Security for the Wireless Network: The Ubiquity of Wireless Access

They’re convenient, and they’re seemingly everywhere. Wireless networks are taking our culture by storm. From businesses and homes to public spaces, it’s easier than ever to work using Wi-Fi. With the help of today’s technology, almost anybody with basic computing skills can successfully set up a wireless network. It’s easy – so easy in fact, that most people don’t fully grasp exactly how their data will be transmitted, and why there are inherent security risks associated with wireless. It has been estimated that approximately 40–50% of all wireless network/data/access users have either inadequate network security or no security at all.$^1$ Whether using a home network, corporate Wi-Fi, or a public hotspot, wireless networking is a convenience that can come with a steep price tag.

The Price Paid for Wireless

The results of a 2005 study done by The Diffusion Group found that one of the primary reasons small-to-medium businesses choose Wi-Fi is its cost-effectiveness. However, according to this study, the security implications of using wireless networks can quickly erase any benefits that Wi-Fi may offer. A business working with sensitive or private information and operating on an insecure network can open itself up to serious litigation in the event of a security breach.$^2$

![Figure 1: Security threats to wireless LANs](image)

From a street in any metropolitan business district, it can be shockingly easy to access any number of wireless networks. In an unscientific “test drive” conducted by Computerworld New Zealand, a casual stroll through Wellington’s business district indicated that only about two-thirds of the business networks available were secured.

$^1$ informit.com, March 2005

$^2$ IT Observer, August 2005
by any kind of encryption. In an unscientific “drive-by” experiment conducted by Edhat.com, 68.7% of the wireless networks found in the Santa Barbara, California area were not secure.

This cavalier attitude toward wireless security can lead to serious problems for any company in the long run.

**Encryption in Action**

There’s a lot of talk about encryption protocols and how important they are, but can they really keep a wireless network safe? The 802.11 specification is a family of protocols developed for wireless LAN technology. Let’s look at the 802.11 protocols in use today, what they do, and how they stack up.

**Wired Equivalent Privacy (WEP)**

Designed for Wireless Local Area Networks (WLANs), WEP provides wireless security equivalent to that of a wired LAN. While it is still considered to be a basic deterrent, it has several known flaws that any moderately skilled hacker could exploit with just a little time and a few tools.

A team from the Association for Computing Machinery stated that, in regard to 802.11 protocol security flaws, “with proper equipment, it is practical to eavesdrop on WEP-protected networks from distances of a mile or more from the target.” At the March 2005 meeting of the Information Systems Security Association (ISSA) in Los Angeles, a team of FBI agents was easily able to hack into a WEP-protected network in approximately three minutes.

While WEP is regarded as the baseline from which subsequent, more effective protocols were developed, today it is primarily used with older equipment. In order to avoid the security issues presented by WEP, a switch to either WPA or WPA2 is recommended.

**Wi-Fi Protected Access (WPA)**

Built upon the foundation of WEP, WPA was created in 2002 to bring enhanced LAN security to the wireless market. WPA uses Temporal Key Integrity Protocol (TKIP) encryption, using the same RC4 algorithm as WEP for encryption, but adding sophisticated key management and effective message integrity checking. Developed in conjunction with the IEEE 802.11 Standards Working Group for WLANs, WPA effectively replaced WEP and the other security features of the original 802.11 standard.

WPA offers dynamic key encryption and mutual authentication. It secures both email packet headers and their payloads, and provides a deterrent to replay attacks. WPA’s enhanced encryption is an ideal solution for wireless networks that deal with many different types of 802.11 radio Message Integrity Checks (MICs) such as public hotspots. Most leading wireless access point and chip set vendors have lent their support to WPA.

WPA is not a miracle cure however, and as with any new solution that addresses existing issues, new issues have emerged as a result. Like its predecessor WEP, WPA has been found to have weaknesses that can be used to bring down a network. Two attack techniques adept at exploiting WPA vulnerabilities are dictionary attacks and Denial of Service (DoS) attacks.

A dictionary attack tries to defeat an authentication mechanism by searching a large number of possibilities to determine its pass phrase. As a WPA-protected connection is being established, four data packets are exchanged. Once a hacker has access to those four packets, he or she can carry out a dictionary attack on the pass phrase. Pass phrases of 14 or more characters are least susceptible to a dictionary attack.

---

3 Wireless Security Shaping Up, But Still Some Leakage, Computerworld New Zealand, August 2005
4 Ed Logs On, Edhat.com, August 2005
5 Communications of the Association for Computing Machinery (ACM), 2005
A DoS attack brings a network down by flooding it with useless traffic. Using an erroneous encryption key, a hacker transmitting two packets of unauthorized data during a one-second interval can fool the system into believing it’s under attack so that it will shut itself down, temporarily disabling all user connections on that access point.

WPA is most effective when supplemented with other wireless security precautions.

Figure 2: Methods to Secure Wireless LANs

Wi-Fi Protected Access 2 (WPA2)

The second generation of WPA, known as WPA2, replaced TKIP encryption with 128-bit Advanced Encryption Standard (AES) encryption for compliance with FIPS140-2 government security requirements.

With each successive generation of standards, there are new issues to address. WPA2 requires a dedicated chip to handle the encryption and decryption, which for many will mean a hardware upgrade in order to take advantage of the benefits.

However, as the standards evolve and solidify, wireless networking will become less about risky business and more about its true objective: flexibility for enterprises and their users.

Anatomy of a Hacker

As the ubiquity of wireless networking is relatively new, it’s a prime target for up-and-coming hackers looking to make an impact, or seasoned criminal hackers out for financial gain. Many people still harbor the stereotypical picture of the geeky hacker in their minds: a lonely social outcast who lives with his parents and
boosts his self-esteem through technological mischief carried out late at night from a darkened suburban bedroom.

But that’s exactly what they want everyone to think.

In reality, a hacker can be anyone: the friendly, businesslike “researcher” on the other end of a phone conversation, the guy sitting innocently in his car outside an office building, or even that freshly-scrubbed college girl sitting next to you at your favorite coffeehouse.

Using a variety of easily accessible tools such as encryption-cracking programs, Denial of Service (DoS) tools, LAN scanners, long-range antennas, wireless sniffers, and automated exploit software, hackers can do everything from eavesdrop on email and Instant Messaging conversations to steal and use financial data such as account information and credit card numbers.

Hackers often look for access points that have been set up without changing the default/factory configuration to prevent the open broadcast of Service Set Identifiers (mobile device passwords for connecting to wireless stations), or without resetting the default password.

In public hotspots, the risk of attack is greater. Hackers can hijack data simply by launching an attack against unsuspecting computer users as they log on to the network.

Sometimes, however, the door to a wireless network is left open for hackers by unconcerned or uninformed employees. Because wireless networks are so easy and inexpensive to install, employees can buy a wireless card for as little as US$75 and set up unauthorized, unencrypted wireless access points by simply attaching them to a “wired” corporate network. It’s estimated that an employee’s ability to buy and install unmanaged access points could result in more than 50% of enterprises exposing sensitive information through wireless networks.”

Assault in Broad Daylight: Wi-Fi Phishing

According to a recent report on the BBC News Web site, the top five countries for wireless hotspots today are the US (31,074), UK (12,004), Germany (8,714), France (4,014), and Japan (2,738). More computer users are taking advantage of the opportunity to get connected or get work done in airports, hotels, coffee houses, and other public places.

![Figure 3: 2005 Wi-Fi hotspot growth](image)

Every modern convenience brings with it a group of opportunists ready to exploit it for destructive purposes, and wireless hotspots are no exception. Anytime a user connects via a wireless hotspot, they are vulnerable to what is called an Evil Twin attack.

---

6 Gartner, 2004
7 Wi-Fi Cities Spark Hotspot Debate, BBC News, October 2005
Also known as “Wi-Fi Phishing,” Evil Twin attacks take place when a hacker sets up a fraudulent, unencrypted Wi-Fi access point (AP) that mimics the look and feel of the legitimate AP at a given site. In a successful attack, the Evil Twin AP has a stronger signal than the legitimate AP, and computers automatically attach to it when trying to connect to a network. Users log on to the Evil Twin rather than the legitimate AP, and unwittingly give the hacker access to their passwords, files, email accounts, personal account data (banks, etc.), and credit card information.

The promiscuity of clients that hop from hotspot to hotspot is the main vulnerability exploited by phony APs. Hotspotter tools provide information on signal availability and strength, as well as essential network data, monitoring Microsoft® Windows® XP client requests and comparing them to common hotspot SSID names. If there is a match with the client's request, the rogue client acts as an AP with the same SSID.

To reduce risk of Evil Twin-type attacks, users should disable network interface cards when not in use. Windows XP should be configured to connect only to Preferred Networks, only in Infrastructure Mode, and only upon request. In smaller WLANs, configure clients with a list of Specified APs.

Information Security Legislation

Not all of the attacks discussed here are illegal in all jurisdictions. Legislative steps are being taken that will provide a uniform response to these types of crimes. In the U.S., a number of bills have been proposed in recent years:

- **The Identity Theft Protection Act**, introduced in the Senate commerce committee by a bipartisan coalition in July 2005, addresses problems with recent high-profile data breaches by requiring entities that collect sensitive information, such as Social Security numbers, to secure the data physically and technologically and to notify consumers nationwide when data is compromised.8

- **The Securely Protect Yourself Against Cyber Trespass Act (Spy Act)** aims to prevent spyware purveyors from hijacking a homepage or tracking users' keystrokes. It requires that spyware programs be easily identifiable and removable, and allows for the collection of personal information only after express consent is given by users.9

- **The Software Principles Yielding Better Levels of Consumer Knowledge Act (SPYBLOCK)** imposes new rules that would make it more difficult for companies to slip software onto users' systems surreptitiously, require easy directions and options for removal, and prohibit harmful spyware.10

- **The Internet Spyware Prevention Act** makes it a crime to intentionally access a computer without authorization or to intentionally exceed authorized access. If the unauthorized intrusion is to further another federal crime such as secretly accessing personal data, the penalty is up to five years in prison.11

- **The ID Theft Notification Bill** requires organizations that collect the personal data of U.S. citizens to inform consumers when their information has been lost or stolen.12

Whether or not these types of legislation will have an impact remains to be seen. In a historic case from 2004, a 21-year-old American man was sentenced to nine years in federal prison for credit card fraud after taking advantage of the unsecured Wi-Fi network of a chain of home improvement stores.

---

8 Bill Strives to Protect Privacy, Wired News, July 2005
9 Revised Spyware Bill Moves Ahead, Wired News, March 2005
10 Anti-Spyware Law Proposed, PC World, February 2004
11 House Toughens Spyware Penalties, internetnews.com, October 2004
12 Tougher Data-Leak Law Proposed, CNET News.com, April, 2005
As more wireless criminals can be held accountable for their actions, we may see a change in the sophistication of the attacks and the level of risk now associated with wireless computing. Then again, the criminals will continue to find alternative means by which to execute their attacks.

Avoiding the Security Pitfalls of Wireless

Wi-Fi hacking often succeeds because users make mistakes. Education can help them recognize attack symptoms and avoid known risks. In order to provide the most comprehensive defense against a hacker assault on your wireless network:

- **Users should never accept certificates or keys presented when connecting to APs or application servers.** This will avoid “downgrade” attacks, where a phony AP operates without 802.1x, or a phony portal operates without SSL.

- **If an AP offering free Internet seems too good to be true, it probably is.** Given a choice between free wireless and paying out of pocket, most people unfortunately choose the riskier free service every time. A company-defined plan that pays for safe Wi-Fi access will help keep users out of trouble.

- **Encourage employees to use “secure hotspot” tools.** Connectivity platforms with an encrypted login protocol eliminate interaction with spoof-able login portals. WPA network options using 802.1x verify authentication server certificates to help defeat Man-in-the-Middle (MITM) attacks. MITM attacks allow an attacker to read, insert, and modify messages between two parties without either party knowing that the link between them has been compromised.

- **Make sure the Operating System (OS) is securely configured.** Make sure to control the wireless station configuration on employee desktops, laptops, and/or PDAs. By taking users out of the equation, or at least reducing their role in determining device settings, the risk of attack can be significantly diminished.

- **Implement 802.1x-based authentication where possible.** Turn off the broadcast of the manufacturer’s service set identifier, and change the default access point or router password to reduce overall vulnerability levels.

- **Set up an access list.** Determining a list of devices authorized to associate with the access point or wireless router gives you more control over risk.

- **Turn off wireless administrative access to the access point.** As access points broadcast in all directions at once, something as simple as physically locating the access point or router away from external walls and windows can make a significant difference in your level of risk.

**Summary**

Wireless security will continue to be a concern for the foreseeable future. Although a single overall solution has yet to be perfected, the best protection is always prevention. As the tools evolve, we’ll no doubt get closer to the goal of secure wireless nirvana. But as soon as we do, you can bet there’s a hacker out there, happy to move the goal posts once again. Perhaps the best teachers will be the hackers themselves. The battle with the Evil Twin may not be over, but at least our armor is getting better all the time.

For information about WatchGuard’s powerful wireless network security solutions, visit us at www.watchguard.com or contact your reseller.
ABOUT WATCHGUARD
WatchGuard provides network security. The company’s Firebox X family of upgradeable appliances delivers the performance, functionality and security strength to meet the needs of organizations of any size. WatchGuard’s Intelligent Layered Security protects against emerging threats and provides the platform to integrate additional services offered by WatchGuard. All WatchGuard products include a LiveSecurity Service subscription for vulnerability alerts, software updates, expert security instruction, as well as individualized and self-help customer care. WatchGuard is headquartered in Seattle, Washington, with offices throughout Europe and Asia.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis.

©2006 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, Fireware, Peak, Core, LiveSecurity, and Stronger Security, Simply Done are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66356_080906