# WLAN Security: Current and Future

Wireless LAN deployment improves users' mobility, but it also brings a range of security issues that affect emerging standards and related technologies.

**Joon S. Park and Derrick Dicoi**
*Syracuse University*

Many companies, organizations, and even individuals implement wireless local area networks (WLANs) in various locations such as their offices, conference rooms, homes, and business areas. This type of connection offers users *portability* because they can move from one location to another while maintaining access to the corporate network, but it does not offer access between locations. *Mobility*, on the other hand, lets users access the corporate network not only near multiple access locations but also everywhere in between. WLANs let users access a high-speed connection in areas where physically wired networks can't penetrate or are not cost effective. Many companies use WLANs as add-ons to their main wired networks.

A recent study found that corporations that implemented WLANs increased the availability of their corporate network by 70 minutes per day for the average user, which in turn also enhanced productivity within the corporation by as much as 22 percent.[1]

WLANs also offer much-needed flexibility in a world of high-speed data networks. Administrators can install them quicker, easier, and more cost-efficiently than traditional wired networks. A WLAN's flexibility provides an easy way to install a new network, whether an extension of a wired network or a pure WLAN. The ease and speed with which these networks can be installed is unprecedented: high-speed networks can be installed for a week or a day and then removed once they are no longer needed. The fact that such temporary installations can be created cost-efficiently is a major selling point for WLAN integrations.

Although WLANs solve some problems that exist in traditional wired LANs, they also introduce new security issues. In this article, we identify current and future WLAN security concerns and possible countermeasures, including standards, technologies, management, policies, and service environments. The risks that WLAN services present can only be mitigated rather than completely eliminated. Although there is no single solution for perfect WLAN security, we believe that WLAN security can be enhanced to an acceptable level by a proper combination of countermeasures.

## 802.11 Standards

In 1997, the IEEE moved to address wire-

 Published by the IEEE Computer Society 1089-7801/03/$17.00©2003 IEEE 

less performance and security concerns and created what became the first WLAN standard: 802.11. The IEEE's main goal was to create a standardized approach for wireless communication in enterprises, homes, and public areas. It also needed to address interoperability among products to ensure that consumers and corporations would support WLAN growth. To that end, the standard addresses performance and security concerns within the wireless realm, and outlines possible technologies to be used for transmission of wireless communication, including direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). As interest in wireless grows, IEEE expands the plethora of standards under 802.11 by developing specific substandards with different specifications for bandwidth, frequency, and transmission technologies.

### 802.11b

The most widely used standard today among the 802.11 family is 802.11b — known as wireless fidelity or Wi-Fi — which specifies a data rate of up to 11 Mbps in the 2.4-GHz ISM (Industrial, Scientific, and Medical) frequency band using DSSS technology. The nonprofit Wi-Fi Alliance rigorously tests 802.11b-based networking products for proper interoperability and functionality and awards Wi-Fi certification to those that pass. (For more, see the Wi-Fi Alliance Index at www.wi-fi.org/OpenSection/index.asp.)

### 802.11a

802.11a is quite different from 802.11b in that it specifies data rates of up to 54 Mbps and runs in the 5-GHz Unlicensed National Information Infrastructure (UNII) band using Orthogonal Frequency Division Multiplexing (OFDM) for transmission. IEEE selected the OFDM modulation scheme over DSSS for 802.11a and future standards primarily because it uses spectrum more efficiently. Although interest in 802.11a came somewhat later than that in 802.11b, it has grown dramatically over the last several years, mainly because of the substantial increase in bandwidth. One significant problem is that, although the IEEE ratified 802.11a and 802.11b on the same day, they are incompatible. Customers and corporations who have invested in 802.11b WLANs must therefore invest additionally to take advantage of 802.11a products — an expense they cannot easily justify.

### 802.11g

With its approval of the 802.11g standard in June 2003, the IEEE brought compatibility to the existing WLAN standards. Like 802.11b, 802.11g runs in the 2.4-GHz ISM band, but it has the same maximum data rate as 802.11a and uses OFDM instead of DSSS. 802.11g's backward-compatibility with 802.11b will facilitate WLAN growth because — unlike switching to 802.11a — it lets current 802.11b users increase WLAN speed fairly easily.

Hoping to capture the initial market share and propel their future growth, several vendors actually released their first 802.11g products prior to the IEEE's official approval of the standard. With the WLAN industry still quite new, several small companies are competing for footholds in the 802.11g market. The danger in this marketing strategy is that the official 802.11g standard differs slightly from the draft upon which the early-release products were based. That said, many vendors already claim that they can address this problem with a simple firmware upgrade.

### 802.1x

Among current WLAN standards are also those for network security. One such standard that was recently updated and implemented is 802.1x, which provides port-based network access control. Although the IEEE initially designed 802.1x for wired communications, the standard has spun off into the wireless world to help provide some much-needed security. 802.1x's main benefit for WLANs is that it provides mutual authentication between a network and its client. This standard can help address the frightening issue of rogue access points that can pop up in corporate environments. With 802.1x, the user is not authenticating to the wireless access point (AP), but to the actual LAN, through an authentication database such as a remote authentication dial-in user service (Radius)[2] server behind the access point.

### 802.11i

802.11i is expected to be complete by late 2003 or early 2004, and it will be a stepping stone for all future WLAN standards. It will add more security services to the 802.11 WLAN world by specifically addressing issues pertaining to both the media access control (MAC) and physical layers of wireless networks. The authentication schemes in 802.11i are based on 802.1x and extensible authentication protocol (EAP),[3,4] which will ultimately let vendors create several types of authentication credentials for WLANs. In the long term, 802.11i might provide a framework for using the advanced encryption standard's (AES)[5,6] for its encryption services, but it will still be compatible with the RC4 algorithm,[7] which is being used

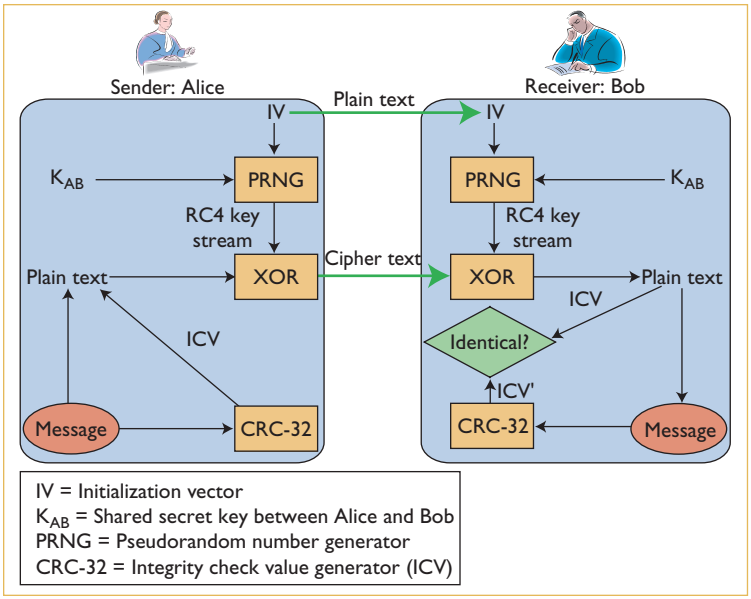


*Figure 1. Security services in wired equivalent privacy protocol (WEP).*

in the current wired equivalent privacy (WEP)[8] protocol (discussed in the next section). To improve the security of keys used in WEP, 802.11i will most likely use a form of temporal key integrity protocol (TKIP).[8,9]

### Proprietary Standards

In response to the IEEE's slow pace in solving the security issues with wireless standards, many vendors are now implementing proprietary security standards for WLANs, hoping to entice corporations and consumers to purchase their products. In October 2002, the Wi-Fi Alliance took a major step in announcing the creation of a new interim industry security standard called Wi-Fi protected access (WPA; www.wifialliance/com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf). WPA will be forward-compatible with the upcoming IEEE 802.11i standard, from which it is derived. One of the design goals of WPA is substitution for WEP, providing more secure and interoperable services.

## WLAN Security Concerns and Strategies

We discuss WLAN security concerns and corresponding strategies.

### WEP Vulnerabilities

Currently, WEP is the security standard outlined for all 802.11 standards (see Figure 1); its goal is to secure WLANs at the same level as wired networks. WEP is based on the RC4 symmetric algorithm. Administrators deploy a secret key on both the access point and wireless devices, which use the key to encrypt data and check data integrity. In addition, the AP can use the key to authenticate its clients. Although RC4 algorithm's overall cryptography is quite powerful, the WEP standard takes a poor approach[10] to using it.

One of WEP's biggest downfalls is that its secret keys (which wireless devices and their access points share) are relatively shorter than other security protocols' keys — typically, 40 bits long in WEP, although the standard does allow up to 104-bit keys. WEP concatenates a shared secret key with a short 24-bit initialization vector (IV) to create the RC4 key stream. For instance, after WEP concatenates a 40-bit secret key with 24-bit IV, it generates a 64-bit RC4 key stream. The IV is sent to the receiver in plain text so that the receiver can generate the same key stream, which means that attackers can see the first 24 bits of every key sent using WEP. Furthermore, the fact that the IV is so short nearly guarantees that it will be used for multiple messages. In fact, the same IV might be reused in as little as half a day if there is significant activity over a company's WLAN. An attacker could easily collect an IV and use it to retrieve the key that the AP and wireless devices use.

The current 802.11 standard has no guidelines for how, or even if, the IV should be changed. Some vendors' equipment actually uses the same IV for every key stream, which means an eavesdropper is guaranteed to uncover the IV. In response to widespread discussion of WEP's flaws, other systems generated the IVs sequentially, incremented with the transmission of each packet.

WEP security also suffers from a poor solution for key management, which can leave the keys in a device unchanged for long periods of time. If the device were lost or stolen, an attacker could use the key to compromise not only that device but any other devices sharing the same key. Dynamic key management solutions could help mitigate the threat of WEP keys falling into the wrong hands, as well as increase complexity.

Further adding to the protocol's shortcomings is WEP's implementation of the Cyclic Redundancy Check (CRC)-32 algorithm,[12] which calculates a 32-bit checksum to check the integrity of packets sent over the WLAN. Because the checksum that CRC-32 creates is a noncryptographic value, known attacks, such as side-channel attacks,[10] can compromise the data's integrity.

### MAC Address Spoofing

A wireless network interface component (NIC) card's MAC address can be used for access-control

decisions in WLAN environments. Because WEP broadcasts MAC addresses in plain text during packet transfers, an attacker can easily eavesdrop to get the addresses associated with clients accessing the WLAN. The attacker can thus gain unauthorized access to the network by using a wireless NIC card with a spoofed MAC address. The attack is particularly useful if the attacker can identify a MAC address that has recently disconnected from the network, thus avoiding any conflicts at the MAC layer.

Another grave concern for network administrators is the theft of wireless NIC cards with MAC addresses defined as `allowed` on a MAC filter. If the owner of a stolen NIC card does not immediately report the theft, an attacker can use the card to gain access to the WLAN. Once the theft is reported, the administrator must update the MAC address filter on each AP to prevent possible unauthorized access to the WLAN through the stolen card's MAC address. Enterprise wireless gateways (EWGs) offer a possible solution to this problem by providing a centralized point of security. EWGs reduce the overhead for administrators by letting them implement all changes to WLAN security features in a single location.

### Default Configuration

Before deploying APs in a WLAN environment, the administrator must properly configure them. Although critical to securing a WLAN, unfortunately, almost all manufacturers ship APs with WEP disabled. WEP does not provide full security, but with proper configuration, it does enhance WLAN security. APs often ship with other default security settings that must be changed; of these, the most critical are the AP's passwords, the simple network management protocol (SNMP) parameters, channel selection, dynamic host configuration protocol (DHCP) setup, and the integrated firewall configuration (if it is available on the AP). Otherwise, an attacker can easily get access to the WLAN or compromise the system using those default values.

Because most products from a specific vendor have the same default service set identifier (SSID), which is required to access the vendor's AP, it is essential to network security that the default SSID be changed. Otherwise, an attacker who knows the SSID for that vendor's AP can easily access the network. It is also critical to turn off the AP's broadcast mode, which broadcasts the unit's SSID. While broadcast mode is enabled, anyone with a wireless NIC card could get the SSID from the AP itself, which would defeat the purpose of changing its SSID. Changing an AP's factory defaults is a simple yet effective step in securing WLANs, although WLAN administrators often overlook it.

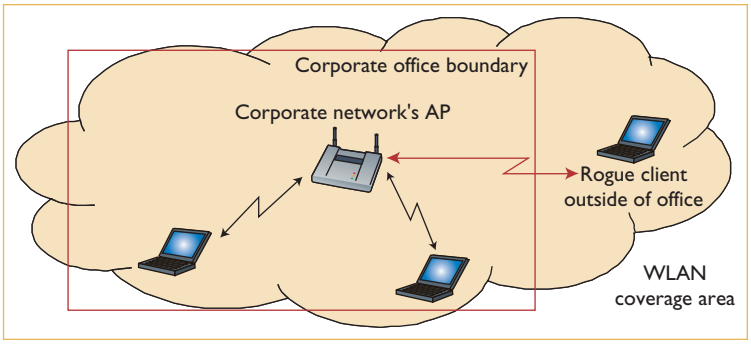


*Figure 2. Corporate office boundary versus Wireless LAN coverage area.*

### Physical Access to APs

To keep APs secure, administrators should locate them in physically protected areas rather than places where anybody can physically access them. Many companies have mistakenly placed APs in lobbies or other public areas, where attackers can access them and reset the default factory settings (which are easy to locate on most vendors' Web sites). This takes much less technical skill than other WLAN attacks, but is just as dangerous.

Another growing threat to corporate network security is from so-called rogue APs. Employees can deploy personal APs in their cubes or offices, for example, and connect to the corporate network, thus becoming an extension of the physical wired network without the IT department's knowledge. Because many employees do not fully understand WLANs, they can incorrectly implement security measures and unknowlingly open a security hole in their company's network.

### Service Coverage Area

Attackers must gain access to a target AP's signal before they can penetrate the network. An AP's signals can travel beyond desired service coverage areas (see Figure 2). For instance, an attacker outside an office can access a company's private network through an AP on a WLAN whose signal has gone beyond the building's physical boundaries. This type of attack, known as *war driving,* often happens in office parking lots. Attackers attach antennas to their automobiles to find WLAN signals and then use sophisticated equipment to sniff packets sent over the network. Sniffing lets attackers intercept each packet, which they can then analyze to find the information they need to pen-

etrate a company's network. The same type of attack can occur if the signal penetrates a building's walls and then leaks into public places or another company's office. Difficulties in controlling a WLAN coverage area can lead to loss of confidentiality, integrity, and ultimately to denial-of-service attacks on the network.

The only real solution to this problem is to actually walk an office building's perimeter with a spectrum analyzer to ensure that signals are not leaving the desired area. Network administrators should perform signal tests regularly to ensure network security. Doing so also makes it possible to detect rogue APs that non-IT employees have added to the network. If an administrator detects a signal beyond a company's office walls, there are a few effective ways to alter the AP's signal so that it is contained within the office's physical boundaries. The administrator can

- lower the AP's signal strength,
- move it to a location where its signal will not break the office's physical barriers, or
- use different types of antennas that control signal strength and direction.

The best solution might be to use more than one of these methods to control WLAN coverage; using none can pose a serious threat to a company's private network.

### Public WLAN Concerns

An individual attempting to connect to a corporate network via a public network can present another threat to a private network. For example, users accessing a public WLAN hotspot in a coffee shop or airport open a channel to their corporate network. Usually, public networks offer no security; this lets attackers in the area sniff the network and view all packets transferred in plain text on the WLAN. This type of attack has increased in recent years as public networks have become more popular and will continue to grow as more hotspots pop up around the world. Users have no idea that they have just opened up a back door into their company's network. Attackers miles away from the network's physical location can thus gain full access. Rather than hacking through a firewall and other security measures to gain access, they can merely monitor usage on public WLANs. Administrators can configure their systems to disallow network access from public WLANS, but this limits the users' mobility and service availability.

## WLAN Security Enhancements

Network administrators must ensure their products have the latest firmware upgrades, which play a key role in a product's performance, security, and management capability. Administrators can use EWG to authenticate WLAN users and filter out unauthorized users. If administrators use centralized key-distribution servers, they can easily and effectively manage WEP keys. However, this increases the possibility of single-point failure, which is a generic problem in a centralized network architecture. An intrusion detection system (IDS) can help network administrators keep a close eye on the WLAN. Some types of IDSs let network administrators set up WLAN policies and rules while other types of software help with WLAN auditing and assessment.

Furthermore, virtual private network (VPN) offers a secure connection through a public WLAN by creating a tunnel, or secure encrypted connection, between the user's device and the destination. This adds much-needed security to public WLAN connections and lets those traveling for business use their devices in public places without worrying about attackers sniffing any packets associated with their connection. A personal firewall loaded on the user's equipment can add an extra layer of security in such scenarios. Finally, administrators can implement a public key infrastructure (PKI) on a WLAN to provide reliable security services.

As with traditional wired networks, policies are important in the world of WLANs. There is no perfect policy that every company should abide by, but all should have and enforce a set of security policies tailored to the needs of their WLAN environment. For instance, WLAN policies should forbid employees to add APs to the network by themselves.

## The Future of WLAN Security

As we discussed earlier, there are several new standards under development for future WLAN security. Currently, the AES seems to be the basis of WEP's next generation under 802.11i. AES lets administrators specify the key size to 128, 192, or 256 bits. The revised WEP standard will likely use a true 128-bit default key size, although this might only happen when AES is ratified as part of the next generation of WEP. Using AES will also eliminate the use of the 24-bit IV, which is one of the largest downfalls of the current version of WEP.

AES does, however, have a few drawbacks. If the next generation of WEP uses AES, it will be a

huge undertaking for a company to replace all of its existing WLAN APs and other equipment in order to be compatible with the new standard. The use of a large key size (at minimum 128 bits) also means client devices will need extra processing power to encrypt and decrypt it. This could slow down the devices and ultimately disturb many users, but the outcome remains to be seen. AES will also require considerably more power consumption than most existing WLAN cards provide. Users fearing extra drain on their mobile devices (laptops, handhelds, and so on) have continually dismissed the idea of increasing WLAN cards' power consumption.

TKIP could be a short-term solution to counter WEP's weaknesses until the IEEE officially ratifies the 802.11i standard. TKIP would use a 128-bit temporal key, but all users on a specific AP would share the same key: if one user is compromised, then all users on that AP become vulnerable to attacks. The major difference between WEP and TKIP is that a temporal key changes every 10,000 packets in TKIP, whereas WEP keys are static.

Other types of physical components are being investigated to promote WLAN security. As we mentioned, EWGs are proving to be an important part of WLANs, and their popularity will continue to grow as the security they provide improves. Several vendors are also unveiling new products that take a more centralized approach to implementing WLANs — with "dumb" physical APs connected to centrally switched brains. This approach could help simplify WLAN implantation and administration.

Antennas might also increase security. Various types of smart antennas are currently in development; some can control an AP's signal to confine it to a specific area and ensure that it does not pass through physical matter. Antenna technology is still in its infancy, but this area of wireless technology might enhance WLAN security in the near future.

## Conclusions

WLANs offer new services that traditional wired LANs cannot provide, but they also introduce new security concerns. Although the security concerns of WLAN services cannot be completely eliminated, we can mitigate them by a proper integration of standards, technologies, management, policies, and service environments.

### References


1. *Wireless LAN Benefits Study*, NOP World-Technology, Sept. 2001; http://newsroom.cisco.com/dlls/tln/WLAN_study.pdf.
2. C. Rigney et al., "Remote Authentication Dial-In User Service (RADIUS)," RFC 2865, June 2000; www.rfc-editor.org/rfc/rfc2865.txt.
3. H. Andersson et al., "Protected EAP Protocol (PEAP)," IETF Internet draft, Sept. 2002; work in progress.
4. L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," RFC 2284, Mar. 1998; www.rfc-editor.org/rfc/rfc2284.txt.
5. J. Nechvatal et al., "Report on the Development of the Advanced Encryption Standard (AES)," *J. Research US Nat'l Inst. Standards and Technology*, vol. 106, no. 3, 2001, pp. 511–576; http://csrc.nist.gov/encryption/aes/round2/r2report.pdf.
6. J. Daemon and V. Rijmen, "AES Proposal: Rijndael," http://csrc.nist.gov/encryption/aes.
7. R. Rivest, *The RC4 Encryption Algorithm*, RSA Data Security, Mar. 1992.
8. *IEEE Std. 802.11-01/550r3, Wireless LANs: Temporal Key Hash*, IEEE Press, Dec. 2001; http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-550.zip.
9. *IEEE 802.11-02/282r2, Wireless LANs: Alternate Temporal Key Hash*, IEEE Press, Apr. 2002; http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-282.zip.
10. *ISO 3309, Information Processing Systems—Data Communication High-Level Data Link Control Procedure—Frame Structure*, 3rd ed., Int'l Organization for Standardization, Oct. 1984.
11. S. Miller, "Facing the Challenge of Wireless Security," *Computer*, vol. 34, no. 7, 2001, pp. 16–18.
12. T. Karygiannis and L. Owens, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices Draft*, special publication 800-48, US Nat'l Inst. Standards and Technology, July 2002.



**Joon S. Park** is an assistant professor at Syracuse University, where he is the director of the laboratory for information security and application (LISA), and a member of the Systems Assurance Institute (SAI). His research interests include information and systems security. He received a PhD in information technology from George Mason University. He is a member of the IEEE Computer Society. Contact him at jspark@syr.edu.

**Derrick Dicoi** is a research associate at the Center for Emerging Network Technologies and a graduate director of the Information Technology Experimental Learning Lab at Syracuse University. His research interests include wireless technologies and strategic IT development. He received his BA in telecommunications from Michigan State University, and is currently pursuing his MS in information management at Syracuse University. Contact him at dtdicoi@syr.edu.