Chapter 2

Layer 1: The Physical Layer

Solutions in this chapter:

- Defending the Physical Layer
- Attacking the Physical Layer
- Physical Layer Security Project

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

The physical layer (layer 1) sits at the bottom of the Open Systems Interconnect (OSI) model, and is designed to transmit bit streams using electric signals, lights, or radio transmissions. For this chapter, the definition of the physical layer is expanded to include *all* physical things. True security means building *defense-in-depth*, which is used in this chapter to expand the OSI concept on a much broader scale. We begin by looking at some of the methods used to defend the physical environment, including common concepts such as lights, locks, and guards. Next, we examine the attacks on the physical layer, which are different from attacks on all of the other layers, therefore requiring different defensive techniques and skills. We believe that physical security should encompass the wiring used to connect systems as well as the system hardware, supporting services, employees, and any other physical assets.

Defending the Physical Layer

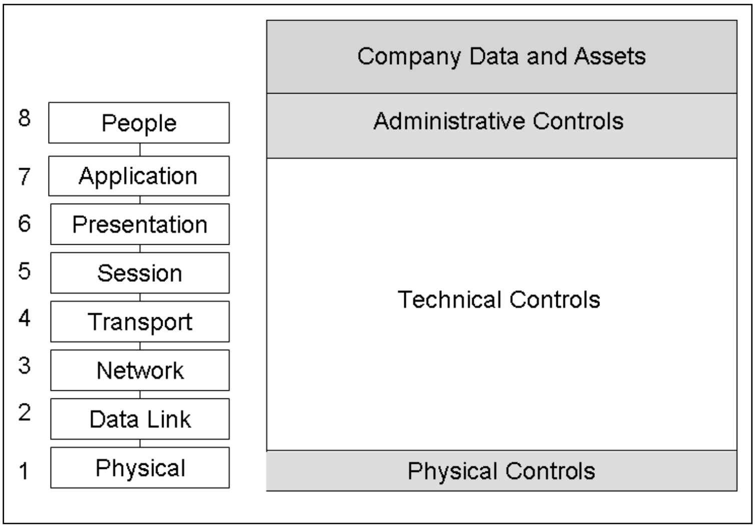
This section examines ways to defend the physical layer. Physical security is the point at which protection should begin. How much physical security you need depends on your situation, assets, and budget. These security controls have three primary goals:

- **Deter** Two methods used to deter intruders are *security lighting* and "Beware of Dog" signs.
- **Delay** Some of the techniques used to delay an intruder include fences, gates, locks, access controls, and mantraps.
- **Detect** Two systems used to detect intruders are intrusion detection systems (IDSes) and alarms.

Physical security (layer 1) should be viewed differently than the controls and vulnerabilities at higher layers. The higher layers deal primarily with security controls designed to prevent disclosure, denial, or alteration of information. Physical security focuses on intruders, vandals, and thieves. Physical security combined with technical security and administrative controls provides a holistic view of security, as seen in Figure 2.1.

Physical security is the oldest aspect of security. In ancient times, physical security was a primary concern of those with assets to protect. Consider the concept of castles, walls, and moats. While primitive, these controls were clearly designed to delay attackers. Physical security is a vital component of any overall security program.

Figure 2.1 Physical, Technical, and Administrative Controls



Design Security

Design security should begin during the design phase, not at the time of deployment. It is usually done when designing new code or applications; some organizations follow the System Design Life Cycle (SDLC) to build security in at every step of software design. This section discusses extending that concept to the physical realm. The physical security of assets and employees should be considered when designing a new facility; well-designed facilities are comfortable and secure.

Location is a key consideration. If you are offered a great deal on an office building in a bad part of town, do the high crime rate, employee security, and potential for loss or theft make it a viable option? Construction is another key issue (e.g., the increase of hurricanes that have hit Florida demonstrates that building substandard facilities can be devastating. Some facilities designed for category 5 hurricanes failed during category 3 storms). For the most part, construction is governed by local, state, and federal laws; however, there are still items that you should watch for. If you are moving into a preexisting facility, pay careful attention to what it was originally designed for (e.g., storage facilities have different requirements than clean rooms).

NOTE

In 1998, President Bill Clinton signed Presidential Decision Directive 63 (PDD-63), which provides the structure that key industries must follow when implementing security controls to prevent logical and physical attacks.

Accessibility is also important. Requirements will vary depending on your business and individual needs; however, roads, freeways, local traffic patterns, and convenience to regional airports should always be considered.

Climatology is another important issue. A building in San Francisco does not have the same weather concerns as a building in Anchorage. Events such as hurricanes, floods, snowstorms, dust storms, and tornados should be discussed and planned prior to the start of construction. Other items to consider when designing a facility include:

- **Transportation** Is the facility easy to get to? How is the traffic? Are there any airports or freight lines located in the vicinity?
- **Utilities** Is there access to more than one electric provider? Is a redundant T1 available?
- **Access Control** The design of the physical environment and the proper layout of access controls can increase security. The discipline known as Crime Prevention Through Environmental Design (CPTED) is built around this concept.

Perimeter Security

The first line in a defense-in-depth model is the perimeter, which prevents unauthorized individuals from gaining access to the facility. Even if someone does circumvent the first layer, additional layers deter, detect, and delay them, thereby preventing them from gaining access to critical assets. If building a new facility, you may be able to include many of these controls. If you are charged with protecting an existing facility, a risk assessment is required to determine how to increase current security. In both new and old facilities, the goal is to design security controls so that a breach of any one defensive layer does not compromise the physical security of the entire organization. Perimeter security controls can be physical barriers (e.g., a wall, a card-controlled entry, or a staffed reception desk). Perimeter security requires you to examine:

- Natural boundaries at the location
- Fences or walls around the site
- The design of the outer walls of a building
- Divisions and choke points within a building

To enhance the physical security of the perimeter and to physically and psychologically deter intruders, a series of mechanisms can be employed, including:

- Fences
- Perimeter Intrusion Detection and Assessment Systems (PIDAS)
- Security lighting

- Closed-circuit television (CCTV)
- Security guards and guard dogs
- Warning signs and notices

Fencing

Fencing is a key component of perimeter security. A fence with the proper design and height can delay an intruder and work as a psychological barrier.

NOTE

In 1969, security failed at the first Woodstock concert when eager concertgoers knocked down yards of poorly constructed hurricane fence, thus allowing thousands of people to enter the concert area without paying.

Before installing a fence, a risk analysis should be performed to evaluate the types of physical assets to be protected. A 4-foot fence will deter a casual trespasser, but an 8-foot fence will keep a determined intruder out. Adding three-strand barbwire to the top increases security even more.

Two more factors to consider are the gauge and mesh size of the wire. When considering a chain link fence, remember that the smaller the mesh, the more difficult it is to climb, and the heavier the gauge, the more difficult it is to cut. Table 2.1 details the security of various types of chain link fences. For more information on fences and their level of security go to the Chain Link Fence Manufacturers Institute at http://codewriters.com/asites/page.cfm?usr=clfma&pageid=887.

Table 2.1 Security of Chain Link Fence Types

Type	Security	Mesh	Gauge
A	Extremely High Security	3/8 inch	11 gauge
B	Very High Security	1 inch	9 gauge
C	High Security	1 inch	11 gauge
D	Greater Security	2 inch	6 gauge
E	Normal Fencing	2 inch	9 gauge

To take security to the next level, install a PIDAS, which has sensors that detect intruders and feel vibrations along the fence. The downside is that the system can produce false positives due to stray deer, high winds, or other natural events.

Gates, Guards, and Grounds Design

There are other items to consider when securing the perimeter. One is choosing the proper gate, which serves as the access point or open port. Gates act as choke points to control the flow of people and vehicles. UL Standard 325 details the requirements for gates, which are divided into the following four classifications:

- **Residential** Class 1
- **Commercial** Class 2
- **Industrial** Class 3
- **Restricted Access** Class 4

Another way to prevent vehicles from entering restricted areas is by using *bollards*. Bollards are made of concrete or steel and are used to block vehicular traffic or to protect areas where pedestrians are entering and leaving buildings. After the bombing of the federal building in Oklahoma City in November 1995, many government and commercial entities installed bollards to prevent vehicles from ramming buildings. Companies now make bollards with electronic sensors that notify building inhabitants if someone has rammed or breached the bollards. Bollards are the second line of defense, because they can deter individuals from ramming a facility with a motor vehicle.

Another way to secure the perimeter is using *security guards*. Some type of background check should be performed on these individuals. At a minimum, security guard applicants should have job references and be subject to a background check. Failure to do so could place a company in legal jeopardy. There are many background screening services, Web site operations, and private investigators that perform these services

Damage & Defense…

Never-Ending Background Checks

New companies such as Verified Person, now offer continuous employment checks, meaning an employer can monitor an employee 24 hours a day, seven days a week.

Employers can monitor employees for everything from major felonies to simple misdemeanors. Depending on the state where you live, an employer might have the right to fire an employee based on that information.

While the idea of continuous computerized background checks upsets privacy rights advocates, federal law offers little protection. Employers are allowed

Continued

to gather such information and use it without advance notification. While this provides employers with added protection, it is not a perfect system and sometimes honest mistakes can lead to immediate termination.

Increased technology also drives the need for security guards. As a company acquires more control equipment, IDSes, and computerized devices, additional guards are required to control the infrastructure. Security guards are trained to use their judgment when deciding how to handle specific situations. The presence of a security guard also provides a visual deterrence. Guards also monitor, greet, sign in, and escort visitors.

Dogs are another potential choice for perimeter security. Breeds such as German Shepherds and Chows have been used for centuries to guard facilities and assets. While they can be trained to be loyal, obedient, and steadfast, they can also be unpredictable. Because of these factors, dogs are usually restricted to exterior control and should be used with caution.

Lighting is another important form of perimeter protection, because it discourages criminals. Most lighting problems occur from overuse. Effective lighting is designed to send light where needed, and in the proper wattage. Most standards list two candlefoot power as the norm for facilities using nighttime security. Too much light causes over-lighting and glare, which creates pockets of extremely dark areas just outside the range of the light. This may result in reduced security. Overly bright lights can also "bleed" over to the adjacent property. Properly designed lights are pointed away from a facility and focused on exterior fences, gates, and other potential access points (e.g., when entering a military post at night, the lights are pointed toward oncoming traffic, away from the guards, which provides good glare protection.

Another perimeter security control is *CCTV*. The British government has installed more than 1.5 million CCTV cameras. It is estimated that the average Londoner's picture is recorded more than three hundred times a day. If anything, this proves that there is an increased reliance on using CCTV for surveillance and security. They can be effective in the business world when used at perimeter entrances and critical access points. Activity can be monitored live by a security officer or recorded and reviewed later.

And, finally, *warning signs* or *notices* should be posted to deter trespassing. A final review of the grounds should be conducted to make sure that nothing was missed (e.g., any opening that is 96 square inches or larger within 18 feet of the ground such as manholes and tunnels, gates leading to the basement, elevator shafts, ventilation openings, and skylights). The roof, basement, and walls of a building may contain vulnerable points of potential entry, and should therefore be assessed.

Facility Security

"Security starts at the front door." Anyone with physical access has the means and the opportunity to commit a crime. This is why it's imperative to practice the principle of *least privilege*, which means providing only the minimum amount of access that is required, and restricting non-authorized individuals from entering sensitive areas. Some of the ways that these goals can be achieved is by examining:

- Windows
- Doors
- Walls
- Locks
- Access control
- Intrusion detection

Entry Points

The weakest point of security is usually the first to be attacked (e.g., doors, windows, roof access, fire escapes, delivery access, and chimneys). Criminals target what is perceived as the weakest point; therefore, all potential points must be examined.

A *doors'* function determines its construction, appearance, and operation. A door designed for security purposes is very solid and durable, with hardened hardware. While most interior doors are made of hollow-core wood, exterior doors should be made of solid-core wood; therefore, a risk assessment must be performed on interior applications. Doors also have a fire rating system, and come in various configurations, including:

- Personal doors
- Industrial doors
- Vehicle access doors
- Bulletproof doors
- Vault doors

The hardware used to install a door must also be examined. The front door of a house is usually hinged on the inside, which is a simple safety feature that makes it harder for a thief to gain access. However, if a door is hinged on the outside, a criminal can easily remove the hinge pins and walk in. Hinges and strike plates must be secure.

Not all doors are hinged inside. Businesses typically have doors with hinges on the outside as a safety feature (i.e., Exit doors open out). This safety feature exists so that people do not get trapped inside a building. These doors are also more expensive, because they are harder to install. Special care must be taken to protect the hinges so that they cannot be easily removed. Most are installed with a panic bar, which helps when large crowds rush the door.

Sometimes one door at a critical access point is not enough. Even with access control, if one person opens a door, twenty people will stream in. To correct this problem, install a *man trap*, which is designed so that when the outer door opens, the inner door locks. This means that a person must step in and close the outer door before the inner door is unlocked.

The final consideration regarding doors is automatic door locks, where you have to use some type of access control key or card to enter and exit a building. If you use these systems, find out if the locks are *fail-safe* or *fail-secure* (i.e., the state the locks are in) case of a power loss. A fail-safe (*unlocked*) state allows employees to exit, but also allows other unauthenticated access. A fail-secure configuration is when the doors default to being locked, thereby keeping unauthorized individuals out while also preventing access.

Windows work well letting light in, and do not have to meet certain security requirements. Whether interior or exterior, windows must be fixed in place and shatterproof. Depending on placement, the windows should be either opaque or translucent. Alarms or sensors may also be needed. Window types include the following:

- **Standard** This is the lowest level of protection. It is also the least expensive, but is easily shattered.
- **Polycarbonate Acrylic** Much stronger than standard glass, this type of plastic offers superior protection.
- **Wire Reinforced** A wire-reinforced window adds shatterproof protection, thereby making it harder for an intruder to break.
- **Laminated** These windows are similar to those used in automobiles. Adding a laminate between layers of glass strengthens the glass and decreases the potential for shattering.
- **Solar Film** These windows provide a moderate level of security and decreases the potential for shattering.
- **Security Film** This type of transparent film is used to increase the strength of the glass in case of breakage or explosion.

Walls are another consideration. A reinforced wall can keep a determined attacker from entering an area, if he or she is unable to use the doors. Walls should be designed with firewalls, and emergency lighting should be in place.

Damage & Defense…

The Value of Physical Security

Rick Rescorla was director of security for Morgan Stanley, which was located in the South World Trade Center Tower. Rick felt strongly about the need for physical security to protect employees and company assets; however, it was difficult convincing management of the need for greater security. The World Trade Center bombings served as a wake up call, and Rick received additional funds for more drills, better evacuation lighting, and increased security.

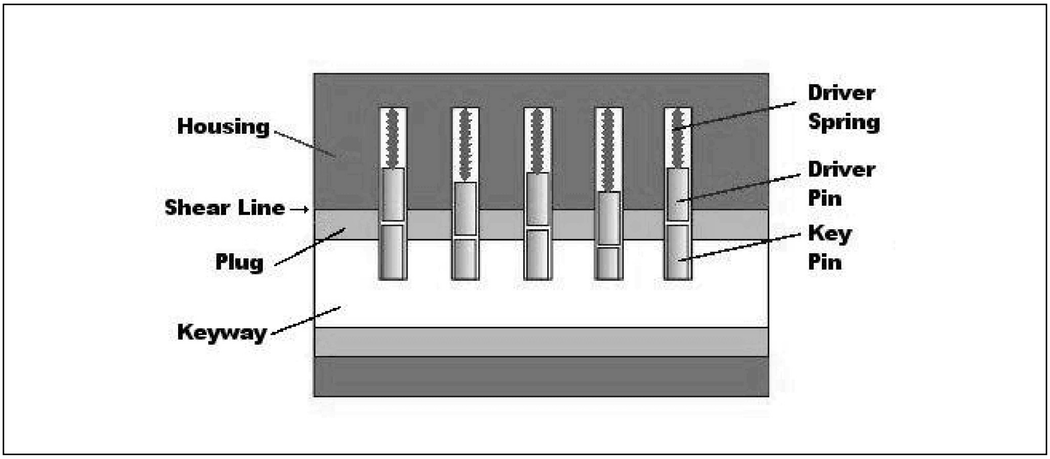
Access Control

Access control is any mechanism by which an individual is granted or denied access. One of the oldest forms of access control are *mechanical locks*. New access controls include identity card technology, which include computerized technology that extends the benefits of automated access control to employee parking lots, facilities, entrances, and restricted areas.

Locks

Mechanical locks are one of the most effective and widely used forms of access control. Locks come in many types, sizes, and shapes and are one of the oldest forms of theft deterrent mechanisms. Attempts to improve lock design resulted in *warded locks* and *tumbler locks*. Warded locks work by matching wards to keys, and are the cheapest mechanical lock and the easiest to pick. *Tumbler locks* contain more parts and are harder to pick. An example of a tumbler lock is seen in Figure 2.2. This diagram appears the following Web page: www.hacknot.info/hacknot/action/showEntry?eid=80.

Figure 2.2 Cross Section of a Pin Tumbler Lock



Source: www.hacknot.info, 2005. Image used under permission of the Creative Commons Public License (CCPL).

The tumbler lock was patented by Linus Yale in 1848. When the right key is inserted into the cylinder of a tumbler lock, the pins lift to the right height so that the device can open or close. The correct key has the proper number of notches and raised areas that allow the pins to be put into the proper position. The pins are spring loaded so that when the key is removed, the pins return to the locked position. Another type of tumbler lock is the *tubular lock*, which is used for computers, vending machines, and other high-security devices.

Locks are divided into different categories and are differentiated by grade. The grade of a lock specifies its level of construction. The three basic grades of locks include:

- **Grade 3** The weakest commercial lock
- **Grade 2** Light duty commercial locks or heavy duty residential locks
- **Grade 1** Commercial locks of the highest security

American National Standards Institute (ANSI) standards define the strength and durability of locks (e.g., grade 3 locks are designed to function for 200,000 cycles, grade 2 locks are designed to function for 400,000 cycles, and grade 1 locks are designed to function for 800,000 cycles). It's important to select the appropriate lock in order to obtain the required level of security; different types of locks provide different levels of protection.

Physical Controls

A range of *physical controls* can be implemented to help increase security. These controls are put in place to ensure that only authorized individuals can access certain areas or perform specific actions. Network cabling security should be considered when initially setting up wiring closets and whenever upgrades are performed. Cabling should be routed through the facility so that it cannot be tampered with. Unused network drops should be disabled and all cable access points should be secured, so that individuals cannot install sniffers or eavesdrop on network communications.

Another important concern is controlling individuals as they move throughout a facility. Most organizations use card keys, badges, smart cards, or other IDs to control the flow of traffic. This category can be divided into two broad groups.

The first category is ID cards, which do not contain electronics and are very low tech. ID cards typically contain a photograph of an individual to verify their identity, and are used in many organizations.

The second category is *intelligent access control devices* that make access decisions electronically. There are two subcategories of these devices: *contact* and *contactless*. Contact access cards require users to slide their card through a reader. These cards come in several different configurations, including:

- **Active Electronic** Can transmit electronic data
- **Electronic Circuit** Has an electronic circuit embedded
- **Magnetic Stripe** Has a magnetic stripe
- **Magnetic Strip** Contains rows of copper strips
- **Optical-coded** Contains laser-burned pattern of encoded dots

Contactless cards function by proximity (e.g., radio frequency ID [RFID]). An RFID is a small electronic device comprised of a microchip and an antenna. An RFID tag can be designed as an *active device* (i.e., a battery or power source is used to power the microchip) or as a *passive device*. Passive devices have no battery; they are powered by a RFID reader. The reader generates an electromagnetic wave that induces a current in the RFID tag. There are also *semi-passive devices* that use batteries to power the microchip, but transmit using the energy from the card reader. When users are allowed into specific areas of a facility, it does not mean that they should have access to all of the systems located there. That's why strong system access controls are so important. Complex passwords or biometric systems can help, as well as multi-factor authentication (e.g., ATM bank cards). Banks require you to have an ATM card and a pin number in order to access funds or account information.

Even with these physical controls in place, misuse and intrusions can still occur; therefore, it is important to use IDSes. Physical intrusion detection includes the components and systems installed to detect misuse or unauthorized intrusion. Physical IDSes are designed around one or more sensor types. Motion detectors can be triggered from audio, infrared wave pattern, or capacitance. These detectors use passive infrared and are usually mounted in the corners of rooms or used as security lights. Motion detectors send out a series of infrared beams that cover an area with protection.

Other types of sensors used with IDSes include *photoelectric sensors* and *pressure-sensitive devices*. Pressure sensitive devices are sensitive to weight. They measure changes in resistance to trigger alerts, and are good for protecting small areas. *Glass breakage sensors* are another component of IDSes. If someone breaks a window or attempts to pry it open, the sensor triggers an alarm.

IDSes are another piece of total security control. The idea is to place them in key areas that contain critical assets or in areas most likely to be violated by intruders. IDSes are not perfect and produce their own share of false positives. Every time an alarm goes off, someone must respond and verify the event. If an IDS is tied to a police department or fire department, false alarms can result in some hefty fines.

TIP

Always be involved in deciding where IDS sensors are placed, and have someone on site when the installers arrive. Sometimes, installers try to place sensors in easily attainable areas instead of the most secure area.

Device Security

Device security addresses the controls implemented to secure devices found in an organization (e.g., computers, networking equipment, portable devices, cameras, iPods, and thumb drives). Computer systems and networking equipment are usually protected with some type of identification and authentication system.

Identification and Authentication

Identification is the process of identifying yourself, and is commonly performed by entering a username. *Authentication* is the process of proving your identity. Various authentication schemes have been developed over the years and can be divided into three broad categories:

- **Something You Know** Passwords
- **Something You Have** Tokens, smart cards, and certificates
- **Something You Are** Biometrics

WARNING

A survey performed at a security conference in Europe found that 71 percent of those polled would give up their password for a piece of chocolate. However, most stated that they would not give their password to someone calling on the phone, and over half said they would give their password to their boss. For more on this story go to www.securitypipeline.com/news/18902074.

Passwords are the most commonly used authentication schemes. For password-based authentication to be effective, passwords cannot be shared. Passwords are problematic: do you invent hard-to-remember complex passwords or ones that can be easily remembered? Most individuals choose easy passwords rather than risk forgetting their password. A Gartner study performed in 2000, reported the following facts about passwords:

- 90 percent of respondents use dictionary words or names
- 47 percent use their name, the name of a spouse, or a pet's name
- 9 percent used cryptographically strong passwords

A good password policy contains the following components:

- Passwords should not use personal information
- Passwords should be eight or more characters
- Passwords should be changed regularly
- Passwords should never be comprised of common words or names
- Passwords should be complex, use upper- and lower-case letters, and miscellaneous characters (e.g., !, @, #, $, %, ^, &)
- Limit logon attempts to three successive attempts

Another authentication method uses tokens, smart cards, and magnetic strip cards (e.g., ATM cards). Many token devices are one-time passwords (i.e., the device generates authentication credentials only once). Tokens are divided into two basic groups. The first type is a *synchronous token*, which is synchronized to an authentication server. Each individual passcode is only valid for a short period of time. After a small window of opportunity, the passcode is useless.

The second type of token authentication is *asynchronous challenge-response*, which uses a challenge-response mechanism. These devices work as follows:

1. The server sends the user a value.
2. The value is entered into the token.
3. The token performs a hashing process on the entered value.
4. The new value is displayed on the Liquid Crystal Display (LCD) screen of the token device.
5. The user enters the displayed value into the computer for authentication.

The third category of authentication is *biometrics*, which is based on behavioral or physiological characteristics unique to an individual. Biometric authentication systems have gained market share and are seen as a potential substitute for password-based authentication systems. However, they are more expensive and not as widely accepted by the general public. Opposition is generally focused around religious and cultural reasons, but some are also concerned that their biometric data might be sold.

Biometric systems have made a lot of progress in the last decade. There are many different types of biometric systems, including iris scan, voice recognition, fingerprint, and signature dynamics; however, they all basically work the same way.

1. **User Enrolls in the System** The user allows the system to take one or more samples for later comparison.
2. **User Requests to be Authenticated** A sample is compared with the user's authentication request.
3. **A Decision is Reached** A match allows access, and a discrepancy denies access.

The accuracy of a biometric device is measured by the percentage of Type 1 and Type 2 errors it produces. Type 1 errors (False Rejection Rate [FRR]) measure the percentage of individuals who should have received access, but were denied. Type 2 errors (False Acceptance Rate [FAR]) measure the percentage of individuals who gained access that shouldn't have. When these two values are combined, the accuracy of the system is established. The point at which the FRR and FAR meet is known as the Crossover Error Rate (CER). The CER is a key accuracy factor: the lower the CER, the more accurate the system. Another attribute of biometric systems is that fingerprints, retinas, or hands cannot be loaned to anyone. Some common biometric systems include:

- **Finger Scan Systems** Widely used, popular, installed in many new laptops
- **Hand Geometry Systems** Accepted by most users; functions by measuring the unique geometry of a user's fingers and hand to identify them
- **Palm Scan Systems** Much like the hand geometry system except it measures the creases and ridges of a palm for identification
- **Retina Pattern Systems** Very accurate; examines the user's retina pattern
- **Iris Recognition** Another accurate eye recognition system, which matches the user's blood vessels on the back of the eye
- **Voice Recognition** Determines who you are using voice analysis
- **Keyboard Dynamics** Analyzes the user's speed and pattern of typing

The final consideration for any biometric system is user acceptance and usability. The acceptability of a system depends on how the user perceives it. User education is helpful, because many individuals worry that retina or iris systems can damage their eyes, or that their information is not adequately protected. To ensure that a biometric system is usable, the processing time and environment must be examined. Make sure that physically challenged employees can easily use the Iris scanners installed at all employee entrances.

Computer Controls

Computer controls are another component of physical access security that can be implemented. While it's not easy to prevent a malicious employee from looking over your shoulder, there are some controls that can be installed to prevent individuals from accessing unauthorized systems. One potential tool is *session controls*.

Session controls are automatic features used to limit the amount of time a user is logged on. Session controls can be used to limit logon times and prevent intruders from accessing a system, and they also reduce the opportunity for unauthorized local access. *System timeouts* automate the logoff process, where users are automatically logged off after a preconfigured period of inactivity. This is a good control for employees that forget to logout. Another session control is a *screensaver lockout*. This mechanism activates a password-protected screensaver after a short period of inactivity.

Finally, there are *warning banners*, which identify acceptable and unacceptable use, and are used to inform would-be intruders that they are being monitored. Legal cases exist in which defendants were acquitted of charges of tampering with computer systems, because no explicit notice was given prohibiting unauthorized use of those computer systems. For more information regarding warning banners go to www.cert.org.

Mobile Devices and Media

Mobile devices and media are also a concern. In most workplaces, there is an array of iPods, Universal Serial Bus (USB) thumb drives, portable hard drives, cell phones with cameras, and

CD/DVD burners being used. Most of these devices have the ability to quickly move vast amounts of information into and out an organization. Connecting these devices to a network can introduce malicious code. The shear number of small portable devices should raise concern. Samsung Corporation banned employees from using Samsung's latest cell phones—which are tiny and have 8GB of storage—because senior management believes that a malicious insider could use one to steal a large amount of confidential information. It is important to establish policies that address all types of media and that enforce management's decisions.

Damage & Defense…

Dumpster Diving

Potential threats to physical security can come from all angles. Even discarded media can be a vulnerability. Sifting through an organization's trash is known as *dumpster diving*, and is a common practice used by hackers and others looking to obtain useful information and items. Dumpster diving can reveal user names, passwords, account numbers, and enough information for identity theft. The best way to prevent this kind of information leak is by using a paper shredder. There are two types of shredders: *strip-cut* and *cross-cut*:

Strip-cut Shredders Strip-cut shredders shred paper into long, thin strips, and generally handle a high volume of paper with low maintenance requirements. Even though the shred size varies from 1/8- to 1/2-inch, strip-cut shredders don't compress well, and shredded documents can be easily reassembled.

Cross-cut Shredders Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces, which makes the shredded document much more difficult to reconstruct. Smaller cross-cut, greater maximum page count shredders generally cost more.

Media controls dictate how floppy disks, CDs, DVDs, hard drives, portable storage, paper documents, and other forms of media are handled throughout their lifecycle. Sensitive media must be controlled, handled, and destroyed in an approved manner. Above all, an organization must decide what devices employees can bring in or install on their desktops (e.g., portable drives, CD burners, cameras, and other devices). Management must also dictate how approved forms of storage are handled, which is where an *information classification system* comes in. Media can be disposed of in many acceptable ways. Paper documents can be shredded, CDs can be destroyed, magnetic media can be degaussed, and hard drives can be wiped (the process of overwriting all addressable locations on a disk). Standard 5220-22M was developed by the Department of Defense (DOD) and states, "All addressable locations must be overwritten with a character, its complement, then a random character and verify." Making several passes over media can further decrease the possibility of data recovery.

As mentioned in the preceding section, a key component of effective media control is an information classification system. Two widely used classification systems are:

- **Government Information Classification System** Focuses on secrecy
- **Commercial Information Classification System** Focuses on integrity

The government information classification system is concerned with protecting the confidentiality of information. Therefore, it is divided into four categories: *Unclassified*, *Confidential*, *Secret*, and *Top Secret*, as seen in Table 2.2.

Table 2.2 Government Information Classification

Classification	Description
Top Secret	Would cause grave damage to national security; requires the highest level of control.
Secret	Would be expected to cause serious damage to national security; may divulge significant scientific or technological developments.
Confidential	Could cause damage to national security; should be safeguarded against disclosure.
Unclassified	Not sensitive and does not need to be protected; its loss or disclosure would not cause damage.

The commercial information classification system is concerned with the integrity of the information; therefore, it is categorized as *Public*, *Sensitive*, *Private*, and *Confidential*, as seen in Table 2.3

Table 2.3 Commercial Information Classification

Classification	Description
Confidential	The most sensitive rating. This information keeps companies competitive. This information is for internal use only; its release or alteration could seriously affect or damage a corporation.
Private	This category includes restricted personal information (e.g., medical records or human resource information).
Sensitive	This information requires controls to prevent its release to unauthorized parties. Damage could result from its loss of confidentiality or its loss of integrity.
Public	Its disclosure or release would not cause damage to a corporation.

It's important to establish guidelines to help organize and categorize sensitive information. Doing so also demonstrates an organization's commitment to security.

Communications Security

Communication security deals with the controls that can be implemented to prevent attackers from physically accessing any part of a telecommunications infrastructure. Communications security requires you to examine the types of communication systems you use and the signals that emanate from these systems. Communications security has been a longstanding concern. In the 1960s, the US government began studying electronic devices and the electromagnetic radiation (EMR) they produced. The original controls for these vulnerabilities were named Tempest, which have now been changed to Emissions Security (Emsec). The controls to limit EMR have also been updated. Newer technologies that have replaced simple shielding are *white noise* and *control zones*. White noise uses special devices that send out a stream of frequencies that make it impossible for an attacker to distinguish the real information. Control zones is the practice of designing facilities (e.g., walls, floors, and ceilings) to block electrical signals from leaving the zone.

Telecommunications systems may be prime targets because they are not usually run by security professionals and may not be as secure as a network infrastructure. The target of this type of attack is the Private Branch Exchange (PBX). If hacked, it is possible for an attacker to make anonymous and/or free phone calls. To secure this portion of the communication infrastructure, default passwords must be changed regularly and remote maintenance must be restricted.

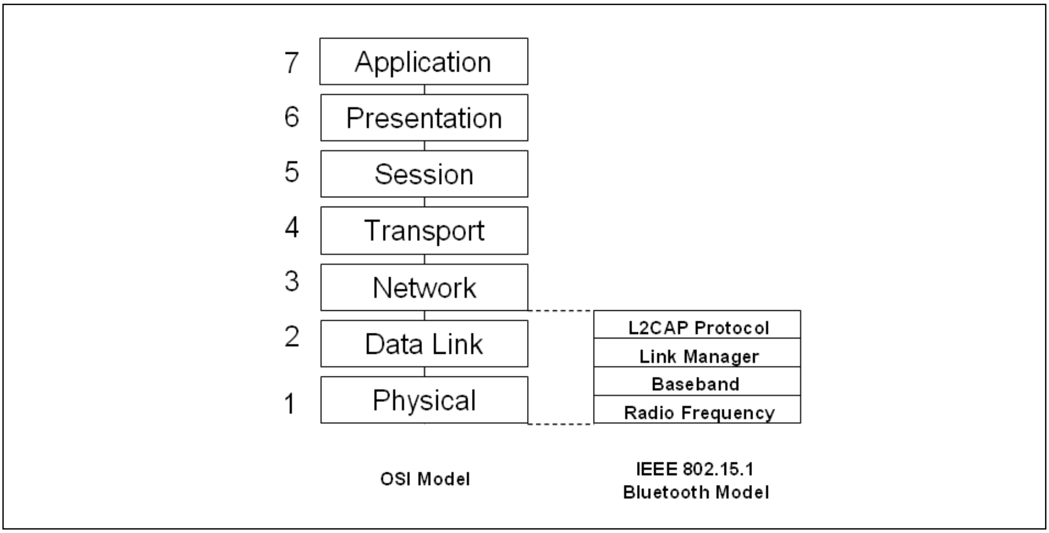
Fax machines are another potential problem, because fax transmissions can potentially be sniffed and decoded while being transmitted. Once a fax arrives at its destination, it may sit in a tray where anyone can retrieve it and review its contents. Cheap fax machines use ribbons; therefore, anyone with access to the trash can retrieve the ribbons and use them as a virtual carbon copy of the original document. The protection of fax transmissions begins with policies that restrict their use to *non-confidential information*. Another potential control is to use a fax server, which sends and receive faxes. Upon receipt, a fax server holds the fax in its electronic memory and notifies the recipient. Upon request, the fax is forwarded to an e-mail account or printed out. Fax encryption can also be used to increase security, by giving fax machines the ability to encrypt communications. To make this system even more robust, activity logs and exception reports should be collected to monitor for potential security problems.

Bluetooth

Bluetooth was developed as the standard for small, cheap, short-range wireless communication. It was envisioned to allow for the growth of wireless personal area networks (PANs), which allow a variety of personal and handheld electronic devices to communicate. Standard 802.15.1 is an Institute of Electrical & Electronics Engineers (IEEE) standard that deals with

Bluetooth and PANs. Portions of the Bluetooth protocol suite reside at the physical layer of the OSI model, as seen in Figure 2.3.

Figure 2.3 Relationship of Bluetooth to the OSI Model



There are three categories of Bluetooth devices:

- **Class 1** Allows for transmission of up to 100 meters and has 100mW of power
- **Class 2** Allows for transmission of up to 20 meters and has 2.5mW of power
- **Class 3** Allows for transmission of up to 10 meters and has 1mW of power; also the widest deployment base

Bluetooth operates at a frequency of 2.45 GHz and divides the bandwidth into narrow channels to avoid interference with other devices utilizing the same frequency. To keep it secure, make sure Bluetooth-enabled devices are set to non-discoverable mode. Because Bluetooth can be monitored by third parties, use secure applications that limit the amount of cleartext transmissions. Practice a "deny all" methodology, meaning if you don't need Bluetooth functionality in a device, turn it off. This is important because Bluetooth-enabled devices can be configured to access shared directories without authentication, which would open it up to viruses, Trojans, and information theft.

NOTE

In 2005, AirDefense released BlueWatch, which was the first commercial security tool designed to monitor Bluetooth devices and identify insecure devices. More information can be found at www.airdefense.net/products/bluewatch/index.php.

802.11 Wireless Protocols

In 1997, the 802.11 family of specifications was developed by the IEEE for wireless local area network (WLAN) technology. WLANs are data communication systems that were developed to transmit data over electromagnetic waves. WLANs are popular because they're convenient and there are no cable plant costs (i.e., a business can move into a new or existing facility without cabling, and incur none of the usual costs of installing cable. Unfortunately, a wireless network can be more insecure than a wired network.

Wireless systems can operate in one of two modes: *ad-hoc* and *infrastructure*. Ad-hoc mode is a simple point-to-point type of communication that's only designed for a few users. Infrastructure mode uses a wireless access point (wireless AP) and is regularly used in corporate environments. A wireless AP is a centralized wireless device that controls traffic in a wireless network. Wireless APs use a Service Set ID (SSID), which distinguishes one wireless network from another and can sometimes provide a minuscule amount of security. WLAN standards have evolved over time, and the most common are shown in Table 2.4.

Table 2.4 Commercial Information Classification

Standard	Speed	Frequencies
802.11b	11 Mbps	2.4000 to 2.2835GHz
802.11a	54 Mbps	5.725 to 5.825GHz
802.11g	54 Mbps	2.4000 to 2.2835GHz
802.11n	540 Mbps	2.4000 to 2.2835GHz

WLANs were designed with basic security features. One such feature is *spread-spectrum* technology, which was originally used for military communications in World War II. It gained popularity because it is resistant to jamming and hard to intercept. Spread-spectrum transmits data over a wide range of radio frequencies. It also allows data rates to speed up or slow down, depending on the quality of the signal. There are two types of spread spectrum technology: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

- **DSSS** This method of transmission divides the stream of information being transmitted into small bits. These bits of data are mapped to a pattern of ratios called a *spreading code*. The higher the spreading code, the more the signal is resistant to interference, and the less bandwidth is available. The transmitter and the receiver must be synchronized to the same spreading code.
- **FHSS** This method of transmission operates by taking a broad slice of the bandwidth spectrum and dividing it into smaller subchannels of approximately 1 MHz. The transmitter then hops between subchannels sending out short bursts of data on each subchannel for a short period of time. This is known as the *dwell time*. For

FHSS to work, all communicating devices must know the dwell time and must use the same hopping pattern. Because FHSS uses more subchannels than DHSS, it supports more wireless devices.

Another protection originally built into WLANs was the Wired Equivalent Privacy (WEP) protocol, which designed to provide the same privacy that a user would have on a wired network. WEP is based on the RC4 symmetric encryption standard. Because of weaknesses in WEP, the wireless industry developed a replacement called WiFi Protected Access (WPA). WPA delivers a more robust level of security and uses Temporal Key Integrity Protocol (TKIP). TKIP scrambles encryption keys using a hashing algorithm, and it adds an integrity-checking feature that verifies that the encryption keys haven't been tampered with. WPA improves on WEP by increasing the initialization vector from 24 bits to 48 bits. In 2004, the IEEE approved the next upgrade to wireless security, which was 802.11i, or WPA2. The 802.11.i standard uses the Advanced Encryption Standard (AES). Key sizes of up to 256 bits are now available, which is a vast improvement over the original 40-bit encryption WEP used. Other options for securing WLANs require building layers of security. Below are some examples that can help make a WLAN more secure:

- Retire WEP devices
- Change the default value of the SSID
- Perform Mandatory Access Control (MAC) filtering
- Turn off Dynamic Host Configuration Protocol (DHCP)
- Limit the access of wireless users
- Use port authentication (802.1x)
- Perform periodic site surveys and scan for rogue devices
- Update policies to stipulate the requirements for wireless users
- Use encryption
- Implement a second layer of authentication such as Remote Authentication Dial-In User Server (RADIUS)

Let's turn our attention to some of the vulnerabilities found at the physical layer and discover how hackers can leverage these potential holes to attack physical security.

Attacking the Physical Layer

The most important aspect of physical security is control. If an attacker gains physical control of a device, it usually means it can be leveraged to control a device's behavior. This is what makes physical security such an important piece of overall security. There are many angles that physical security can be attacked from (e.g., stealing data, lock picking, wiretapping, and scanning, hardware modification). Each angle offers a potential to gain access or understand how a security control works. Once an attacker can map the security control, he or she is in a better position to bypass it. Most of the tools needed to perform these attacks can be purchased online or in brick and mortar stores.

Stealing Data

Stealing data is one of the easiest attacks for a malicious insider to attempt, probably because they already have access to the system. Data theft and business espionage are on the rise, and businesses feel the need to be more competitive. State-sponsored industries can also benefit from insider information and trade secrets. These types of attacks have become easier as advancements in electronics and optoelectronics have made spying, interception, and information theft harder to detect. These tools typically require physical access.

Rogue employees and corporate spies are not the only people that perform this type of activity; big companies have also been caught in the act. Sony began using covert data collection tools in 2004. What initially appeared to be an honest attempt to build in copy protection, ended up being much more. The company was using a copy protection scheme devised by a company called First 4 Internet. Once a music CD with this copy protection was physically loaded, there was no way to uninstall it. Instead, it was installed on a type of rootkit that collected data from users about the songs they listened to and the CDs they played, and then secretly reported that information back to Sony. Only after a huge outcry was Sony forced to end the practice.

NOTE

The Economic Espionage Act of 1996 was signed into law by President Clinton. It makes the theft or misappropriation of trade secrets a criminal offense. It is unique in that it is the first federal law to broadly define and severely punish such misappropriation and theft.

Data Slurping

An insider can easily steal data using nothing more than an iPod. The security issue with iPods and similar devices is the amount of data they can hold. All a user has to do is plug it into a desktop system, search for the needed files, and copy them to the portable music device. Abe Usher has written a new program called *pod slurp*, which is designed to be used with an iPod. While this software is only a proof of concept, it should serve as a wakeup call for anyone not yet concerned about the potential threat of these devices.

The program is designed to systematically search through the *C:\Documents and Settings* folder and recursively search all subfolders and copy all document files. Thus, an insider could move between a few dozen workstations and collect over 20,000 files in less than an hour. For more information go to www.sharp-ideas.net/downloads.php. The downloadable version of this tool only works when a valid logon has been performed. It copies a list of the file names but not the actual files.

WARNING

Cleaning crews are often overlooked as being security threats even though they work at night, typically alone, and have full access to the facility. Unlocked computers are a tempting and easy target.

Portable USB drives pose another big problem. Many new USB drives, such as the Sandisk U3 USB drives, are designed to make program installation easier. These devices are recognized as CD-ROM drives and can execute *autorun*. While autorun capabilities are normally restricted to CD-ROMs and fixed disks, these portable storage devices toggle from 1 to 0 during the initial inquire that occurs between the computer and the USB device to indicate that the device is non-removable. To learn more about USB device functions, review Microsoft's USB FAQ located at www.microsoft.com/whdc/device/storage/usbfaq.mspx.

autorun requires very little work:

1. Create a file called *autorun.inf* in the root of the USB drive.
2. Open the *autorun.inf* file in notepad and write the script

```
[AutoRun]
Open=Launch-logger.exe
Icon=HarmlessLookingIcon.ico
```

To keep things interesting, load other non-descript files and photos onto the drive so that the intended targets are kept occupied. Next, take several USB drives and scatter them in the employee parking lot or the smoking area of the targeted business. This technique is used during penetration tests to gain insider access to files and systems. To learn more about penetration tests go to www.securityfocus.com/news/11397. The best defense for these types of attacks is to disable autorun.

Lock Picks

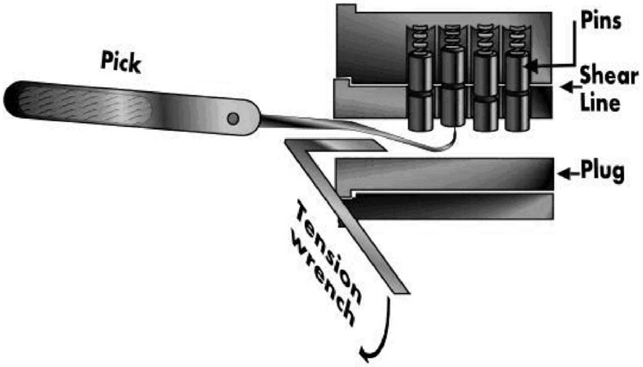
Lock picking is one way to bypass a lock, but is not the fastest way. Burglars will typically break a window, pry a doorframe, or knock a hole in a sheetrock wall before they will pick a lock. If you don't think lock picking is a hacker skill, check out DefCon, which is a yearly hacker conference that has presentations and seminars devoted to lock picking. To see how quickly some individuals can bypass a lock, check out the videos located at www.digital-trash.org/defcon/.

Most lock picking is self-taught. Lock picking is the manipulation of a lock's components in order to open a door without a key. The basic components used together to pick locks are:

- **Tension Wrenches** Small, angled flathead screwdrivers that come in various thicknesses and sizes
- **Picks** Small, angled, and pointed, similar to a dentist pick.

One of the easiest techniques of lock picking is called *scrubbing*, as shown in Figure 2.4. Scrubbing occurs when tension is held on a lock with a tension wrench while the pins are quickly scraped. Some of the pins are placed in a mechanical bind and stuck in the unlocked position. With practice, this can be done quickly.

Figure 2.4 Common Lock-Picking Techniques



Source: Answers.com (www.answers.com/topic/pin-and-tumbler-lock-picking-png), 2006. Drawn by Theresa Knott. Image used under permission of the CCPL.

There are a host of tools in the lock picks arsenal, including the following:

- **Lock Pick Sets** Lock pick sets contain a variety of picks and tension wrenches, which vary in price and design.
- **Electric Lock Pick Guns** These devices attempt to speed up manual lock picking by working like an electric toothbrush or an electric knife. These devices take the shotgun approach to lock picking.
- **Jackknife** Much like a lock pick set, these small folding lock picks house several lock pick tools in a knife-like handle.

- **Tubular Picks** These are designed to pick Ace locks, which are the same locks used on Kryptonite bicycle locks. They were thought to be highly secure until 2004, when someone opened one with a Bic pen.
- **Lock Shims** Formed pieces of thin stiff metal that can be inserted into the latch of padlock.

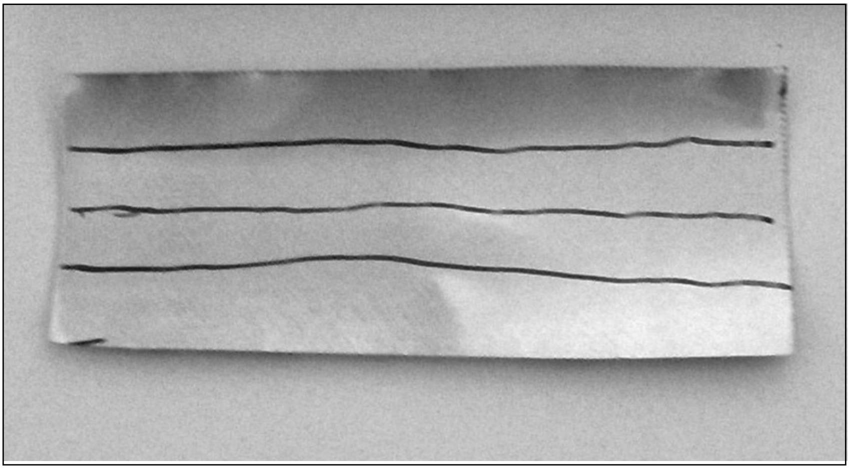
Lock shims are easy to make and work well at opening common padlocks. The design used here is credited to Deviant Ollam. To complete this project, you need the items shown in Table 2.5.

Table 2.5 Lock Shim Supply List

Item
Aluminum can
Scissors
Marker
Pen
Pad lock

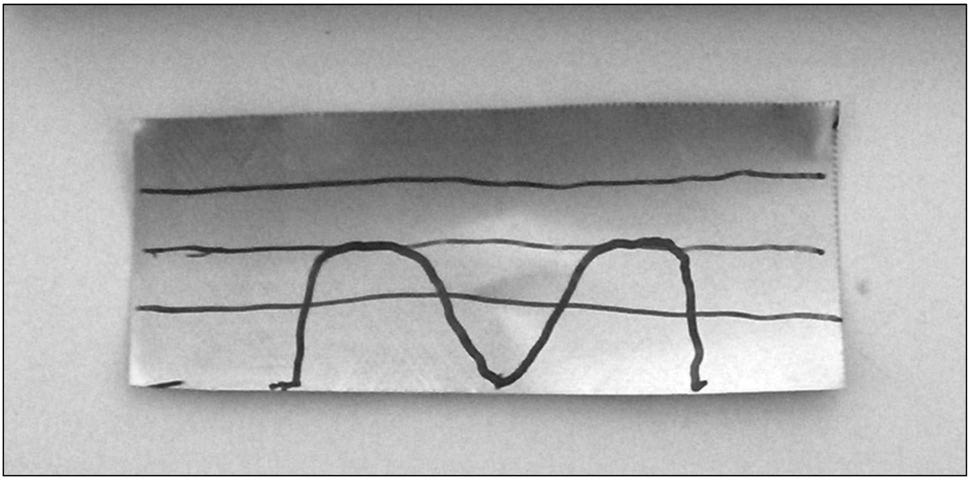
1. Cut a 1-inch × 3-inch square out of an aluminum can. The square should be clean with no cuts or ragged edges.
2. Use the marker to divide the metal into four equal sections, as shown in Figure 2.5.

Figure 2.5 Basic Assembly



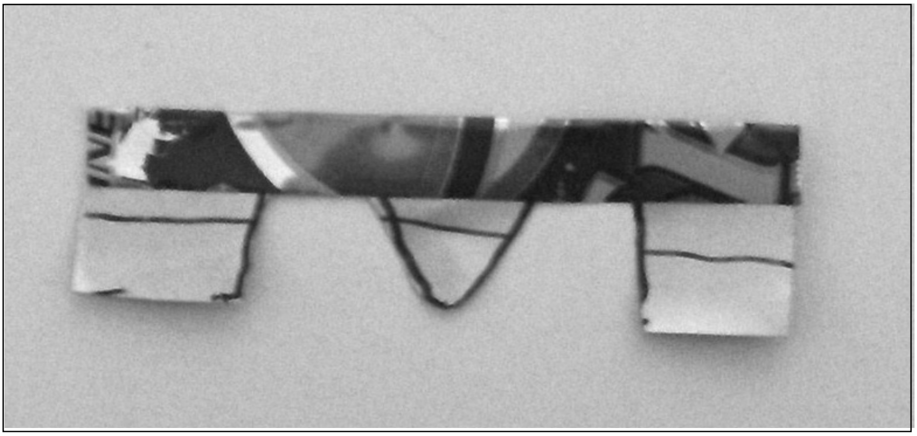
3. Next, use the marker to draw out a smoothly curved "M" that is about half the width of the aluminum square, as shown in Figure 2.6.

Figure 2.6 Preparing for the Cut



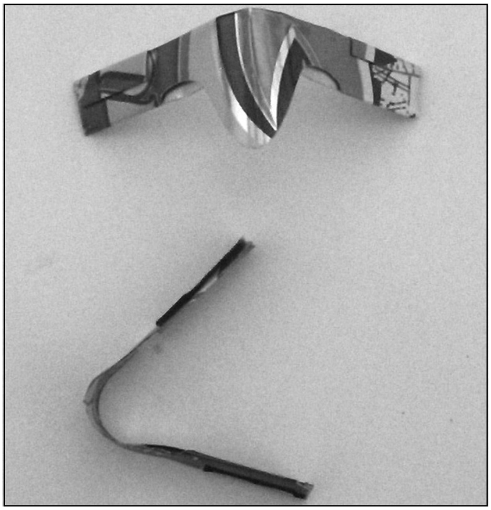
4. Take the scissors and cut out the "M," keeping the lines smooth. Try to avoid making any cuts or tears in the aluminum.
5. With the "M" facing you, fold down the top of the aluminum square to the middle line drawn earlier, as shown in Figure 2.7.

Figure 2.7 Building the Shim



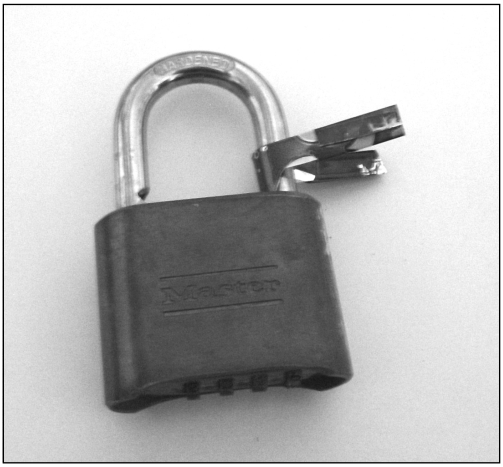
6. At this point, take the two outer sides of the "M" and fold them all the way up past the fold you made in step 5. Finish this step by folding the pieces that extend above the middle ridge down and around the stiffened middle.
7. Take the finished tool and wrap it slightly around a pen or pencil to give it the proper shape, as shown in Figure 2.8.

Figure 2.8 The Completed Shim



8. Take the shim and work it into the lock to see its operation, as shown in Figure 2.9

Figure 2.9 Cracking Open Your First Lock



Wiretapping

Wiretapping is the interception of voice calls by an unauthorized party. It is illegal to wiretap or record telephone conversations under most conditions.

There are several ways that wiretapping can be carried out. The simplest way is to record the conversation. Equipment for recording phone calls is available at most electronic shops, and typically use a *coil-tap* or an *in-line tap* to pick up and record conversations. The next method is called a *direct-line tap*. This form of wiretapping is where a user's phone line is physically tapped near the phone box on the side of the house or near the terminal boxes that feed phone lines into all the homes in an area. It can be used to listen in on calls or make calls on someone else's phone line. The third type of wiretapping is called *radio tap*. This bug like device fits on the phone line and transmits a radio signal back to the receiver.

Scanning and Sniffing

Cordless phones, cell phones, and wireless networking equipment are all potential risks for corporations. These devices can cause huge problems because, unlike lock picking or wiretapping, no physical access is required. Anyone within range of a signal can launch a host of attacks. Let's start by looking at the history of some common communication systems.

The Early History of Scanning and Sniffing

Communication security problems didn't begin with the introduction of 802.11b or the WEP protocol. Phone systems have been hacked since the 1960s. These early hackers, called *phreakers*, were mainly interested in making free long-distance phone calls.

Early satellite TV companies were attacked by freeloaders that set up their own C-band satellite dishes to intercept free HBO and Showtime. The satellite TV companies responded by implementing the videocipher encryption system.

First generation cordless phones had no security and therefore, completely vulnerable to interception. While manufacturers eventually provided ten frequencies, they were easy to intercept in the 43 to 44 MHz range. Those frequencies are shown in Table 2.6.

Table 2.6 Original Cordless Phone Frequencies

Channel	Base Frequency	Handset Frequency
1	43.720 MHz	48.760 MHz
2	43.740 MHz	48.840 MHz
3	43.820 MHz	48.860 MHz
4	43.840 MHz	48.920 MHz
5	43.920 MHz	49.000 MHz
6	43.960 MHz	49.080 MHz

Continued

Table 2.6 continued Original Cordless Phone Frequencies

Channel	Base Frequency	Handset Frequency
7	44.120 MHz	49.100 MHz
8	44.160 MHz	49.160 MHz
9	44.180 MHz	49.200 MHz
10	44.200 MHz	49.240 MHz

Serious phone hackers would wire a CB antenna to a cordless phone and attempt to find vulnerable phone systems to exploit, now called *wardriving*. Others bought off-the-shelf scanners to intercept any cordless phone calls within range. By 1994, 900 MHz phones began appearing, and while they offered more features than their earlier counterparts, they offered little more in the way of security.

The first cell phones, known as 1st technology (1G) cell phones, worked at 900 MHz and were vulnerable to a variety of attacks. *Tumbling* is a type of cell phone attack that makes attackers' phones appear to be legitimate. It works on specially modified phones that tumble and shift to a different electronic serial number (ESN) and mobile identification number (MIN) after each call. 1G cell phones are also vulnerable to cloning attacks, which required the hacker to capture the ESN and the MIN of a device. Hackers used sniffer-like equipment to capture these numbers from an active cell phone and then install them in another phone.

These events led the Federal Communications Commission (FCC) to pass regulations in 1994, banning the manufacture or import of scanners that can pick up cell-phone frequencies or be altered to receive such frequencies. The passage of Federal Law 18 USC 1029 makes it a crime to knowingly and intentionally use cell phones that are altered in any way to allow unauthorized use of such services. Federal Law 18 USC 1028 Identity Theft and Assumption Deterrence addresses subscription fraud.

Cordless phone providers made it harder for hackers by switching to spread spectrum technologies, which use digital signals and operate in the 2GHz range. Current cell phones are in the 3G range and are much more secure. These devices work in the 2GHz range, and use spread spectrum technologies and strong encryption.

Modern Wireless Vulnerabilities

While scanners that pick up cordless phones and other wireless communications in the 45 MHz and 900 MHz frequencies can no longer be manufactured in the US, there still is potential vulnerability from existing pre-ban equipment. These scanners are usually found at swap meets, eBay, and pawnshops. Radio Shack and Uniden are the most popular brands. Hackers can identify the manufacture date by the date code. Uniden scanner date codes consist of a two-digit code representing the month and another two-digit code representing the year. This simple code replaces the numeric value with its alphanumeric equivalent as follows: A=1, B=2, C=3, D=4, E=5, F=6, G=7, H=8, I=9, 0=0. Therefore, a code of 0CI2 is

March 1992. Radio Shack date codes consist of a number from 1 to 12. Next is the letter "A," which acts as a separator between the month and year codes. The last portion is a number from 0 to 9. The first number represents the month of manufacture, and the last number represents the year (e.g., date code 2A3 would decode as February 1973, February 1983, February 1993, or February 2003).

WARNING

In the US, it is illegal to intercept, record, or monitor phone conversations without the consent of all parties to the communication, including cordless and cellular calls.

Other tools are available for targeting cell phone communication, including the International Mobile Subscriber Identity (IMSI) catcher. This device is used for intercepting Global System for Mobile Communications (GSM)-based cell phones. It's a type of man-in-the-middle (MITM) tool that informs the GSM phone under attack that it is the base station of choice. Another useful tool is a cell phone jammer, which transmits a signal on the same frequencies as cell phones, thereby preventing all cell phone communication within a given area. While these devices are widely used in Europe, they are illegal in the US. On the other end of the spectrum are *cell phone detectors*, which can detect when a cell phone is powered on. These devices are found in high security areas (e.g., hospitals and prisons).

Bluetooth is another tool that offers great functionality, but has not been fully secured and is vulnerable to attacks. Bluejacking allows an individual to send unsolicited messages over Bluetooth to other Bluetooth devices (e.g., text, images, or sounds). Bluesnarfing is the theft of data, calendar information, and phone book entries. A demonstration given at DefCon by Flexilis, a wireless think-tank based in Los Angeles, demonstrated that a modified Bluetooth system can pick up Bluetooth signals from up to a mile away. The key to these attacks was the design of a higher gain antenna that was not designed to be used with Bluetooth devices. Combined with Bluetooth software tools, these attacks proved successful. Some of the software tools used to attack Bluetooth include:

- **RedFang** A small proof-of-concept application used to find non-discoverable Bluetooth devices.
- **Bluesniff** A proof-of-concept tool for Bluetooth wardriving.
- **Btscanner** A Bluetooth scanning program with the ability to do inquiry and brute force scans, identify Bluetooth devices that are within range, export the scan results to a text file, and sort the findings.
- **BlueBug** Exploits a Bluetooth security loophole on some Bluetooth-enabled cell phones. Allows unauthorized downloading of phone books and call lists, and

sending and reading Short Message Service (SMS) messages from the attacked phone.

The bootable CD Auditor **www.remote-exploit.org/index.php/Auditor_main** contains all of the tools above. However, you also need the right hardware in order to build a long-range system and gain real capability.

WLANs are also vulnerable to attack, which generally put into four basic categories: *eavesdropping*, *open authentication*, *rogue access points*, and *denial of service (DoS)*.

- **Eavesdropping** The interception and sniffing of data. If insecure applications such as File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP) are used, the intercepted data was sent in cleartext.
- **Open Authentication** The failure to use WEP, WPA, or other protection mechanism. Open access points do not require authentication. All that is required is that someone be within range of the wireless signal to authenticate.
- **Rogue Access Point** This is a MITM attack where the attacker places their own access point in the same area as another user's and attempts to get them to login.
- **DoS** The easiest form of attack. WLANs operate on the same frequencies as cordless phones and microwave ovens, which makes jamming the signal trivial.

Hardware Hacking

Most people have done hardware hacking at one time or another. Maybe you removed the region code from your DVD player so that you can watch cool DVDs that you picked up in Japan. Or maybe you loaded Linux on your iPod. Hardware hacking is about using physical access to bypass controls or modify the device in some manner. This is sometimes called *modding*, which is nothing more than modifying a piece of hardware to do more than what it was designed to do.

WARNING

Users attempting to modify the next generation DVD player, Blu-ray, may get an unwelcome surprise. It has been reported that because these players will feature Internet connectivity, manufacturers are building in technology to monitor for tampering. Any attempted hardware hack will be reported and allow the vendor to send a signal to permanently disable the player.

Bypassing Physical Controls

Computers with a Basic Input Output System (BIOS) password are designed to increase security and prevent users from changing settings. However, if you have access to the locked system, there are several techniques that can be used to bypass this control.

1. Try a default password. There are many lists of default passwords available, as listed below in Table 2.7. A more complete list can be found at www.phenoelit.de/dpl/dpl.html.

Table 2.7 Default Passwords

Manufacturer	Password
AMI	condo
Compaq	Compaq
Dell	Dell
Epox	central
Enox	Xo11nE
Jetway	Iwill
Siemens	SKY_FOX
TMC	BIGO
Toshiba	Toshiba
Phoenix	BIOS

2. Use a software program such as the AMI Decode script, which is designed to grab the Cellular Management Operation System (CMOS) password from any system. This script works on systems using an American Megatrends (AMI) BIOS.
3. Use the motherboard's clear CMOS jumper. Most motherboards feature a jumper that can be used to clear the CMOS. While the location may vary, it shouldn't be hard to find because it is usually located near the battery or the processor. Most motherboard manufacturers label the jumper. Look for labeling such as CLRPWD, CLEAR, CLEAR CMOS, or something similar.
4. If all else fails, remove the CMOS battery, which are easy to find and usually not soldered in place. Some are backed up by a capacitive circuit, so you may want to leave it unplugged for a while to make sure that it has fully discharged.

The bottom line is that once physical access is obtained, it is difficult to maintain security. A quick review of the password reset page on the Cisco Web site www.cisco.com/warp/public/474/index.shtml demonstrates this. The page states that the information is maintained for those with physical access to the console port and need to reset passwords. You are also at risk if someone accesses an open session. Some Cisco devices have controls to prevent the recovery of passwords, which are implemented by issuing the **no service password-recovery command** from the *router config* menu. This command prevents an attacker from accessing the original configuration and forces the attacker to reset the device to its factory default load.

Bypassing Authentication

With physical access, just about anything is possible. If someone wants access to a Windows computer without having the proper password, there are a couple of ways to bypass the normal authentication process: *password hash insertion* and *password cracking*.

Password hash injection targets the *Windows/System32/Config/Sam* file, which is where usernames and passwords are stored. While it is normally protected, programs like ntpasswd bypass this protection. A copy of this tool can be found at http://home.eunet.no/pnordahl/ntpasswd/ and downloaded onto the bootup disk. During bootup, the system will ask what you want to change the administrator password to. Enter the new password and shut down the system. You will now be able to logon using the new password. While this does work, there are a couple of problems. First, if anyone other than you uses this system, that person will not be able to log in. Second, if an Encrypted File System (EFS) is being used, the files have effectively been locked.

Password cracking offers a more stealth method to access a targeted system. To start this process, you will need a copy of Knoppix, which can be downloaded for free from http://s-t-d.org/. Once you boot the targeted system with Knoppix, copy the same file to a USB drive. The passwords can be extracted with a tool such as saminside, www.insidepro.com/eng/saminside.shtml. With this step completed, all that's left to do is take the encrypted passwords and load them into LC5 or John the Ripper.

There is a host of other tools such as NTFSDOS and LINNT that allow you to gain access to a system if you have physical control.

Modifying Hardware

Most hardware devices have controls in place to limit their functionality or control security (e.g., satellite TV systems). Years ago, they were analog, but providers got tired of freeloaders stealing their signals and implemented smart card technology. DirecTV and Dish Network are the two major providers of these encrypted digital signals in the US. Both of these systems have been attacked by determined hackers, but over a period of years, Dish Network and DirecTV were able to defeat most of these hacking attempts. The best way to see how this works is to look at a hardware modification using Bluetooth.

Modifying Bluetooth Hardware

To attempt this hardware hack at home, you need the basic items listed in Table 2.8. Basic electronic skills are not required, but will be helpful.

Table 2.8 Supply List

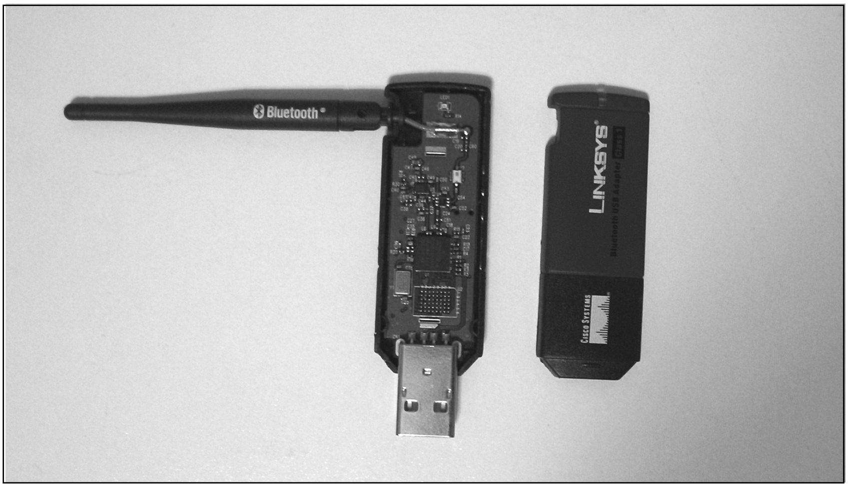
Item	Description
Bluetooth USB Adaptor	LINKSYS USBT100
External Antenna	Airlink 7 dBi external antenna
Soldering Iron	Standard soldering iron
Solder	21 gauge solder
Wick	Fine braid solder wick
Asst. Tools	Small pry bar/wire strippers
Glue	Super glue or other adhesive

1. **Disassembly** The first step of the project. Take a small screwdriver and carefully open the case holding the Bluetooth adaptor. Work your way around the seam of the adaptor and the case will easily open. Once the case is opened, remove the printed circuit board (PCB) and antenna. Figure 2.10 shows the disassembled adapter.

WARNING

This modification is for demonstration purposes only. Modification to a Bluetooth adaptor antenna may violate FCC rules. Disassembly and modification of your Bluetooth adaptor will void your warranty.

Figure 2.10 Opening the Bluetooth Adapter Case

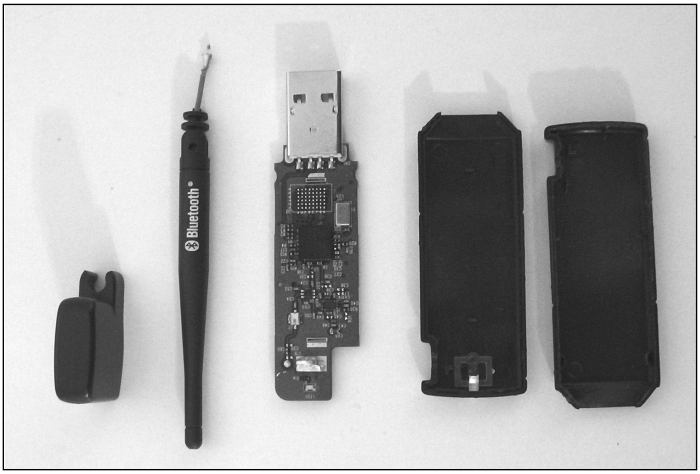


2. **Remove the Stock Antenna** This step takes some skill because you will be using a soldering iron. First, let the soldering iron get to the correct temperature. Next, apply the tip to the soldered antenna lead. As the solder starts to melt, remove the antenna from the PCB. Figure 2.11 shows the PCB with the antenna removed.

WARNING

Applying heat to the PCB for more than 60 to 90 seconds can cause permanent damage to the adaptor. If the antenna is not removed quickly, wait a few minutes to allow the PCB to cool and then try again.

Figure 2.11 Antenna Removal



3. **Preparing the PCB for the New Antenna** When the old antenna is removed, there will be excess solder left on the PCB where the antenna was connected. Take a length of solder wick and apply it to the pad while heating it with the soldering iron. This will soak up the excess solder and allow you to clean the antenna feed through the hole in the PCB (see Figure 2.12).

4. **Preparing the Antenna Cable for Soldering** You need to strip the outer shield of about ?-inch of insulation. The first ? inch must have the inner insulation stripped away to reveal the inner copper wire conductor. Next, you need to tin the outer conductor, which will make it easier to mount to the ground pad on the PCB. An example of the tinned, prepped antenna cable is shown in Figure 2.13.

Figure 2.12 Preparing for the New Antenna

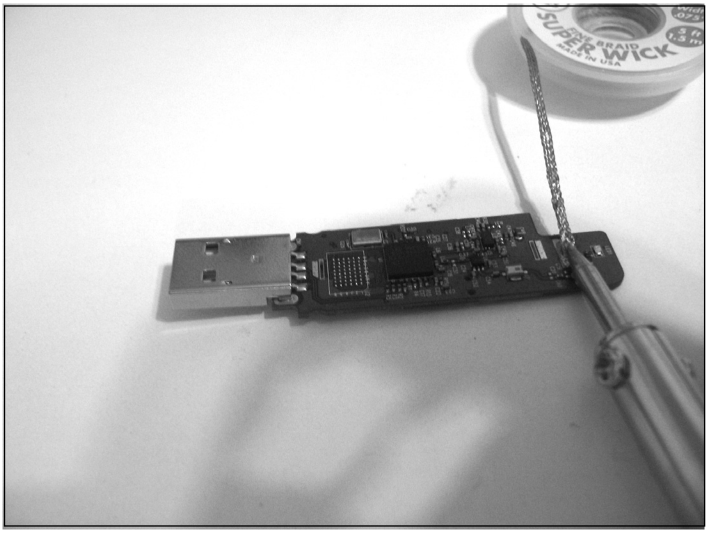
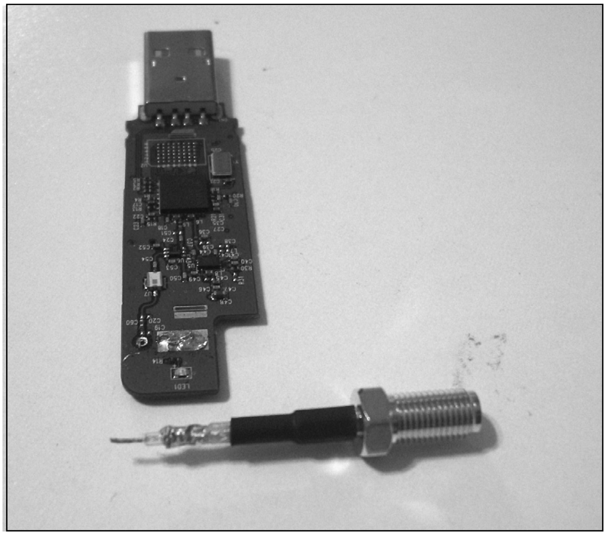
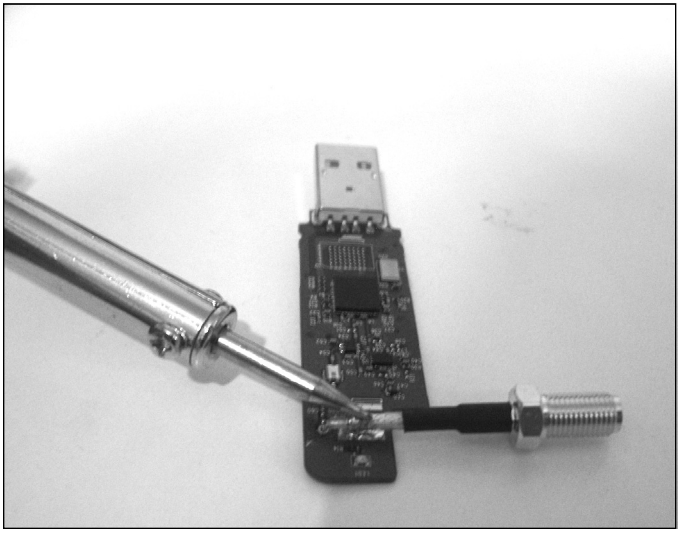


Figure 2.13 Tinning the Cable



5. **Mounting the New Cable** Insert the center connector of the antenna wire through the hole. Next, bend the antenna cable down so that it is perpendicular with the PBD and positioned the same as the original antenna. At this point, solder the outer shielding to the ground pad of the PCB as shown in Figure 2.14. After the solder cools, turn the PCB over and solder the center connector of the antenna to the PCB.

Figure 2.14 Mounting the New Cable



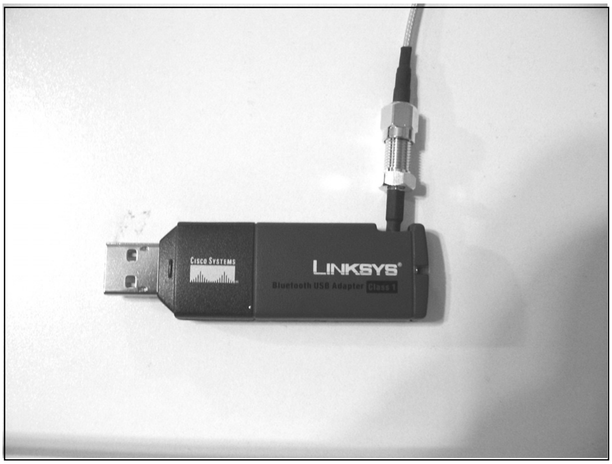
6. **Cleaning the Assembly** Clip any excess wire protruding from the center connector you just soldered. Then turn the PCB back over and make sure none of the antenna wire shielding is touching any other metal conductors or components.

WARNING

Look closely at the final product to make sure none of the wires of the antenna's ground is touching any other conductors, and that there are no shorts.

7. **Closing the Case** Place the PCB back into the case, being careful not to place excessive strain on the newly soldered wires. Use glue to reseal the case.
8. **Reviewing the Final Product** Congratulations, you have modified your first piece of physical hardware. Now's the time to look over your completed assembly, as shown in Figure 2.15. You are now ready to scan for Bluetooth with much greater range than was previously possible.

Figure 2.15 Reviewing the Final Product



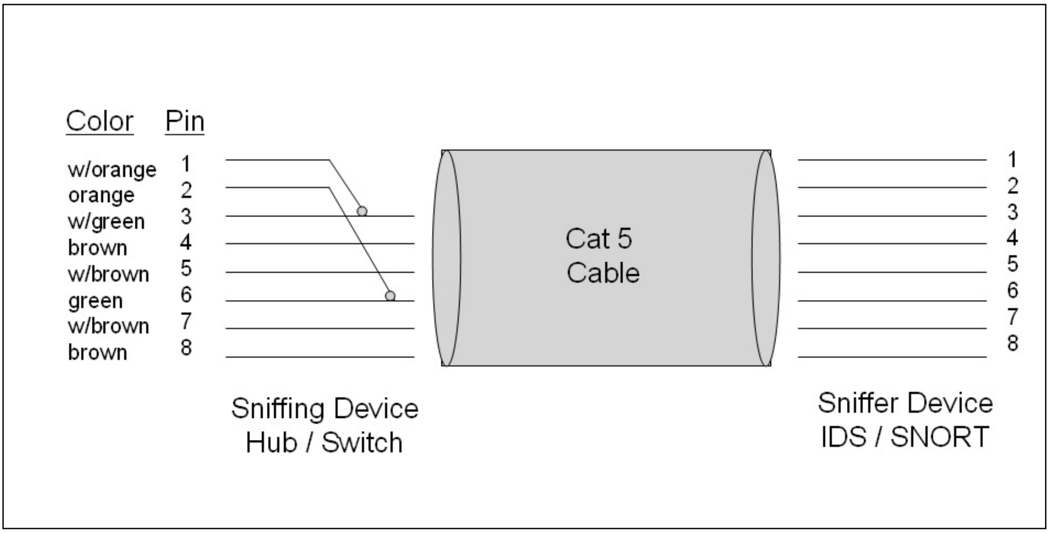
Layer 1 Security Project

This chapter and each of the following chapters feature a security project, which is designed to give you hands on skills at "Hack the Stack" activities. One of the tools featured in this book is Snort. In order to use Snort effectively, it should be configured in such a way that attackers cannot detect its presence.

One-Way Data Cable

A *one-way data cable* is designed to receive but not transmit information. This makes it impossible for an attacker to receive data from the IDS and makes for an undetectable but direct way to monitor traffic. You will be building a Snort system, so a one-way data cable is a useful add-on. All you need to assemble your one-way cable is a length of Category 5 cable and a couple of RJ-45 connectors. Figure 2.16 shows the wiring diagram. The end of the cable that plugs into the sniffer will be wired as a normal patch cable using pins 1, 2, 3, and 6. The end that plugs into the switch will be modified; you will want to remove an inch or so of wire 1 and wire 2. Both ends of the removed wires should be stripped. Wire 1 should be soldered to wire 3, and wire 2 should be soldered to wire 6 so that transmit and receive are looped. These wires should be carefully placed in an RJ-45 connecter and crimped.

Figure 2.16 One-Way Data Cable



Summary

Physical layer security is the cornerstone of all security controls. While security controls at other layers may fail without catastrophic results, the loss of physical security usually results in total exposure. Security controls cost money and many times their value is under-rated. A large portion of security controls limit the access of insiders with the side effect being that it limits many companies' motivation to implement strong controls. We like to think that these trusted employees are on our team, but numbers show that many more attacks originate from inside of an organization than from the outside. Physical controls are not always expensive. Items like locks are relatively cheap yet deter and delay attackers. Session controls, password protected screen savers, and auto logoffs are also cheap to deploy. Good physical security also requires the control of paper documents. Shredders are an easy way to prevent dumpster diving.

Attacks on physical security are nothing new. They existed long before computer networks or modern organizations were envisioned. There are many tools at an attacker's disposal. Lock pick sets, wiretapping equipment, and scanners are easy for an attacker to acquire. Attackers with basic computer skills can use wireless hacking tools or acquire security equipment for disassembly and analysis. In the end, security professionals must realize that they are not fighting a single battle, but are part of an ongoing war that will continue for the unforeseeable future.

Solutions Fast Track

Defending the Physical Layer

☑ Without physical security, no other security measures are considered sufficient to prevent an attack.

☑ Physical security is about deterring, delaying, and detecting breaches in security.

☑ Physical security requires a defense-in-depth approach, which means that security controls are layered on top of one another to mitigate risk.

Attacking the Physical Layer

☑ Physical security attacks are some of the most effective. They can bypass all controls that reside at higher layers of the stack.

☑ Insiders with the means, motive and opportunity can easily launch physical layer attacks.

☑ Mobile devices increase the risk of physical security attacks as they can introduce malicious code into the network or easily remove large amounts of data.

Physical Layer Security Project

☑ A one-way network cable is useful for IDS operation.

☑ Building a one-way network cable allows an IDS to receive but not transmit data.

☑ One-way network cables prevent an IDS from being logically compromised.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Should all physical security controls be visible to the attacker?

A: Physical controls work best when some are seen and others are unseen. Controls that are seen tend to deter attacks, while those that are unseen offer protection because they are harder for the attacker to analyze and bypass.

Q: How do you know what grade or type of lock to use to delay an attacker?

A: The amount of delay provided by a lock should equal the security of the other components (e.g., the most secure lock is of little value if the door, doorframe, and hinges are of a weak design).

Q: What is the difference between a residential fence and a fence used in high security sites?

A: Fences used for high security sites use a smaller mesh and a thicker gauge of wire, which means it is harder for an attacker to climb or to cut.

Q: What is the number one problem that occurs with security lighting?

A: Security lighting requires placing the right amount of light in the proper location. Overlighting leads to a less secure environment by creating dark pockets outside of the lit area.

Q: Is it impossible to pick up cordless phone conversations?

A: While not impossible, it is much harder than in years past. The FCC changed the law in 1994, to make it illegal to sell scanners that can intercept cordless phone. While older scanners with this functionality included can still be found, cordless phone manufacturers have invested in spread spectrum technologies that further limit the possibility of interception.

Q: What is the easiest type of physical attack to launch?

A: Data theft. The proliferation of small, mobile devices with massive storage makes it easy for anyone to remove large amounts of data quickly.

Q: Who typically has the most physical access?

A: The cleaning crew typically has access to all areas of a facility and work at night when most employees are gone.

Q: Is it illegal to buy lock-picking tools?

A: The legality of lock picking tools varies from state to state. Many states have laws stating that possession of lock picks with intent to break in is illegal. Check your state's laws to see if having lock picks for learning purposes is legal.