802.11: Are You Sure You're Secure?

by Gary Audin
Delphi, Inc.

Attacking computer networks is a challenge for some, a business for others, and a hobby for many. Why break into a network at all? Motivations may be political, social, religious, economic, a result of boredom, or simply satisfying a need to feel superior. Whatever the motivation, time, money, and staff must be devoted to increasing network security. While wired networks and their computers are the usual targets for security attacks, wireless networks have the same problems, but also add new dimensions to the security factor. As pointed out in war-driving events, most enterprises do not adequately configure and activate the security features that are already available to them.

War Driving

War driving is an effort by individuals with wireless devices, usually laptops, to drive around in their cars and trucks attempting to connect themselves, as authorized users, to wireless networks. The First Worldwide War Drive was held from August 31 to September 7, 2002. The Second Worldwide War Drive followed quickly, during the week of October 26 to November 2, 2002. The war drive is an effort, supported by security professionals and hobbyists, to create awareness for users, encouraging them to secure their access points (APs). The war drive (www.worldwidewardrive.org/) collected and analyzed statistics relating to the ease of access to wireless networks. The November drive located 24,958 access points at risk for security breaches. The results of this war drive are summarized in Table 1. The study concluded that:

- users do not use the security features that they already own;
- those who do use the available security features adopt the default settings for the service set identifier(SSID), like everyone else, making the SSID a useless identifier;
- very few users are expending any effort to discover whether their networks are secure.

Table 1: Worldwide War Drive (November 2002).

Category	Total APs	Percentage
WEP Enabled	6,970	27.92
No WEP Enabled	17,988	72.07
Default SSID	8,802	35.27
Default SSID and No WEP Enabled	7,847	31.44
Most Common SSID Used	5,310	21.28
2nd Most Common SSID Used	2,048	8.21

What's Next? 802.11i

Improving WLAN security is an ongoing debate. The IEEE is close to completing the 802.11i standard. This standard, known as the robust security network (RSN) feature, is one that many in the industry want to adopt. RSN works, however, only when the WLAN has completely transitioned to the standard.

RSN defines two security networks: The legacy method is hardware based on RC4 (see Wireless Dictionary at left for acronyms). The newer hardware

method is based on the advanced encryption standard (AES). The AES standard has an open format that will allow new methodologies to be incorporated as they are developed. RSN uses the IEEE 802.1x LAN port authentication standard to authenticate wireless devices and to provide dynamic keys for encryption.

The migration effort to RSN includes the concept of a transition security network (TSN). The standard states that a TSN is insecure, because the pre-RSN equipment can compromise the larger network. Access points broadcast and multicast packets using the weakest configured security methods: WEP (wired equivalent privacy), or TKEP (RSN + RC4), or CCMP (RSN + AES). Critics point out that the IEEE 802.11i standard provides only legacy approaches to authentication, key distribution, and data confidentiality.

Cisco-Compatible vs. Wi-Fi Certified

If the lack of standards implementation and emerging standards were not enough, consider Cisco's announcements in February 2003. Cisco is offering to license, free of charge, its WLAN security suite to chip vendors and WLAN network interface card manufacturers. This is good... and bad. Cisco has seen the weaknesses of WEP and has been a leader in plugging the gaps. Because Cisco has more than 30 percent of the WLAN market, many users will take advantage of its security improvements. Many may have already done so. These security strengths have helped keep the WLAN market going. The WLAN market could benefit by using the Cisco technologies at no cost.

The other side of the argument sees Cisco as trying to circumvent the 802.11i standard. The standard, as supported by the Wi-Fi Alliance, will be defined as Wi-Fi protected access (WPA). This circumventing of the standard would allow products supporting WPA to be stamped "Wi-Fi Certified." We can expect subsequent levels of certification, such as WPA2, WPA3, and so on, to be introduced. Symbol and Proxim have already announced WPA compliance.

This leaves the WLAN industry with two competing and incompatible approaches: Cisco compatible vs. WPA compatible. The Cisco version uses a proprietary authentication protocol called LEAP. LEAP is Cisco's version of extensible authentication protocol (EAP). LEAP has already been licensed to Apple, Interlink, LXE, and Funk Networks. The question then arises: Is this a generous gesture or an effort to dominate the WLAN market through security features? We need to watch this competition as well as the reaction of WPA-compliant vendors.

What Can You Do to Improve WLAN Security?

First, understand that WLAN security is a moving target. The tools, techniques, and methodologies that exist have weaknesses. However, if the security tools are *not* used, there is no security. The user organization that says "We have not had a security breach" should finish the sentence with "that we know of." Undetected breaches will be hard to quantify and even harder to prevent. Security is like insurance; you don't want to collect on the policy, but you also don't know if you have enough coverage until it is too late.

Much has been published on the subject of network security. There are many products, standards, methodologies, and techniques that cover the network itself. WLAN security is really dealing with the data-link (OSI Layer 2) and physical (Layer 1) aspects of network security. In wired networks, there is some semblance of security because of the physical nature of the cabling. The user authentication and authorization can be related to a fixed physical cable, port, and connection. The wired devices are immobile. The protocol support at Layer 2 (data link) is very similar, if not the same, for both wired and wireless networks. You must de-encrypt Layer 2, or else you must have all devices use the same encryption key when initially accessing the network. I recommend that you not encrypt the Ethernet protocol. If you do, then everyone has to have the same key—which compromises the security of the network.

Anything that increases the time it takes to break into a network improves security—maybe a little, maybe a lot—and is worth implementing. My recommendations include the following:

- *Service set identifier.* Make it more difficult to access the network by picking an unusual network name or SSID, and do not distribute it widely. *Do not* use the defaults. Turn off the SSID broadcast. Doing this may at least slow down initial intrusion attempts.
- *802.11x* . Buy the additional hardware and software to implement this standard.
- *WEP.* If you do not, or cannot, implement 802.11x, at least effect WEP. As stated earlier, WEP is not perfect, but it will make it harder to breach the network. Unfortunately, free WEP-cracking tools, such as WEPCrack and AirSnort, are readily available on the Internet. Try these against your own network to see how secure it is against attacks from these sources. Changing keys frequently will help make it more difficult to continuously hack into a network. *Never* distribute new key

information over the network. Find a secure method to distribute key information manually.

- *RADIUS.* Implement this authentication protocol. A RADIUS server can be used for both wired and wireless networks.
- *Windows 2000.* Use the Internet Access Service (IAS) server option that comes from Microsoft. It has to be installed and configured before use; it is not part of the initial setup.
- *Windows XP.* This is an operating system that supports 802.1x and provides a native client that can take advantage of IAS for wired and wireless LAN security service.
- *Extensible authentication protocol* . Supported by IAS, versions include EAP-TLS (EAP with transport layer security), PEAP (protected EAP), and PEAP with EAP-MS-CHAP. All of these improve upon and make up for the deficiencies of EAP.
- *Firewalls.* Provide a boundary that, when placed between the WLAN and the wired LAN, will prevent most attacks from penetrating the wired resources.
- *IP address.* Make each of the wireless device's IP address static and turn off the dynamic host configuration protocol (DHCP) on the access point.
- *MAC address.* Require a legal address for access. This will make it more difficult to even begin an illegal authentication.
- *VPN tunneling.* This is a technique in which users' packets are wrapped in protected network packets commonly using IPsec.
- *Diversifying antenna locations.* This technique allows a single radio to use two or more antennas. The best antenna location will be automatically chosen for access. This can help prevent a denial-of-service attack.
- *Distance is not enough.* Assuming the signal will be too weak from hundreds of feet away is not a valid supposition. By rotating the antennas, the location of users and their distance from the AP can be extended. A recent vendor announcement described a phased array antenna, an electronically (not mechanical) rotatable antenna that can focus signals and increase the distance for 802.11 devices to 900 feet.
- *Disabling the stolen device.* This is a newer idea wherein a central authority downloads an internal code that triggers a disabling function and renders the stolen device useless.
- *Identifying rogue access points.* An unauthorized AP does not usually conform to the security policies that have been established. Sniffing tools such as AirMagnet or NetStumber can be used to detect security breaches of this type. AirWave can provide centralized monitoring.

Planning and Policing Security

Defense in depth, a common term in the security industry, is a multilayered security architecture that combines security tools with good management. In addition to the recommendations above, some nontechnical measures must also be implemented. Consider the following three important components of a well-managed nontechnical approach to security:

First, establish a security team of at least two people, never just one person, in order to have a system of checks and balances. You may even want to establish a chief security officer for all network and computer security.

Next, create, publish, and distribute policies that are well written, that define acceptable resource usage, and that will ensure that users understand what the potential threats may produce.

Finally, train, train, train the users and especially the first responders to a security breach.

The goals of a well-organized security team are prevention, detection, and reaction. *Prevention* requires strong user authentication, authorization and access control, good software patch management, configuration management, and recurring verifications that the security tools are working properly.

Detection of breaches or attempts on your system means you are successfully identifying threats with firewalls, intrusion-detection systems, and activity logging.

Reaction should be swift and sure. The security response team must always be ready to react immediately to isolate the problem and limit the liabilities. They must also have the tools necessary to produce evidence of the intrusion.

Typically, those who manage networks do not have a security background. Since September 11, 2001, the necessity for increased security in just about every aspect of our lives has been obvious to us all. Planet3 Wireless (www.cwne.com) is one company that offers training and certification for network professionals. Their Certified Wireless Security Professional (CWSP™) program will be available by mid-2003. The training covers WLAN intrusion, security policy, and security solutions.

In an article that appeared in the February 2003 issue of *Security Insight*, Pete Lindstrom expressed the following five DON'Ts of network security:

1. Don't say "No" to new technology.
2. Don't assume a high-security, low-risk posture; balance benefits and risk.
3. Don't react without thinking.

4. Don't neglect valuation of information assets.

5. Don't focus on the trees and ignore the forest.

When you build a WLAN you can generally close the closet door. You need only inspect it occasionally. Building a *secure* WLAN requires that you go into the closet every day. How can you know what has changed since yesterday unless you look?

Gary Audin is president of Delphi, Inc., a consulting firm based in Arlington, Virginia. A familiar face to ACUTA, he has spoken at numerous ACUTA events. Reach Gary at delphi-inc@att.net or 973/492-5655.

Reprinted with permission from The ACUTA Journal of Communications Technology in Higher Education, *Volume 7, No. 2, Summer, 2003. To learn more about ACUTA, visit us at www.acuta.org.*