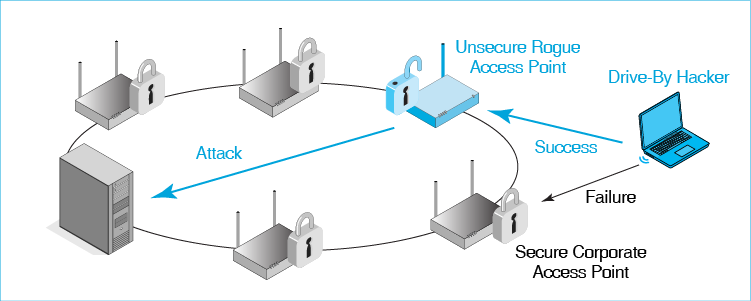
Again, the 802.11i standard protects communication between the wireless access point and wireless clients. This greatly reduces risks. However, two types of attack can succeed even if a company implements 802.11i security well. These are attacks on rogue access points and evil twin attacks.

## Rogue Access Points

The first threat that can defeat 802.11i security is the creation of rogue access points. A rogue access point is an unauthorized access point set up within a firm by an employee or department. Rogue access points are dangerous because they are typically configured with no security or poor security. Figure 7-11 shows that even if a firm carefully applies 802.11i to every last one of its authorized access points, the presence of a single unsecure rogue access point will give a drive-by hacker access to the firm’s internal network. In other words, a single rogue access point destroys the security that the firm has so laboriously created with 802.11i. In the terminology of Chapter 3, this is a weakest link problem. The least secure access point determines the strength of the entire network.

A rogue access point is an unauthorized access point set up within a firm by an employee or department.

Figure 7-11: Rogue Access Point (Study Figure)



Test Your Understanding

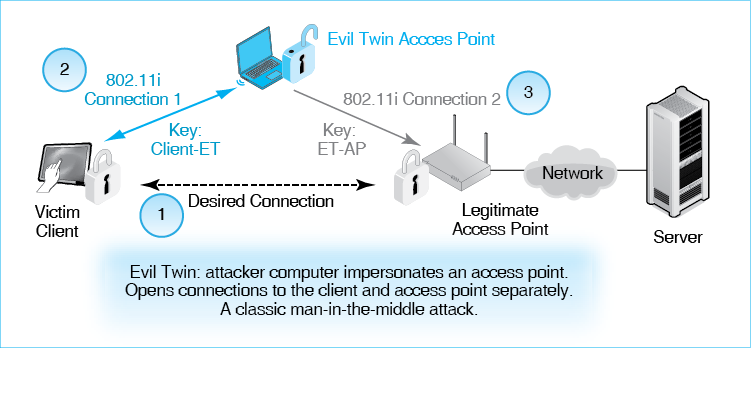
9. a) Who creates a rogue access point? b) Why are they dangerous?

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

The second type of attack that 802.11i will not stop is the ominous-sounding evil twin access point. An Evil Twin attack is a man in the middle attack in which the evil twin intercepts traffic passing between a wireless host and a legitimate access point.

Evil Twin Access Points.  Figure 7-12 illustrates an evil twin access point attack. Normally, the wireless client shown in the figure will associate with its legitimate access point. The two will establish an 802.11i connection between them.

Figure 7-12: Evil Twin Access Point Operation



An evil twin access point (usually a notebook computer) has software to impersonate a real access point. The evil twin operates at very high power. If the wireless host is configured to choose the highest-power access point it can reach, it will associate with the evil twin access point instead of with the legitimate access point. The evil twin will establish a secure 802.11i connection with the wireless victim client. This is *Security Connection 1*. It uses *Key Client-ET* for encryption.

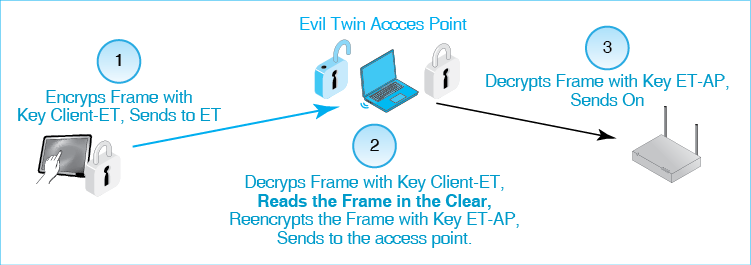
An evil twin access point is a notebook computer configured to act like a real access point.

Next, the evil twin associates with the legitimate access point using 802.11i, creating *Security Connection 2*. This connection uses *Key ET-AP* for encryption. The evil twin now has two symmetric session keys—one that it shares with the victim client and one that it shares with the legitimate access point.

Normal Operation. Figure 7-13 shows what happens when an evil twin operates normally.

* When the host transmits a frame, the host first encrypts it with key Client-ET. It then transmits the encrypted frame to the evil twin.
* The evil twin decrypts the received frame with key Client-ET. It then reads the message in the clear. Its eavesdropping task is done.
* To continue the deception, the evil twin reencrypts the frame, this time with Key ET-AP. Then it sends the encrypted frame to the legitimate access point, which decrypts it and passes it on.

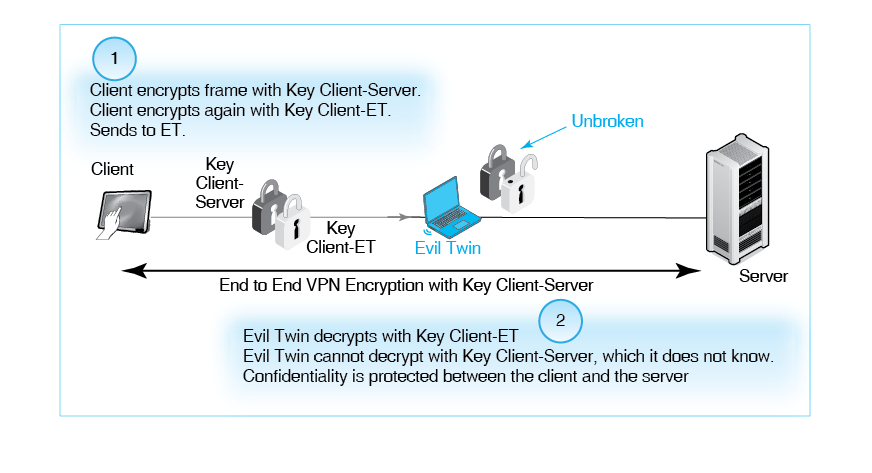
Figure 7-13: Normal Encryption with an Evil Twin Access Point



A man in the middle attack is difficult to detect because it is transparent to both the wireless client and the access point. Both operate as usual. Neither can tell that it is dealing with an impostor.

Using a VPN to Defeat Evil Twins.  If a client cannot detect that it is being taken by an evil twin access point attack, how can it protect itself? The answer is that it can take a simple precaution. As Figure 7-14 shows, a client can implement a virtual private network (VPN) between itself and the server it wishes to communicate with.

Figure 7-14: Defeating an Evil Twin Attack by Using a Virtual Private Network (VPN)



The evil twin still intercepts traffic. Now, however, intercepting the traffic does it no good. Consider what happens when the client transmits a frame.

* The client first encrypts the frame it wishes to send with the VPN key, Key Client-Server, which it shares with server. It then encrypts the frame again, this time with the key it shares with the evil twin (Client-ET). It then sends the doubly encrypted frame to the evil twin.
* The evil twin decrypts the frame with the Client-ET key. However, the frame is still encrypted with the VPN key. So the ET cannot read it.

Test Your Understanding

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

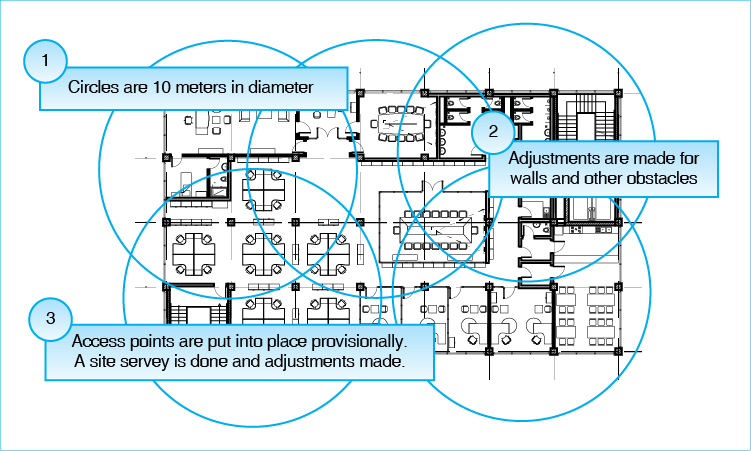
Until recently, the term WLAN management was almost an oxymoron. Large WLANs were like major airports without control towers. Companies quickly realized that they needed tools to centralize WLAN management. Vendors began to provide these tools.

## Access Point Placement

The first management issue is where to place access points throughout a building or site. If access points are placed poorly, there will be overloaded access points, dead spots, and crippling interference between access points.

Initial Planning . The first step in placing access points is to determine how far signals should travel. In many firms, a good radius is about 10 meters. If the radius is too great, many hosts will be far from their access points. Hosts far from the access point must drop down to lower transmission speeds, and their frames will take longer to send and receive. This will reduce the access point’s effective capacity. If the radius is too small, however, the firm will need many more access points to cover the area to be served. Having access points too close together will also increase co-channel interference if it is present.

Figure 7-15: Access Point Placement in a Building (Study Figure)



Once an appropriate radius is selected (say 10 meters), the company gets out its architecture drawings and begins to lay out 10-meter circles that cover all points in the building. Where there are thick walls, filing cabinets or other obstructions, shorter propagation distances must be used. When this is done, it will be clear that access points often cannot be placed precisely in the middle of the circle, so other adjustments must be made.

Of course, in a multistory building, this planning must be done in three dimensions. The “circles” are now bubbles with radiuses of 10 meters. Again, the goal is to provide coverage to all points within the building while reducing overlap as much as possible.

Finally, planners assign channels to access point positions. They attempt to minimize co-channel interference while doing so.

Installation and Initial Site Surveys.  Next, the access points are installed provisionally in the planned locations. However, the implementation work has just begun. When each access point is installed, an initial site survey must be done of the area to discover any dead spots or other problems. This requires signal analysis software, which can run on a notebook computer or even a smartphone.

When areas with poor signal strength are found, surrounding access points must be moved appropriately, or their signal strengths must be adjusted until all areas have good signal strength. Users should now have good service.

Ongoing Site Surveys . Although the initial site survey should result in good service, conditions will change with time. More people may be given desks in a given access point’s range, signal obstructions may be put up for business purposes, and other changes may occur. Site surveys must be done frequently and routinely; they may also be done in response to specific reports of problems.

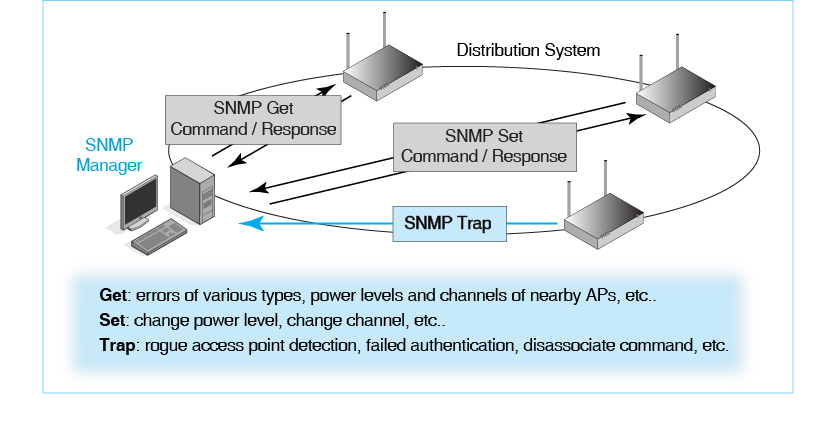
Test Your Understanding

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

Large organizations have hundreds or even thousands of access points. Traveling to each one for manual configuration and troubleshooting would be extremely expensive. To keep management labor costs under control, organizations need to be able to manage access points remotely. The Simple Network Management Protocol, which we saw in Chapter 4, makes this possible. Figure 7-16 shows that the management console constantly requests data from the individual access points. This data may include includes signal strengths, indications of interference, error rates, configuration settings, the power levels, channels, the security setting of nearby access points, and other diagnostic information.

Figure 7-16: Remote Access Point Management



If the administrator, while reading the data, detects a problem in the network, he or she can send SNMP Set commands to access points to increase power, decrease power, change channels, or make other changes.

The figure also shows a wireless access point initiating an SNMP trap command. Traps are sent when a managed access point detects a problem. No manager command is needed for this transmission. A trap might indicate an abnormal error rate, the detection of a rogue access point, or disassociate messages. The last category, disassociate messages, may indicate that an attacker is committing a denial of service attack by sending disassociate messages to wireless clients, telling them to stop using the access point. This knocks them off the network. Any disassociate command not sent by the access point is highly suspicious.

Centralized network management software and hardware on the management console and switches or access points is expensive. However, it should greatly reduce management labor, so there should be considerable net savings from its use.

In addition, centralized WLAN management’s wireless intrusion detection functionality is the only real way to manage WLAN security. Manual detection of threats would be far too slow and require prohibitive amounts of labor.

Test Your Understanding

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

Signal power is usually measured in milliwatts (mW). Networking professionals often have to compare two signal strengths. For instance, if signal power is 20 mW (milliwatts) at 10 meters and 2 mW at 20 meters, the ratio of the second power to the first is 0.1. To give another example, if a larger antenna doubles a transceiver’s transmission power, then the ratio of the final power to the initial power is 2:1. Power ratios are expressed in several ways—as decimal numbers, percentages, or ratios (such as 2:1).

## Calculating Decibel Values for Power Ratios

Networking professionals typically express the ratio of two powers in decibels (dB), using Equation 7-1. *LdB* is the decibel relative value of two power levels, *P1* and *P2*. *P1* is the initial power level. *P2* is the final power level. The equation shows that the decibel expressions use a logarithmic scale.

Equation 7-1:

This looks complicated, but it really is not. Figure 7-17 shows how to do decibel calculations in Excel or some other spreadsheet program. In the first example, the initial power is 40 mW and the final power is 10 mW. This gives a power ratio of 0.25. Excel has a LOG10 function, and this is applied to the power ratio. The result is -0.60. This logarithm is multiplied by a factor of ten. This gives a value of -6.02 decibels. Whenever the second value is smaller than the initial value, the decibel value is negative.

Whenever the second value is smaller than the initial value, the decibel value is negative.

Figure 7-17: Decibel Calculation for Power Levels

|  |  |  |
| --- | --- | --- |
| Data or Formula | Example 1: Attenuation | Example 2: Amplification |
| Initial Power: P1 (mW) | 40 | 10 |
| Final Power: P2 (mW) | 10 | 30 |
| P2/P1 | 0.25 | 3 |
| LOG10(P2/P1) | -0.602059991 | 0.477121255 |
| Ldb: 10\*LOG10(P2/P1) | -6.020599913 (negative) | 4.771212547 (Positive) |

In the second example, the final power is *larger* than the initial power. For example, the signal may be amplified by a larger antenna. The initial power is 10 mW, and the final signal power is 30 mW. This gives a power ratio of 3:1. This time, the decibel value is 4.77 dB, a positive value. Whenever the second value is larger than the initial value, the decibel value is positive.

Whenever the second value is larger than the initial value, the decibel value is positive.

Test Your Understanding

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.

## Approximating Decibel Values

You do not always have a spreadsheet program with you. Nobody can calculate logarithms in their head. However, there are two useful approximations you can use to roughly estimate decibel values if you know the power ratio.

First, Figure 7-18 shows that if you double signal power, this is a gain of approximately 3 dB. If you quadruple the signal power, this is a gain of approximately 6 dB. For each additional doubling, the gain is another approximately 3 dB. This calculation is approximate, but it is close. The exact value is 3.0103.

Figure 7-14: Decibel Approximations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Powers of 2 | |  | Powers of 10 | |
| Power Ratio | Approximate dB |  | Power Ratio | Exact dB |
| 2 | 3 dB |  | 10 | 10 dB |
| 4 | 6 dB |  | 100 | 20 dB |
| 8 | 9 dB |  | 1,000 |  |
| 16 |  |  | 10,000 |  |
| 32 |  |  | 100,000 |  |
| 1/2 | -3 dB |  | 1/10 | -10 dB |
| 1/4 |  |  | 1/100 |  |
| 1/8 |  |  | 1/1,000 |  |

Each doubling of power gives a gain of approximately 3 dB.

Each multiplying by ten in power gives a gain of approximately 10 dB.

What if the power ratio is less than one? If it is 0.5, then the decibel value is approximately -3 dB. Cutting this power in half gives -6 dB. Every additional halving is another -3 dB. Again, if the power ratio is greater than one, the decibel value will be positive, and if the power ratio is less than one, the decibel value will be negative.

If the power ratio is greater than one, the decibel value will be positive, and if the power ratio is less than one, the decibel value will be negative.

For positive or negative powers of ten, the situation is similar. A power ratio of 10:1 is exactly 10 dB. (There is no approximation.) A power ratio of 100 is 20 dB. Each further increase by a factor of ten is another 10 dB. Likewise, a power ratio of 0.1 is -10 dB, and a power ratio of 0.01 is -20 dB.

What if a ratio is *not* a multiple of two or ten? What if it is, for example, 3:1? Well, 2:1 is 3 dB; and 4:1 is 6 dB. So the answer is somewhere between 3 dB and 6 dB. That is not very precise, but it can be useful in practical situations. The 2:1 and 10:1 approximation will not always be useful, but they are good tools for networking professionals to have.

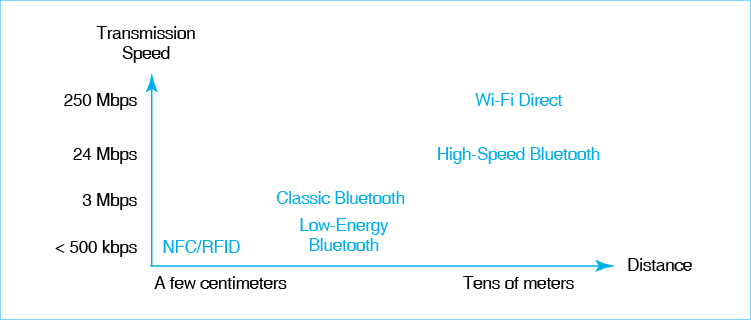
Test Your Understanding

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)

In Chapter 1, you learned that the Internet of Things involves hosts talking to other hosts without human involvement. Machine will simply communicate with one another to coordinate their work. Much of their traffic will be peer-to-peer, in which one device communicates directly with another device, without going through a traditional network. As Figure 7-19 shows, a number of communication peer-to-peer protocols promise to be attractive for IoT communication. They vary widely in the possible distance between the two devices and in transmission speed.

Figure 7-19: Peer-to-Peer Communication Protocols for the Internet of Things (IoT)



Our personal experiences typically suggest that more distance and speed are desirable. But “fast and far” is also a recipe for draining batteries rapidly. If communication can take place over short distances and slower speed, “slow and short” communication extends battery life. As we will see later, RFID tags can transmit without have *any* internal power.

Security is a more complex issue. If signals do not travel as far, they will be more difficult for an eavesdropper to intercept. However, as companies learned with drive-by hackers and traditional Wi-Fi, high-gain antennas may allow eavesdroppers to read signals at far longer distances that the devices use to communicate. In addition, encryption to protect transmissions places a large drain on batteries, and there is a tendency for short and slow protocols to have no encryption or other protections.

Test Your Understanding

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

## Wi-Fi Direct

In Figure 7-19, Wi-Fi Direct is the poster child for fast-and-far peer-to-peer communication. When you have used 802.11, it has probably always involved an access point. However, the 802.11 standard has always included an ad hoc mode, in which two Wi-Fi hosts communicate directly. This provides high-speed communication over typical Wi-Fi distances. It has no problem connecting devices that are at different ends of a house.

Figure 7-20: Wi-Fi Direct



Test Your Understanding

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

## Bluetooth

If you have a wireless headset for your mobile phone or pocket music player, or if you have a hands-free cellular system in your car, you probably are already using Bluetooth. These are precisely the kinds of fairly short distance, moderate-speed applications that Bluetooth was created to handle. Bluetooth is a short-range radio technology designed for personal area networks (PANs)—small groups networked of devices around a person’s body or in the area around a single desk. It is useful to think of Bluetooth as a cable replacement technology.

Bluetooth is a short-range radio technology designed for personal area networks (PANs)—small groups networked of devices around a person’s body or in the area around a single desk. It is useful to think of Bluetooth as a cable replacement technology.

Bluetooth Modes. How fast is Bluetooth? The answer is that the latest version of the Bluetooth standard, Bluetooth 4.0, has three important modes of operation with different transmission speeds, distances, and power requirements. Figure 7-21 compares these Bluetooth modes.

Figure 7-21: Bluetooth Modes of Operation

|  |  |  |  |
| --- | --- | --- | --- |
| Operating Mode | Classic Bluetooth | High-Speed Bluetooth | Low-Energy Bluetooth |
| Principal Benefit | Good performance at low power | High-speed transfers available when needed; longer operating distances | Low-speed transmission |
| Speed | Up to 3 Mbps | Up to about 24 Mbps | Up to about 200 kbps |
| Expected Duty Cycle | Low to High | Low | Very Low |
| Power Required | Low | High | Very Low |
| Maximum Distance | ~10 m | ~30 m | ~10 m |

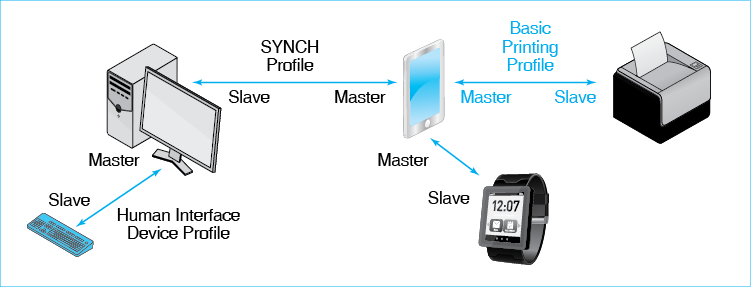
* Classic Bluetooth.  The Bluetooth Special Interest Group, which is the association that standardizes Bluetooth, first created what people think of as classic Bluetooth, with a speed of 2 to 3 Mbps and a distance of about ten meters. This is slow compared to current versions of 802.11, but it is fast enough for wireless mice, music headsets, and many other things.
* High-Speed Bluetooth.  A newer standard is high-speed Bluetooth, which operates in the 2.4 GHz band, has a speed up to about 24 Mbps, and also has Wi-Fi range. In fact, high-speed Bluetooth essentially uses early Wi-Fi physical-layer technology.
* Low-Energy Bluetooth. A newer development is low-energy Bluetooth, which is for device pairs that have very low duty cycles, that is, that only communicate with each a very small percentage of the time. In addition, low-energy Bluetooth is limited to only about 200 kbps. Using low-energy Bluetooth, devices like light switches that only rarely send brief messages can operate with “coin” batteries that last for several years between replacements.

Test Your Understanding

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?

One-to-One, Master–Slave Operation. Figure 7-22 shows several devices communicating with Bluetooth. The device in the top center is a mobile phone. To its right is a printer. The mobile phone user wishes to print a webpage showing on the mobile’s screen. The user selects print, chooses the target printer, and prints. In seconds, the user walks up to the printer and picks up the output.

Figure 7-22: Bluetooth Operation



Bluetooth always uses a one-to-one connection between each pair of devices. Bluetooth cannot do many-to-many networking, which is possible with 802.11 and Ethernet. Reducing operation to one-to-one service simplifies Bluetooth protocols. In the figure, Bluetooth implements a one-to-one connection between the mobile and the printer. It also implements one-to-one connections between the mobile and the desktop computer, the desktop computer and its Bluetooth keyboard, and the mobile and a smart watch. Although the mobile connects to three different devices, these are three separate Bluetooth connections.

Bluetooth always uses point-to-point communication between a pair of devices.

Bluetooth uses master–slave control. One device is the master, and the other device is the slave. In the printing scenario, the mobile device is the master and the printer is the slave. The mobile phone drives the printing process.

In Bluetooth, one device is the master and the other device is the slave. The master controls the slave.

Although communication is always one-to-one, a master may have multiple slaves. In addition to controlling the printer, the mobile phone in Figure 7-22 also controls the user’s smart watch and the desktop computer. In this case, a single master controls three slaves.

It is possible for a Bluetooth device to be a master and slave simultaneously. Consider the relationship between the mobile phone and the desktop computer. The two are synchronizing information. The mobile phone is the master, and the desktop is the slave. However, the desktop is simultaneously master to the keyboard.

A Bluetooth device may be a master of one device and a slave to another device simultaneously.

Test Your Understanding

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?

Bluetooth Profiles. Like 802.11, Bluetooth specifies transmission at the physical and data link layers. The 802.11 Working Group did not have to worry about applications because the desktop and laptop PCs on 802.11 WLANs already had many applications.

However, the Bluetooth SIG faced a different situation. Not only were there no transmission standards for short-range one-to-one communication; there also were no application protocols in existence for PAN applications such as wirelessly controlling keyboards, telephone headsets, printers, and other devices. Consequently, in addition to defining physical and data link layer transmission standards, the SIG also defined application profiles, which are called Bluetooth profiles. Profiles govern how devices share information and specify control messages for various uses. Figure 7-22 shows three Bluetooth Profiles. (A smart watch profile has not been developed at the time of this writing.)

* For printing, the mobile phone uses the Basic Printing Profile (BPP). A Bluetooth device can print to any BPP compliant printer without having to install a printer driver on the Bluetooth device.
* For synchronizing information with the desktop computer, the mobile phone uses the Synchronization Profile (SYNCH).
* Desktop computers, in turn, use the Human Interface Device (HID) Profile for mice, keyboards, and other input devices.

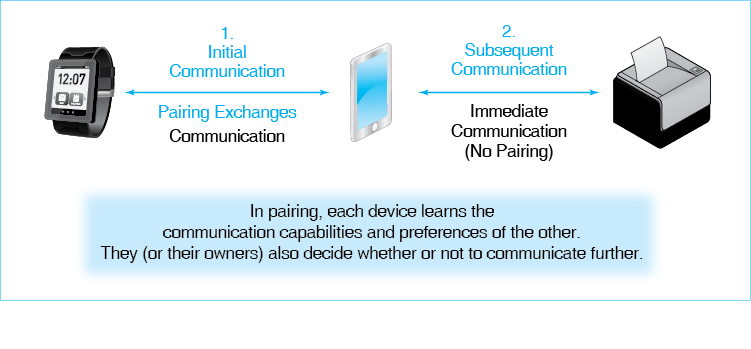
Test Your Understanding

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?

Pairing. When you meet someone, learn how to communicate with them. At the most fundamental level, you learn what language they speak. As importantly, you decide whether you wish to communicate with them or not. In future meetings, you do already have this information, so you can dispense with this learning phase.

Bluetooth is similar. When two devices first interact, they engage in a series of message exchanges called pairing. In pairing, each device learns the communication capabilities and preferences of the other. Pairing is voluntary. If you do not want your device to communicate with a particular device, you can prohibit it from doing so. In fact, the user typically has to put the device in pairing mode, select what nearby Bluetooth device to communicate with, and initiate the communication.

Figure 7-23: Pairing in Bluetooth



Later when the two Bluetooth devices again come into range of each other, they usually connect automatically. Pairing exchanges are unnecessary because they already know about each other. Communication begins immediately, with no user involvement.

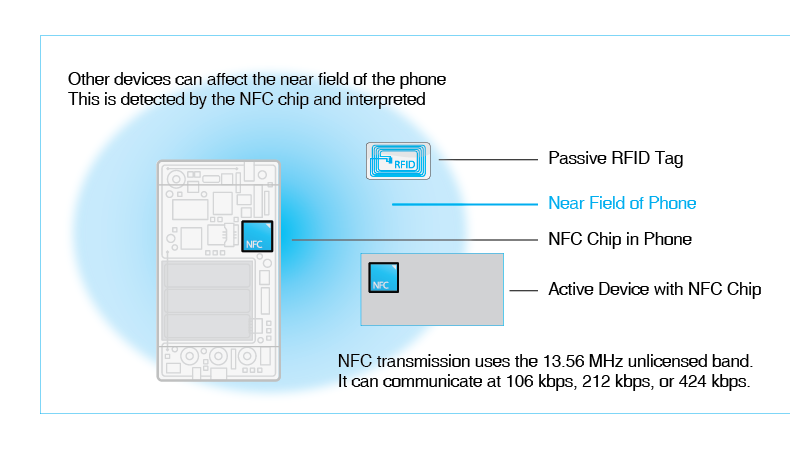
Test Your Understanding

20. a) Must two Bluetooth devices pair each time they meet? b) When must they pair?

## Near Field Communication (NFC)

We have seen that when radios transmit, they produce electromagnetic waves that propagate away, taking energy with them. Very close to an antenna, there is another phenomenon, a near field, which pulses outward a short distance, then is reabsorbed into the antenna. This near field does not propagate away from the antenna. As Figure 7-24 shows, the near field only extends a few inches from a phone with a near field communication (NFC) chip.

Figure 7-24: Near-Field Communication



The figure also shows another active device with an NFC chip. This might be a hotel room door lock, a point-of-sale terminal, or any one of innumerable other devices. The chips in the phone and the other device create near fields that become synchronized. Each can modulate (deliberately change) this near field. If it does, the other device will detect this and can interpret it as a signal. This requires almost no energy.

Figure 7-24 also shows a passive radio frequency ID (RFID) tag. This functions like a bar code. However, as long as the tag passes within a few inches of the scanner, it is read by the device with an active NFC chip. In other words, passive devices can also modulate the near field of the NFC chip, sending a small amount of information.[[12]](#footnote-12)

Although NFC transmission takes place at such extremely low speeds as 434 kbps, it cannot transfer very much information. Also, as noted, transmission distances are only good for a few inches. However, this is fine for many purposes. In addition, a phone can connect to the Internet, so the information exchanged can be used for complex purposes.

NFC standards are still in flux. All NFC protocols use transmission in the 13.56 MHz unlicensed service band created for this purpose. Its three transmission speeds are also the same across standards. However, for applications such as point-of-sale payments, there are competing standards as phone vendors and others push for dominance in a rapidly changing market.

Test Your Understanding

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

## Synopsis

This chapter continues our discussion of local wireless communication. We began with a discussion of 802.11 wireless LAN security threats, including drive-by hackers and war drivers.

The 802.11i cryptographic standard can protect transmissions between a wireless client and a wireless access point. (It does not provide end-to-end protection between the wireless client and the server it uses.)

The 802.11i standard has two initial authentication modes. Pre-shared key (PSK) mode is for use in homes and small businesses with a single access point. The Wi-Fi Alliance calls this personal mode. All users must know a pre-shared key to be authenticated. After authentication, this pre-shared key is replaced by a one-time unshared session key to encrypt further communication between the access point and a particular wireless client. PSK mode provides strong security but only if it is carefully implemented with a strong passphrase, if it is changed when someone leaves the firm, and if the PSK is not given out to unauthorized people.

Corporations with multiple access points must use 802.1X initial mode, which the Wi-Fi Alliance calls enterprise mode. In Chapter 5, we saw that the 802.1X security standard requires an authenticator and a central authentication server. In Ethernet, the authenticator is a switch. In 802.1X mode in 802.11i, the authenticator is the access point. The 802.11i standard adds extra SSL/TLS security to transmissions between the access point and the client *before* the 802.1X authentication phase. When you configure an access point’s security, it is important to specify 802.11i security, which is sometimes listed as WPA2 security. It is important not to select WEP or WPA security.

The 802.11i standard offers very good security between the wireless client and the access point. However, it does not stop all security threats. Sometimes, individuals or departments install their own rogue access points. Even if all other access points are properly secured, a single rogue access point without security gives a drive-by hacker an easy way to get into the firm. A more complex problem is the evil twin access point, which is an attacker computer outside the walls of the company. The evil twin implements a man-in-the-middle attack, intercepting and reading all communication between the victim wireless client and the access point. A virtual private network (VPN) connection between the wireless client and the server it uses is needed to defeat evil twin access points.

We discussed wireless LAN management, including strategies for placing access points to give good coverage with a minimum of overlap and a minimum of interference from nearby access points. Good access point placement requires initial and ongoing site surveys of signal strength and interference. We also looked at the remote management of access points using smart access points or dumb access points controlled by wireless LAN switches. A central manager can detect rogue access points and evil twins, allow the remote adjustment of access point power, push software updates out to the access points, and do all this and more automatically, with a minimum of intervention.

An optional box showed how to express power relationships as ratios and as decibel values. Power ratios in radio transmission are often expressed in decibels, so it is useful to be able to work with decibels.

We looked at other local wireless technologies, which will be important in the Internet of Things. Several wireless protocols promise to be important in IoT communication. One is Bluetooth, which is for personal area networks (PANs) in which all devices are located nearby, often on the same desk or around the body of a person. We discussed Bluetooth in some detail because Bluetooth is growing rapidly in importance. We also looked at near field communication (NFC) and Wi-Fi Direct, which are competitors of Bluetooth for mobile device interactions. We finished by discussing the general level of security in emerging local wireless standards.

## End of Chapter Questions

Thought Question

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 not a trivial 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.*

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 not a trivial 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.*

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?

[Figure 7-1: Drive-By Hacking 4](#_Toc415389992)

[Figure 7-2: Scope of 802.11i Security Protection 5](#_Toc415389993)

[Figure 7-3: Components of 802.11i Security 6](#_Toc415389994)

[Figure 7-4: 802.11i Modes of Initial Authentication (Study Figure) 6](#_Toc415389995)

[Figure 7-5: 802.11i Pre-Shared Key (PSK) Initial Authentication Mode 7](#_Toc415389996)

[Figure 7-6: Unshared Pairwise Session Key after Initial Authentication 8](#_Toc415389997)

[Figure 7-7: Operational Security Threats in Pre-Shared Key Mode (Study Figure) 8](#_Toc415389998)

[Figure 7-8: 802.11i in 802.1X Mode for Initial Authorization 9](#_Toc415389999)

[Figure 7-9: The Need for Security in 802.1X Initial Authentication Transmissions 10](#_Toc415390000)

[Figure 7-10: 802.11i Protection for 802.1X Initial Authentication Communication 10](#_Toc415390001)

[Figure 7-11: Rogue Access Point (Study Figure) 12](#_Toc415390002)

[Figure 7-12: Evil Twin Access Point Operation 12](#_Toc415390003)

[Figure 7-13: Normal Encryption with an Evil Twin Access Point 13](#_Toc415390004)

[Figure 7-14: Defeating an Evil Twin Attack by Using a Virtual Private Network (VPN) 14](#_Toc415390005)

[Figure 7-15: Access Point Placement in a Building (Study Figure) 15](#_Toc415390006)

[Figure 7-16: Remote Access Point Management 16](#_Toc415390007)

[Figure 7-17: Decibel Calculation for Power Levels 17](#_Toc415390008)

[Figure 7-18: Decibel Approximations 18](#_Toc415390009)

[Figure 7-19: Peer-to-Peer Communication Protocols for the Internet of Things (IoT) 19](#_Toc415390010)

[Figure 7-20: Wi-Fi Direct 20](#_Toc415390011)

[Figure 7-21: Bluetooth Modes of Operation 20](#_Toc415390012)

[Figure 7-22: Bluetooth Operation 21](#_Toc415390013)

[Figure 7-23: Pairing in Bluetooth 23](#_Toc415390014)

[Figure 7-24: Near-Field Communication 24](#_Toc415390015)

1. Mark Jewel, “Encryption Faulted in TJX Hacking,” MSNBC.com, September 25, 2007. www.msnbc.msn.com/id/20979359/. [↑](#footnote-ref-1)
2. Ross Kerber, “Details Emerge on TJX Breach,” *The Boston Globe*, October 25, 2007. http://www.boston.com/business/articles/2007/10/25/details\_emerge\_on\_tjx\_breach/. [↑](#footnote-ref-2)
3. Mark Jewel, op. cit. [↑](#footnote-ref-3)
4. Mark Jewel, op cit. [↑](#footnote-ref-4)
5. Evan Schuman, “In 2005, Visa Agreed to Give TJX Until 2009 to Get PCI Compliant,” StorefrontBacktalk, November 9, 2007. storefrontbacktalk.com/story/110907visaletter. [↑](#footnote-ref-5)
6. Federal Trade Commission, “Agency Announces Settlement of Separate Actions Against Retailer TJX and Data Broker Reed Elsevier and Seisint for Failing to Provide Adequate Security for Customers’ Data,” March 27, 2008. www.ftc.gov/opa/2008/03/datasec.shtm. [↑](#footnote-ref-6)
7. John Leyden, “TJX Consumer Settlement Sale Offer Draws Scorn,” TheRegister.com, November 20, 2007. http://www.theregister.co.uk/2007/11/20/tjx\_settlement\_offer\_kerfuffle/. [↑](#footnote-ref-7)
8. U.S. Department of Justice, “Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers,” August 5, 2008. www.usdoj.gov/criminal/cybercrime/gonzalezIndict.pdf. [↑](#footnote-ref-8)
9. Kim Zettrer, “TJX Hacker Charged with Heartland, Hannaford Breaches,” *Wired Magazine*, August 17, 2009. http://www.wired.com/2009/08/tjx-hacker-charged-with-heartland/. [↑](#footnote-ref-9)
10. Merely collecting wireless transmission to determine such things as SSID, signal strength, and channel is not illegal. This practice, although called war driving, is built into every Wi-Fi program. It cannot be illegal because you need this information to connect to an access point. The attempt to connect to an access point without authorization, however, *is* illegal. [↑](#footnote-ref-10)
11. Some people recommend further security protections, such as turning off the periodic broadcasting of the access point’s SSID. Users need to know this SSID to use an access point. However, the SSID is transmitted in the clear (without encryption) in every frame header. Hacker software reads it effortlessly. Another common recommendation is to accept only computers whose wireless network interface cards have pre-approved EUI-48 addresses. Again, however, the EUI-48 address is transmitted in the clear in every packet. Overall, these measures take a great deal of work, and they are easily pushed aside by readily available hacking software. They might make sense if you are only concerned about a home network and unsophisticated but nosy neighbors, but turning on 802.11i protection is easier, and it provides security automatically without additional rabbits-foot gambits. [↑](#footnote-ref-11)
12. For most phones, applications are also available to write on passive NFC tags. This can be used to insert a few commands, so that when the tag is scanned, the phone will take specific actions. For example, you could place one on your business card. Someone scanning it might be taken to your web site or download your vita. [↑](#footnote-ref-12)