

The Self-Defending Network: A Business Imperative in a Wireless World

Table of Contents

The Hidden Dangers of a Wireless World: A Manhattan Nightmare	2
Banks Overcome Wireless Dangers	3
The Good News About Wireless	5
The Benefits of a Self-Defending Network	7
The Self-Defending Network About ReymannGroup, Inc.	8
	9

Prepared by:

Dan Verton

Author, *The Insider: A True Story* (Llimina Press, August 2005), *Black Ice: The Invisible Threat of Cyber-Terrorism* (McGraw-Hill, 2003), and *The Hacker Diaries: Confessions of a Teenage Hacker* (McGraw-hill, 2002).

**THE HIDDEN DANGERS OF A WIRELESS WORLD:
A MANHATTAN NIGHTMARE.**

Thursday, Sept. 2, 2004
New York City

Dozens of security checkpoints, hundreds of heavily armed Secret Service agents, thousands of New York City police officers on foot, horses and motorcycles, city blocks barricaded by dump trucks filled with sand and an invisible wireless back door that was virtually impossible to control. That was the security situation at the Republican National Convention (RNC) at New York's Madison Square Garden on September 2, 2004.

While city officials had taken extraordinary measures to bolster physical security and crowd control during the convention, IT security researchers uncovered a disturbing number of unencrypted wireless devices that opened up the convention as well as the networks of hundreds of private businesses to hackers, criminals, viruses and worms.

During a two-hour "war drive" around the site of the RNC as well as Manhattan's financial district, security researchers from Boston-based Newbury Networks Inc. discovered more than 7,000 wireless devices, 1,123 of which were located within blocks of the convention, including a network named WirelessForKerry. Of those devices, 67% were access points that did not have encryption protection enabled. While all of the devices could have been properly and securely deployed, only 37 percent of the devices were configured to help ensure proper security – *a key catalyst for this thought leadership paper on how to deploy wireless technology correctly.*

During the war drive, to which the author was granted exclusive access, technicians set up an unsecured wireless "honeypot" that masqueraded as a Linksys access point. According to log analysis of the honeypot system, a wireless device attempted to automatically connect to the honeypot every 90 seconds as the technicians drove around Manhattan.

The researchers also discovered as many as 2,161 access points and 821 client devices that were broadcasting unique service set identifiers (SSID). An SSID is basically the name of a wireless network that is used to identify the network to its authorized clients. Theoretically, only client PCs with the same SSID are allowed to establish a connection to the network. However, the SSIDs emitted by clients are particularly valuable from an attacker's perspective. Why? Because once an attacker knows that a client is searching for a particular SSID, he can change the SSID of his AP and trick the client into connecting to the attacker's access point.

When it comes to most modern, IT-enabled enterprises, the "security perimeter" has disappeared. In fact, for most companies and government organizations today, the security perimeter is a thing of the past. The breakneck pace of technology insertion in the modern enterprise has created a plethora of new avenues of approach for everything from hackers to viruses, worms and Trojan horses disguised as spam. But a relatively

new avenue of approach remains hidden and often neglected – wireless LANs (WLAN), both authorized and unauthorized.

Almost every sector of the economy is adopting WLAN technology. Today, you can find wireless access points serving the networks of public utilities, manufacturing plants, banking and finance institutions, chemical-processing facilities, nuclear materials processing operations, railroad networks, as well as healthcare institutions, emergency response organizations and even the Defense Department. And the faster these industries deploy such systems without the proper security protections in place, the faster they are putting themselves, their customers and the general public at risk.

BANKS OVERCOME WIRELESS DANGERS

The modern American bank has recognized the security risks associated with the new electronic frontier and, as a result, has deployed all the state-of-the-art electronic security devices that one would expect to find in a security-conscious enterprise – firewalls, intrusion detection devices, password management systems, and powerful encryption technologies. But one technology they have been reluctant to deploy has been wireless networking.

In a 2004 survey of 900 North American financial services companies, Forrester Research Inc. found that only 39% of the financial services firms said they had adopted mobile business applications. That is well below the 47% average adoption rate across all industries. And the reason for this lack of interest is clear: security is still the number one concern.

But there is a growing demand for wireless applications in the banking and financial services industry. The New York Stock Exchange, for example, last year purchased 3,000 Java-based handheld wireless devices for use by its floor traders. Fidelity Investments in Boston has also adopted wireless to support brokerage trading. The firm's program, Fidelity Anywhere, has more than 350,000 subscribers. Raymond James Financial Inc. in St. Petersburg, Fla., is in the midst of an enterprise-wide deployment of wireless networks across its 2,200 locations. The technology is considered necessary to increase productivity, streamline operations and reduce costs – all of which are likely to result in greater customer service and retention. Other major adopters of wireless in the banking and financial services industry include Chicago Mercantile Exchange Inc., Chicago Board Options Exchange, The Hartford Financial Services Group Inc., and Allstate Corp.¹

American Savings Bank in Honolulu, for example, is evaluating a Voice over WLAN (VoWLAN) system with a WLAN infrastructure and WLAN phones.

¹ See "Wireless Leaders and Laggards: Financial Services," by Lucas Mearian, Computerworld, <http://www.computerworld.com/industrytopics/financial/story/0,10801,101708,00.html>

See "Snapshot: Wireless in Financial Services," Lucas Mearian, Computerworld, <http://www.computerworld.com/industrytopics/financial/story/0,10801,101692,00.html>

“We’re evaluating a VoWLAN solution because the bank is morphing itself into a full-service community bank, with greeters at certain branch a WLAN and integrated wireless voice system, the greeter will be able to walk through the branch with customers, and have the phone available to them at all times without being tied to a desk.”

Philadelphia-based Sovereign Bank, the third largest financial institution in the northeast U.S., turned to wireless networking as a means to enable employee mobility and increased productivity, as well as provide an effective disaster backup solution. Brad Rightmyer, manager of network engineering at the bank, said “the adoption of wireless technologies was really the result of the bank’s desire to bring the employee to the customer.”

By adopting wireless technologies, Sovereign has enabled its staff to be more productive by accessing e-mail, Websites, and file sharing for corporate applications when working in a conference room or a colleague’s office. For disaster recovery, wireless communications allow the bank technical staff to access data applications using laptop computers.

The wireless solution for six regional offices encompasses more than 25 Cisco Aironet 1200 Series and Aironet 350 Series access points. Cisco Aironet 1400 Series wireless bridges provide point-to-point networking at five locations. And the Cisco Wireless Security Suite provides enterprise-class security for the bank's entire wireless LAN (WLAN)

And Rightmyer is comfortable with the level of security he gets from his wireless solution. “We check the access points regularly to ensure that configuration parameters haven’t changed, because this is very important for auditing of our security measures,” he said.

Central management is achieved through the use of Cisco’s Structured Wireless-Aware Network (SWAN). Cisco SWAN is a secure, integrated WLAN solution of Cisco "wireless-aware" infrastructure products that minimize WLAN total cost of ownership (TCO) through optimized deployment and management of Cisco’s Aironet Series access points. Core components of Cisco SWAN include Cisco Aironet access points running Cisco IOS Software; CiscoWorks WLSE; an IEEE 802.1X authentication server, such as Cisco Secure Access Control Server (ACS); and Wi-Fi certified WLAN client adapters.

In fact, bank officials are so confident that wireless can be deployed securely that the bank has plans to increase their use of wireless, particularly throughout the bank’s branches and retail centers. Wireless network access enables the bank to support handheld computers used by employees working at a kiosk in a non-branch location and allows mobility within a branch. For example, wireless networks enable Sovereign Bank staff to access e-mail, websites, and file sharing for corporate applications when working in a conference room or a colleague's office. In addition, the bank’s technical staff can access data applications using laptop computers. And by using the Cisco Wireless IP Phone 7920, the technical staff can take their phone extensions to a disaster recovery

center for continuous availability to voice callers.

THE GOOD NEWS ABOUT WIRELESS

The good news about wireless networking is that while it has had security challenges in the past, the technology and our understanding of the security requirements have improved dramatically. The reality is that with a little knowledge and the patience to deploy your wireless network correctly, wireless networking can be made safe and secure.

The mountain of bad press that wireless security has received to date is largely the result of a lack of understanding and knowledge on the part of the victim organizations. Today, there are effective methods of making your wireless network as secure as your wired network. All you have to do is start with the basics and add additional layers of more sophisticated security protections.

The basics of wireless security are, well, pretty basic. But in the aggregate, these steps amount to a well-rounded security posture.

1. Policies. Users at all levels of the organization must be made aware of when and how they are allowed to use wireless systems, and the ramification of not following the company's published wireless security policy.
2. Default Insecure. Wireless access points are often shipped without their security features enabled. It is up to you to configure them properly. One of the most important first steps is to change the Service Set Identifier (SSID) from its manufacturer default value to your own value. Fail to do this, and you make it easier for an attacker to gain unauthorized access to your wireless network.
3. Naming Conventions. You probably shouldn't changed your SSID to read "Bank Vault." Try using a less obvious string of characters that will not tell the bad guys that they've stumbled upon a bank full of money and personal identities. And change your SSIDs on a regular basis.
4. SSID Passwords. Remove the SSID password (the password that allows an administrator to gain access) from its normal location in the Windows Registry to a location known only to a handful of trusted administrators and encrypt it.
5. Don't allow broadcast of your SSID. Force users to type in the correct SSID to make a connection.
6. Encryption. All wireless access points ship with the Wired Equivalent Privacy (WEP) encryption protocol in the "off" position. Despite the known weaknesses of the WEP protections, you might consider turning WEP "on" as a bare minimum. Ideally, you should use more sophisticated encryption, such as Advanced Encryption Standard (AES) below. If you do use WEP, you should also remove the WEP key from the Windows Registry and store it in a less obvious location.
7. Learn WPA. Take the time to learn about the Wi-Fi Protected Access (WPA) standard, which was developed to fill the gap left by WEP. WPA is designed to work with technologies that use WEP. But it has several advantages over WEP.

-
- WPA is based on 802.1x authentication and strong encryption. 802.1x is used for wireless and wired networks, and implements dynamic per user, per session authentication. Additionally WPA has stronger encryption than basic WEP. WPA uses the Temporal Key Integrity Protocol (TKIP) to scramble the keys and ensure that they have not been tampered with. WPA also provides user authentication, which WEP does not. While WEP conducts authentication at the computer hardware level, which is relatively easy to intercept, WPA relies upon the Extensible Authentication Protocol (EAP), a public key infrastructure technology that ensures only authorized users are granted access.
8. Learn 802.11i. WPA is an interim standard that has been replaced by the IEEE's 802.11i standard. The 802.11i architecture will use the Advanced Encryption Standard (AES) block cipher. It also includes security improvements covering authentication, tracking associations, integrity and origin authentication. WPA2 is the corresponding Wi-Fi Alliance testing suite for 802.11i, requiring 802.1x authentication and AES-based encryption. 802.11i-based security is the recommended level for WLANs today.
 9. The DHCP Factor. Disable Dynamic Host Configuration Protocol (DHCP) and use a static IP Address instead. DHCP provides the system's IP address (its street address on the Internet) to anybody who can see your wireless network. Disabling DHCP simply makes it harder for bad guys to operate and could gain you critical time during an intrusion attempt.
 10. Coverage patterns. When implementing the WLAN, ensure that a proper site survey is done such that there is a good coverage pattern for the users, but minimize the "bleed through" outside company walls (as well as above & below – think 3D).

The more advanced methods of securing wireless networks are, well, you guessed it, more advanced than the basics. And yes, they are well worth the effort.

1. Deploy a VPN for remote access. Virtual Private Networks (VPNs) will ensure that only authorized users can access your wireless network and that the data cannot be intercepted. To accomplish this goal, all network traffic should be encrypted.
2. Use RADIUS, which is part of 802.1x authentication. A Remote Authentication Dial-in User Service can be built into an access point, or available as a separate server, to provide an additional layer of user authentication. Users can be directed to a user database and through RADIUS can be checked for authenticity and access credentials. RADIUS servers are typically used with VPNs as well, so they can serve multiple purposes.
3. Layer encryption technologies on top of standard network encryption algorithms, such as Secure Socket Layer (SSL).
4. Use time-sensitive tokens that users must type in within a set period of time to gain access.
5. Conduct regular and ongoing security audits, including detecting rogue APs. This can be automated through many WLAN management platforms to minimize operational impact.

But the wireless security challenge is unique because senior managers of an enterprise may not even know that their employees are using wireless devices to connect to the hard-wired corporate network. Not surprisingly, policies and procedures are not always adhered to. In that case, an enterprise network's last line of defense may be the network itself – a self-defending network.

THE BENEFITS OF A SELF-DEFENDING NETWORK.

An intelligent, self-defending network is critical to security for one reason: of the four core components of any security program — people, policy, process and technology — history teaches us that people, policy and process are rarely enough to prevent serious security breaches. All effective security programs are designed in a way that leverages technology's ability to provide checks and balances to the inherent weaknesses of people, policy, and process.

But what do we mean when we talk about the inherent weaknesses of people, policy and process? First, the people we employ to help manage our businesses are fallible. They are not always trained and educated properly in security. As a result, many of their security missteps are inadvertent. In addition, many employees are extremely good at their jobs and understand how to leverage technology to their advantage. But this can often open a Pandora's Box of potential security problems. Technologically savvy employees know how to work around what they consider to be unreasonable security precautions (process & policy). They understand how to leverage technical and procedural weaknesses to the advantage of job performance. In the wireless realm, this often takes the form of rogue wireless access points that are installed within an office area without the knowledge or consent of security administrators.

These facts of the modern IT-enabled enterprise demand that companies of all sizes deploy network technologies that can fill the gaps created by human fallability and enforce the processes and policies deemed essential to security.

An intelligent, self-defending network can also mean the difference between a proactive security posture that stops major security breaches in their tracks or a stagnant security posture that is riddled with gaps and could lead to a legal or regulatory nightmare.

New laws and regulations passed during the last few years in the wake of massive identity thefts and corporate accounting scandals have raised the security ante for corporate executives at all public corporations. Proactive security, therefore, is now a business imperative. In many ways, it is about survival and accepting the fact that new threats can originate anywhere.

The Gramm-Leach-Bliley Act (GLBA) of 1999, for example, requires financial institutions, including insurance entities, to protect the confidentiality of their customers' personal information and ensure that it is secure during transfer and collection. The GLBA also requires regulators, including state insurance regulators, to enforce these protections.

The Sarbanes-Oxley Act of 2002, for example, was designed to eliminate the ability of executives to illegally “cook the books” by inflating stock prices and filing misleading or false financial statements. And with virtually all financial data being controlled and managed electronically, the risk of insider abuse or external sabotage is significant.

This was evident to many in the aftermath of the firing of Kenneth Livesay from his position as the chief information officer (CIO) at HealthSouth Corp. in Birmingham, Ala. The case against Livesay, who pled guilty in federal court in 2003 to falsifying the company’s earnings and financial statements, highlighted the impact that new laws such as Sarbanes-Oxley are having on IT operations. Suddenly, it became imperative that IT security controls be sufficient to prevent such abuses from happening. Internal control of the corporate enterprise was no longer the sole responsibility of the CEO and CFO (chief financial officer), but of every officer of the company – including the officer responsible for the electronic infrastructure, the CIO.

The third law to make up the ‘big three’ potential legal nightmares for companies is California’s S.B. 1386 privacy statute. The law, which went into effect on July 1, 2003, requires companies that do business with California residents (regardless of where the companies are located in the U.S.) to inform customers when their names, in combination with personally identifiable information, have been accessed by an unauthorized person. When one considers the type and frequency of both internal and external security breaches that are taking place throughout the public and private sectors in America, the implications of these laws are profound.

In the aftermath of several massive security breaches in the credit card and credit reporting industries, proactive information security is receiving renewed attention within the financial services industry.

Whether you have an established information security program or are just beginning to realize the importance of ensuring your financial institution has a safe, sound, and secure infrastructure, today’s risk management strategies call for a broad set of layered security solutions that are proactive, not reactive.

Proactive security demands a layered approach — a defense in depth that identifies, channels and neutralizes threats before they reach critical systems and data. This approach should include intrusion-prevention systems, network traffic anomaly detection, security policy enforcement tools, spyware and malware filters, and a containment mechanism that enables administrators to isolate threats that make it through the outer layers of security.

THE SELF-DEFENDING NETWORK.

A self-defending network is an intelligent network that delivers antivirus, antispyware and worm mitigation capabilities not as standalone devices, but as living, adaptable components of the network ecosystem. By putting these defensive technologies “in” the network rather than “on” the network, an enterprise can effectively improve response

times to threats and increase overall situation awareness.

Today's attacks appear too quickly for IT staff or reactive products to respond. Likewise, the internal makeup of these attacks is changing too rapidly for defenses based on previously identified threat profiles. This brave new world of Internet and network security demands that the network be capable on its own of improvising, adapting, overcoming and surviving whatever security threat it encounters.

An intelligent, self-defending network extends the virtual security perimeter by adding threat intelligence to network endpoints, switches and even remote user connections. By pushing the detection and mitigation of mainstream threats out beyond the edge, the self-defending network puts the advantage of time back in the hands of the security professional and frees up human bandwidth to deal with the truly novel security threats.

A self-defending network also provides system-wide security intelligence that can effectively deal with an incident without bringing the entire enterprise down. The goal is to provide a network immune system that is similar to the human immune system — one where viruses and other malicious microorganisms are incapable of bringing us to our knees. Such a network immune system is critical. Like the human body, the modern electronic enterprise is far too complex for any one device or series of devices working individually to handle. Defenses must be integrated and coordinated. And intelligent, self-defense mechanisms must live in the wire. That's what a self-defending network is all about.

ABOUT REYMANNGROUP, INC.

ReymannGroup, Inc. provides finance, healthcare, retail and manufacturing subject matter expertise. The firm helps companies evaluate their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. ReymannGroup provides customers with independent, highly-qualified professionals, authors of regulations, and subject matter experts familiar with financial, healthcare, retail and manufacturing industry regulations and best practices. For more information, contact ReymannGroup at (410) 956 7334 or info@reymanngroup.com.