Don't Let Wireless LAN Security be the Weakest Link in Your IT Infrastructure

Implement Strong Authentication and Encryption using the 802.11i Security Protocol and Industry-Standard Hardware Chips

Abstract

The objective of this white paper is to review the state of wireless network security in today's enterprise, detailing the most common attacks and the techniques used to thwart them. The cost of implementing wireless networks with inadequate safeguards is greater than most businesses realize, reinforcing the need for stronger, more effective measures. The solution outlined in this white paper focuses on the IEEE protocol for wireless security, 802.11i, coupled with the Trusted Platform Module security chips found in most business-class PCs shipping today. In combination, these two industry standards afford the best in strong authentication and encryption, the two essential elements identified by experts for sound wireless network security.

WLAN Implementation is on the Rise

Employees are consistently clamoring for greater mobility, flexibility and easy access to information. They want access to company data no matter where they're physically located in the enterprise—whether powering up their laptop PCs in a conference room or the company cafeteria.

It's no wonder that, in the last few years, a growing number of firms have been lured by the promises of Wireless Local Area Networks (WLANs). In a report released in November, 2006, Forrester Research polled 752 technology decision makers at North American enterprises about their WLAN adoption plans. More than half said they planned to increase their spending on WLAN technologies in the year ahead[1].

[1] "WLAN Adoption in the Enterprise 2006," Chris Silva, November 20, 2006, Forrester Research Inc.

wave®

While employees prize the flexibility of WLANs, employers love the cost savings. A handful of access points distributed around a building can support dozens of users for a fraction of the cost of "pulling cable"— with none of the disruption. There's usually no additional cost at the client side either as the hardware required for wireless network configurations has become nearly endemic in the modern PC.

But all this flexibility, convenience and cost savings comes with a huge risk: without proper security, an inadequately secured WLAN leaves an organization's information assets vulnerable.

Threats to WLANs Abound

In a wired network, the physical plant acts as the first line of defense. For someone to gain access, he or she must compromise a physical component of the network — a network drop, a cable run or a switch. Wireless technology removes this barrier to the would-be hacker. With a wireless access point connected to the network, any WiFi-enabled device poses a threat, merely by its presence within range of an access point.

Invariably, this leaves the WLAN exposed to various forms to attack. Among them:

- *Denial-of-service attacks* occur when an attacker bombards a targeted access point with requests, connection or failure messages causing legitimate users to be unable to access the network.

- *Network injection* takes place when a hacker makes use of access points that are exposed to non-filtered network traffic, enabling the assailant to inject fake network reconfiguration commands and obtain sensitive data.

- *Man-in-the-middle attacks* occur when a hacker entices users to log into a phony or "soft" access point running on a compromised computer. Once this is done, the attacker connects to the real access point through another wireless card. The attacker can then "sniff" traffic for personal data, passwords and credit card numbers.

These attacks are far more common than some might imagine. According to a PriceWaterhouse Coopers survey, nearly 43 percent of organizations that have deployed wireless networks have had security breaches. Of those, 83 percent reported monetary losses. While it's difficult to determine the amount of money lost specifically to wireless network breaches, network vulnerabilities top the list of concerns among IT administrators. In fact, 86 percent of companies consider network vulnerabilities their top priority, surpassing fears of security compromises of client computers, internal attacks and physical theft.[2]

---

[2] "Aligning Data Protection Priorities with Risks," Jonathan Penn, April 13, 2006, Forrester Research Inc.

wave®

Steps Organizations Are Taking — Are They Enough?

Most current WLAN security protocols focus on two elements: *authentication* of those who access the network and the *encryption* of data that flows over it.

As with wired networking, the simplest security steps are physical and structural. A wireless networking infrastructure can simply make itself harder to find. Taking steps such as locating access points away from the parking lot and neighboring businesses, and disabling the broadcast of the access point's identity (SSID) are the first security measures that an organization can do. This is the easiest method of access control. Beyond these initial steps, many firms implement authentication and encryption in their basic forms: Media Access Control (MAC) filtering, Wireless Equivalent Privacy (WEP) or WiFi Protected Access (WPA).

MAC Filtering

MAC filtering is a method of authorizing only known computers to a wireless network. The MAC address is a unique identifier assigned to every piece of networking equipment by the manufacturer. Most wireless access points can maintain a list of authorized network devices by their MAC address and deny service to unlisted devices. While this is a step in the right direction toward machine authentication, it falls short due to the ease of spoofing MAC addresses across the network. It is also a hassle to administer since anytime a new device comes online or an authorized device requires decommissioning, every access point needs an update.

Wireless Equivalent Privacy (WEP)

Another attempt toward authenticating only known machines, as well as encrypting data as it flies through the air, is to turn on WEP for each access point. WEP takes a single shared secret – a key – and relies on the access point and each authorized device knowing the secret. That shared secret is then used to encrypt the data across the network. WEP is better than no encryption — but falls short for two big reasons:

- *Keeping a shared key secret is hard to do.* Because everyone has the same key, the whole system depends on every employee guarding the secret. And, since the keys are often complex and random, they frequently end up taped onto the side of the very access point they're designed to protect, or worse, written on the conference room bulletin board.

- *WEP keys can be hacked using freeware.* In the era of slow computers and minimal wireless traffic, WEP was "good enough." However, in today's world, even a perfectly provisioned WEP access point can be cracked in minutes using a cheap laptop and freeware tools. Just Google "WEP crack."

WiFi Protected Access (WPA)

A step up from employing relatively easy-to-hack WEP keys is WPA, an encryption standard that was proposed as an intermediate solution after the industry realized the severe security weaknesses of WEP. WPA is configurable in a similar way to WEP and also relies on key-sharing. Yet while still relying on relatively insecure encryption algorithms, it adds a key-rotation protocol that makes "sniffing" the key out of the air far more difficult for a would-be network assailant. More importantly, it works with an entirely different key management and authentication protocol, 802.1x, paving the way for a truly viable security environment.

wave®

A Better Wireless Security Protocol: 802.11i

Despite the shortcomings of the aforementioned wireless network security protocols and methods, there are two widely available industry standards that, when combined, create a best-practice, world-class solution to the wireless networking problem. The first is the IEEE standard called 802.11i, which offers both elegant authentication mechanisms and strong encryption. The second is an industry-standard hardware security chip, the Trusted Platform Module (TPM), found on millions and millions of PCs in businesses around the world.

> *There are two widely available industry standards that create a best-practice, world-class solution to the wireless networking problem.*

The authentication component of 802.11i, called 802.1x, is designed to lock down network access ports in any network. When configured correctly, an 802.1x system limits that port's access only to authentication data until a successful authentication occurs. Still, in setting up 802.1x authentication, the standard does not decide who gets access to an enterprise's network. That critical decision point requires an authentication scheme with the most secure method being Infrastructure (PKI). PKI involves generating two unique keys that can validate each other: a private key stored on the PC and a public key embedded in a digital certificate. The private key is used to encrypt information, and the public key is used to validate and decrypt information sent by the certificate owner. 802.1x makes passing and validating PKI certificates essentially transparent. It also creates substantial assurance that the claimed identity of the laptop or PC seeking access is valid.

For a wired network, the simple implementation of 802.1x authentication might be sufficient, but for a wireless network, the process does nothing to protect the subsequent traffic between the end user and the network resources that is exposed through the air waves. The 802.11i standard thus mandates the use of WPA2 encryption following 802.1x authentication. WPA2 is an enhanced version of WPA that was created to overcome the security weaknesses of WEP. Therefore, when the client connects to the network and his identity is verified, all the data in the connected session is uniquely encrypted with minimal key management overhead. Shared keys are eliminated and there is a low risk of data or system compromise. When combined with 802.1x, WPA2 creates an extremely robust end-to-end authentication and encryption ecosystem for protecting network resources when deploying a wireless network.

wave®

A Certificate is Only as Secure as its Private Key

The private key is the unique secret that provides trust, and it must be kept private. Typically, when the private key is created, it is stored either in software (itself encrypted), or on a token such as a smartcard. While certificate-based authentication is certainly better than relying on spoof-able MAC addresses, the private key's storage method creates additional concerns for locking down the network. In a software-based 802.1x implementation, the private key can be transported for use on a rogue platform. Or with smartcards, the smartcard can be stolen. In either case, the weak link is the method in which the private key is protected.

Beyond protection, this simple step irrevocably binds the certificate to the platform.

As a result, a secure environment on the client PC for creating and storing the private key is required. That's where Wave Systems plays a crucial part. To harden the process, Wave Systems' software ensures that the private key is created by, and secured by, a dedicated security chip, called a Trusted Platform Module or TPM. In the standard Microsoft certificate issuance process, users and administrators use the client-side Cryptographic Service Provider (CSP) to generate and store a certificate's key pair. Using the Wave TCG-Enabled CSP ensures that the TPM generates the key pair, and protects the private key with secure, dedicated hardware.

Beyond protection, this simple step irrevocably binds the certificate to the platform. Even with a highly secure process of authentication, using multiple authentication factors and valid certificates, there's little evidence that the PC connecting to your secure network is a known, trusted endpoint. Using Wave software and TPM hardware, network access and policy decisions can be based not only on the identity of the user, but also on the identity of the platform itself.

Additionally, Wave provides mechanisms for using multi-factor authentication to access the private key for authentication. This means that when using a certificate for authentication, administrators can require users to first authenticate with any combination of a password, a PIN or a fingerprint.

wave®

Wireless Security Solved: Now What?

Enabling 802.11i wireless security is just one of dozens of examples of how leveraging the industry-standard TPM security chip enhances the security of a corporate network. And it can be done without having to retrofit the entire installed base. By taking these steps, administrators have — whether they're conscious of it or not — taken the preliminary steps needed to implement a Trusted Computing enterprise, where security is rooted in trusted client hardware and administrators have the tools to manage the technology.

Using Wave's back office products, an enterprise can easily administer, manage, provision and control the TPMs present on the machines in the network. In a typical Microsoft Active Directory infrastructure, network administrators are allowed to make policy decisions based on the level of assurance they have in the end platforms.

Policy decisions can be as simple as allowing TPM-authenticated wireless clients to access the printer on the 11th floor. Or, network administrators can deploy a complex group management policy allowing step-up authentication for managers accessing pockets of sensitive data on the network. These types of policy decisions are fundamental in establishing a best-practices infrastructure for Sarbanes-Oxley, HIPAA and Privacy Act regulations.

Enterprises can know with a higher level of certainty than ever before that only known users, acting on known machines from known locations have access to their most critical resources. *That's* security.

Enabling a More Secure Network

Having full confidence in the identity of the platform requesting access to the network is at the heart of the Trusted Computing initiative, pioneered by the Trusted Computing Group, which sets standards for a more secure computing environment and counts as its members 150 industry leaders, including virtually all the leading PC OEMs.

This group has been responsible for defining the open standards of a hardware security chip now shipping on tens of millions of PCs each year. That chip, the TPM, is the cornerstone of the next generation of security solutions, from strong authentication to data encryption to password management and more. Business-class machines from major OEMs already ship with a TPM as standard equipment. Furthermore, the next generation of the Windows operating system, Vista, makes use of the TPM in its BitLocker Full Disk Encryption product.

Enabling TPM authentication for secure wireless networks is something enterprises can do today. Machines with TPM-hardened certificates will be more trusted than those using legacy

wave®

authentication methods, and network administrators can use this additional level of trust to make policy decisions. Over time, corporate networks will become increasingly more secure as TPM-enabled machines become more widespread. In addition to the security benefit, if businesses are using external tokens, they can begin to lessen their reliance on them and leverage the industry-standard token functionality of the TPM, thus helping reduce costs and support hours.

While using TPMs to lock down 802.11i security is a smart move, TPMs are an important security tool to be applied in many network processes such as Network Access Control (NAC), data encryption, secure e-mail and VPN access. Building wireless network support for TPMs prepares network administrators for many other easy-to-implement network security solutions.

Conclusion

The combination of 802.11i and TPM standards offers a solution for wireless networking security that is ready for widespread implementation. Every network administrator can benefit from the deployment of this technology. The skills learned in deploying this solution are highly reusable and are part of most NAC and VPN solutions. The solution is not complicated to set up, is scalable to tens of thousands of users and is easy for the user to manage on a day-to-day basis. Security is always a challenge but, with the right tools, can become easy-to-deploy and easy-to-use.

About Wave Systems

Wave Systems solves the most critical security problems for enterprises and government with solutions that are trustworthy, reliable, easy-to-use and offer a speedy return on investment. Wave's trusted computing solutions include strong authentication, data protection, advanced password management and enterprise-wide trust management services.

Wave's network management products include:

- **EMBASSY**® **Authentication Server** provides centralized management, provisioning and enforcement of multifactor domain access policies. With EMBASSY Authentication Server, authentication policies can be based on TPM credentials, smartcard credentials, user passwords or fingerprints.

- **EMBASSY**® **Network Access Control** allows network administrators to easily deploy strong authentication policies on a corporate network integrating with standard Windows functions.

- **EMBASSY**® **Key Transfer Manager** is a key archive system that ensures recovery of TPM keys in the event of hardware failure or system transfer to a new user.

- **EMBASSY**® **Remote Administration Server** allows network administrators to remotely manage the security settings and administration of TPM-enabled PCs.