

# **The Importance of Wireless Security**

Because of the increasing popularity of wireless networks, there is an increasing need for security. This is because unlike wired networks, wireless networks can be easily hacked from outside of your building unless the proper security measures are in place. This paper examines the various issues regarding wireless security and the methods you can employ to safeguard your wireless network.

**White paper by SILEX TECHNOLOGY Europe GmbH**

**July 31, 2007**

Copyright © 2007 SILEX TECHNOLOGY Europe GmbH

REV. 1

## **Why Do I Need to Be Concerned about Security on My Wireless Network?**

Wireless local area networks give you unprecedented freedom to locate your computers, printers, and other computing devices anywhere in a building or campus environment without the need for cumbersome cabling. Unfortunately, this capability also allows unauthorized users like hackers to easily intercept your data. That's because wireless networks use radio waves, and radio waves can "leak" outside of your building at distances up to 300 feet or even more. Therefore, everything that you do on your network can theoretically be monitored by anyone with a laptop computer that has wireless capabilities. Such a person could view your company's financial records, customer database, E-mails, and other important information that you send locally or over the Internet. And once this person has discovered your passwords, he can also log into your computer and servers to steal valuable data off the hard drive or connect to secure sites on the Internet. He could also set up your server as a relay for spam, which would impact network performance and possibly cause your company to be blacklisted on the Internet (many companies will not allow E-mail from blacklisted companies) or even sued.

As a result, you need additional levels of security for your wireless network. That is, in addition to your normal password protection, firewalls, and virus detectors, you must have special security to address the specific issues associated with wireless networks. Fortunately, there are now many industry standard security procedures that you can use to secure your wireless network.

## **Why do my Wireless Device Servers Need to be Secure?**

Device servers are dedicated intelligent products that connect devices like medical instrumentation, industrial equipment, security monitors, and point of sale products to networks. With the emergence of wireless local area networks, wireless versions of device servers have become popular because they allow devices to be mobile.

Security is an issue with device servers because they often send and receive sensitive data. For example, a device server connected to a medical instrument is sending confidential patient information across the network. Therefore, strong security is required to prevent unauthorized users from monitoring this information. In addition, security measures must be taken to prevent hackers from "spoofing" the device server in order to gain access to the network. Note that device servers use the same TCP/IP protocol as computers, so they are subject to the same kinds of security vulnerabilities.

Network security is only as strong as its weakest link. Therefore, if you put a poorly secured device server on your network, it can expose your entire network to hackers. In fact, many network administrators now require that all devices conform to specific network security standards, and devices that do not support these standards cannot be used on the network!

## **How You Can Protect Your Wireless Network**

In order to completely protect your wireless local area network, you need to implement both *encryption* and *authentication* security procedures:

- Encryption scrambles your data so that it is very difficult for someone to read unless they have the proper code known as a "key". Therefore, although a hacker can detect the signals on your network, your data will look to him like random garbage. As a result, he will not easily be able to see your passwords, social security number, or any other important information.
- Authentication is a procedure that ensures a user is who he says he is, based on pre-defined credentials. Such credentials might include passwords, digital certificates,

tokens, smart cards, or other security credentials that you choose to require. Basically, you can look at authentication as the equivalent of letting an employee into the building only after he or she displays a valid badge.

The various encryption and authentication options available for wireless local area networks are discussed in the following sections of this document.

## **WEP, Shared Key and Open Systems Authentication, and SSID – The First Generation of Wireless Security**

The designers of the first wireless local area networks realized that security would be a major issue, so they incorporated both encryption and authentication capabilities into the IEEE 802.11 standard. Although these capabilities are now considered obsolete, it is important to understand how they work in order to fully understand the benefits of the new improved security procedures like WPA and WPA2.

The Wired Equivalent Privacy protocol, or WEP, provides encryption capabilities that the designers hoped would provide the same level of basic security as a hardwired local area network. WEP is included as a standard feature with all 802.11b, 802.11g, and 802.11a network equipment, and is also supported by most popular operating systems.

The 802.11 standard also specifies two types of authentication, Open System and Shared Key. Open System authentication is very simple, since basically the access point grants authentication to any client that requests it. With shared key authentication, the client requests authentication, and the access point sends a challenge in unencrypted text. The client responds by encrypting the challenge text using its WEP key. The access point then decrypts the text and compares it with the original challenge text. If the texts match, then the client is authenticated.

In addition to WEP and authentication, the 802.11 standard defines the Server Set ID (SSID or ESSID). SSID is simply an identification provided by the access point that enables a wireless client like a laptop to communicate with it. An SSID is also referred to as a Network Name because it is a name that identifies a wireless network. By default, the SSID is usually broadcast for anyone to see or use, but this broadcast can be turned off to provide a limited amount of network security.

Using the original 802.11 security is pretty simple, at least on a relatively small network. You use the network configuration program for each of your wireless devices to manually enter up to four keys, which are (depending on the equipment) entered as a string(s) of decimal or hexadecimal characters, or via an alphanumeric passphrase. WEP supports either 40-bit or 104-bit encryption keys (also called 64-bit or 128-bit, since the 24-bit initialization vector described in the next paragraph is added to the basic key during the encryption process). All of the devices, including the access point, must be configured with the exact same keys. Whenever a device wants to send data, it uses one of the configured keys with a complex mathematical algorithm to encrypt the data. The encrypted data stream is unencrypted by the receiving device using the same key. Note that a WEP key is static; that is, it does not change unless you manually reconfigure it.

Each wireless network device must also be configured with the SSID (which the clients can obtain automatically via broadcasts from the access point), and the type of authentication must be specified.

Unfortunately, weaknesses in 802.11 security were discovered as soon as wireless networks became popular. Some of these flaws include:

- WEP standard combines a variable initialization vector (IV) with the static WEP key to encrypt the data using an algorithm known as RC4. The IV is generally (but not necessarily) changed each time a packet of data is sent. This variability should prevent hackers from easily decrypting the data, but in practice this is not the case. Because the IV is 24 bits in length, there are 16,777,216 possible values for the IV. Since millions of packets can be sent each hour on a busy network, the same IV value can be re-used with a few hours. If such a duplication, known as an IV collision, occurs, a hacker monitoring the network can use statistical techniques to extract to decrypt the packet and extract the WEP key and your data.
- Authentication procedures are very poor:
  - With Open System authentication, anyone requesting authorization is granted it (although they will not be able to communicate unless that have the correct WEP key).
  - Although shared key authentication may seem more secure, it is actually less safe than Open System because the access point's unencrypted challenge and the station's encrypted response contain the same text. A hacker could therefore monitor the authentication process, compare the challenge and response, and deduce the WEP key using simple mathematical techniques.
  - Advanced authentication using digital certificates, smart cards, etc. is not supported
- The SSID is unencrypted, so hackers can easily discover it even if SSID broadcasts are turned off.
- The Integrity Check Value (ICV), a 32-bit value that checks the integrity of the data packet, is a simple mathematical algorithm (a checksum). As a result, it is relatively easy for a hacker to change bits in the encrypted data and calculate which bits to change in the ICV to make the packet valid without knowing the WEP key. This could allow, for example, the hacker to redirect a packet by changing the destination address.
- If the WEP keys are generated using passphrases, the number of possible unique values is greatly reduced (since punctuation and non-printing control characters are not typically used in passphrases), thereby making it much faster for a hacker to find the WEP key value(s).

These weaknesses (and others) have been widely publicized and information about exploiting them is readily available on the Internet. As a result, any relatively sophisticated hacker can exploit these weaknesses to break into your network. Nevertheless, the basic 802.11 security is much better than nothing, so you should definitely use it if nothing better is available.

## **WPA and WPA2 – Better Ways to Secure Your Network**

The Wi-Fi Alliance, a consortium of companies involved in 802.11 technology and services, realized that WEP security was not adequate, and consequently developed a more robust standard known as Wi-Fi Protected Access (WPA). WPA enhances the basic 802.11 security in the following ways:

- Improved security of encryption keys via the Temporal Key Integrity Protocol (TKIP). Basically, this means that unlike the fixed WEP key, the key in WPA is dynamically changed (rekeyed), making it much more difficult for a hacker to decrypt a packet.
- Expansion of the length of the initialization vector (IV) to 64 bits, which greatly reduces the possibility of an IV collision.
- Provision for strong authentication capabilities and key management via the IEEE 802.1X standard and a RADIUS authentication server.

- Elimination of problems with the ICV by using the ICV in conjunction with a new 8-byte message integrity code (MIC) that is calculated through an algorithm called Michael. The MIC also includes a frame counter, which helps prevent replay attacks.

WPA is supported on Windows XP and MacOS X. It is a subset of the IEEE 802.11i standard for wireless network security, and was designed to allow field upgrades of existing 802.11 products. In order to maintain backwards compatibility, WPA uses RC4 encryption, which results in additional overhead on TKIP. In addition, there is also increased vulnerability to Denial of Service attacks due to weakness in MIC.

To address the weaknesses in WPA, a second generation standard known as WPA2 was developed. WPA2 is a superset of WPA that is an implementation of the full IEEE 802.11i standard. It is supported on Windows XP and MacOS X, and it is required for all Wi-Fi certified devices starting in 2006.

WPA2 uses the Advanced Encryption Standard (AES) as an alternative to RC4 (the version of AES used in WPA2 is AES-CCMP). AES provides stronger encryption than RC4, and has the additional advantage of requiring less bandwidth. Note that AES is sometimes called Rijndael (its original name before the AES standard was finalized), although there are technically some differences between AES and Rijndael.

WPA2 also provides some other advantages compared to WPA, including:

- Improved resistance to Denial of Service attacks due to the replacement of Michael with the Cipher Block Chaining Message Authentication Code (CBC-MAC) method for calculating the MIC.
- The ability to use 802.1x authentication with ad hoc (peer-to-peer) wireless networks.
- Options for improving the speed of 802.1X re-authentication.

Both WPA and WPA2 can operate in either of two modes:

- Pre-shared key mode (WPA-PSK or WPA2-PSK). This mode is designed for small home networks. In this mode, you create key by manually entering a passphrase (also known as a *shared secret*) into each station and the access point similar to the way you create a WEP key. This passphrase can be up to 63 characters in length and can contain letters, numbers, and punctuation. The pre-shared key is then used to generate the dynamic keys that are used to encrypt the data, and is also used for authentication.
- Enterprise mode (WPA-Enterprise or WPA2-Enterprise). Enterprise mode is used for larger wireless networks. Rather than using a pre-shared key, the Enterprise mode uses a separate authentication server (which may be a standalone network device, software running on a server, or part of the access point) to provide authentication services and to generate unique master keys for each station. The authentication server uses the IEEE 802.1X standard for port security to pass these keys to the stations lets the authentication server generate unique keys for each station, which are then used by TKIP to generate the dynamic keys used to encrypt data.

The problem with WPA-PSK and WPA2-PSK encryption is the Pre-Shared Key, primarily because it is a single point of failure for network security. If a hacker knows the PSK, he can easily determine everything else he needs to access your network and steal your data. PSK security issues include:

- If the PSK is less than 20 characters long, hackers can relatively easily determine the PSK with dictionary attacks (software based attacks in which likely to succeed combinations of letters, such as English words, are continually sent to the computer until

the correct PSK is guessed). The solution, of course, is to use a PSK that is longer than 20 characters, but unfortunately, the WPA-PSK and WPA2-PSK specifications do not enforce this type of security.

- The PSK is a potential security hole if you have a disgruntled ex-employee, since such a person could potentially know the PSK and use it to access your network for malicious purposes. In order to prevent this type of problem, you need to change the PSK in each of your wireless devices every time an employee leaves the company.
- One of the advantages of 802.11 networks is that they allow guests to temporarily connect to your network. But with WPA-PSK, this type of temporary connection is only possible if you reveal the PSK to your guests, which is clearly a security problem.

Because of these issues, WPA-PSK or WPA2-PSK should only be used for small home networks. For businesses, WPA-Enterprise and WPA2-Enterprise provide vastly superior security, as well as better management capabilities, through the use of the robust field-proven IEEE 802.1X standard and the RADIUS authentication server technology.

In WPA-Enterprise and WPA2-Enterprise networks, there three basic types of devices with roles defined by 802.1X (see figure 1):

- Supplicants. Supplicants include client devices like PCs, printers, and device servers.
- Authenticator. The authenticator enforces authentication before allowing a supplicant to access network services. It passes authentication requests and responses to and supplicants and the authentication server. The authenticator is usually the access point.
- Authentication Server. The authentication server is a special network server that contains a list of all users and their credentials. It works on behalf of the authenticator by verifying the user's credentials whenever a supplicant attempts to connect to the network. The authentication server can be implemented as software on one of your servers (for example, Microsoft's IAS software), as a dedicated network device, or as an embedded part of the access point. RADIUS (Remote Authentication Dial-in User Service) servers are generally used with WPA-Enterprise and WPA2-Enterprise, although other types of authentication servers are also allowable.

A big advantage of WPA-Enterprise and WPA2-Enterprise is that the authentication server with 802.1X provides a unique master key to the client upon completion of the authentication process. This eliminates the problems with the Pre-Shared Key used in WPA-PSK and WPA2-PSK, since there is no single key for the entire network. An added benefit is that the keys are much easier to manage on large networks, since you don't need to manually enter the keys into each wireless device.

802.1X is based on a protocol called EAP (Extensible Authentication Protocol). EAP is not actually an authentication protocol in itself, but rather is a low-level transport protocol that does not use TCP/IP and is designed to be used in conjunction with a variety of different authentication protocols. This gives 802.1X (and consequently, WPA, WPA2, and 802.11b) the flexibility to handle new authentication capabilities as they emerge in the future.

Basically, whenever a client (supplicant) attempts to connect with an access point (authenticator), the access point enables a port that only allows EAP packets to pass from the client to the authentication server (i.e., no TCP/IP, HTTP, SNMP, etc. is allowed). Upon request from the authentication server, the client then forwards its identity and credentials to the authentication server. When the authentication server successfully authenticates the client, it then notifies the client and allows the access point to allow non-EAP traffic.

The WPA and WPA2 standards allow for five different types of EAP authentication:

- EAP-TLS. EAP-TLS is the most commonly supported type of EAP. It is very secure (it is based on the same protocol used for secure Web traffic via the SSL protocol), because a

valid digital certificate is required on both the authentication server and the client (a digital certificate is a digital identity that is generally signed by a trusted third party known as a certificate authority) and because it supports mutual authentication of the server and the client. However, the requirement for digital certificates means that you will need to support a public key infrastructure (PKI) to manage the certificates, keys, and authorities.

- PEAPv0/EAP-MSCHAPv2. This is the EAP type that is supported by Microsoft. It creates an encrypted logical link between the client and the access point known as a tunnel, which encapsulates data and protocol information into TC/IP packets. The EAP-MSCHAPv2 authentication protocol runs in this tunnel. A digital certificate is required on the authentication server, and mutual authentication is supported. Although there are several versions of PEAP, PEAPv0/EAP-MSCHAPv2 is so popular that it is commonly referred to as simply "PEAP".
- EAP-TTLS/MSCHAPv2. EAP-TTLS was invented by Funk Software, and it creates a similar secure tunnel as PEAP. It is actually more flexible than PEAP because the protocols that run in the tunnel do not have to be EAP protocols (note that PEAPv0/EAP-MSCHAPv2 runs the EAP version of MSCHAPv2, while EAP-TTLS/MSCHAPv2 runs the original version of MSCHAPv2. However, even though it was introduced before PEAPv0, it is much less popular (due to Microsoft's marketing muscle).
- PEAPv1/EAP-GTC. PEAPv1/EAP-GTC was developed by Cisco, and was designed with Generic Token Cards in mind (token cards are hardware devices, like smart cards or USB dongles that contain a user's digital credentials). Because it supports logon passwords and one-time passwords, it works with the broadest range of user password databases, including LDAP and NDS (MSCHAPv2 is primarily limited primarily to Windows NT Domain and Active Directory). Cisco has not actively promoted this EAP type, however, so it has not yet had widespread usage.
- EAP-SIM. EAP-SIM is designed for use with GSM Subscriber Identity Modules, in order to provide a seamless authentication for users roaming between GSM cellular networks and Wi-Fi 802.11 wireless local area networks.

Other types of EAP include:

- Lightweight Extensible Authentication Protocol (LEAP). LEAP is Cisco's proprietary authentication. It utilizes usernames and passwords, and is no longer considered very secure.
- EAP-FAST. LEAP-FAST is another Cisco proprietary authentication standard that uses a TLS. It is designed to fix the problems with LEAP, and it optionally supports the use of server certificates.
- EAP-MD5 uses username/password authentication for clients. It is vulnerable to dictionary attacks and is uncommonly used in wireless local area network authentication.

## **Other Ways to Secure a Wireless Network**

In addition to 802.1X and EAP with RADIUS servers, there are other methods for secure authentication. Kerberos, for example, was one of the first authentication protocols, and it is still in use today. However, vendors have abandoned support for Kerberos in favor of more modern protocols, so it is probably not a good idea to implement Kerberos for new wireless network installations.

Some networks have implemented virtual private network (VPN) connectivity with IPsec between wireless devices and the wired network. However, VPNs offer no security advantages compared to WPA or WPA2, and they have a number of drawbacks, including lack of transparent operation

(a user has to manually connect to the VPN server), no security on the wireless LAN (the data in the tunnel is secure, but there is nothing to prevent unauthorized users from connecting to the wireless LAN), poorer roaming capabilities (VPN sessions can timeout), higher costs (a VPN server may be required for each site), and lower performance.

## **Summary**

Wireless networks are very vulnerable to unauthorized users. Fortunately, the latest wireless security standards are quite solid. If you have a new network, you should implement the WPA2-Enterprise standard because of its superior capabilities and better protection against intruders. Otherwise, implement the WPA-Enterprise standard on legacy equipment wherever possible. Older devices that cannot support WPA should ideally be replaced, but WEP security should be enabled on them if replacement is not an option. Remember, your network's security is only as strong as the weakest link.