

# Wireless 802.11 Security: Questions & Answers to Get Started

## SystemExperts Corporation

*Brad C. Johnson*

---

### Abstract

802.11-based wireless LAN technology is finding ready acceptance. The combination of low cost and ease of deployment is leading to rapid adoption. In many organizations, the deployments are so rapid that the situation is out of control; individual departments are setting up wireless environments that the corporate IT department doesn't even know about. In most cases, these homegrown setups are not configured to provide security at the same level as the organization's security policies require on networks carrying data of comparable value.

Because the wireless signals carry beyond the physical buildings and it is easy for anyone with a laptop and inexpensive hardware to capture those signals, securing these environments is of paramount concern. Recognizing the inherent limitations of the technology, this paper is intended to provide some basic context and practical recommendations for improving the security of 802.11 networks.

### Inside

- How prevalent is the problem of unsecured wireless LANs?
- Are organizations taking wireless security seriously enough?
- What are the vulnerabilities with the technology?
- What practical measures can you take to make 802.11 wireless networking more secure?
- Is it safe to use public 802.11 environments?

### SystemExperts Corporation

**Boston   New York   Washington D.C   Tampa**  
**San Francisco   Los Angeles   Sacramento**

Toll free (USA only): +1 888 749 9800  
From outside USA: +1 978 440 9388

[www.systemexperts.com](http://www.systemexperts.com)  
[info@systemexperts.com](mailto:info@systemexperts.com)

## How prevalent is the problem of unsecured wireless LANs?

*Almost all wireless deployments are, at this time, fundamentally insecure.* This is not fear mongering; it is an accurate assessment of the reality of the current state of security of wireless 802.11-based environments.

The only practical approach for any business to take is to assume that end-to-end security can only be provided outside the bounds of the wireless infrastructure. That is, you should not count on the wireless environment for any protection of sensitive business data.

The current state of insecurity is caused by a combination of factors:

- The default configurations of the wireless “servers” (Access Points) are insecure. That is, they are set to be “open” to make them easy to deploy and use out of the box.
- The physical transport is invisible and therefore it is difficult to control its boundaries.
- There are interoperability problems between Access Points because important security functions are different or incompatible from the various vendors.
- Many wireless setups are installed by end-users and not by IT professionals. This means that important security features are often not used.
- The standard data encryption protocol (WEP) that is used on almost every Access Point in the market has been proven to be insecure.

Several characteristics exacerbate the problem. Deploying a basic wireless network does not require special expertise. If a department is eager to expand its network and it either can't or doesn't want to wait for the normal IT schedule, it can do it itself both cheaply (about \$200 for an Access Point and \$100-200 per client) and easily. Plug an Access Point into your Ethernet jack, plug a wireless card into your laptop, and in most cases you're done. The problem, of course, is that the basic default configuration is purposely “open” to make it easy to use out of the box. This open configuration usually allows *any* client within reach to connect to the Access Point. All of the data passes both in the air and on the wire in the clear, so somebody outside your building could have access to it too.

## What are the vulnerabilities in the technology?

Major exposures in a wireless network are *everywhere*. Every important component in a wireless network has at least one significant vulnerability that can directly lead to a major exploit.

Let's take a look at the major components of the current 802.11b standard and the corresponding problems in available products.

- Access Point configuration: All major Access Point products are setup to be in their most insecure configuration out of the box.
- The IEEE protocol: The wireless network traffic is largely controlled through what is called management and control packets. Management packets are sent in the clear, even if WEP (encryption) is enabled.
- Authentication: The default authentication mode for most Access Points is open which allows any client to connect (associate) with it.
- Authorization: The common form of authorization control on most Access Points is MAC level address filtering (i.e., these filters allow or disallow the forwarding of packets). Not surprisingly, by default, this MAC filtering table is empty. What is more problematic, however, is that MAC addresses can be manually set by almost any client.
- Access Point management: Most Access Points are setup to use well-known SNMP community strings (passwords) and for those that provide an HTTP interface, to be accessible by anybody who happens to know the IP address of the device.
- Encryption: The standard WEP protocol has been proven to be insecure in several fundamental ways. It requires only a modicum of CPU capability and network traffic to determine the supposedly “secret” WEP encryption keys.
- Client WEP key storage: Many major vendors either store the WEP keys directly on the client wireless card (so stealing it gives you the capabilities associated with the card) or on the local disk in a way that is obvious and easy for anybody to copy and use.
- Wireless networking boundaries: Most Access Points and client wireless cards come with omni-directional antennas that are hard to control and often quite complex to determine their actual range and capabilities. Unless an organization installs very expensive shielding material, its ability to control how far the network actually goes is limited.

Deploying a wireless environment is fundamentally easy. Deploying a wireless environment that meets the requirements of your existing security policies, while minimizing business risk, is not. It can be done, but requires substantial forethought and a commitment to address the architectural, design, and implementation issues described above.

## Are organizations taking wireless security seriously enough?

Let's look further at the problem of managing the boundaries of the wireless environment. As opposed to the wired environment where you can literally follow the path from one component to the next, the wireless boundaries are amorphous and constantly changing. They expand and contract for all sorts of reasons. Barriers (e.g., walls, people) can reduce the distance that an Access Point and a client can be from each other. Antennas can increase the distance. Interference (e.g., other wireless devices) can reduce the distance. Antenna adjustments (e.g., turning it around or making it horizontal vs. vertical) can either reduce or increase the distance depending on the antenna type (directional vs. omnidirectional) or just the angle of the radio waves coming out of your wireless card. These and other attributes can make it very hard to answer the simple question: Where does our network go?

The overall problem is that most businesses don't have the discipline, controls, or policies in place to handle the dynamic nature of the wireless components. Most security guidelines are geared towards the more slowly changing wired environment that, in many cases, forces the end-user to get help or permission to change their computing environment. It's not that organizations don't take wireless security seriously, it's just that most don't yet have the tools or expertise in-house to effectively manage this new technology area.

## What practical measures can make 802.11 wireless networking more secure?

The reality is that wireless networks are here to stay. Despite the known security risks, wireless environments are being deployed in large numbers. Given this reality, there are a number of practical measures that organizations must consider to make the environment as secure as possible.

Despite the large number of documented deficiencies with the existing technology, there are a number of straightforward steps that one can take to at least improve the security of wireless deployments. Here are a few measures that are

applicable to almost all of the wireless products that exist today.

- Use WEP to encrypt the data while it is in transit. This will help thwart casual snoopers from seeing your data in the clear.
- Change the default Access Point Service Set ID (SSID, aka Network Name). Also, before you leave your corporate environment (e.g., to go on a business trip), make sure that you have changed it to be blank.
- All Access Points can be managed over the network via SNMP. Change the default SNMP community strings (passwords). Also consider making changes to your routers or firewalls such that SNMP requests to your Access Point are only allowed from specific IP addresses.
- Disable the broadcast SSID feature on your Access Point. Otherwise, your SSID is broadcast out for all to see. This can be used by an intruding client to "connect" (associate) with your Access Point.
- Change the default password for administrative access (e.g., through HTTP) to your Access Point.
- Consider the use of MAC level (Ethernet) address filtering to limit which clients your Access Point will "listen" to.
- Consider whether or not your Access Point should offer DHCP for new clients trying to connect to the wireless environment. DHCP by its very nature makes it very easy for outside clients (that you don't want to use your network) to get legitimate connection information such as a valid IP address, the local gateway address, and the location of the local DNS server.
- If sensitive data is going to be transmitted to or from the clients, you need to look into some type of end-to-end security solution to protect it (e.g., some type of Virtual Private Network (VPN) technology or other third-party authentication, authorization, and encryption mechanisms).
- Survey your site to understand how far your Access Points are actually broadcasting their signals. To restrict the signal, you may need to change their placement or to consider the use of more specialized (directional) antennas.

Each of these measures by itself is unlikely to dramatically reduce your overall risk. However, taken together, they will make your environment more secure than it was before.

There are a number of industry wide efforts underway that are aimed at improving the security of wireless environments. Some of these include the efforts of the IEEE Security Subgroup (Enhanced Security Network and a replacement for WEP), IETF's Extensible Authentication Protocol (EAP), and vendor specific extensions such as Cisco's Lightweight EAP.

As these initiatives produce results the measures available to secure wireless environments will become more effective.

## Is it safe to use public 802.11 environments?

Most users have no idea how risky it is to use a public 802.11 wireless environment. The main problem is that people either don't understand the subtle exposures that they may be creating for themselves or they don't appreciate how truly open the wireless environment really is.

It's not an accident that these types of environments are potentially risky. Organizations that create public wireless networks understand that the main objective is to provide a convenient connection point to the Internet. The more standard, open, and generic the setup is, the easier it will be for their consumers to use it.

In most public wireless networks, you will be required to set your SSID to null (i.e., blank or no value) such that their Access Point can "connect" (associate) with you (and vice versa). A blank client SSID means that you are willing to associate with any Access Point that is offering an open network. Most people achieve this by first booting up their laptop, then using

their client software to change the SSID to be blank, and then trying to associate with the public Access Point. Unfortunately, your client remembers what your last SSID was. In many cases, this is the SSID from your corporate network. When your laptop is turned on, it will try and find an Access Point as soon as possible. In fact, as soon as it has power, it will start sending out requests to try and (re)connect. Anybody sniffing the wireless traffic will now have seen your SSID (in between the time you booted it up and you changed it) and can potentially take advantage of that by using that SSID when they are close to *your* company's Access Points.

Another vulnerability is that many people don't appreciate that the wireless card in their laptop is capable of receiving and sending data on any of the wireless channels and that it is capable of seeing the same data that the Access Point is seeing. In other words, just like in the Ethernet world, all packets are broadcast out for everybody to see. There are a number of programs that are available for free that allow anybody to setup his client to listen to this traffic. In addition, there is no way to tell if someone else is sniffing your data.

So, while most people intuitively understand that a public wireless network is not a secure environment, they are likely to accidentally or unknowingly expose private information to other people within the same environment.

## About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, NetworkWorld-Interop, CSI, and InternetWorld are among the most popular and highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

*Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients.*

### Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

### Security Blanket & Emergency Response

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked and web sites or critical business resources are compromised, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment.

### Intrusion Detection and Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

### Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

### Security Policy & Best Practices

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice.

### Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

### VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

**Boston**   **Los Angeles**   **New York**   **San Francisco**   **Tampa**   **Washington DC**   **Sacramento**  
**www.SystemExperts.com**

**info@SystemExperts.com**