
Wireless Security: Here We Go Again

Aldora Louw and William A. Yarberry, Jr.

Wireless LANs and wireless applications are springing up in organizations everywhere. Their usefulness is undeniable, but do they put an organization's information at risk? The authors say yes. But, they add, IT organizations have dealt with this kind of vulnerability before.

Ronald Reagan's famous rejoinder in the 1980 presidential debates — "There you go again" — applies equally well to wireless security. In the early days of personal computers, professional IT staff were alarmed at the uncontrolled, ad hoc, and unsecured networks that began to spring up. PCs were bought by users out of "miscellaneous supplies" budgets. The VP of Information Systems had no reliable inventory of these new devices; and certainly corporate data was not particularly secure or backed up on the primitive hard drives. Now, 20 years later, we have architectures and systems to control traditional networked systems.

Unfortunately, history is repeating itself with wireless LANs and wireless applications. It is convenient to set up a wireless LAN or an application that uses wireless technology; however, the convenience means that sometimes wireless technology is spreading throughout organizations without oversight or adequate security functions. CIOs today, like VPs of Information

Systems 20 years ago, are missing key information. Where are the wireless devices? Are they secure? Exacerbating the problem of wireless security is the general lack of awareness of the risks. Interception and even spoofing are easier over the airwaves than with cables — simply because it is not necessary to get physical access to a conduit in order to tap into the information flow.

Background

Like old cities developed around cow-paths, wireless technology meanders around a confusing history of regulations, evolving and proprietary standards, a plethora of protocols, and ever smaller/faster hardware.

To simplify this discussion, a "wireless" transmission is one that does not travel through a wire. This approach is not as dull-witted as it would seem. The media focus so much on the newer technologies, such as Bluetooth, that traditional wireless communications — microwave, satellite, and radio transmissions — are often ignored.

Regardless of the precise definition of "wireless," it is clear that the technology is growing quickly. In his book *The Wireless Web*, Frank Coyle estimates that 90 percent of the smart phones shipped to the United States and Western Europe will be WAP (Wireless Application Protocol) enabled by 2003. Following are some of the key protocols and standards that are driving the industry.

Aldora Louw, CISA, is a senior associate in PricewaterhouseCooper's Global Risk Management Solutions group and is based in Houston, Texas. She can be reached at aldora.louw@us.pwcglobal.com.

William A. Yarberry, Jr., CPA, CISA, is a telecommunications consultant and technical writer based in Houston, Texas (billyarberry@bigfoot.com).

Standards and protocols (software)

802.11b (Evolving to 802.11g). This specification is today's choice for wireless LAN communications. Based on work by the IEEE, 802.11b uses radio frequencies to transmit higher-level protocols, such as IP. Wireless LANs are convenient and quick to set up. Applications, servers, and other devices see the traffic going over the airwaves as no different than wire-based Ethernet packets. In a typical wireless LAN, a transmitter/receiver device, such as that shown in [Exhibit 1](#), connects to the wired network at a fixed location. An alternative to the fixed access point is the ad hoc network that uses devices such as notebook PCs equipped with wireless adaptor cards to communicate with each other via peer-to-peer transmissions. The recently adopted 802.11g standard, the successor to 802.11b, allows for considerably greater bandwidth (up to 54 Mbps versus 1 or 2 Mbps originally). With this increase in bandwidth, wireless LANs will likely become much more prevalent. Using the appropriate access points and directional antennas, wireless LANs can be linked over more than a mile. As discussed later, it is not difficult to see why "war driving" around the premises of buildings is so popular with hackers.

iMode. To date, the iMode service of DoCoMo is used almost exclusively in Japan. However, it is a bellwether for the rest of the world. Using proprietary (and unpublished) protocols, iMode provides text messaging, E-commerce, Web browsing, and a plethora of services to Japanese customers. Another advantage to the service is that it is always on and thus can be viewed as any other packet-switched service. What has grabbed the business community's full attention is the degree of penetration within Japan — 28 million iMode users out of a total of 60 million cellular subscribers. Japanese teenagers have created a pseudo-language of text codes that rivals the cryptic language of Internet chat rooms (brb for "be right back," etc.).

Exhibit 1. IntelPro Wireless 2011B LAN Access Point (Courtesy Intel (www.intel.com))



Bluetooth. Intended as a short-distance (generally less than ten meters) communication standard, Bluetooth allows many devices to communicate with each other on an ad hoc basis, forming a "pico-net." For example, PDAs can communicate with properly equipped IP telephones to transfer voice-mail to the PDA when the authorized owner walks into her office. Bluetooth is a specification that, when followed by manufacturers, allows devices to emit radio signals in the unlicensed 2.4-GHz frequency. By using spread spectrum, full-duplex signals at up to 1600 hops per second, interference is greatly reduced, allowing up to seven simultaneous connections in one location. It is intended to be used by laptops, digital cameras, PDAs, devices in automobiles, and other consumer devices. Because of its short range, interception from outside a building is difficult (not to mention the additional effort required to overcome frequency hopping). Nevertheless, there are scenarios that could result in security breaches. For example, transmission between Ericsson's Bluetooth wireless headset and a base cellular phone could be intercepted as an executive walks through an airport.

Cellular. Standards for mobile wireless continue to evolve. The United States and parts of South America originally used the AMPS analog system; this system is not secure at all, much to the chagrin of some embarrassed politicians. More current protocols

laptops communicate with each other or with servers linked to an access point.

Cell phones. The technologies of cellular phones, PDAs, dictation machines, and other devices are merging. Cell phones, especially those with displays and mini-browsers, provide the form factor for Internet, public telephone system, and short-range communications.

Technologies never seem to die.

include TDMA, CDMA, and the world standard GSM. Data can travel over the first two protocols at a slow rate; GSM now supports broadband digital data transmission rates using general packet radio services (GPRS).

Miscellaneous, older wireless technologies. Any consideration of wireless security should include older technologies such as satellite communications (both geostationary and low earth orbit), microwave, infrared (line of sight, building to building), and CDPD for narrowband data transmission over unused bandwidth in the cellular frequencies and cordless phones operating in a number of public frequencies (most recently 900 MHz and 2.4 GHz). It is important to note that — particularly in telecommunications — technologies never seem to die. Any complete review of wireless security should at least consider these older, sometimes less-secure transmission media.

Hardware

Personal digital assistants. Palm Pilots, iPAQs, Blackberrys, and other devices are proliferating. Typically, they use frequencies somewhere in the cellular range and require sufficient tower (transmitter) density to work well. For example, ordering a book on amazon.com using a Palm Pilot is not likely to work in Death Valley, California.

Laptops with wireless adaptor cards. Using adaptor cards or wireless connections like Compaq's Bluetooth multiport Module,

The ISO stack still applies

The ubiquitous, seven-layer ISO stack applies to wireless communications as well. Although a discussion of this topic is (thank goodness!) outside the scope of this article, there is one protocol stack concept that should be kept in mind: traveling over the air is the logical equivalent to traveling over a copper wire or fiber. Airwave protocols represent layer 2 protocols, much like Frame Relay or ATM.¹ If a TCP/IP layer 3 link is established over a wireless network, it is still an IP network. It merely rides over a protocol designed for transmission in the air rather than through copper atoms or light waves. Hence, many of the same security concepts historically applied to IP networks, such as authentication, nonrepudiation, etc., still apply.

Wireless risks

A January 2002 article in *Computerworld* described how a couple of professional security firms were able to easily intercept wireless transmissions at several airports. They picked up sensitive network information that could be used to break in or to actually establish a rogue but authorized node on the airline network.

More threatening is the newly popular "war driving" hobby of today's *au courant* hackers. Using an 802.11b-equipped notebook computer with appropriate software, hackers drive around buildings scanning for 802.11b access points. The following conversation, quoted from a newsgroup for wireless enthusiasts in the New York City

area, illustrates the level of risk posed by war driving:

Just an FYI for everyone, they are going to be changing the nomenclature of 'War Driving' very soon. Probably to something like 'ap mapping' or 'net stumbling' or something of the sort. They are trying to make it sound less destructive, intrusive and illegal, which is a very good idea. This application that is being developed by Marius Milner of BAWUG is great. I used it today. Walking around in my neighborhood (Upper East Side Manhattan) I found about 30 access points. A company called www.rexspeed.com is setting up access points in residential buildings.

Riding the bus down from the Upper East Side to Bryant park, I found about 15 access points. Walking from Bryant Park to Times Square, I found 10 access points. All of this was done without any external antenna. In general, 90 percent of these access points are not using WEP. Fun stuff.

The scanning utility referred to above is the Network Stumbler, written by Marius Milner. It identifies MAC addresses (physical hardware addresses), signal-to-noise ratios, and SSIDs.² Security consultant Rich Santalesa points out that if a GPS receiver is added to the notebook, the utility records the exact location of the signal.

Many more examples of wireless vulnerability could be cited. Looking at these wide open links reminds us of the first days of the Internet when the novelty of the technology obscured the risks from intruders. Then, as now, the overriding impediment to adequate security was simple ignorance of the risks. IT technicians and sometimes even knowledgeable users set up wireless networks. Standard — but optional — security features such as WEP (wired equivalent privacy) may not be implemented.

Viewing the handheld or portable device as the weak sibling of the wireless network is a useful perspective. As wireless devices increase their memory, speed, and operating system complexity, they will only become

more vulnerable to viruses and rogue code that can facilitate unauthorized transactions.

The following sections outline some defenses against wireless hacking and snooping. We start with the easy defenses

The overriding impediment to adequate security was simple ignorance of the risks.

first, based on security consultant Don Parker's oft-repeated statement of the obvious: "Prudent security requires shutting the barn doors before worrying about the rat holes."

Defenses

Virtually all the security industry's cognoscenti agree that it is perfectly feasible to achieve a reasonable level of wireless security. And it is desperately needed — for wireless purchases, stock transactions, transmissions of safety information via wireless PDA to engineers in hazardous environments, and other activities where security is required. The problems come from lack of awareness, cost to implement, competing standards, and legacy equipment. Following are some current solutions that should be considered if the business exposure warrants the effort.

Awareness and simple procedures

First, make management, IT and telecom personnel, and all users aware that wireless information can be intercepted and used to penetrate the organization's systems and information. In practical terms, this means:

- Obtain formal approval to set up wireless LANs and perform a security review to ensure WEP or other security measures have been put in place.
- Limit confidential conversations where security is notoriously lax. For example, many cellular phones are dual mode and

operate on a completely unsecured protocol/frequency in areas where only analog service is available. Some cell phones have the ability to disable dual mode so they only operate in the relatively more secure digital mode.

Like the concentric walls of medieval castles, the best defense includes multiple barriers to access.

- Use a password on any PDA or similar device that contains sensitive data. An even stronger protection is to encrypt the data. For example, Certicom offers the MovianCrypt security package, which uses a 128-bit advanced encryption standard to encrypt all data on a PDA.
- Ensure that the security architecture does assume that the end device (e.g., a laptop) will always be in physical possession of the authorized owner.

Technical solutions

There are several approaches to securing a wireless network. Some, like WEP, focus on the nature of wireless communication itself. Others use tunneling and traditional VPN (virtual private network) security methods to ensure that the data is strongly encrypted at the IP layer. Of course, like the concentric walls of medieval castles, the best defense includes multiple barriers to access.

Let's start with WEP, an optional function of the IEEE 802.11 specification. If implemented, it works by creating secret shared encryption keys. Both source and destination stations use these keys to alter frame bits to avoid disclosure to eavesdroppers. WEP is designed to provide the same security for wireless transmissions as could be expected for communications via copper wire or fiber. It was never intended to be the Fort Knox of security systems.

WEP has been criticized because it sends the shared secret over the airwaves; sniffers can ferret out the secret and compromise the system. Some Berkley researchers broke the 40-bit encryption relatively quickly after the IEEE released the specification. WEP also has a few other weaknesses, including:

- Vendors have added proprietary features to their WEP implementation, making integration of wireless networks more difficult.
- Anyone can pick up the signal, as in the "war driving" scenario described above. This means that even if hackers do not want to bother decoding the traffic using a wireless sniffer — which is somewhat difficult — they can still get onto the network. That is, they are plugged in just the same as if they took their laptop into a spare office and ran a cable to the nearest Ethernet port.

A partial solution is to enable MAC³ address monitoring. By adding MAC addresses (unique to each piece of hardware, such as a laptop) to the access point device, only those individuals possessing equipment that matches the MAC address table can get onto the network. However, it is difficult to scale the solution because the MAC address tables must be maintained manually.

None of these deficiencies should discourage implementation of WEP. Just implementing WEP out-of-the-box will discourage many hackers. Also, WEP itself is maturing, taking advantage of the increased processing power available on handheld and portable devices to allow more compute intensive security algorithms.

As mentioned, authentication of laptops and other devices on the user end is as important in wireless as it is in dialup remote access. It is beyond human diligence not to lose or have stolen a portable device. VPNs with remote, two-factor authentication superimpose a layer of security that greatly enhances any native

wireless protection system. RSA's SecurID, shown in [Exhibit 2](#), is an example of a two-factor system based on something the user knows (a password) and something the user possesses (an encrypted card).

In addition to VPNs, software-based firewalls such as Black Ice are useful for end-computer security. Relying on tools such as these takes some of the pressure off application-level security, which is sometimes weak due to loose password management, default passwords, and other flaws.

A hole in the fabric of wireless security

Wireless security protocols are evolving. WAP 1.2.1 uses Wireless Transport Layer Security (WTLS), which very effectively encrypts communications from, for example, a cell phone to a WAP gateway. At the WAP gateway, the message must be momentarily unencrypted before it is sent onto the Web server via SSL (Secure Sockets Layer). This "WAP GAP" exists today but is supposed to be eliminated in WAP version 1.3 or later. A temporary fix is to strengthen physical security around the WAP gateway and add additional layers of security onto the higher-level applications.

Traditional security methods still work

Of course, existing security methods still apply — from the ancient Spartan's steganography techniques (invisible messages) to the mind-numbing complex cryptography algorithms of today. Following are some major security algorithms that can easily support a high level of E-commerce security:

- *Digital hashing*: a lower-strength security technique to help prevent unauthorized changes to documents transmitted electronically
- *Digital signatures*: provides the same function as digital hashing but is a much more robust algorithm
- *Public key cryptography*: the cornerstone of much digital-age security (key management, such as the use of smart cards, is important in the various implementations of public key infrastructure (PKI))
- Inventory of access points
- Identification of encryption method (if any)
- Identification of authentication method
- Determination of WEP status (has it been implemented?)
- Notation of any GPS information (useful for determining location access point)
- Analytics on probe packets
- Identification of firmware status (up-to-date?)

Exhibit 2. Two-Factor Authentication from RSA (Courtesy RSA (www.rsasecurity.com))



Auditing wireless security

Auditing an organization's wireless security architecture is not only useful professionally, but also excellent personal exercise. The reason: physically walking around the premises with a wireless LAN audit tool is necessary to determine where wireless LANs and other wireless networks have been set up. Often, these LANs have been implemented without approval or documentation and, hence, a documentation review is not sufficient. Using a device such as IBM's Wireless Security Auditor, a reliable inventory of wireless networks and settings can be obtained (see [Exhibit 3](#)).

Using IBM's Wireless Security Auditor as an example, the following are some of the configurations and potential vulnerabilities that might be evaluated in a wireless security review:

Exhibit 3. Wireless Security Auditor Tool (Courtesy IBM)
(www.research.ibm.com/gsal/wsa/)



Aside from the technology layer, standard IT/telecom controls should be included in the review: change control, documentation,

standards compliance, key management, conformance with technical architecture and appropriate policies for portable devices.

Summary

Wireless security is important to both leading and trailing-edge organizations. Applications and infrastructure uses are showing up everywhere from the shop floor to the techie whose Bluetooth PDA collects his voice-mail as he walks into the office. This rapid growth, reminiscent of the first days of PCs and the Internet, should be accompanied by a corresponding level of security, control, and standards. Here we go again.... ▲

Notes

1. In a sense, "air" also represents layer 1, the most basic and physical layer. Copper, fiber, and even (in the earliest days of the telegraph) barbed wire stand as examples of layer 1 media.
2. Service Set Identifier. An encoded flag attached to packets sent over a wireless LAN that indicates it is authorized to be on a particular radio network. All wireless devices on the same radio network must have the same SSID or they will be ignored.
3. MAC (medium access control) addresses are unique. "03:35:05:36:47:7a" is a sample MAC address that might be found on a wireless or wired LAN.