CHAPTER 17

Wireless Network Security

When the first edition of this book was published ten years ago, wireless security was one of the major topics in the security field. The fear of insecurity and the associated risk of wireless attacks against private networks were major obstacles to worldwide wireless market expansions. Many organizations simply banned wireless altogether. In fact, many products on the market were designed solely to locate and stop rogue wireless networks. Some of those products are still around today.

The security problems of wireless networking taxed the best minds in IT for years. At conferences and exhibitions, wireless security salespeople often issued statements like this: "Wireless insecurities and threats are made possible by a new advanced technology developed in recent years to provide novel forms of mobile networking." To keep things in perspective: at that time, war driving and open wireless home networks were ever-present; today, it's common knowledge that identity theft and insecure Wi-Fi can lead to serious consequences. This public awareness is fortunate, as most modern smartphones have the power to intercept WEP-encrypted wireless and to crack the keys with free software in a matter of minutes.

Although the advances in mobile device computing have driven the development and furthering of wireless protection standards, some of the history behind these methods started long ago. In reality, the history of radio signal interception and jamming predates modern network sniffing and denial of service (DoS) attacks by nearly a century, going back to the First World War. The first wireless local area network (LAN) was operational in 1969—four years before Ethernet's birth. In fact, this network, the *ALOHA packet radio net* deployed by the University of Hawaii, gave Bob Metcalfe from Xerox PARC an idea that led to the creation of the *CSMA/CD algorithm* (discussed later in this chapter, which Metcalfe initially called Alto Aloha Network), used in all modern TCP/IP networks.

This chapter covers how wireless networking works—because securing a wireless network requires understanding how protocols and signals work—along with wireless threats and countermeasures. We focus on the *802.11 family* of wireless LAN protocols, collectively known as *Wi-Fi* and commonly found in many organizations and households. Wireless security has improved significantly over the past several years, through the use of advanced encryption and access control methods, which means the low-security simple Wi-Fi targets from ten years ago are no longer prevalent. Securing a wireless network today can be done through the features of the Wi-Fi products themselves, to the point that today your wireless network will probably be more secure than your wired LAN.

The focus of this chapter is on protecting wireless local area networks from both external attackers and internal abuse.

Radio Frequency Security Basics

In the information security field, it is an accepted fact that in order to defend against attacks, you have to understand what you're defending. Unfortunately, this fact is not as well understood in wireless networking in general because many network and IT security professionals lack essential knowledge about radio technology, as this topic is not typically included in computer science degree courses or common IT certification preparation materials. At the same time, radio frequency (RF) experts who switch to the IT field may not be familiar with networking protocols, in particular, complex security-related protocols such as *IPSec*.

Security Benefits of RF Knowledge

The following sections describe the security benefits of understanding RF fundamentals.

Proper Network Design

Security must be taken into account at the earliest stage of network planning and design. This applies to wireless network design even more than to its wired sibling. Poorly designed wireless networks are unfortunately quite common and easy for attackers to spot; they possess low resistance to attacks and tend to slow down to a standstill if network traffic overhead is increased by VPN deployment and rich content such as streaming voice and video.

The Principle of Least Access

Your wireless LAN (WLAN) should provide coverage where users need it and not anywhere else. The WLAN must be installed and designed in such a way as to encompass your premises' territory and minimize outside signal leakage as much as possible. This ensures that potential attackers have less opportunity to discover your network, less traffic to collect and eavesdrop on, and a lower bandwidth to abuse, even if they are successful at circumventing your security measures and manage to associate with the network. It also means the attacker has to stay close to your offices, which makes triangulating and/or physical and video surveillance (CCTV) detection of wireless attackers more likely to succeed.

Distinguishing Security Violations from Malfunctions

Is it radio interference, or has someone launched a DoS attack? Are these SYN TCP packets coming because the sending host cannot receive SYN-ACK properly, or is an attacker trying to flood your servers? Why are there so many fragmented packets on the network? Is an attacker running a scanning tool, or is your wireless LAN's maximum transmission unit (MTU) value, which limits the size of network packets, causing frequent retransmits when large packets are sent? The answer is not always obvious. Attacks and malfunctions can appear identical. Most problems on wireless networks can be traced to layer one connectivity issues. Some problems can be caused by neighboring wireless LANs. You shouldn't transmit on the same frequency as your neighbors or one close to it for at least two reasons: interference and the risk of your neighbor accidentally tapping into your data.

Compliance with FCC Regulations

You don't want to get in trouble with the Federal Communications Commission (FCC) in the United States or its equivalents abroad. Because wireless LAN devices operate in unlicensed bands, these wireless networks can break regulations only by using inappropriately high transmission power. In addition to creating possible legal problems, very high transmission power may send your data further than it needs to go, as discussed in the previous section.

Layer One Security Solutions

Most issues pertaining to wireless network layer one security can be solved by tuning the transmitter's output power, choosing the right frequency, selecting the correct antennas, and positioning those antennas in the most appropriate way to provide a quality link where needed, while limiting your network's "fuzzy" borders. Proper implementation of these measures requires knowledge of RF behavior, transmitter power estimation and calculations, and antenna concepts.

NOTE A *decibel (dB)* in the context of wireless networking is a measure of power level on a logarithmic scale. A common reference unit is dBm, where 0 dBm is equal to 1 *milliwatt* and 30 dBm is equal to 1 Watt (1000 watts). For antennas, a common reference unit is dBi, which measures the gain of an omnidirectional antenna, and dBd, which measures the gain of a dipole antenna. Usually, 802.11b/g WLAN cards have 15–23 dBi of transmission power; the current "unofficial standard" is 20 dBi. The receiving sensitivity lies within the range of 80–90 dBm. Without using external antennas and amplifiers, this provides a distance range of 100 meters to 1 kilometer, depending on whether the network is indoors or outdoors, what obstacles are in the way, the building wall materials, interference, and other factors.

Most enterprise controller-based systems with lightweight access points (LWAPs—basically dummies that take all instructions from a central controller) have features like auto frequency switching/hopping, which allows access points to choose the ideal radio frequency depending on current conditions, and dynamic power sensing and adjustment, which raises or lowers the power of the signal so that the communication is optimized without being too weak or too strong. Some systems even have add-on components that can perform real-time frequency management and can use an access point as a "sampler" or air monitor to read the environment around it to provide feedback on how "busy" the air is.

Importance of Antenna Choice and Positioning

A radio frequency signal is a high-frequency alternating current (AC) passed along the conductor and radiated into the air via an antenna. The emitted waves propagate away from the antenna in a straight line and form RF beams or lobes, which are dependent on antenna horizontal and vertical beam-width values. There are three generic types of antennas, which can be further divided into subtypes:

Omnidirectional	Semidirectional	Highly Directional
Mast mount omni	Patch antenna	Parabolic dish
Pillar mount omni	Panel antenna	Grid antenna
Ground plane omni	Sectorized antenna	
Ceiling mount omni	Yagi antenna	

TIP As part of a general vigilance and incident response practice, familiarize your security guards with the appearance of various wireless equipment types, such as antennas and PCMCIA cards. The guards should not normally chase people with wireless client cards, but if something strange takes place on the network—new MAC addresses appear that are not on the access list, a sudden increase in bandwidth consumption, a wireless intrusion detection system (IDS) alarm is triggered—the guards should be told to look out for misplaced wireless equipment or users connecting at inappropriate times or just looking out of place, such as strangers using equipment like antennas and laptops that are not provided by the organization. Something as simple as a typical 802.11 antenna sticking out of an apartment window across the road should also be cause for concern. Another common suspicious case is someone sitting in a car with a laptop and car-mounted antenna. Small ground plane omnidirectionals (often called "omnis") with magnetic mounts are commonly sold as parts of "war-driver kits" and are very popular among war drivers.

Antennas are the best friends of wireless network designers, administrators, and consultants alike. They can also be their worst enemy in the hands of a skillful attacker. They can increase the range of your wireless signal, and capture higher volumes of data, should the attacker manage to associate with the target network.

Examples of antenna irradiation patterns are given in Figure 17-1. When choosing necessary antennas, you need to consider antenna irradiation patterns. Get it right, and your coverage is exactly where you need it. Get it wrong, and you'll have dead areas where no one can connect, or you'll exceed the normal boundaries of your environment and broadcast your network beyond reasonable boundaries.

When planning network coverage, remember that the irradiation happens in two planes: horizontal and vertical. Try to envision the coverage zone in three dimensions: for example, an *omnidirectional* beam forms a doughnut-shaped coverage zone with the antenna going vertically through the center of the "doughnut" hole. Sectorized, patch, and panel antennas form a "bubble" typically spreading 60–120 degrees. *Yagi antennas*, named for one of their designers, are *directional* antennas composed of a dipole and reflector. Yagis form a more narrow "extended bubble" with side and back lobes. *Highly directional antennas* irradiate a narrowing cone beam, which can reach as far as the visible horizon. Horizontal and vertical planes of semi- and highly directional antennas are often similar in shape but have different beam widths; consult the manufacturer's description of the antenna irradiation pattern before selecting an appropriate antenna for your site.

NOTE The irradiation patterns shown in Figure 17-1 are taken from the manufacturers' descriptions of representative antenna types. Traditionally, the descriptions of antenna beams are presented as drawn schemes for the sake of clarity. Here, this tradition is broken on purpose—the reality is different. An attacker can be positioned behind the Yagi or even a directional dish and still be able to discover the network and eavesdrop on passing traffic.

As you can see from the patterns shown in Figure 17-1, the omnidirectional antennas are typically used in point-to-multipoint (hub-and-spoke) wireless network topologies, often together with a variety of semidirectional antennas. *Multiple-input multiple-output (MIMO)* antennas, which use multiple antenna types to improve coverage, have become common in enterprise systems today.

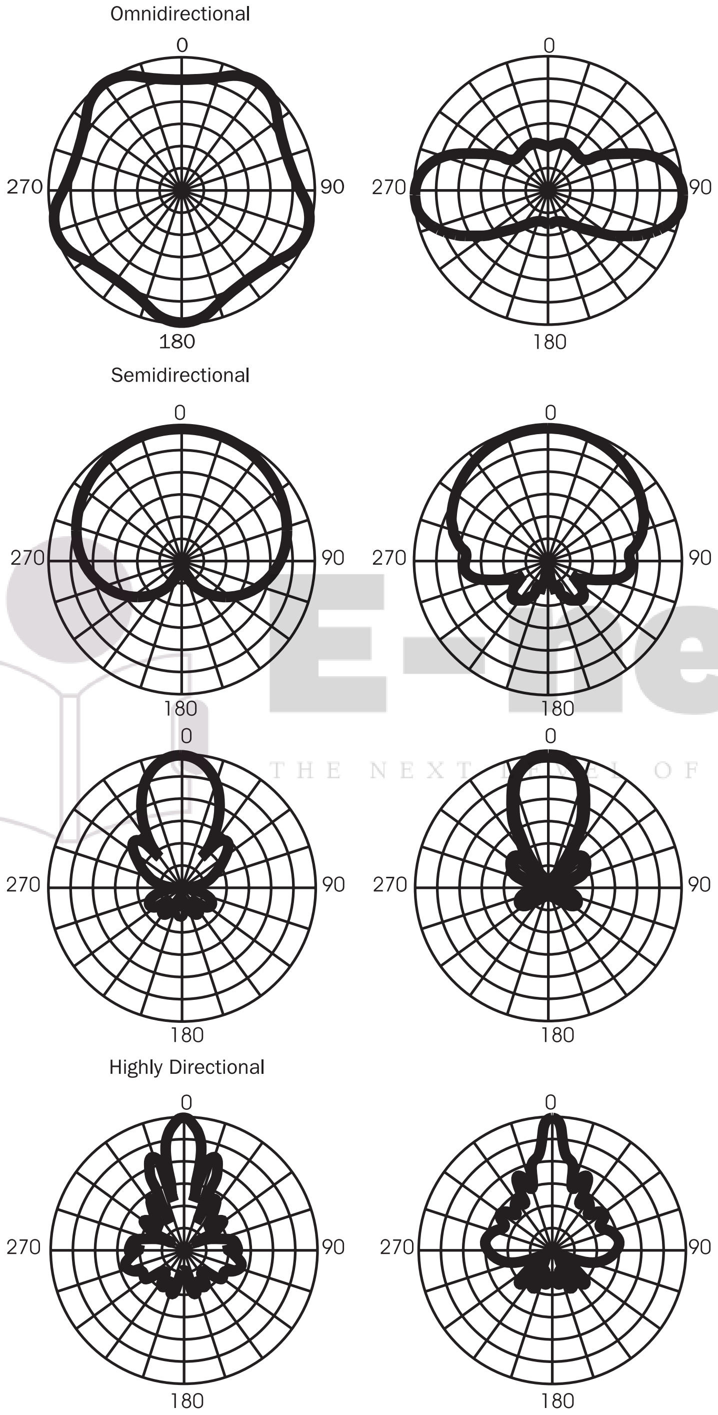


Figure 17-1 Examples of antenna irradiation patterns supplied with quick antenna type–specific beam-width reference values

Tips for Wireless Network Antennas

Here are some tips for choosing antennas for wireless networks:

- *Use omnidirectional antennas only when they are really needed.* In many cases, a sectored or panel antenna with the same gain can be used instead, thus decreasing the perimeter and detectability of your LAN; be creative.
- *When deploying a wireless network inside a tall building, use ground plane omnis to make your LAN less "visible" from the lower floors and streets.* The ground plane reflects the downward signal, thus cutting the bottom of the omni irradiation "doughnut."
- *Position your indoor omnis in the center of a corporate building.* If deploying a wireless LAN through a long corridor linking multiple offices, consider using two panel antennas on opposite ends of the corridor, rather than an array of omnis along the corridor.
- *Take into account antenna polarization.* If the majority of client device antennas are positioned horizontally (such as built-in PCMCIA wireless card antennas), position your omni- or semidirectional antenna horizontally as well. CompactFlash (CF) wireless cards and built-in microchip Bluetooth antennas have vertical polarization. The war driver's favorite, the magnetic mount omni, is always positioned vertically using the car as a ground plane. If your access point's antennas have horizontal polarization, the possibility of war drivers picking up your signal with the magnetic mount omni is decreased.

Yagis are frequently deployed in medium-range point-to-point bridging links, whereas highly directional antennas are used when long-range point-to-point connectivity is required. Highly directional antennas are sometimes used to blast through obstacles such as thick walls. Please note that attackers can also use highly directional dishes to blast through the thick wall of a corporate building, or even through a house that lies in the way of the targeted network. From the top of a hill or a tall building, they can also be used to reach targeted networks 20 to 25 miles away, which makes tracing such attackers hard. On the other hand, at least three highly directional antennas are necessary to triangulate transmitting attackers in order to find their physical position.

TIP If you are an IT professional seriously interested in wireless security, consider getting a narrow beam-width (8 degrees or less) high-gain directional dish/grid antenna alongside other wireless LAN testing equipment.

Controlling the Range of Your Wireless Devices via Power Output Tuning

One way to control your wireless signal spread is, as we just described, correct antenna positioning. Another method is to adjust the transmitter power output to suit your networking needs and not the attackers'. Understanding the concept of gain is essential to doing this.

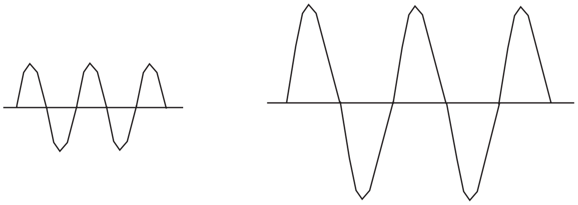


Figure 17-2 Radio frequency signal gain is an increase in the signal's amplitude.

Gain is a fundamental RF term and has already been referred to several times. Gain describes an increase in RF signal amplitude, as shown in Figure 17-2.

You can achieve gain in two ways. First, focusing the beam with an antenna increases the signal's amplitude: a narrower beam width means higher gain. Contrary to popular belief, omnidirectional antennas can possess significant gain reached by decreasing the vertical beam width (squeezing the coverage "doughnut" into a coverage "pancake"). Second, using an amplifier to inject external direct current (DC) power fed into the RF cable (so-called "phantom voltage") can increase gain. Whereas the antenna's direction and position influence *where* the signal will spread, gain affects *how far* it will spread by increasing the transmitting power of your wireless devices.

TIP Security is about control. Try to get wireless access points, bridges, and even client devices with regulated power output. Controlling the signal spread area will be much easier to achieve. Alternatively, you can use an amplifier or attenuator with regulated power output. Attenuators are employed to bring the power output back to legally accepted levels. For Bluetooth devices, the most powerful class 1 (20 dBm) transmitters must possess power controls allowing you to decrease the emission at least down to 4 dBm.

The transmitting power output is estimated at two points on a wireless system. The first point is the *intentional radiator (IR)*, which includes the transmitter and all cabling and connectors but excludes the antenna. The second point is the power actually irradiated by the antenna, or *equivalent isotropically radiated power (EIRP)*. Both IR and EIRP output are legally regulated by the U.S. Federal Communications Commission (see Part 47 CFR, Chapter 1, Section 15.247) or the European Telecommunications Standards Institute (ETSI). To measure the power of irradiated energy (and the receiving sensitivity of your wireless device), watts (more often milliwatts [mW]) or decibels are used. Power gain and loss (the opposite of gain—a decrease in signal amplitude) is estimated in decibels or, to be more precise, dBm. The *m* in dBm signifies the reference to 1 mW: 1 mW = 0 dBm. Decibels have a logarithmic relationship with watts: Pdbm = 10 log pmW. Thus, every 3 dB would double or halve the power, and every 10 dB would increase or decrease the power by an order of magnitude. The receiving sensitivity of your wireless devices would be affected in the same way. Antenna gain is estimated in dBi (*i* stands for *isotropic*), which is used in the same manner as dBm in RF power calculations.

TIP If you deal with wireless networking, familiarize yourself with RF power calculations; even though, most modern enterprise systems do most of the hard work for you. To make life easier, there are many RF power calculators including online tools.

The best way to find how high your EIRP should be, so it provides a quality link without leaving large areas accessible to attackers, is to conduct a site survey with a tool capable of measuring the *signal-to-noise ratio* (*SNR*, also estimated in dB as signal strength minus RF noise floor) and pinging remote hosts. Such a tool could be a wireless-enabled laptop or PDA loaded with the necessary software or a specialized wireless site survey device.

TIP A 22 dB SNR or greater is considered by wireless communication professionals to be appropriate for a decent wireless link on 802.11 LANs. The Bluetooth specification defines the so-called golden receive power range: an incoming signal power should lie in the range between –56 dBm and the receiver sensitivity value +6 dBm.

You can estimate EIRP and loss mathematically before running the actual site survey, taking into account the events depicted in Figure 17-3.

Free space path loss is the biggest cause of energy loss on a wireless network. It happens because of the radio wave front broadening and transmitted signal dispersion (think of a force decreasing when it is applied to a larger surface area). Free space path loss is calculated as 36.56 + 20 $\log_{10}$ (frequency in GHz) +20 $\log_{10}$ (distance in miles). The *Fresnel zone* in Figure 17-4 refers to a set of specific areas around the line of sight between two wireless hosts. You can try to envision it as a set of elliptical spheres surrounding a straight line between two wireless transmitters, building a somewhat rugby ball–shaped zone along this line. The Fresnel zone is essential for wireless link integrity, since any objects obstructing this zone by more than 20 percent introduce RF interference and can cause signal degradation or even complete loss. At its widest point, the radius of the Fresnel zone can be estimated as

$$43.3 \times (\text{link distance in miles} \;/\; (4 \times \text{signal frequency in GHz}))$$

Free space path loss and Fresnel zone calculators are available online at the web sites already mentioned when referring to RF power output calculations. In the real world, the power loss between hosts on a wireless network is difficult to predict, owing to the likely objects in the Fresnel zone (for example, trees or office walls) and the interaction of radio waves with these objects and other entities in the whole coverage area. Such interactions can include signal reflection, refraction, and scattering (see Figure 17-4).

Apart from weakening the signal, these interactions can leak out your network traffic to unpredicted areas, making network discovery more likely and giving potential attackers the opportunity to eavesdrop on network traffic where no one expects the traffic's (and the attackers') presence.

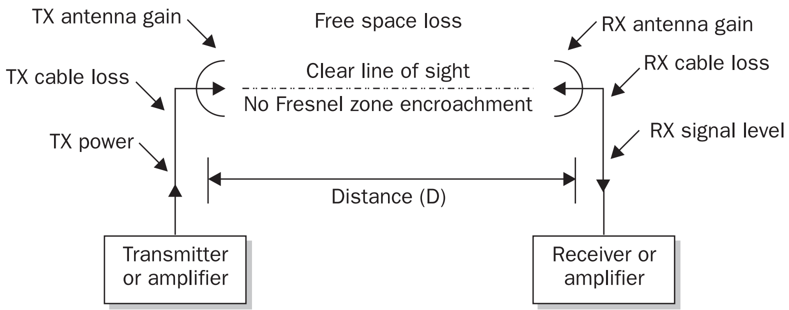


Figure 17-3 Wireless link power gain and loss

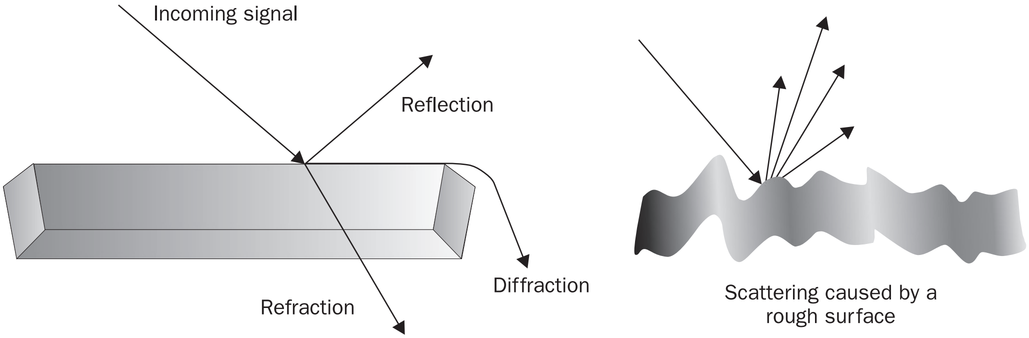


Figure 17-4 Electromagnetic wave-object interactions

NOTE Any experienced "war driver" knows how a dozen new wireless LANs may "pop up" on a network discovery tool interface when passing a road crossing in a large city center. Radio waves flow along the streets, get reflected from the houses on the sides, sneak through narrow gaps between houses, and bend around corners. A lonely reflected beacon frame is an "animal" often seen in dense urban areas. It can give an attacker (or just a curious individual) an indication of some rather "interesting" network to find and investigate. The interest can be caused by the network *service set identifier (SSID)*, the access point vendor's *organizational unique identifier (OUI)*, or other information it may carry that makes attacks easier to perform.

Although you may wonder what the relationship is between legal limitations on acceptable wireless power output and wireless security, you don't want to be a major source of interference in your area and end up on the same side of the law as the attackers. Besides attackers are not limited by the FCC—if one is going to break the law anyway, why care about FCC rules and regulations? This point is important when reviewing layer one DoS (jamming) and layer one man-in-the-middle attacks on wireless networks. Although a wireless systems administrator cannot "outpower" attackers by exceeding the legal power limits, he or she can implement other measures, such as a wireless IDS capable of detecting layer one anomalies like sudden RF power surges or signal quality failures on the monitored network, to alleviate the problem.

Interference, Jamming, and the Coexistence of Spread Spectrum Wireless Networks

The basic concepts of spread spectrum communications are necessary for an understanding of interference, jamming, and the coexistence of wireless networks. Spread spectrum refers to wide-frequency low-power transmission, as opposed to narrowband transmission, which uses just enough spectrum to carry the signal and has a very large SNR (see Figure 17-5).

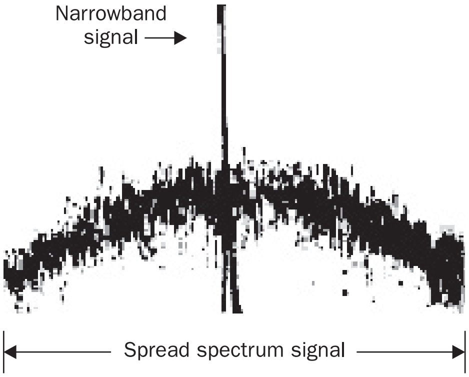


Figure 17-5 Spread spectrum versus narrowband transmission

All 802.11 and 802.15 IEEE standards–defined wireless networks employ spread spectrum band technology. This technology was originally developed during World War II, with security being the primary development aim. Anyone sweeping across the frequency range with a wideband scanner who doesn't know *how* the data is carried by the spread spectrum signal and which particular frequencies are used will perceive such a signal as white noise. Using spread spectrum technology in military communications is a good example of "security through obscurity" that actually works and is based on very specific equipment compatibility. In everyday commercial and hobbyist wireless nets, however, this obscurity is not possible. The devices used must be highly compatible, interoperable, and standards-compliant (in fact, interoperability is the main aim of the Wireless Ethernet Compatibility Alliance (WECA) "WiFi" certification for wireless hardware devices, which many confuse with the IEEE 802.11b data-link layer protocol standard). When the link between communicating devices is established, the two devices must agree on a variety of parameters such as communication channels. Such agreement is done via unencrypted frames sent by both parties. Anyone running a wireless sniffer can determine the characteristics of a wireless link after capturing a few management frames off the air. Thus, the only security advantage brought to civil wireless networks by implementing spread spectrum technology is the heightened resistance of these networks to interference and jamming as compared to narrowband transmission.

There are two ways to implement spread spectrum communications:

- Frequency hopping spread spectrum (FHSS)
- Direct sequence spread spectrum (DSSS)

In FHSS, a pseudorandom sequence of frequency changes (hops) is followed by all hosts participating in a wireless network (see Figure 17-6).

The carrier remains at given frequency for a *dwell time* period and then hops to another frequency (spending a *hop time* to do it); the sequence is repeated when the list of frequencies to hop through is exhausted. FHSS was the first spread spectrum implementation technology

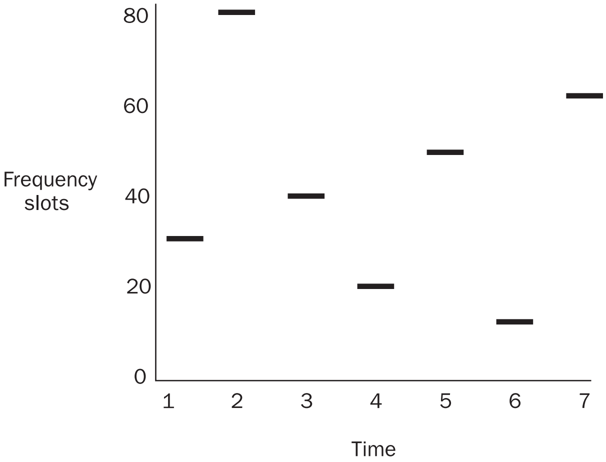


Figure 17-6 FHSS frequency hopping

proposed. It is used by legacy 1–2 Mbps 802.11 FHSS networks and, most importantly, 802.15 networks (Bluetooth). Bluetooth hops 1600 times per second (~625 μs dwell time) and must hop through at least 75 MHz of bandwidth in the middle ISM band. As such, Bluetooth is very resistant to radio interference unless the interfering signal covers the whole middle ISM band. At the same time, Bluetooth devices (in particular Class 3 transmitters) introduce wideband interference capable of disrupting 802.11, 802.11b, and 802.11g LANs. Thus, a Bluetooth-enabled phone, PDA, or laptop can be an efficient (unintentional or intentional) wideband DoS/jamming tool against other middle ISM band wireless networks.

As to interference issues arising from using multiple Bluetooth networks in the same area, it is theoretically possible to keep 26 Bluetooth networks in the same area owing to the different frequency hopping sequences on these networks. In practice, however, exceeding 15 networks per area is not recommended, but the time when widespread Bluetooth use will create such a density of networks is coming—and is closer than it seems—colleges now plan for 7 devices per user for campus-provided wireless networks. You can imagine that in a dorm room with 4 to 6 tenants in close proximity, the number of Bluetooth networks could easily exceed 15 networks.

NOTE Check your country's frequency table to see which devices can introduce interference or be used for jamming wireless LANs. Frequency allocation tables for the U.S. are available online.

DSSS combines a meaningful data signal with a high-rate pseudorandom "noise" data bit sequence, designated as processing gain or chipping code (see Figure 17-7).

The 802.11 range of networks uses DSSS. As compared to FHSS networks (with a maximum 5 MHz–wide carrier frequency), DSSS networks use wider channels (802.11b/g: 22 MHz, 802.11a: 20 MHz), which allow higher data transmission rates. On the other hand, because the transmission on a DSSS network goes through a single 20- to 22-MHz channel and not the whole ISM/UNII band range or the 75 MHz defined by the FCC for FHSS networks, DSSS networks are more vulnerable to interference and jamming. An 802.11b or g LAN would suffer from colocation with a Bluetooth network to a greater extent than the network would be negatively affected by the 802.11b/g LAN.

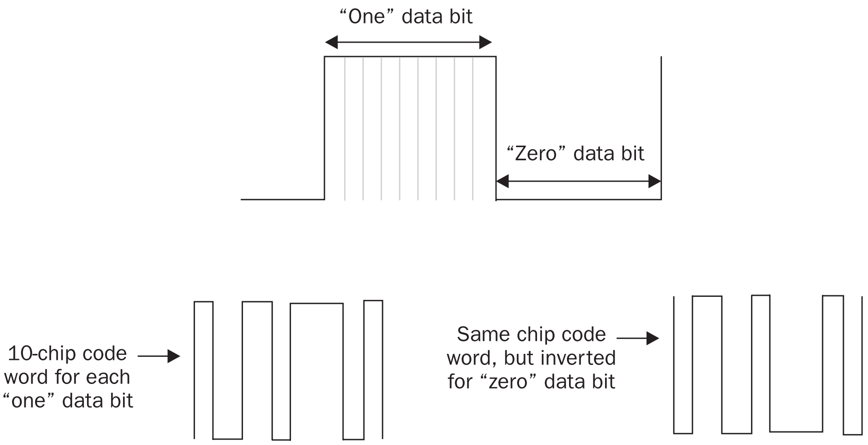
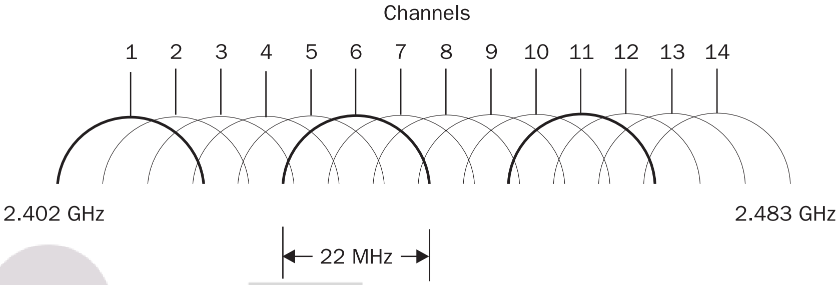

"One" data bit
"Zero" data bit
10-chip code word for each "one" data bit
Same chip code word, but inverted for "zero" data bit

Figure 17-7 DSSS data "hiding" and transmission

UNII band DSSS channels are split by 5 MHz between the channel "margins"; thus, they do not overlap. On the contrary, middle ISM band DSSS channels are split by the 5-MHz distance between the middle of each channel, which means severe channel overlapping takes place. The 802.11b/g channel width is 22 MHz, so you need at least 5 channels (5×5 MHz = 25 MHz > 22 MHz) between two nonoverlapping channels, or so the theory goes. In reality, even these channels would interfere with each other for a variety of reasons. In the U.S., you can use 11 802.11b/g channels, so the maximum number of coallocated access points is three, taking channels 1, 6, and 11, as the following illustration of the 802.11b/g frequency channels allocation shows.



In Europe, 13 channels are allocated for 802.11b/g use, making access point coallocation more flexible (however, only the channels from 10 to 13 are used in France and 10 to 11 in Spain). All 14 channels can be used in Japan. Channel allocation has high relevance to the much-discussed issue of *rogue access points*. There are various definitions for a "rogue access point" and, therefore, different ways of dealing with the problem:

- **Access points and bridges that belong to neighboring LANs and interfere with your LAN by operating on the same or overlapping channels**

  Solution: Be a good neighbor and reach agreement with other users on the channels used so they do not overlap. Ensure your data is encrypted, and an authentication mechanism is in place. Advise your neighbors to do the same if their network appears to be insecure.

Note that interference created by access points operating on close channels (such as 6 and 7) is actually higher than interference created by two access points operating on the same channel. Nevertheless, two or more access points operating on the same channel do produce significant signal degradation. Unfortunately, many network administrators who do not understand RF basics tend to think that all access points belonging to the same network or organization must use the same channel, which is not true.

- **Access points, bridges, USB adapters, and other wireless devices installed by users without permission from enterprise IT management**

  Solution: Have a strictly defined ban on unauthorized wireless devices in your corporate security policy and be sure all employees are aware of the policy contents. Detect wireless devices in the area by using wireless sniffers or specific wireless tools and appliances. Remove discovered unwanted devices and check if the traffic that originated from such devices produced any alerts in logs.

- **Access points or other wireless devices installed by intruders to provide a back channel into the corporate LAN, effectively bypassing egress filtering on the firewall**

  Solution: This is a physical security breach and should be treated as such. Apart from finding and removing the device and analyzing logs (as in the preceding point), treat the rogue device as serious evidence. Handle it with care to preserve attackers' fingerprints, place it in a sealed bag, and label the bag with a note showing the time of discovery as well as the credentials of the person who sealed it (see Chapter 33 to learn more about incident response procedures). Investigate if someone has seen the potential intruder and check the information provided by CCTV.

- **Outside wireless access points and bridges employed by attackers to launch man-in-the-middle attacks**

  This is a "red alert" situation and indicates skill and determination on the part of the attacker. The access point can be installed in the attacker's car and plugged into the car accumulator battery, or the attacker could be using it from a neighboring apartment or hotel room. Alternatively (and more comfortably for an attacker), a PCMCIA card can be set to act as an access point. An attacker going after a public hotspot may try to imitate the hotspot user authentication interface in order to capture the login names and passwords of unsuspecting users.

  Solution: Above all, such attacks indicate that the assaulted network was wide open or data encryption and user authentication mechanisms were bypassed. Deploy your wireless network wisely, implementing security safeguards described later in the chapter. If the attack still takes place, consider bringing down the wireless network and physically locating the attacker. To achieve the latter aim, contact a specialized wireless security firm capable of attacker triangulation.

Data-Link Layer Wireless Security Features, Flaws, and Threats

The peculiarities of physical layer operations, as well as the expected wireless network topology and size, determined the design of data-link layer protocols and associated security features for wireless communications. Unfortunately, the reality rarely meets the designer's expectations. Wireless LANs were initially developed for limited-size networks and short-to-medium point-to-point bridging links.

802.11 and 802.15 Data-Link Layer in a Nutshell

Here, we'll briefly review layer two operations of commonly used wireless networks such as 802.11 LANs and Bluetooth networks. Despite the common use of the terms "wireless Ethernet" and "ethX" as wireless interface designations, the data-link layer on 802.11 networks is quite different from Ethernet frames, as Figure 17-8 demonstrates.

A wireless LAN's mode of operation is also dissimilar to that of Ethernet. Because a radio transceiver can only transmit or receive at a given time on a given frequency, all 802.11-compliant networks are half-duplex. Whereas an access point is a translational bridge in relation to the wired network it may be connected to, for wireless network clients,

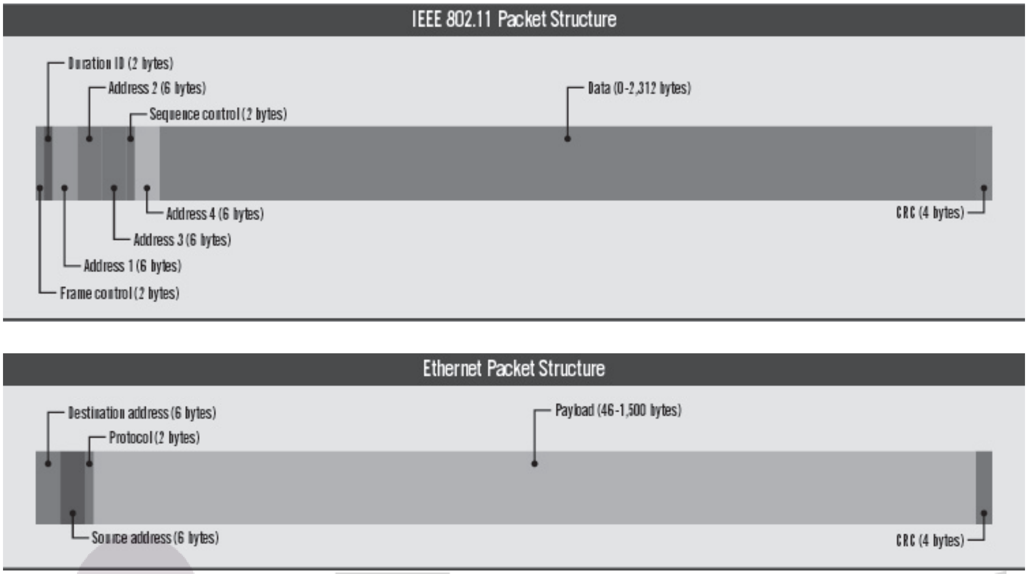


Figure 17-8 Comparison between 802.11 and 802.3 frames

the access point acts as a hub, making packet sniffing an easy task. Because detecting collisions on a wireless network is not possible, the Carrier Sense Media Access/Collision Avoidance (CSMA/CA) algorithm is used on wireless LANs instead of Ethernet's CSMA/CD algorithm. CSMA/CA is based on receiving a positive ACK for every successfully transmitted frame and retransmitting data if the ACK frame is not received. On wired networks, by plugging in the cable, you are associated with the network. On wireless networks, you can't do this, and the exchange of association request and response frames followed by the exchange of authentication request and response frames is required. Before requesting association, wireless hosts have to discover each other. Such discovery is done by means of *passive scanning* (listening for beacon frames sent by access points or ad hoc wireless hosts on all channels) or *active scanning* (sending probe request frames and receiving back probe responses). If a wireless host loses connectivity to the network, another exchange of reassociation, request, and response frames takes place. Finally, a deauthentication frame can be sent to an undesirable host.

MIMO, in the context of Wi-Fi, is still half-duplex, but MIMO allows a fancy way to "hide" or get around the duplex limitation by simultaneously transmitting in both directions (send and receive) on different antennas.

Bluetooth wireless networks can function in circuit-switching (voice communications) and packet-switching (TCP/IP) modes, which can be used simultaneously. The Bluetooth stack is more complicated than its 802.11 counterparts, spanning all the OSI model layers (see Figure 17-9).

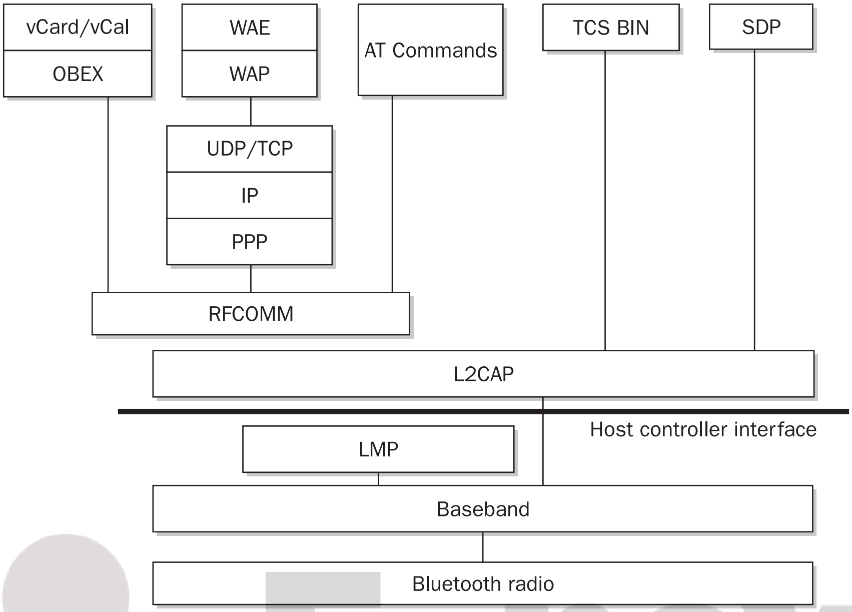


Figure 17-9 Bluetooth protocol stack

The Link Manager Protocol (LMP) is responsible for setting up the link between two Bluetooth devices. It decides and controls the packet size, as well as provides security services such as authentication and encryption using link and encryption keys. The Logical Link Control and Adaptation Protocol (L2CAP) is responsible for controlling the upper-layer protocols. RFCOMM is a cable replacement protocol that interfaces with the core Bluetooth protocols. The Service Discovery Protocol (SDP) is present so that Bluetooth-enabled devices can gather information about device types, services, and service specifications to set up the connection between devices. Finally, there are a variety of application-layer protocols such as TCS BINARY and AT Commands; these are telephony control protocols that allow modem and fax services over Bluetooth.

802.11 and 802.15 Data-Link Layer Vulnerabilities and Threats

The main problem with layer two wireless protocols is that in both 802.11 and 802.15 standards, the management frames are neither encrypted nor authenticated. Anyone can log, analyze, and transmit them without necessarily being associated with the target network. While intercepting management frames is not the same as intercepting sensitive data on the network, it can still provide a wealth of information, including network SSIDs (basically, the network name), wireless hosts' MAC addresses, DSSS LAN channels in use, FHCC frequency hop patterns, and so on. Every Bluetooth device has a unique ID transmitted in clear text in the management frames. Thus, eavesdropping on these frames can be helpful in tracking such a device and its user. Preventing this is hard—short of turning off the Bluetooth device entirely.

TIP Never use a meaningful SSID. Using the name of the organization as an SSID attracts attackers' attention and helps them to locate your network physically. Don't leave a default SSID value in place either. Attackers assume that LANs with default SSIDs have other default settings as well and consider these to be easy prey. In the majority of cases, this assumption is correct. In addition, default SSIDs (the most common one these days appears to be "linksys") help attackers to identify the access point manufacturer (so does the MAC address in captured management frames). Some access points have known security flaws and misconfigurations in default settings (e.g., default SNMP communities containing usernames and passwords). Attackers could be well aware of such flaws and look for the particular access point brands to exploit them.

Unfortunately, the information presented by management frames is only a tiny fraction of the problem. The attacker can easily knock wireless hosts offline by sending deauthenticate and disassociate frames. Even worse, the attacker can insert his or her machine as a rogue access point by spoofing the real access point's MAC and IP addresses, providing a different channel to associate, and then sending a disassociate frame to the target host(s).

Closed-System SSIDs, MAC Filtering, and Protocol Filtering

Common nonstandard wireless LAN safeguards include closed-system SSIDs, MAC address filtering, and protocol filtering.

Closed-system SSID is a feature of many higher-end wireless access points and bridges. It refers to the removal of SSID from the beacon frames and/or probe response frames, thus requiring the client hosts to have a correct SSID in order to associate. This turns SSID into a form of shared authentication password. Closed-system SSIDs can be found in management frames other than beacons and probe responses, however. Just as in the case of shared key authentication mode, wireless hosts can be forced to disassociate in order to capture the SSID in the management frame's underlying reassociation process. Attackers can easily circumvent closed-system SSID security by using deassociation/deauthentication frames.

MAC filtering, unlike closed-system SSID, is a common feature that practically every modern access point supports. It does not provide data confidentiality and is easily bypassed (again, an attacker can force the target host to disassociate without waiting for the host to go offline so its MAC address can be assumed). Nevertheless, MAC filtering may stop *script kiddie* (unsophisticated) attackers from associating with the network.

Finally, protocol filtering is less common than closed systems and MAC address filtering; it is useful only in specific situations and when it is sufficiently selective. For example, when the wireless hosts only need web and mail traffic, you can filter all other protocols and use the built-in encryption capabilities of web and mail servers to provide a sufficient degree of data confidentiality. Alternatively, SSH port forwarding can be used. Protocol filtering combined with secure layer six protocols can provide a good security solution for wireless LANs built for handheld users with low-CPU power devices limited to a specific task (barcode scanning, browsing the corporate web site for updates, and so on).

Built-in Bluetooth Network Data-Link Security and Threats

Bluetooth has a well-thought-out security mechanism covering both data authentication and confidentiality. This mechanism relies on four entities: two 128-bit shared keys (one for encryption and one for authentication), one 128-bit random number generated for every transaction, and one 48-bit IEEE public address (BD_ADDR) unique to each Bluetooth device. Setting up a secure Bluetooth communication channel involves five steps:

1. An initialization key is generated by each device using the random number, BD_ADDR, and shared PIN.
2. Authentication keys (sometimes called *link keys*) are generated by both ends.
3. The authentication keys are exchanged using the initialization key, which is then discarded.
4. Mutual authentication via a challenge-response scheme takes place.
5. Encryption keys are generated from authentication keys, BD_ADDR, and a 128-bit random number.

Streaming cipher E0 is used to encrypt data on Bluetooth networks. A modification of the SAFER+ cipher is used to generate the authentication keys. Three Bluetooth security modes are known: insecure mode 1, service-level security mode 2, and link-level enforced security mode 3. Mode 3 is the most secure and should be used where possible.

Wireless Vulnerabilities and Mitigations

Since Wi-Fi primarily operates at layer two in the OSI stack, most of the attacks against it occur at layer two. But wireless attacks, such as jamming, can also occur at layer one. In this section, we describe five types of wireless attacks.

Wired Side Leakage

Network attacks—whether on the wired or wireless network—typically begin with some form of reconnaissance. On wireless networks, reconnaissance involves promiscuously listening for wireless packets using a wireless sniffer so the attacker can begin to develop a footprint of the wireless network. We will ideally focus on layer two packets, whereby we are not connected (associated) to an access point. If the attacker were associated to an access point, then he or she could sniff layer three and above.

Broadcast and multicast traffic run rampant on most wired networks, thanks to protocols such as NetBIOS, OSPF, and HSRP (which were discussed in Chapter 14), among others that were designed to be chatty about their topology information because they were envisioned to be used only on protected internal networks. What many administrators don't realize is that when they connect wireless to their wired networks this broadcast and multicast traffic can leak into the wireless airspace, as shown in Figure 17-10, if not properly segmented and firewalled. Most access points and wireless switches allow this traffic to leak into the airspace

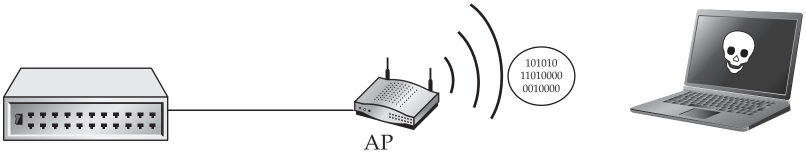


Figure 17-10 Network device traffic can leak onto the wireless airspace.

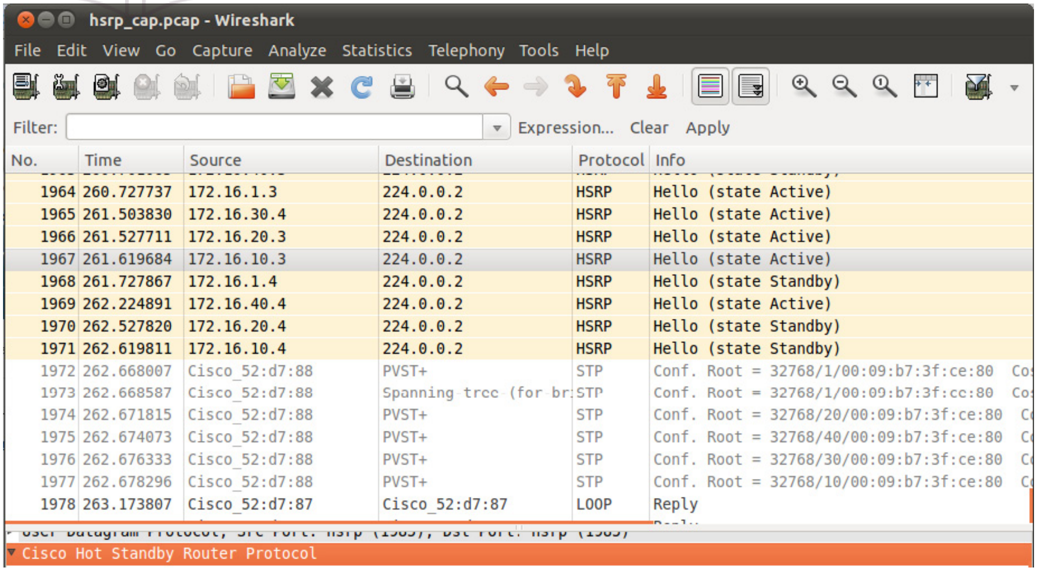
without being blocked. Figure 17-10 illustrates this concept with a network device that is connected to an AP via a wired network, leaking internal protocol communications onto the airwaves. Unfortunately, this traffic may reveal network topology, device types, usernames, and even passwords!

For instance, Cisco's Hot Standby Router Protocol (HSRP), which is used for gateway failover, sends multicast packets. By default, these packets broadcast heartbeat messages back and forth that include the hot standby password for the router in clear text. When these packets leak from the wired network to the wireless airspace, they reveal information about the network topology as well as the password, as shown in Figure 17-11.

When deploying wireless, you need to ensure that, like a firewall, ingress as well as egress are considered. Outbound traffic on the wireless switch and access point should be properly filtered of broadcast traffic to prevent this sensitive wired traffic from leaking into the local airspace. A wireless intrusion prevention system (IPS) can help identify this wired-side leakage by monitoring packets for signs of data leakage, so administrators can block any leaks on their access points, wireless switches, or firewalls.

Rogue Access Points

The most common type of *rogue access point* involves a user who brings a consumer-grade access point like a Linksys router into the office. Many organizations attempt to detect rogue APs through wireless assessments. It is important to note that although you may detect access points in your vicinity, it is equally important to validate if they are connected to your physical network. The definition of a *rogue AP* is an unsanctioned wireless access point connected to your physical network. Any other visible AP that's not yours is simply a neighboring access point.


hsrp_cap.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply

No.	Time	Source	Destination	Protocol	Info
1964	260.727737	172.16.1.3	224.0.0.2	HSRP	Hello (state Active)
1965	261.503830	172.16.30.4	224.0.0.2	HSRP	Hello (state Active)
1966	261.527711	172.16.20.3	224.0.0.2	HSRP	Hello (state Active)
1967	261.619684	172.16.10.3	224.0.0.2	HSRP	Hello (state Active)
1968	261.727867	172.16.1.4	224.0.0.2	HSRP	Hello (state Standby)
1969	262.224891	172.16.40.4	224.0.0.2	HSRP	Hello (state Active)
1970	262.527820	172.16.20.4	224.0.0.2	HSRP	Hello (state Standby)
1971	262.619811	172.16.10.4	224.0.0.2	HSRP	Hello (state Standby)
1972	262.668007	Cisco_52:d7:88	PVST+	STP	Conf. Root = 32768/1/00:09:b7:3f:ce:80 Co
1973	262.668587	Cisco_52:d7:88	Spanning tree (for br	STP	Conf. Root = 32768/1/00:09:b7:3f:ce:80 Co
1974	262.671815	Cisco_52:d7:88	PVST+	STP	Conf. Root = 32768/20/00:09:b7:3f:ce:80 C
1975	262.674073	Cisco_52:d7:88	PVST+	STP	Conf. Root = 32768/40/00:09:b7:3f:ce:80 C
1976	262.676333	Cisco_52:d7:88	PVST+	STP	Conf. Root = 32768/30/00:09:b7:3f:ce:80 C
1977	262.678296	Cisco_52:d7:88	PVST+	STP	Conf. Root = 32768/10/00:09:b7:3f:ce:80 C
1978	263.173807	Cisco_52:d7:87	Cisco_52:d7:87	LOOP	Reply

```
▸ User Datagram Protocol, Src Port: hsrp (1985), Dst Port: hsrp (1985)
▾ Cisco Hot Standby Router Protocol
```

Figure 17-11 A password is revealed by an internal routing protocol via wireless.

Vetting out the potential rogue APs requires some prior knowledge of the legitimate wireless environment and sanctioned access points. This approach for detecting rogue APs involves determining the anomalous access points in the environment and, therefore, is really a best effort approach. As mentioned earlier, this approach doesn't necessarily confirm whether the access points are physically connected to your network. That requires assessing the wired side as well and then correlating the wired assessment to the wireless assessment. Otherwise, your only other option is to check each physical access point to determine if the anomalous AP is connected to your network. Doing this can be impractical for a large assessment. For this reason, wireless IPSs are far more effective at detecting rogue APs. A wireless IPS correlates what it sees with its wireless sensors to what it sees on the wired side. Through a variety of algorithms, it determines if the access point is truly a rogue access point, one that is physically connected to the network.

Even quarterly spot checks for rogue access points still give malicious hackers a huge window of opportunity, leaving days if not months for someone to plug in a rogue access point, perform a compromise, and then remove it without ever being detected.

Misconfigured Access Points

Enterprise wireless LAN deployments can be riddled with misconfigurations. Human error coupled with different administrators installing the access points and switches can lead to a variety of misconfigurations. For example, an unsaved configuration change can allow a device to return to its factory default setting if, say, the device reboots during a power outage. And numerous other misconfigurations can lead to a plethora of vulnerabilities. Therefore, these devices must be monitored for configurations that are in line with your policies. Some of this monitoring can be done on the wired side with WLAN management products. Additionally, mature wireless IPS products can also monitor for misconfigured access points if you predefine a policy within the wireless IPS to monitor for devices not compliant with policy.

Modern systems have different considerations—the controller-based approach largely prevents this issue, but some organizations, especially smaller ones, will still face this type of problem. Human error on the controller side poses a larger and more significant risk—all the access points will have a problem or configuration vulnerability, not just one.

Wireless Phishing

Since organizations are becoming more disciplined with fortifying their wireless networks, trends indicate that wireless users have become the low-hanging fruit. Enforcing secure Wi-Fi usage when it concerns human behavior is difficult. The average wireless user is simply not familiar with the threats imposed by connecting to an open Wi-Fi network at a local coffee shop or airport. In addition, users may unknowingly connect to a wireless network that they believe is the legitimate access point but that has, in fact, been set up as a honeypot or open network specifically to attract unsuspecting victims.

For example, they may have a network at home called "Linksys." As a result, their laptop may automatically connect to any other network known as "Linksys." This built-in behavior can lead to an accidental association to a malicious wireless network, more commonly referred to as *wireless phishing*.

Once an attacker gains access to the user's laptop, not only could the attacker pilfer information such as sensitive files, but the attacker could also harvest wireless network credentials for the user's corporate network. This attack may be far easier to perform than attacking the enterprise network directly. If an attacker can obtain the credentials from a wireless user, he or she can then use those credentials to access the corporate enterprise wireless network, bypassing any encryption or safety mechanisms employed to prevent more sophisticated attacks.

Client Isolation

Users are typically the easiest target for attackers, especially when it comes to Wi-Fi. When users are associated to an access point, they can see others attempting to connect to the access point. Ideally, most users connect to the access point to obtain Internet access or access to the corporate network, but they can also fall victim to a malicious user of that same wireless network.

In addition to eavesdropping, a malicious user can also directly target other users as long as they're associated to the same access point. Specifically, once a user authenticates and associates to the access point, he or she obtains an IP address and, therefore, layer three access. Much like a wired network, the malicious wireless user is now on the same network as the other users of that access point, making them direct targets for attack.

Wireless vendors are aware of this vulnerability and have released product features to provide client isolation for guest and corporate networks. Essentially, client isolation allows people to access the Internet and other resources provided by the access point, minus the LAN capability. When securing a Wi-Fi network, isolation is a necessity. Typically the feature is disabled by default, so ensure that it's enabled across all access points.

Wireless Network Hardening Practices and Recommendations

We have already discussed the defense issues related to physical and RF security of wireless networks. In this section, we outline data-link layer countermeasures against the possible abuse of your wireless LAN. These countermeasures include

- Secure replacements for WEP
- Proper wireless user authentication
- Intrusion detection and anomaly tracking on wireless LANs

Of course, the security of wireless networks can (and should) be provided using higher-layer safeguards such as various IPSec modes or SSL-based secure protocols.

Wireless Security Standards

In 2004, the IEEE "i" task group developed a unified wireless security standard, parts of which have been implemented by many wireless equipment and software manufacturers in order to mitigate known 802.11 security problems. Originally known as 802.11i, this standard is now widely known as WPA2, which stands for Wi-Fi Protected Access version 2. WPA2 replaced WPA, which was a hybrid of the old, insecure WEP standard that was backward compatible for existing wireless infrastructures. WPA used RC4 encryption, which is weaker than the AES encryption used in WPA2. WPA2 is the current, best security solution for wireless networks and is expected to remain so for the foreseeable future.

CAUTION Note that most wireless access points that support WPA2 have a feature known as Wi-Fi Protected Setup (WPS), which has a security flaw that allows an attacker to obtain the WPA2 password, allowing him or her to connect to the network without authorization. This feature should be turned off if possible to avoid the attack.

Temporal Key Integrity Protocol and Counter Mode with CBC-MAC Protocol

The WPA2 architecture can be split on two "layers:" encryption protocols and 802.11x port-based access control protocols. The Temporal Key Integrity Protocol (TKIP) and the Counter Mode with CBC-MAC Protocol (CCMP) are WPA2 encryption protocols on 802.11 LANs. TKIP encrypts each data packet with a unique encryption key. To increase key strength, TKIP includes four additional algorithms:

- A cryptographic message integrity check to protect packets
- An initialization-vector (IV) sequencing mechanism that includes hashing
- A per-packet key-mixing function to increase cryptographic strength
- A rekeying mechanism to provide key generation every 10,000 packets

Although TKIP is useful for upgrading security on older wireless devices, it does not address all of the security issues facing WLANs and may not be reliable or efficient enough for enterprise and government use.

TKIP uses 48-bit IVs to avoid IV reuse and does per-packet key-mixing of the IVs to introduce additional key confusion (reducing the relationship of the statistical composition between the ciphertext and the key value). It also implements a one-way hash message integrity code (MIC or Michael) checksum instead of the insecure CRC-32 used for WEP integrity check vector (ICV) computation. TKIP is not mandatory for WPA2 implementations, is backward compatible with WEP, and does not require hardware upgrade. Together with 802.1x, TKIP is the basis for the first version of Wi-Fi Protected Access (WPA).

CCMP uses the Advanced Encryption Standard (AES, Rijndael) cipher in a counter mode with cipher block chaining and message authenticating code (CBC-MAC). The AES key size defined by the WPA2 standard is 128 bit. Like TKIP, CCMP implements 48-bit IV (called *packet number,* or *PN*) and MIC.

802.1x-Based Authentication and EAP Methods

The 802.1x standard was originally designed to implement layer two user authentication on wired networks. On wireless networks, 802.1x can also be used for the dynamic distribution of WEP keys. Because wireless LANs have no physical ports, an association between the wireless client and the access point is assumed to be a network access port. In terms of 802.1x, the wireless client is defined as a *supplicant* (or *peer*), and the access point, as an *authenticator* (similar to an Ethernet switch on wired LANs). Finally, an authentication server is needed on the wired network segment to which the access point is connected. This service is usually provided by a RADIUS server supplied with some form of user database, such as

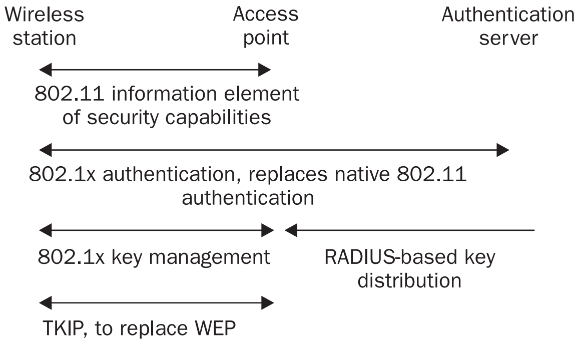

Wireless station
Access point
Authentication server
802.11 information element of security capabilities
802.1x authentication, replaces native 802.11 authentication
802.1x key management
RADIUS-based key distribution
TKIP, to replace WEP

Figure 17-12 An overview of 802.1x/TKIP functionality

native RADIUS, LDAP, NDS, or Active Directory. Wireless gateways can implement the authentication server, as well as the authenticator functionality. Figure 17-12 gives an overview of the 802.1x and TKIP implementation on a secure wireless LAN.

User authentication in 802.1x relies on the layer two Extensible Authentication Protocol (EAP, RFC 2284). EAP is an advanced replacement of CHAP under PPP, designed to run over local area networks (EAP over LAN [EAPOL] describes how EAP frames are encapsulated within Ethernet, Token Ring, or FDDI frames). EAP frame exchange between the supplicant, authenticator, and authentication server is summarized in Figure 17-13.

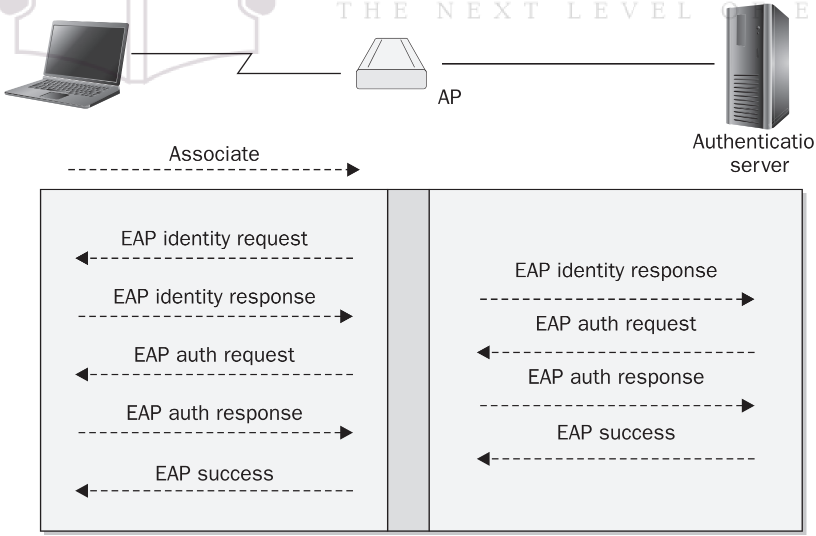


Figure 17-13 EAP authentication process

There are multiple EAP types, adding to compatibility problems in 802.1x implementations. The most commonly implemented EAP types are described next:

- EAP-MD5 is the base level of EAP support by 802.1x devices. It is the first EAP type that duplicates CHAP operations. Because EAP-MD5 does not provide server authentication, it is vulnerable to "rogue authenticator/authentication server" type of attacks. When choosing 802.1x solutions and products for your wireless network, take care that the authentication is mutual in order to reduce the risk of man-in-the-middle attacks.
- EAP-TLS (Transport Layer Security) provides mutual certificate-based authentication. It is built on the SSLv3 protocol and requires deployed certificate authority.
- EAP-LEAP (Lightweight EAP or EAP-Cisco Wireless) is a Cisco-proprietary EAP type, implemented on Cisco access points and wireless clients. Unfortunately, EAP-LEAP uses modified MS-CHAPv2 with insecure MD4 hashing and weak DES key selection for challenge/response procedures. Thus, it is susceptible to optimized dictionary attacks as implemented by LEAP attack tools. Take care that you choose really strong passwords when using EAP-LEAP and rotate the passwords on a regular basis.
- PEAP (Protected EAP, an IETF standard) and EAP-TTLS (Tunneled Transport Layer Security are other forms of EAP. EAP-TTLS supports multiple legacy authentication methods, including PAP, CHAP, MS-CHAP, MS-CHAPv2, and EAP-MD5. To use these methods in a secure manner, EAP-TTLS creates an encrypted TLS tunnel inside of which the less secure legacy authentication protocol operates. EAP-PEAP is similar to EAP-TTLS but does not support less secure authentication methods such as PAP and CHAP. Instead, it employs PEAP-MS-CHAPv2 and PEAP-EAP-TLS inside of the secure TLS tunnel. Both EAP-TTLS and EAP-PEAP require server-side certificates only, and a copy of the server certificate is commonly distributed to clients with the supplicant software.

Wireless Intrusion Detection and Prevention

The preceding points notwithstanding, intrusion detection on wireless networks should always cover the data-link layer. The principles of intrusion detection are outlined in Chapter 18. Here, we briefly cover wireless-specific IDS issues. Many applications claim to be wireless IDS systems but detect new MAC addresses on a LAN only as long as these addresses are not permitted by an ACL. Such functionality is implemented in the firmware of some access points as well. Of course, anyone able to bypass MAC-based ACL will bypass MAC-based "IDS." A true wireless IDS is a dedicated 802.11 (or 802.15) protocol analyzer supplied with an attack signature database or knowledge base and inference engine, as well as an appropriate report and alarm interface. Some suspicious events to look for on a wireless LAN include

- Probe requests (a good indication of someone using active scanning mode)
- Beacon frames from unsolicited access points or ad hoc wireless clients
- Floods of disassociate/deauthenticate frames (man-in-the-middle attack?)

- Associated but not authenticated hosts (attempts to guess the shared key?)
- Frequent reassociation frames on networks without enabled roaming, and frequent packet retransmits ("hidden node," bad link, or possible DoS attack?)
- Multiple incorrect SSIDs on closed networks (SSID brute-forcing?)
- Suspicious SSIDs such as "AirJack" (or plain old "31337")
- Frames with unsolicited and duplicated MAC addresses
- Randomly changing MAC addresses (attackers using Wellenreiter or FakeAP)
- Frames transmitted on other 802.11 channels within the five-channel range, or frames with different SSIDs transmitted on the same channel (misconfigured and probably unsolicited host, interference, DoS?)
- Hosts not using implemented cryptographic solutions (should not be there)
- Multiple EAP authentication requests and responses (brute-forcing EAP-LEAP?)
- Malformed and oversized EAP frames and various EAP frame floods (802.1x DoS attack?)
- 802.11 frame sequence numbers that don't match the established sequence cycle (man-in-the-middle attacks, MAC spoofing on LAN?)
- ARP spoofing and other attacks originating from wireless LANs

Organizations are challenged with controlling who and what connects to their enterprise network through wireless access points. Many of the enterprise wireless vendors have enhanced their access point and wireless controller products that natively include firewalls, RADIUS, network access control, and wireless IPS. This integration provides better control of the wireless users who connect to the wireless infrastructure and control where these users can go on the enterprise network. This was a much-needed defense-in-depth approach because a wired-side firewall and IPS cannot provide the protection necessary to defend against wireless attacks. Most wireless attacks occur at layer two and within the wireless medium. Traditional wired firewalls are not equipped to detect these attacks, and wired IPS doesn't have the ability to inspect these types of packets. This has led to specialized wireless IPS products.

Wireless IPS and IDS

Wireless IPS identifies wireless attacks using wireless sensors. These wireless sensors typically use the same Wi-Fi radios that are found in access points, which is why many vendors allow for dual usage of access points, both for access as well as for detecting attacks. How this occurs varies from vendor to vendor. There are many hybrid approaches. The most common approach is to pause the wireless radio when no one is using it for access, and perform a quick snapshot of the wireless airspace for rogue access points and attacks. But this part-time approach to wireless IDS means that you'll only detect attacks when the wireless radio is in detection mode. For the rest of the day, wireless attacks go undetected. This shortcoming has prompted some vendors to use a secondary Wi-Fi radio in their access points so one radio is used for full-time access and the other radio for full-time wireless IPS.

The Wi-Fi protocol allows channels to be assigned to various frequencies, with one channel assigned to each frequency. In heavily congested wireless environments, using different channels (or frequencies) allows the administrator to minimize interference, which is also referred to as *co-channel interference*. As a result, appropriately detecting wireless attacks requires routinely checking each channel for attacks. There are essentially two groups of frequencies: 802.11b and 802.11g operate in the 2.4-GHz spectrum; 802.11a operates in the 5-GHz spectrum; 802.11n operates in both spectrums, 2.4 GHz and 5 GHz; and 802.11ac operates in the 5-GHz spectrum only.

As the wireless sensor jumps from channel to channel collecting wireless packets for analysis, it will not collect some packets, and therefore, those will be missed because the sensor can only monitor one channel at a time. Therefore, some vendors now allow the sensor to optionally "lock on channel" to allow only one channel (or frequency) to be monitored. For highly sensitive environments where only one channel is used, this feature helps the administrator to minimize packet loss. The reality is that some loss will always occur because wireless is a physical medium. This is a result of a myriad of factors, including mobile wireless devices, the devices' distance from the sensor, the sensor's antenna strength, and so on.

Wireless IDS involves receiving packets only. Its coverage is, therefore, more physically broad compared to an access point, which transmits and receives. In a typical access point and sensor deployment, the rule of thumb is one sensor for every three access points. A wireless site survey will help determine the best sensor coverage and placement.

As most people deploy wireless IDS to detect rogue access points, triangulation is also a consideration. Although a rogue AP can be detected with a single sensor, its physical location cannot. Triangulation is required to identify the physical proximity of the rogue AP. Triangulation involves a minimum of three sensors, all of which are managed by the same management system that correlates the information for all three sensors and, based on sophisticated algorithms, determines the physical location of the rogue AP. Typically the AP is displayed on a floor map within the IDS management software.

Bluetooth IPS

As Bluetooth is also a wireless technology and operates in the same frequency range as 802.11b and 802.11g, some wireless IPS products have been designed to detect Bluetooth. Why would you want to detect Bluetooth? Bluetooth can occasionally cause interference problems since it operates in a shared frequency range with Wi-Fi, but Bluetooth attacks have also occurred. The most common and arguably one of the most severe is the Bluetooth Rogue.

Bluetooth attacks have affected many organizations but most significantly retailers. Attackers have identified ways in which to hack point of sale systems and register keypads by inserting a Bluetooth radio. Either a malicious employee or fake technician opens the point of sale system or register keypad and attaches a Bluetooth broadcasting radio to the device. As credit cards are swiped, they're simultaneously broadcast to the neighboring airspace. If the attacker is nearby, either in the store or in the parking lot, he or she simply uses a Bluetooth device to listen and receive these credit card numbers.

All Bluetooth devices operate at the 2.4-GHz band and use 79 channels to hop (frequency hopping) from channel to channel, performing 1600 hops per second.

There are three classes of Bluetooth devices commonly differentiated by their range. Class 3 devices are the ones most of us are familiar with and usually include Bluetooth headsets. With a limited range of approximately 1 meter, they don't serve attackers well. Therefore, attackers commonly use Class 2 and Class 3 devices, which can be easily purchased online for under $20.

Class	Maximum Permitted Power		Range (approximate)
	mW	dBm	
Class 1	100	20	~100 meters
Class 2	2.5	4	~10 meters
Class 3	1	0	~1 meters

Some vendors have tuned their wireless IPS products to also detect Bluetooth, so administrators can detect the presence of these devices, especially in top-secret locations and on trading floors. Placement is a key consideration with Bluetooth detection owing to the relative strength of the communication range. If a wireless IPS sensor is out of range, it simply may not detect the Bluetooth device.

Wireless Network Positioning and Secure Gateways

The final point to be made about wireless network hardening is related to the position of the wireless network in the overall network design topology. Owing to the peculiarities of wireless networking, described earlier in this chapter in "Radio Frequency Security Basics," wireless networks should never be directly connected to the wired LAN. Instead, they must be treated as an insecure public network connection or, in the most lax security approach, as a DMZ. Plugging an access point directly into the LAN switch is asking for trouble (even though 802.1x authentication can alleviate the problem). A secure wireless gateway with stateful or proxy firewalling capability must separate the wireless network from the wired LAN.

The most common approach today is to have APs that can be connected anywhere on the LAN, but create an encrypted tunnel back to the controller and send all traffic through it before it hits the local network. The controller will run firewalling and IDS/IPS capabilities to check this traffic before it is exposed to the internal network. If the wireless network includes multiple access points across the area and roaming user access, the access points on the "wired side" must be put on the same VLAN, securely separated from the rest of the wired network. Higher-end specialized wireless gateways combine access point, firewalling, authentication, VPN concentrator, and user roaming support capabilities. The security of the gateway protecting your wireless network—even the security of the access point itself—should never be overlooked. The majority of security problems with wireless gateways, access points, and bridges stem from insecure device management implementations, including using telnet, TFTP, default SNMP community strings, and default passwords, as well as allowing gateway and access point remote administration from the wireless side of the network. Ensure that each device's security is properly audited and use wireless-specific IDS features in concert with more traditional intrusion-detection systems working above the data-link layer.

Summary

Wireless security is a multilayered time- and resource-consuming process, which is nevertheless essential because wireless networks are a highly prized target for attackers looking for anonymous, free Internet access and backchannel entry into otherwise securely separated networks. Wireless security encompasses wireless-specific security policy (many tips in this chapter are helpful in constructing one), radio frequency security, layer two–specific wireless protocol security issues and solutions, higher-layer VPN and device management security, and above all, correct wireless network design with security in mind.

References

Cache, Johnny, Joshua Wright, and Vincent Liu. *Hacking Exposed Wireless.* McGraw-Hill, 2010.

Chandra, Praphul. *Bulletproof Wireless Security: GSM, UMTS, 802.11, and Ad Hoc Security.* Newnes, 2005.

Holt, Alan, and Chi-Yu Huang. *802.11 Wireless Networks: Security and Analysis.* Springer, 2010.

National Institute of Standards and Technology. *NIST Special Publication SP 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.* NIST, 2007. http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

National Institute of Standards and Technology. *NIST Special Publication SP 800-48: Guide to Securing Legacy IEEE 802.11 Wireless Networks.* NIST, 2008. http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

National Institute of Standards and Technology. *NIST Special Publication SP 800-121: Guide to Bluetooth Security.* NIST, 2012. http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf

Wimmer, Christian. *Wireless LAN Security in a SOHO Environment: A Holistic Approach.* GRIN Verlag, 2012.