Unit IV
Cyber Security Terminology

Virus Scanner

A *virus scanner* is essentially software that tries to prevent a virus from infecting your system. This fact is probably abundantly obvious to most readers.

How Does Virus Scanner Works?

In general, virus scanners work in two ways.

- The first method is that they contain a list of all known virus definitions. The virus definitions are simply files that list known viruses, their file size, properties, and behavior. Generally, one of the services that vendors of virus scanners provide is a periodic update of this file. This list is typically in a small file, often called a *.dat* file (short for data). When you update your virus definitions, what actually occurs is that your current file is replaced by the more recent one on the vendor's website. The antivirus program can then scan your PC, network, and incoming email for known virus files. Any file on your PC or attached to an email is compared to the virus definition file to see whether there are matches. With emails, this can be done by looking for specific subject lines and content. The virus definitions often also include details on the file, file size, and more. This provides a complete signature of the virus.
- The second way a virus scanner can work is to look for virus-like behavior. Essentially, the scanner is looking to see if the file in question is doing things that viruses typically do—things like manipulating the Registry or looking through your address book, any program that attempts to write to your hard drive's boot sector, change system files, automate your email software, or self-multiply. Programs that attempt to modify the system Registry (for Windows systems) or alter any system settings may also be indicative of a virus. Another feature that virus scanners search for is a file that will stay in memory after it executes. This is called a Terminate and Stay Resident (TSR) program. Some legitimate programs do this, but it is often a sign of a virus. Additionally, some virus scanners use more sophisticated methods, such as scanning your system files and monitoring any program that attempts to modify those files.
- Whatever the behavior, antivirus software uses specific algorithms to evaluate the likelihood that a given file is actually a virus. It should be noted that modern virus scanners scan for all forms of malware, including Trojan horses, spyware, and viruses.

Virus-Scanning Techniques

In general, there are five ways a virus scanner might scan for virus infections. Some of these were mentioned in the previous section, but they are outlined and defined here:

- **Email and attachment scanning:** Since the primary propagation method for a virus is email, email and attachment scanning is the most important function of any virus scanner. Some virus scanners actually examine your email on the email server before downloading it to your ma- chine. Other virus scanners work by scanning your emails and attachments on your computer before passing it to your email program. In either case, the email and its attachments should be scanned prior to your having any chance to open them and release the virus on your system.
- **Download scanning:** Anytime you download anything from the Internet, either via a web link or through some FTP program, there is a chance you might download an infected file. Download scanning works much like email and attachment scanning but does so on files you select for downloading.
- **File scanning:** This is the type of scanning in which files on your system are checked to see whether they match any known virus. This sort of scanning is generally done on an on-demand basis instead of an ongoing basis. It is a good idea to schedule your virus scanner to do a complete scan of the system periodically. I recommend a weekly scan, preferably at a time when no one is likely to be using the computer.
- **Heuristic scanning:** This was briefly mentioned in the previous section. Perhaps the most advanced form of virus scanning, this uses rules to determine whether a file or program is behaving like a virus and is one of the best ways to find a virus that is not a known virus. A new virus will not be on a virus definition list, so you must examine its behavior to determine whether it is a virus. However, this process is not foolproof. Some actual virus infections will be missed, and some nonvirus files might be suspected of being a virus.
- **Sandbox:** Another approach is the sandbox approach. This basically means that you have a separate area, isolated from the operating system, in which a download or attachment is run. Then if it is infected, it won't infect the operating system.

Firewall

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Firewall Types and Components

There are numerous types of firewalls and variations on those types. But most firewalls can be grouped into one of the following three families of firewalls.

- Packet inspection
- Stateful packet inspection
- Application

Packet Filtering

Basic packet filtering is the simplest form of firewall. It looks at packets and checks to see if each packet meets the firewall rules. For example, it is common for a packet filtering firewall to ask three questions:

1. Is this packet using a protocol that the firewall allows?
2. Is this packet destined for a port that the firewall allows?
3. Is the packet coming from an IP address that the firewall has not blocked?

Stateful Packet Inspection

The Malwarebytes firewall will examine each packet, denying or permitting access based not only on the examination of the current packet, but also on data derived from previous packets in the conver- sation. This means that the firewall is aware of the context in which a specific packet was sent. This makes these firewalls far less susceptible to ping floods and SYN floods, as well as less susceptible to spoofing. For example, if the firewall detects that the current packet is an ICMP packet and a stream of several thousand packets have been continuously coming from the same source IP, it is clearly a DoS attack and the packets will be blocked.

An *application gateway* (also known as *application proxy* or *application-level proxy*) is a program that runs on a firewall. When a client program, such as a web browser, establishes a connection to a destination service, such as a web server, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to gain access to the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. This process actually creates two connections. There is one connection between the client and the proxy server and another connection between the proxy server and the destination.Once a connection is established, the application gateway makes all decisions about which packets to forward.

Firewall Configurations

In addition to the various types of firewalls, there are various configuration options. The type of firewall tells you how it will evaluate traffic and hence decide what to allow and not to allow. The configuration gives you an idea of how that firewall is set up in relation to the network it is protecting. Some of the major configurations/implementations for firewalls include the following:

- Network host–based: A *network host–based firewall* is a software solution installed on an existing machine with an existing operating system.
- Dual-homed host: A *dual-homed host* is a firewall running on a server with at least two network interfaces. The server acts as a router between the network and the interfaces to which it is attached.
- Router-based firewall: As was previously mentioned, you can implement firewall protection on a router. In larger networks with multiple layers of protection, this is commonly the first layer of protection. Although you can implement various types of firewalls on a router, the most common type used is packet filtering.
- Screened host: A *screened host* is really a combination of firewalls. In this configuration, you use a combination of a bastion host and a screening router.

Antispyware

Antispyware, as discussed earlier in this book, scans your computer to see whether there is spyware running on your machine. This is an important element of computer security software that was at one time largely ignored. Even today, not enough people take spyware seriously or guard against it. Most antispyware works by checking your system for known spyware files. Each application must simply be checked against a list of known spyware. This means that you must maintain some sort of subscription service so that you can obtain routine updates to your spyware definition list. Most antivirus solutions now also check for spyware. In today's Internet climate, running antispyware is as essential as running antivirus software. Failing to do so can lead to serious consequences. Personal data, and perhaps sensitive business data, could easily be leaking out of your organization without your knowledge. And, as was pointed out earlier in this book, it is entirely possible for spyware to be the vehicle for purposeful industrial espionage.

Barring the use of antispyware, or even in conjunction with such software, you can protect yourself via your browser's security settings as was discussed in a previous chapter. Additionally, several times throughout this book, you have been warned to be cautious about attachments and Internet downloads. You would also be well advised to avoid downloading various Internet "enhancements," such as "skins" and "toolbars." If you are in an organization, prohibiting such downloads should be a matter of company policy. Unfortunately, many websites today require some sort of add-in such as Flash in order to function properly. The best advice for this situation is to only allow add-ins on trusted, well-known sites.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.

IDS Categorization

There are a number of ways in which IDS systems can be categorized. The most common IDS catego- rizations are as follows:

- Passive IDS
- Active IDS (also called Intrusion Prevention System, or IPS)

Passive IDS

A passive IDS just monitors suspicious activity and then logs it. In some cases it may notify the admin- istrator of the activity in question. This is the most basic type of IDS. Any modern system should have, at a minimum, a passive IDS along with the firewall, antivirus, and other security measures taken.

Active IDS

An active IDS or IPS takes the added step of shutting down the suspect communication. Just like anti- virus, it is possible for an IDS to have a false positive. It might suspect something is an attack when in fact it is legitimate traffic. Whether one uses an IDS or IPS is a decision that must be made after a thorough risk analysis.

IDS Elements

Whether it is an active IDS or a passive IDS, and regardless of whether it is commercial or open source, certain elements/terms are common to all IDSs.

- A *sensor* is the IDS component that collects data and passes it to the analyzer for analysis.
- The *analyzer* is the component or process that analyzes the data collected by the sensor.
- The *manager* is the IDS interface used for management. It is a software component to the IDS.
- The *operator* is the person primarily responsible for the IDS.
- *Notification* is the process or method by which the IDS manager makes the operator aware of an alert.
- An *activity* is an element of a data source that is of interest to the operator. It may or may not be a possible attack.
- An *event* is any activity that is deemed to be suspicious and a possible attack.
- An *alert* is a message from the analyzer indicating that an event has occurred.
- The *data source* is the raw information that the IDS is analyzing to determine if there has been an event.

Honey Pots

A honey pot is an interesting technology. Essentially, it assumes that an attacker is able to breach your network security. And it would be best to distract that attacker away from your valuable data. Therefore, one creates a server that has fake data—perhaps an SQL server or Oracle server loaded with fake data, and just a little less secure than your real servers. Then, since none of your actual users ever access this server, monitoring software is installed to alert you when someone does access this server.

A honey pot achieves two goals. First, it will take the attacker's attention away from the data you wish to protect. Second, it will provide what appears to be interesting and valuable data, thus leading the attacker to stay connected to the fake server, giving you time to try to track them. There are commercial solutions, like Specter (www.specter.com). These solutions are usually quite easy to set up and include monitoring/tracking software. You may also find it useful to check out www.honeypots.org for more information on honey pots in general, and on specific implementations.

Database Activity Monitoring

Database activity monitoring (DAM) is monitoring and analyzing database activity that operates independently of the database management system (DBMS). It is separate from the DBMS auditing, logging, and monitoring. Database activity monitoring and prevention (DAMP) is an extension to DAM that goes beyond monitoring and alerting to also block unauthorized activities.

Authentication

When a user logs on to a system, the system needs to authenticate her (and sometimes the user needs to authenticate the system). There are many authentication protocols. A few of the more common are briefly described here:

- **PAP:** Password Authentication Protocol is the simplest form of authentication and the least secure. Usernames and passwords are sent unencrypted, in plain text. This is obviously a very old method that is not used anymore. However, in the early days of computing, there were no widely available packet sniffers, and security was far less of a concern.
- **SPAP:** Shiva Password Authentication Protocol is an extension to PAP that does encrypt the username and password that is sent over the Internet.
- **CHAP:** Challenge Handshake Authentication Protocol calculates a hash after the user has logged in. Then it shares that hash with the client system. Periodically the server will ask the client to provide that hash. (This is the challenge part.) If the client cannot, then it is clear that the communications have been compromised. MS-CHAP is a Microsoft-specific extension to CHAP. The steps are basically these:

1. After the handshake phase is complete, the authenticator (often the server) sends a “chal- lenge” message to the peer.
2. The peer responds with a value calculated using a “one-way hash” function.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection should be terminated.
4. At random intervals, the authenticator sends a new challenge to the peer and repeats steps 1 to 3.

The entire goal of CHAP is to not only authenticate, but periodically reauthenticate, thus preventing session hijacking attacks.

- **EAP:** A framework frequently used in wireless networks and point-to-point connections. It was originally defined in RFC 3748 but updated since then. It handles the transport of keys and related parameters. There are several versions of EAP. It has many variations, including these:
  - **LEAP:** Lightweight Extensible Authentication protocol was developed by Cisco and has been used extensively in wireless communications. LEAP is supported by many Micro- soft operating systems including Windows 7 and later versions. LEAP uses a modified version of MS-CHAP.
  - **Extensible Authentication Protocol—Transport Layer Security:** This utilizes TLS in order to secure the authentication process. Most implementations of EAP-TLS utilize X.509 digital certificates to authenticate the users.
  - **Protected Extensible Authentication Protocol (PEAP):** This encrypts the authenti- cation process with an authenticated TLS tunnel. PEAP was developed by a consortium including Cisco, Microsoft, and RSA Security. It was first included in Microsoft Win- dows XP

Kerberos

Kerberos is used widely, particularly with Microsoft operating systems. It was invented at MIT and derives its name from the mythical three-headed dog that was reputed to guard the gates of Hades. The system is a bit complex, but the basic process is as follows:When a user logs in, the authentication server verifies the user’s identity and then contacts the ticket-granting server. (These are often on the same machine.) The ticket-granting server sends an encrypted “ticket” to the user’s machine. That ticket identifies the user as being logged in. Later when the user needs to access some resource on the network, the user’s machine uses that ticket-granting ticket to get access to the target machine. There is a great deal of verification for the tickets, and these tickets expire in a relatively short time.

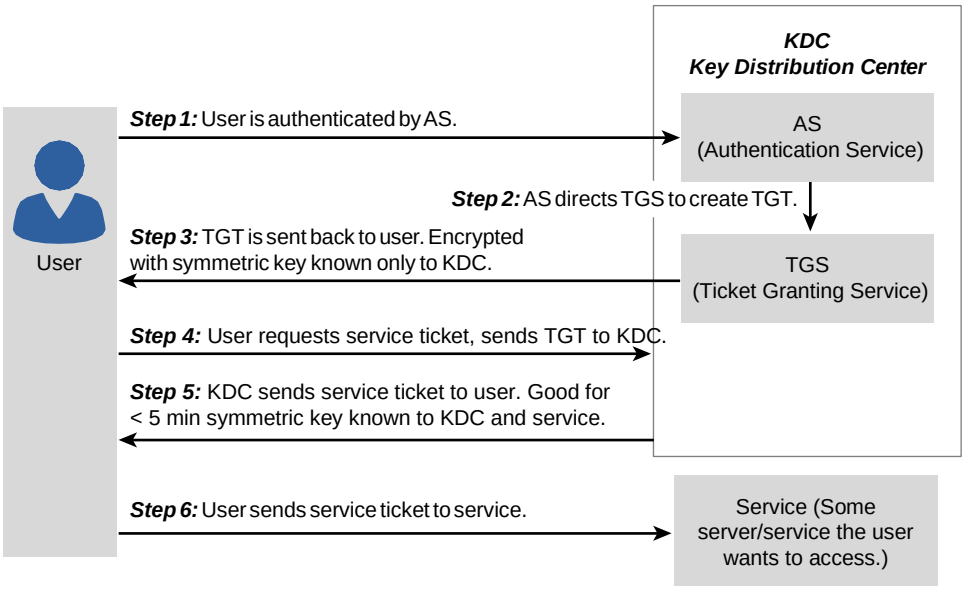


FIGURE 9.9 Kerberos

The elements of Kerberos follow:

- **Principal:** A server or client that Kerberos can assign tickets to.
- **Authentication server (AS):** Server that authorizes the principal and connects it to the ticket- granting server.
- **Ticket-granting server (TGS):** Provides tickets.
- **Key distribution center (KDC):** A server that provides the initial ticket and handles TGS requests. Often it runs both AS and TGS services. It must be noted that Kerberos is one of the most widely used authentication protocols. Europe often uses an alternative SESAME Secure European System for Applications in a multivendor environment.

Digital Signatures/Certificate

A digital signature is not used to ensure the confidentiality of a message but rather to guarantee who sent the message. This is referred to as nonrepudiation. Essentially, it proves who the sender is. Digital signatures are actually rather simple, but clever. They simply reverse the asymmetric encryption process. Recall that in asymmetric encryption, the public key (which anyone can have access to) is used to encrypt a message to the recipient, and the private key (which is kept secure, and private) can decrypt it. With a digital signature, the sender encrypts something with his private key. If the recipient is able to decrypt that with the sender's public key, then it must have been sent by the person purported to have sent the message. This process is shown in Figure 8.8.

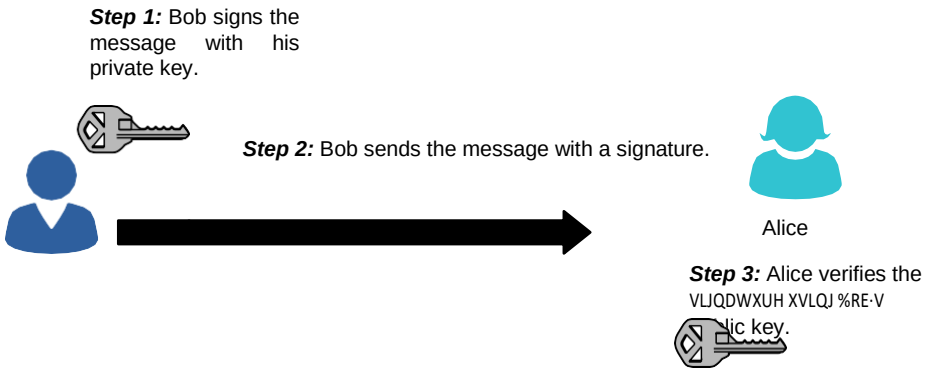


Figure 8.8 *Digital signatures.*

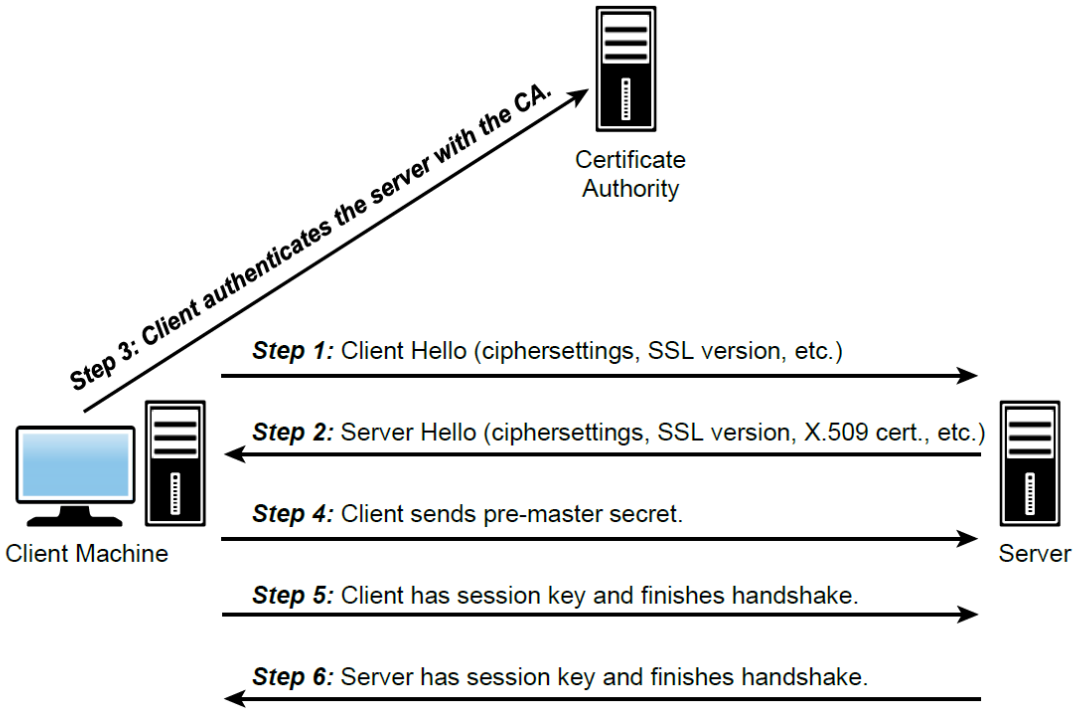
Most Standard Digital Certificate is X.509, and following are the basic items in an X.509 certificate.

- **Version:** This is the version of X.509 that this certificate complies with.
- **Certificate holder's public key:** This is the primary way of getting someone's public key from his X.509 certificate.
- **Serial number:** This is a unique identifier for this certificate.
- **Certificate holder's distinguished name:** This is often a domain name or email associated with a certificate.
- **Certificate's validity period:** One year is the most common validity period.
- **Unique name of certificate issuer:** This is the certificate authority that issued this certificate.
- **Digital signature of issuer:** This field, and the next, are used to verify the certificate itself.
- **Signature algorithm identifier:** Identifies the actual digital signature algorithm used.

SSL /TLS

SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personal identifiable information or with payroll information).

TLS (Transport Layer Security) is just an updated, more secure, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term, but when you are buying SSL from DigiCert you are actually buying the most up to date TLS certificates with the option of ECC, RSA or DSA encryption



The basic process of establishing an SSL/TLS connection is shown in Figure .

The process involves several complex steps, as defined here:

1. The client sends the server information regarding the client's cryptographic capabilities. That includes what algorithms it is capable of, what hashing algorithms it can use for message integ- rity, and related information.
2. The server responds by selecting the best encryption and hashing that both client and server are capable of and sends this information to the client. The server also sends its own certificate, and if the client is requesting a server resource that requires client authentication, the server requests the client's certificate.
3. The client uses the information sent by the server to authenticate the server. This means authen- ticating the digital certificate with the appropriate CA. If this fails the browser warns the user that the certificate cannot be verified. If the server can be successfully authenticated, the client proceeds to the next step.

4. Using all data generated in the handshake thus far, the client creates the pre-master secret for the session, encrypts it with the server's public key that it received from the server's X.509 certificate, and then sends the encrypted pre-master secret to the server.
5. If the server has requested client authentication, then the server will also authenticate the client's X.509 certificate. This does not happen in most e-commerce and banking websites.
6. Both the client and the server use the master secret to generate the session keys. These are symmetric keys (such as AES) that will be used throughout the session to encrypt information between the client and the server.
7. The client sends a message to the server informing it that future messages from the client will be encrypted with the session key.
8. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key.

Virtual Private Networks

A *VPN* is a *virtual private network*. This is essentially a way to use the Internet to create a virtual connection between a remote user or site and a central location. The packets sent back and forth over this connection are encrypted, thus making it private. The VPN must emulate a direct network connection.

There are three different protocols that are used to create VPNs:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Internet Protocol Security (IPsec)

These are each discussed in more depth in the following sections.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) is the oldest of the three protocols used in VPNs. It was orig- inally designed as a secure extension to Point-to-Point Protocol (PPP). PPTP was originally proposed as a standard in 1996 by the PPTP Forum—a group of companies that included Ascend Communications, ECI Telematics, Microsoft, 3Com, and U.S. Robotics. It adds the features of encrypting packets and authenticating users to the older PPP protocol. PPTP works at the data link layer of the OSI model (discussed in Chapter 2, "Networks and the Internet").

PPTP offers two different methods of authenticating the user: Extensible Authentication Protocol (EAP) and Challenge Handshake Authentication Protocol (CHAP).

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) was explicitly designed as an enhancement to PPTP. Like PPTP, it works at the data link layer of the OSI model. It has several improvements to PPTP. First, it offers more and varied methods for authentication—PPTP offers two, whereas L2TP offers five. In addition to CHAP and EAP, L2TP offers PAP, SPAP, and MS-CHAP.

IPsec

IPsec is the latest of the three VPN protocols. One of the differences between IPsec and the other two methods is that it encrypts not only the packet, but also the header information. It also has protection against unauthorized retransmission of packets. This is important because one trick that a hacker can use is to simply grab the first packet from a trans- mission and use it to get their own transmissions to go through. Essentially, the first packet (or packets) has to contain the login data. If you simply resend that packet (even if you cannot crack its encryption), you will be sending a valid logon and password that can then be followed with additional packets. Preventing unauthorized retransmission of packets prevents this from happening.

Wi-Fi Security

With wireless networks being so prevalent, it is important to consider wireless network security. There are three Wi-Fi security protocols, ranging from the oldest and least secure (WEP) to the most recent and most secure (WPA2). They are each briefly described here.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) uses the stream cipher RC4 to secure the data and a CRC-32 checksum for error checking. Standard WEP uses a 40-bit key (known as WEP-40) with a 24-bit initialization vector (IV) to effectively form 64-bit encryption. 128-bit WEP uses a 104-bit key with a 24-bit IV.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) was definitely an improvement over WEP. First, WPA uses AES, which is a very good encryption algorithm. Then WPA uses Temporal Key Integrity Protocol. TKIP dynamically generates a new key for each packet. So even if you crack a WPA key, there will be a different key for the next packet.

WPA2

This is the most modern form of Wi-Fi security, and if it is at all possible, this is what you should be using. Thus, we will give it a bit more attention. WPA2 is based on the IEEE 802.11i standard. It provides the Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP) that provides data confidentiality, data origin authentication, and data integrity for wireless frames.