

Wireless Security FAQ



Providing mobile IT pros with remote access to all business apps may put a company's vital information at risk. Read [Security in the Wireless Revolution](#) to find out about today's available wireless systems and the type of security you need to avoid costly and dangerous security concerns.

Going wireless is a big step, and maintaining wireless security is an ongoing process. So it's little surprise that IT pros have so many questions about wireless technology. We've gathered some of those most frequently asked and invited our wireless expert, Brien Posey, to answer them. The FAQ list will be constantly evolving, so you're invited to send us other questions you may have. Just [mail them to us](#) or post them in the discussion area at the end of this FAQ.

Table of contents

| | |
|--|---|
| Is it true that WEP can be easily hacked? | 2 |
| Can a Pringles can be used as an antenna by hackers? | 2 |
| Can a VPN ensure wireless privacy? | 2 |
| If WEP encryption is so insecure, then why does 802.1x rely on it? | 2 |
| Is it true that wireless network users are themselves vulnerable to security breaches even when connected to a corporate LAN via a wireless VPN connection? | 2 |
| Is it safe not to tunnel traffic that is ultimately destined for the Internet? | 3 |
| How can a wireless workstation be subject to buffer overflow attacks? | 3 |
| How does public key security work? | 3 |
| Can a hacker attack an access point? | 3 |
| Is SSID broadcasting a security threat? | 4 |
| Does MAC filtering work as a security measure? | 4 |
| Is DHCP a security threat? | 4 |
| Is signal jamming a security issue? | 4 |
| Can adjusting the signal strength help secure a wireless network? | 4 |
| If I have implemented all of the standard security mechanisms, can I guarantee network security? ... | 4 |
| Should I use SNMP to manage my wireless network? | 5 |
| I can't adjust the power level on my access point, and the antenna is not removable. Is there any way to help to prevent the signal from leaving the building? | 5 |
| How can I audit a wireless network? | 5 |
| How can I detect rogue access points on my wireless network? | 5 |

Is it true that WEP can be easily hacked?

Anyone with a laptop and a wireless network card can sniff encrypted packets as they flow across a wireless network. Depending on the content and structure of captured packets, a hacker simply needs to capture anywhere from 100 MB to 1 GB worth of packets. Such a sampling size guarantees that the hacker will have all of the information he needs to break the WEP encryption. Once the necessary volume of data has been captured, the hacker can simply run a freeware utility against the captured packets to derive the WEP key.

Can a Pringles can be used as an antenna by hackers?

Yes. Although a typical wireless NIC has a range of 100 to 300 feet, faint radio signals are transmitted far beyond the network's operational area. By investing about ten dollars for a few parts from Radio Shack and for a can of Pringles, you can easily build an antenna that can intercept a signal from as far as 10 miles away (assuming that there is a clear line of sight). Other industrial-strength antennas can intercept a signal from even further away.

Can a VPN ensure wireless privacy?

Setting up a VPN greatly enhances the privacy of a wireless network, especially when used in conjunction to WPA or WEP encryption. If you are considering implementing a wireless VPN though, there are a couple of issues that you need to consider. First, if the wireless signal drops for a second, users' connections will be terminated, and they will have to reestablish their VPN connections. Second, a wireless VPN offers no protection against rogue access points. Third, a wireless VPN doesn't provide wireless users the same seamless network access as wired users have since they will usually have a separate login for the VPN connection.

If WEP encryption is so insecure, then why does 802.1x rely on it?

802.1x by itself is not secure. 802.1x only becomes secure when combined with the Extensible Authentication Protocol (EAP). EAP makes it possible to securely distribute WEP keys. Rather than relying on static WEP keys, the 802.1x and EAP combination allow each session to have a unique WEP key. Additionally, WEP keys automatically expire every ten minutes. Since each session is frequently rekeyed, it makes it impossible for a hacker to collect the necessary volume of packets between key changes.

Is it true that wireless network users are themselves vulnerable to security breaches even when connected to a corporate LAN via a wireless VPN connection?

Yes, there are three primary ways in which wireless users are at risk. First, if volumes or folders on the users' machines are shared, it is possible for other users within the subnet to access the contents of those shares. Second, someone on the same subnet as the user could perform a buffer overflow attack against the user. Finally, not all traffic is routed over the VPN. Traffic related to Internet usage is routed over the Internet. This traffic is subject to capture through the usual methods.

If I have never shared any files or folders on my hard disk, is my information still vulnerable to compromise while I am using a wireless connection?

Yes. Even if you never create a share point, Windows has a few shares of its own. There is a share called Admin\$ and another share for each hard drive (C\$, D\$, etc.). You can't disable these shares because Windows depends on them. To prevent these shares from being exploited, make sure that the system is running a personal firewall. Also change the local Administrator's username and password to further reduce the chances of these shares being exploited.

Is it safe not to tunnel traffic that is ultimately destined for the Internet?

When a wireless user is connected to the corporate network via a VPN link, it may seem that since traffic destined for the Internet must be first routed through the corporate network that it will pass through the VPN. However, this isn't always the case. VPN tunnels can become congested rather easily. To conserve bandwidth, some VPN implementations transmit traffic destined for the Internet over the wireless network but outside of the VPN tunnel. This means that Internet traffic is unencrypted. This shouldn't be a problem since nothing sensitive should be flowing across the Internet. However, some users use the same password for Web sites as they use for access to the corporate network. If such a site doesn't encrypt passwords, it might be possible for someone to steal a password and use it to gain access to the corporate network.

How can a wireless workstation be subject to buffer overflow attacks?

Unless a workstation is running a personal firewall, other machines on the same subnet as the workstation can communicate with the system across all TCP and UDP ports. The corporate firewall only blocks malicious traffic from the outside world; it does nothing to prevent attacks from within.

How does public key security work?

The basic idea behind public key security is that every user has two mathematical encryption keys, a public key and a private key. A user's public key is accessible to anyone, but the private key is accessible only to the user. When someone needs to encrypt traffic before sending it to a specific user, the encryption process begins by downloading the user's public key. The public key is used to encrypt the packets, but is useless for decrypting it. The packets can only be decrypted by the corresponding private key, which is only held by the recipient.

Can a hacker attack an access point?

Absolutely. Almost all access points ship from the factory set to use either 192.168.0.0 or 192.168.1.1 as their IP address. Furthermore, the default login credentials are usually Administrator or Admin and "PASSWORD" or a blank password. Of course, the credentials vary among brands of access points, but it is very easy to perform a simple query against an access point to find out its make and model. From there, it's simply a matter of looking up the default login credentials on the manufacturer's Web site. Unless the default password has been changed, the attacker will be able to gain full control over the access point.

Is SSID broadcasting a security threat?

Have you ever tried to connect to your wireless network only to have a neighbor's network show up on the list of available wireless networks? The reason your neighbor's network displayed as an available choice is because SSID broadcasting was enabled. SSID broadcasting causes the wireless access point to tell all available clients the name of the network. If SSID broadcasting is disabled, hackers can still hack the network, but they will have to figure out what the SSID is rather than having it handed to them.

Does MAC filtering work as a security measure?

Many access points allow you to enable MAC filtering so that only clients with specific MAC addresses can connect to the wireless network. MAC filtering works to an extent as a security measure, however, it is fairly easy to spoof a MAC address. You can make it a bit harder by enabling MAC filtering. That way, before a hacker can spoof a MAC address, he must first figure out which MAC addresses are authorized to use the wireless network, which can be done by sniffing packets. So, while MAC filtering will protect you against less skilled hackers, it won't stop a really determined one. It will only slow him down.

Is DHCP a security threat?

Almost all access points have DHCP (Dynamic Host Configuration Protocol) enabled by default so that they will automatically hand out IP addresses to any workstation that connects to them. In a way, DHCP is an indirect security issue because you are simply handing a hacker an IP address related to your network. On the other hand though, most access points will not issue an IP address until a station's WEP (Wired Equivalent Privacy) pass phrase has been verified.

Is signal jamming a security issue?

While there have been a few reports of signal jamming being used as a denial of service attack, signal jamming often comes from other sources. 802.11B networks operate in the 2.4-GHz frequency range. This is the same frequency range used by many cordless phones. It is possible for a wireless network signal to be disrupted by a cordless phone, a microwave oven, or another wireless network. In the past, one solution was to upgrade to a wireless network that used the 5.8-GHz frequency range. However, cordless phones now exist that operate on the 5.8-GHz frequency. Further, the signal from a 5.8-GHz network has a tougher time penetrating walls than the signal from a 2.4-GHz network.

Can adjusting the signal strength help secure a wireless network?

When you install a wireless network, it's tempting to use a big antenna and the highest available transmitting power so that everyone gets a great signal. However, it's often better to turn down the power in an effort to prevent the signal from leaving the premises. After all, you don't want people in the parking lot snooping on you.

If I have implemented all of the standard security mechanisms, can I guarantee network security?

Although it's relatively safe to assume that the network will be secure, it's important to put your security to the test through penetration testing. Penetration testing is basically hacking your own network to see if vulnerabilities exist.

Should I use SNMP to manage my wireless network?

SNMP is a double-edged sword. If an access point supports SNMP, then you will be able to manage it in the same way that you would manage any other SNMP-enabled device. At the same time though, if your access point were to be hacked, then the hacker could use SNMP to gain all sorts of information about your network. I recommend disabling SNMP on your access point unless you really need it.

I can't adjust the power level on my access point, and the antenna is not removable. Is there any way to help to prevent the signal from leaving the building?

Place the access point near the middle of the facility. Avoid having it near a window at all costs and try not to place it near an exterior wall.

How can I audit a wireless network?

You would audit a wireless network in the same way that you audit any other network. The exception is that many access points also compile logs of which stations have connected to them and when. If your access point offers such a feature, then I recommend taking a quick look at the logs at least once a day.

How can I detect rogue access points on my wireless network?

There are a number of free utilities available, such as NetStumbler and WaveRunner, that will scan for wireless devices for you. You can also use commercial products such as RogueWatch that offer more features.

Related TechRepublic resources:



TechRepublic books and CDs:

[Wireless Networking Survival Guide](#)

[802.11 Wireless Networking Resource Guide](#)

Downloads:

[Wireless Equipment Checkout Tool](#)

[Wireless policy template](#)

Articles and columns:

[At last, real wireless LAN security](#)

[VPNs are good but not perfect](#)

[Final step in security audit process](#)

[How to troubleshoot your wireless network](#)

TechRepublic communities engage IT professionals in the ultimate peer-to-peer experience, providing actionable information, tools, and services to help members get their jobs done. TechRepublic serves the needs of the professionals representing all segments of the IT industry, offering information and tools for IT decision support and professional advice by job function.

CIO Republic: Get analysis and insight on e-business, leadership, executive careers, business strategy, and technology.

IT Manager Republic: Access technology insights, project and personnel management tips, and training resources.

NetAdmin Republic: Get tips on Windows, NetWare and Linux/UNIX administration, infrastructure design, and network security.

Support Republic: Obtain detailed solutions to desktop hardware, software, and end-user support problems.

IT Consultant Republic: Find information and advice on client and vendor relations, project management, and technology.

TechRepublic site features

Free e-newsletters: Keep up-to-date on any aspect of the IT industry with e-newsletters—from tech stocks to daily software tips, from IT careers to hot trends—delivered right to your e-mail Inbox.

Free downloads: We've collected resources to make your job easier, including ready-to-use IT forms and templates, checklists, tools, executables, Gartner product analyses, and white papers.

TechRepublic's books and CDs: Find the latest books and CDs about today's critical IT topics, including PC troubleshooting, VPN, TCP/IP, Windows client and server issues, and Cisco administration.

Discussion center: Open a discussion thread on any article or column or jump into preselected topics: career, technology, management, and miscellaneous. The fully searchable Discussion Center brings you the hottest discussions and threads and allows you to sort them by topic and by republic.

Try our premium subscription product, TechProGuild, free for 30 days. Our online IT community provides real-world solutions and the latest articles, resources, and discussions affecting frontline IT pros. Get access to more than 250 full-text IT books, along with exclusive downloads and in-depth articles on network and system administration, PC troubleshooting, help desk and support issues, and more.