Securing Wi-Fi Wireless Networks with Today's Technologies

Wi-Fi Alliance
February 6, 2003

Executive Summary

Over the past few years, the popularity of Wi-Fi networking has grown spectacularly. "Going wireless" is becoming mainstream and the costs of implementing Wi-Fi have dropped dramatically. But just as the popularity of Wi-Fi is growing, so are the well-documented security concerns of wireless networks. Wi-Fi's native security mechanism, WEP, while still useful for home networking and other light security needs, was proven insufficient for enterprise class networking. Some corporate networks have overcome the problems posed by WEP by deploying complementary technologies to strengthen Wi-Fi's native security to a level suitable for enterprise class protection.

This paper will provide a background and history of Wi-Fi and its security evolution. It will explore the means of securing Wi-Fi with complementary technologies such as Virtual Private Networking (VPN), 802.1X, the Extensible Authentication Protocol (EAP) and RADIUS. In addition, the paper will offer a glimpse into the future of native Wi-Fi security, Wi-Fi Protected Access (WPA) and 802.11i.

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless local area network products based on IEEE 802.11 specifications. Wi-Fi product certification began in March of 2000. One of the goals of the Wi-Fi Alliance is to ensure that consumers realize maximum benefit from their Wi-Fi products in a secure and productive environment.

Table of Contents

I. Introduction

Few subjects have commanded as much attention in the international discussion of how to secure digital assets as the issue of securing wireless local area networks (WLANs). The inherent vulnerability of networks that transmit data across radio waves, the ease with which researchers have cracked the scheme designed to secure WLANs, and stories of "war driving" hackers who penetrate corporate networks using little more than laptops with antennas fashioned from Pringles® cans have made wireless security one of the hottest issues on the international technology agenda.

Not only is it possible to run wireless networks securely, it can be achieved in a relatively straightforward fashion using existing technologies, including the encryption scheme built into the 802.11 specification (Wired Equivalent Privacy or WEP) for the manufacture of WLAN devices. The specification and its selection of encryption technologies were deliberately designed to meet the export restrictions of the US government at that time.

That mandate has changed. Today, it is the weakness of the encryption algorithm designed to protect wireless technology—not its export from the US—that tops worldwide security concerns.

This paper presents an overview of the issues involved in securing WLAN devices, the technologies that are available to secure WLANs now, and the emerging standards that will enhance the range of security options available to consumers in the future.

Table I. Poised for Growth

Wi-Fi interoperability, standardization, volume production, demand and competition have driven WLAN product pricing to a level that anyone can afford. By 2002, the worldwide market reached nearly $2 billion in sales. Gartner Inc. estimates it will reach nearly $5 billion by 2006.

The market is poised for even greater growth with the recent introduction of higher-speed 802.11a products, and in the future with 2.4 GHz-based 802.11g products, which will both operate at 54Mbps as compared to 802.11b's 11 Mbps data rate.

All Wi-Fi CERTIFIED wireless LAN technology specifications share that same security solution.

A Short History of WLANs

A WLAN is exactly what its name implies—a local area network with no wires. Unlike wired networks in which workstations (or clients) send and retrieve data across cables, a wireless network uses the radio waves. Wireless LANs communicate via the 2.4 GHz or 5 GHz band—the unlicensed Industrial, Scientific, and Medical (ISM) radio band where cordless phones, microwave ovens, infant monitors, and other personal and household devices also operate.

It was not until 1997, when the Institute of Electrical and Electronics Engineers (IEEE) released the 802.11 specification for the manufacture of WLAN devices operating in the 2.4 GHz spectrum, that an industry standard for WLAN operation was established. These WLANs ran at speeds of 1 and 2 Mbps (megabits per second)—useful for certain applications, but far slower than their wired Ethernet counterparts that runs at 10 and 100 Mbps. Two years later, the 802.11b enhancement increased the data rates to 11 Mbps and put WLANs on par with their wired cousins. That year, several industry players,[1] realizing that the technology was now mature and fast enough for mainstream applications, formed the Wireless Ethernet Compatibility Alliance (now renamed the Wi-Fi Alliance) to ensure the rapid adoption of these 802.11b-based products. The association created the Wi-Fi (Wireless Fidelity) logo to indicate that a product had been certified for interoperability. The Wi-Fi CERTIFIED logo ensured rapid adoption of 802.11b-based products and opened the door to a market explosion of Wi-Fi products in

both home and enterprise. In 2002, the Wi-Fi Alliance began certification of 802.11a products.

The 802.11 standard includes an encryption mechanism designed to secure the data being transmitted wirelessly. That mechanism, Wired Equivalent Privacy (WEP), was intended to make a WLAN as secure as an unsecured wired network. When WEP was designed it was required to comply with US government export restrictions for encryption technology. The government has since lifted these original restrictions.

Open by Design

By their very design, WLANs afford open access. Similar to cordless phones, they use radio waves to transport data. Unless security is enabled, these signals can be readily intercepted by nearby receivers. However, because the default settings on wireless access points, Small Office/Home Office (SOHO) gateways, and wireless network interface cards (NICs) are designed to ensure simple, out-of-box operation, security features are typically not enabled at the factory. Customers can easily and successfully set up a WLAN in its default configuration. It is up to the customer to apply the means of locking out intruders.

Just as the security for an international bank in Singapore or the US gold reserves at Ft. Knox differs from the home security requirements of a typical residence, each network's security configuration should also differ. The Wi-Fi Alliance recommends that network managers and even home users do a risk assessment and select appropriate security according to the sensitivity of their data and the likelihood of an attack. Security is a personal decision.

For most home or SOHO environments, where the WLAN primarily serves entertainment, research, and personal and business needs of a less sensitive nature, WEP provides adequate security to deter the casual intruder. This is particularly true when it is used with other inexpensive (and frequently built-in) security measures such as firewalls and anti-virus software. By contrast, large business enterprise networks typically require a much higher level of security. This can be achieved using advanced and proven security technologies that are widely available today.

Choosing an appropriate solution requires an understanding of how WLANs work and what makes them vulnerable.

How WLANs Work

A WLAN uses radio waves to communicate among devices. An access point (AP) with an antenna is physically connected to a conventional wired Ethernet network and serves as a bridge to the wireless network. Wi-Fi WLANs also support communications among the client systems, allowing the devices to communicate directly with one another in a peer-to-peer fashion.

Up to approximately 150 feet, a Wi-Fi 802.11b WLAN typically can deliver broadband performance with a signaling speed of up to 11 Mbps. Beyond that distance, it can operate at fallback speeds of 5.5 Mbps, 2 Mbps and 1 Mbps. At these lower speeds the signal can travel as far as 1,500 feet. Directional antennas can be used to extend the range significantly. Actual performance depends upon the signal pattern and the number of walls, floors and other architectural obstacles in the area. Wi-Fi 802.11a WLANs can achieve speeds of up to 54 Mbps within a somewhat reduced range.

In order to indicate its presence to wireless clients in its listening area, an AP announces itself by beaconing, or broadcasting, a Service Set Identifier (SSID) approximately 10 times per second. The SSID identifies the name of the network. PCs that are within

range and equipped with a wireless network interface card can receive the SSID, associate with the WLAN and request an IP address that will allow them to connect to the local network, surf the Internet, and view network folders.

II. The Challenges

The open broadcast of the SSID and the ease with which a mobile PC, laptop or handheld computing device equipped with a wireless NIC can associate with an unsecured WLAN spawned a hacker movement known as "war driving" that has achieved significant press.

"War" Culture

War driving is the practice of driving in a car with a Global Positioning System (GPS), a laptop equipped with a wireless NIC and an antenna to document the location of WLANs. War driving derives its name from the movie, *War Games*, in which hackers found networks by "war dialing," randomly dialing telephone numbers until a modem answers.

Figure 1. War chalking

War drivers spawned "war chalkers" who chalk buildings or sidewalks with back-to-back Cs, or open circles, to alert other hackers to a WLANs presence. It has also given rise to "war flyers" that employ small airplanes to pinpoint WLAN locations with the additional assistance of a GPS receiver. The locations of the WLANs that are discovered, and their corresponding SSIDs, are published in databases on the Internet.

However, WLANs are not necessarily at risk simply because their SSIDs and locations are known to the public. Reports of the number of Wi-Fi WLANs "seen" in war driving expeditions have resulted in inflated estimates of security oversights and fed public confusion about the issue. Simply "seeing" a network name and determining that the network has not enabled WEP does not mean a security risk exists. At a minimum it means that the network is broadcasting an SSID. Whether the network is secured is a completely different issue.

What these reports fail to acknowledge is that many of the enterprise networks are actually secured by proven technologies, some of which are discussed here. Others, such as those operated by Elektrosmog and NYCWireless, are intentionally left open as a public service. Unfortunately though, there are individuals and organizations that do not secure their wireless network. It is very important that these networks be secured unless they are intentionally left "open."

Encryption and Authentication

The two primary means of securing a network are encryption and authentication. Encryption is a means of disguising, or scrambling, messages according to a secret key known only to the sender and receiver. Authentication is a means of ensuring that users are who they say they are before they are authorized to access the network. Both should be present in an enterprise-class security solution. And, ideally, the methods should work together and complement each other.

Virtually any encryption scheme can be broken if a hacker has the time and resources to gather a sufficient amount of data that can be analyzed to deduce the secret key. Keys are determined by algorithms that specify the length and content of the key or how often the key is changed, or both. As a rule of thumb, as the key size lengthens, a greater amount of data must be collected and analyzed in order to correctly deduce it. The ability

to eventually "hack" an encryption method is the primary reason that security should be a constantly evolving technology.

Similarly, the shorter the amount of time that is allowed before the key is changed, the less likely it becomes that the data can be analyzed and the key deduced. This compares to the proverbial "needle in a haystack." If you think of the shared secret key as the "needle" that is being hunted, a long key length and a short duration of time before the key is regenerated significantly increases the size of the haystack.

Although authentication schemes vary widely, all provide a method of credential-checking—requiring a user name and password, for instance, or a digital certificate. Credentials are checked against an authentication server that determines their validity before granting a user access to the network. It is important that the scheme for proving identity cannot be easily counterfeited or "spoofed."

WEP and its Weaknesses

Not long after WEP was developed, a series of independent research studies began to expose its cryptographic weaknesses. The first practical attack on WEP was identified by researchers Scott Fluhrer, Itsik Mantin and Adi Shamir who found that, even with WEP enabled, third parties with a moderate amount of technical know-how and resources could breach WLAN security. Three key difficulties were identified:

1. WEP uses a single, static shared key. It remains the same unless a network administrator manually changes it on all devices in the WLAN, a task that becomes ever more daunting as the size of the WLAN increases.
2. At the time of its introduction, WEP employed a necessarily short 40-bit encryption scheme. The scheme was the maximum allowed by US export standards at that time. In 1997, the US government deemed the export of data cryptography to be as threatening to national security as the export of weapons of mass destruction. By necessity, Wi-Fi security had to be weak if the specification was to be adopted as an international standard and if products were to be freely exported.
3. Other technical problems contributed to its vulnerability, including attacks that could lead to the recovery of the WEP key itself. [2]

Together, these issues exposed that WEP was not sufficient for enterprise-class security.

III. Current Solutions

Concerned that WEP encryption was not enough, several vendors introduced longer 128- or 152-bit, and even 256-bit keys. However, as the 802.11 standard only called for 40-bit WEP, these longer key variations were proprietary and often not interoperable. Because they were not part of a standard, the Wi-Fi Alliance did not do interoperability testing on them. Finally, it was proven that, due to technical problems within WEP, the longer keys added no significant protection.

It was understood that additional proven security technologies must be added to achieve acceptable levels of security for Wi-Fi networks in the enterprise. Proven technologies such as Virtual Private Networks (VPNs) and Remote Access Dial-In User Service (RADIUS) authentication servers were deployed to extend the high levels of security they provided on wired networks to WLANs in corporate settings.

These can be deployed today in a variety of configurations to provide improved security in an enterprise setting.

Table 2. Home and SOHO Security

SOHO users can use options that are built into the equipment to ensure that the network is not broadcasting "in the clear." These include:

- Enable WEP encryption. WEP remains a useful method to deflect the casual attacks commonly made against home and small business networks.
- Use Media Access Control (MAC) filtering. On a WLAN, a MAC address is a unique hardware number, or 12-digit address, of the wireless NIC. The MAC addresses of authorized hardware devices can be entered into a "permit" list against which the AP reviews and filters requests for access. MAC address filtering, however, is neither part of the 802.11 standard nor tested by the Wi-Fi Alliance for interoperability.

VPNs

Virtual Private Network technology (VPN) has been used to secure communications among remote locations via the Internet since the 1990s. A familiar and already widely used technology in the enterprise, it can readily be extended to Wi-Fi WLAN segments on existing wired networks. Although VPNs were originally developed to provide point-to-point encryption for long Internet connections between remote users and their corporate networks, they have recently been deployed in conjunction with Wi-Fi WLANs.

When a WLAN client uses a VPN tunnel, communications data remains encrypted until it reaches the VPN gateway, which sits behind the wireless AP. Thus, intruders are effectively blocked from intercepting all network communications. Since the VPN encrypts the entire link from the PC to the VPN gateway in the heart of the corporate network, the wireless network segment between the PC and the AP is also encrypted. This is why VPNs have been recommended to help secure Wi-Fi.

While VPNs are generally considered an enterprise solution, integrated products that offer VPN pass-through connections, firewalls and routers are available to accommodate telecommuters who work from home. Although they provide excellent security, VPNs are not self-managing. User credentials and, often, VPN software must be distributed to each client. However, when properly installed, VPNs extend the high level of security they provide on wired networks to WLANs. In fact, some Wi-Fi vendors themselves have utilized VPNs in networks to secure their own internal Wi-Fi networks.

802.1X

Where VPN represents an excellent extension of a proven wired security technology to wireless networks, 802.1X represents a different approach to wireless security. Like VPNs, 802.1X was originally designed for wired networks. Approved in August 2001, it leverages the success of RADIUS authentication servers to provide a higher level of security for WLAN users. Since its adoption by the IEEE, it has received widespread industry support.

Also known as port-based network access control, 802.1X uses the Extensible Authentication Protocol (EAP) and RADIUS to authenticate clients and distribute keys.

EAP provides an infrastructure that allows users to authenticate to a central authentication server. When the server accepts proof of the client's identity, keying material is sent to both the client and the APs with which the authentication server enjoys a previously established "trusted relationship." This relationship and the use of "mutual authentication"—in which the clients and the server prove their identities to each other—ensures that the APs that are on the network are the ones that are supposed to be there and protects clients from communicating with rogue APs.

802.1X and EAP also ensure that new encryption keys are generated and distributed frequently. This frequent distribution is known as "dynamic key" distribution, an essential element in a good security solution. By minimizing the time period in which any one encryption key is used, 802.1X and EAP reduce the time in which data can be collected to deduce the key. It effectively foils an eavesdropper by dramatically shrinking the size of the data set that can be collected to break an encryption key.

A wide number of EAP implementations have been proposed for use in the market, including EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected Extensible Authentication Protocol (PEAP). Several of these have been proposed as standards and are under review by the Internet Engineering Task Force (IETF). As these protocols gain multivendor support, some of these will eventually be recognized as IETF standards.

IV. The Future

Though the above-mentioned existing technologies are indeed useful for helping secure Wi-Fi, the Wi-Fi Alliance and IEEE have both realized the importance of security enhancements to Wi-Fi itself. Two important initiatives—the proposed 802.11i standard expected to be adopted by the IEEE in 2003 and Wi-Fi Protected Access, which has been recently announced by the Wi-Fi Alliance—are worthy of discussion:

802.11i

Task Group i within IEEE 802.11, is developing a new standard for WLAN security. Expected to be released by the end of 2003, the proposed 802.11i standard is designed to embrace the authentication scheme of 802.1X and EAP while adding enhanced security features, including a new encryption scheme and dynamic key distribution. Not only does it fix WEP, it takes WLAN security to a higher level.

The proposed specification uses the Temporal Key Integrity Protocol (TKIP) to produce a 128-bit "temporal key" that allows different stations to use different keys to encrypt data. TKIP introduces a sophisticated key generation function, which encrypts every data packet sent over the air with its own unique encryption key. Consequently, TKIP greatly increases the complexity and difficulty of decoding the keys. Intruders simply are not allowed enough time to collect sufficient data to decipher the key.

802.11i also endorses the Advanced Encryption Standard (AES) as a replacement for WEP encryption. AES has already been adopted as an official government standard by the U.S. Department of Commerce. It uses a mathematical ciphering algorithm that employs variable key sizes of 128-, 192- or 256-bits, making it far more difficult to decipher than WEP. AES, however, is not readily compatible with today's Wi-Fi CERTIFIED WLAN devices. It requires new chipsets, which, for WLAN customers, means new investments in wireless devices. Those looking to build new WLANs will find it attractive. Those with previously installed wireless networks must justify whether AES security is worth the cost of replacing equipment.

Wi-Fi Protected Access

The Wi-Fi Alliance is addressing the need for an immediate, software-upgradeable security solution. Realizing the importance of enhanced Wi-Fi security, the Alliance has led an effort to bring strongly improved, interoperable Wi-Fi security to market early this year. The result of that effort is Wi-Fi Protected Access.

Wi-Fi Protected Access is a specification of standards-based, interoperable security enhancements that strongly increase the level of encryption and authentication for existing and future wireless LAN systems. Wi-Fi Protected Access is derived from the upcoming IEEE 802.11i standard and will be forward compatible with it.

Wi-Fi Protected Access addresses the vulnerabilities of WEP encryption and adds user authentication. Thus, Wi-Fi Protected Access will provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network. Significantly, it is designed as a software upgrade to Wi-Fi CERTIFIED devices, requiring no additional hardware.

Wi-Fi Protected Access includes 802.1X and TKIP technology. Cryptographers working with the Wi-Fi Alliance have reviewed Wi-Fi Protected Access and endorsed the fact that it solves all of WEP's known vulnerabilities. Wi-Fi Protected Access support will be available from vendors of WLAN equipment in early 2003. The Wi-Fi Alliance is planning to begin interoperability certification testing on Wi-Fi Protected Access at roughly the same time.

As Wi-Fi interoperable solutions improve, users might find that the expense and complexity of add-on solutions such as VPNs is no longer necessary—at least not for the express purpose of securing the wireless link in a Wi-Fi network. The future holds that promise in the form of 802.11i and Wi-Fi Protected Access.

---

[1] The Wireless Ethernet Compatibility Alliance (WECA) was formed by 3Com, Aironet (now Cisco) Harris Semiconductor (now Intersil), Lucent Technologies (now Agere), Nokia and Symbol Technologies in August of 1999. WECA was renamed the Wi-Fi Alliance in October of 2002.

2 These issues with WEP have been addressed by the introduction of Wi-Fi Protected Access.