

# Securing the Enterprise Wireless LAN

How to protect against security breaches in a wireless age



Viewpoint Paper



---

# Table of contents

<b>Introduction: The hacker threat</b> .....	1
So how did it happen? .....	1
<b>Overview</b> .....	1
<b>The challenge: more mobility = increased threats</b> .....	2
<b>New threats require new solutions</b> .....	3
<b>Best practices to secure your wireless LAN</b> .....	3
Develop a wireless LAN security policy .....	3
Manage the wireless adapter and client .....	3
<b>Protect the data transport</b> .....	4
<b>Use intrusion detection, protection, and containment</b> .....	9
<b>Protection from external threats</b> .....	10
Policy management and compliance .....	10
Ensure policy compliance .....	11
<b>Conclusion</b> .....	11
<b>Why HP?</b> .....	12
<b>Checklist of recommended practices for WLAN security</b> .....	13

The depth and breadth of wireless devices continues to grow, and it's a boon for businesses as workers are more mobile than at any time in the past. But that freedom comes with a very real threat of significant security breaches. Companies must protect themselves by employing solutions that secure the enterprise wireless local-area network.

## Introduction: The hacker threat

Earlier this year, giant clothing retailer TJX Companies, Inc., acknowledged that hackers had invaded its encrypted software and lifted private customer information from 45.7 million credit and debit cards. Like most businesses, the retailer had in place what it considered to be viable security policies, processes, and technologies. But that wasn't enough.<sup>1</sup>

### So how did it happen?

An investigation continues. But, according to a Wall Street Journal report, it's likely the cyber attacker or attackers who stole the customer records stumbled across a vulnerable store location while staking out a strip mall or shopping center from their car, using only a laptop, a telescope antenna, and an 802.11 wireless LAN adapter. No fancy gadgetry required. But, for them, they were in the right place at the right time.

IP Locks, a database security company, estimates the total potential cost of the TJX incident at more than \$4.5 billion. The breach grabbed national headlines and reignited legitimate fears that hackers continue to have the upper hand. For companies that have been hacked, or those with vulnerable data, and even those who believe their data is completely secure,

there have never been more examples of why wireless LAN security must be taken seriously as a business imperative. News of network security breaches or impending virus attacks appears routinely in trade publications, business sections, and email strings. Some are legitimate warnings. Others turn out to be hoaxes. Nonetheless, the threat is real—and growing.

## Overview

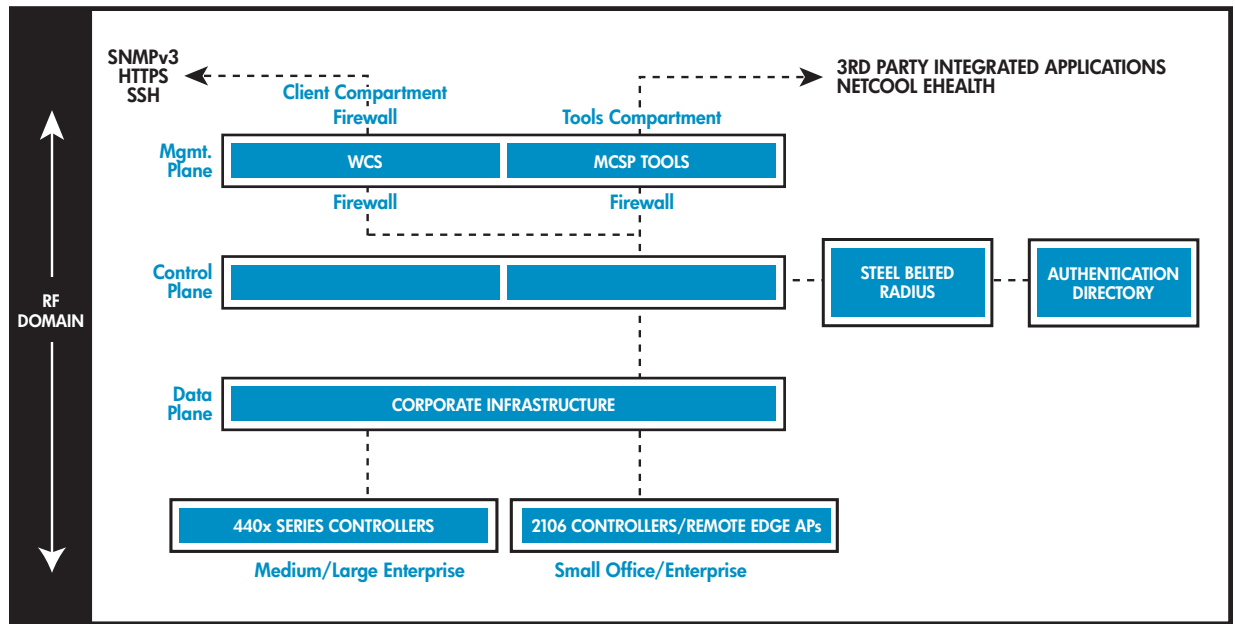
According to the Department of Homeland Security's National Vulnerability Database, an average of 19 new vulnerabilities are posted to the Internet every day. With Wi-Fi technology growing consistently, enterprises must adopt security methodologies designed to the unique requirements and inherent weaknesses of wireless networks. Network and security staff must first assess an extensive list of network authentication and encryption methodologies. Depending on the methodology selected, the IT staff will also need to document the corporate WLAN security policy, as well as define the solutions that will validate user compliance and monitor network vulnerabilities. With a security policy in place, IT staff can then turn their attention to protecting the network from snooping and an ever-expanding list of potential wireless attacks. In this paper, we will address each of these areas and identify the best practices needed to deploy and maintain a secure wireless network.

---

<sup>1</sup> MSN—<http://www.msnbc.msn.com/id/17853440/>

---

**Figure 1.** HP WLAN v3.0 solution architecture overview



## The challenge: more mobility = increased threats

Wireless fidelity, or Wi-Fi, encompasses all things relevant to the generic wireless interface of mobile computing devices in local-area networks (LANs). No matter how it's described though, Wi-Fi has spread like wildfire, leveraging consumer popularity and business benefits to penetrate corporate networks. Many back-end applications, including inventory tracking, mobile printing, and front-end systems, such as point-of-sale terminals, rely on wireless connectivity. The same is true for many front-office applications, such as email and Internet access. Unfortunately, that wireless connectivity exposes the user company to wireless security threats, whether it realizes it or not.

And as the TJX illustration showed, Wi-Fi misuse, abuse, or attack can cause financial harm. Direct costs typically include expenses associated with investigation, response, down-time, and recovery.

Indirect losses are less tangible and include revenue loss, brand damage, and decline in competitiveness and market value, as well as directed remedies and penalties caused by noncompliance with data privacy regulations. Litigation expenses will push expenses even higher.

Mobile workers unwittingly introduce new threats to wireless security. They routinely tap into corporate networks from "unmanaged" locations, including their homes, hotels, airports, and other wireless hotspots. For example, laptops can attract viruses, spyware, and malware. Meanwhile wireless clients can exacerbate the problem by connecting to wireless access points or other wireless clients without the user's knowledge.

To maintain protection, existing security policies, implementations, and practices must evolve to address these new threats and avoid incidents such as the one that plagued TJX. An effective network defense now requires the ability to control all wireless activity that affects your business. This paper also discusses the challenge of doing so and what HP recommends for securing the enterprise wireless LAN (WLAN).

# New threats require new solutions

Because of the quickness of network threats—and the often comparatively slow human response to them—companies are now turning to technologies that automatically identify, prevent, and adapt to them. HP provides a comprehensive solution for protecting wired enterprise networks from wireless threats, ensuring secure and private communications over an authorized LAN.

HP continues to offer its autonomous, stand-alone access points for some small office and mission-critical WLAN solutions. These solutions can now be supplemented by, and upgraded to, the HP V3.0 WLAN Lightweight Access Point (LWAP), controller-based solution. With the HP V3.0 Wireless LAN, every device in the network—from clients to access points to wireless controllers and the management system—plays a part in forming a distributed defense to secure the wireless network environment. Figure 1 illustrates the WLAN v3.0 solution architecture.

The mobility embedded in the HP WLAN solution requires a multilayered security approach to mitigate risks to wireless threats. HP recommends the following:

- Develop a wireless security policy.
- Manage the wireless adapter and client.
- Protect the data transport.
- Use threat control and containment.
- Provide protection from external threats.

## Best practices to secure your wireless LAN

Ideally, companies should validate the practices HP has adapted in its multilayered approach to security against their own risk-management processes. They should also have a strong security implementation. This combination protects each client from inappropriate resource use, theft, and damage to its reputation with customers and partners. HP consultants provide a comprehensive evaluation of the client organization's network-security posture, analyzing the network security compared to industry best practices, and identifying vulnerabilities that could threaten the business. Based on in-depth analysis, HP consultants

offer recommendations on how to improve overall network security and prioritize actions for remediation. In all cases, there should be strong access control and security policies. While the following information will identify important best practices, a comprehensive checklist is provided in the appendix of this paper.

### Develop a wireless LAN security policy

Initially, HP develops a strong WLAN security policy that includes security policy documents detailing the following:

- Purpose
- Scope
- Policy
- Responsibilities
- Violations
- Definition of terms/glossary/education/certifications

The WLAN security policy is vital to success because most security breaches today can still be traced to oversights or errors in security policies. John Stehman, principal analyst with the Robert Frances Group, advises that “enterprises must be capable of actively monitoring WLAN security to detect both security breaches and improperly configured security options.”

### Manage the wireless adapter and client

The next step involves managing the wireless adapter and client. Many laptops today are shipped with built-in Wi-Fi capabilities. The same is true for many handheld devices. These ubiquitous client devices must be protected from wireless threats, ranging from over-the-air viruses and Transmission Control Protocol/Internet Protocol (TCP/IP) exploits to unsafe, unauthorized, or accidental Wi-Fi connections initiated by inexperienced or unaware users.

Conventional defenses commonly deployed on Internet hosts, including file encryption, anti-virus, and personal firewall programs, should also be used with Wi-Fi clients. These measures help insulate Wi-Fi clients from TCP/IP intrusions, such as accidental file sharing and worm propagation at wireless hotspots outside the corporate enterprise. However, these measures cannot stop risky Wi-Fi connections. New client defenses are needed to prevent employees from associating with neighbor WLANs, ad-hoc peers, “evil twins” or malicious “honeypots.”

Unauthorized Wi-Fi connections jeopardize corporate assets by exposing confidential data and bridging between networks. HP recommends a third-party client, Juniper's Odyssey, for example, to regain control over employees' Wi-Fi connections in the corporate enterprise. HP recommends the following:

- Maintain the latest operating system patches and wireless adapter drivers. This protects wireless devices from recent vulnerabilities that expose wireless users to dangerous security flaws. Microsoft, Intel, and Broadcom have recently issued patches and wireless-driver updates.
- Use matched clients and RADIUS servers—for example, Juniper's Odyssey, Steel-belted radius or Microsoft XP/Vista with Microsoft IAS—except in circumstances where wireless clients are integrated with the handheld device serving a specific function, such as manufacturing and retail applications. Ensure that vendors remain responsible for the integration and operation of these tools. Additional interoperability testing is usually necessary to guarantee that security mechanisms, data flow, and other features are optimized. Ensure you have analyzed the risks versus the rewards of a mismatched client/server solution, as it could lack valued functionality or security features.
- Configure the clients to associate only with authorized service set identifiers (SSIDs) in the enterprise without having to broadcast the SSID. The HP Consistent Office Environment (COE) solution uses Juniper's Odyssey client, which is configured with only the essential SSIDs for the four regions of the world. This allows the HP user wireless connectivity to corporate resources at any HP facility in which the COE wireless LAN solution is deployed without additional intervention by the user.
- Establish a policy that denies all ad-hoc connections, unless business requirements demand otherwise.
- Use wireless suppression to prohibit simultaneous connections to wired (Ethernet) and wireless networks. Odyssey is one of the first in the industry to deploy this mechanism.
- Use a permission editor, such as MD5 challenge and Lightweight Extensible Authentication Protocol (LEAP) for enterprise laptop use, to lock out insecure or unused protocols.
- Lock Wi-Fi-client configurations. While care is still required when adding new, trusted wireless networks, all other administrative controls can be locked in the Odyssey client. This prevents users from inadvertently changing critical wireless network parameters that could cause vulnerabilities within the enterprise network.

## Protect the data transport

WLAN deployments have evolved from guest access in conference rooms and limited "hot" zones of connectivity to full-blown, companywide coverage. Unfortunately, many of today's deployments are insecure, leaving opportunities for the curious—or even malicious hackers—to gain access to confidential information. Fortunately, securing a WLAN is not difficult. Technological advances and the HP WLAN V3.0 make doing so easier than ever.

HP uses the Cisco Unified Wireless LAN controller-based product for the HP WLAN V3.0 solution. The following recommendations constitute HP best practices for securing the data transport layer of the WLAN:

- **Complete site surveys**—This measures and establishes access point (AP) coverage and physical placement. Proper placement of access points helps ensure adequate wireless coverage, while minimizing the amount of power radiating from the device. This also limits exposure to an external attack. Companies should locate access points in the interior of buildings instead of near exterior walls or windows, when possible. Access points should also be located in secured areas, out of reach of unauthorized physical access and user manipulation.
- **Change all default parameters**—Because default settings are generally known and not secure, they should be changed and should comply with the organizational security policy. These include, but are not limited to, SSIDs, system names, passwords, and firewall ports.

Standard network names—such as “tsunami,” “default” or “Linksys”—advertise the availability of access points. To prevent unauthorized usage, change the network name immediately after installation, preferably with one unrelated to your company. Avoid renaming the access-point service set identifier (SSID) with your company’s name, phone number, URL or other information easily mined on the Internet. HP offers an established naming convention for the creation of SSIDs and system names.

Access points automatically broadcast the SSID to any wireless client within range. Such applications as enterprise hotspots or guest access allow users to find the network without assistance. For corporate networks, however, the broadcast should be disabled to block people who may be casually browsing for an open wireless network.

- **Use authentication and key management**—When the wireless equivalent privacy (WEP) was exposed as a weak, standalone encryption method, industry professionals scrambled for better solutions. One of the preeminent alternatives to strengthen the solution was 802.1x, which provides a means for leveraging traditionally strong authentication mechanisms, such as a RADIUS server in a wireless network. In such a scenario, the client must authenticate itself to the RADIUS server or active directory (AD), and the AP authenticates itself to the client before either are granted access to the larger network. In addition, 802.1x can be used to automatically deliver new keys to a client and AP dynamically, overcoming the static key weakness of WEP. When used with server certificates, 802.1x can also help clients avoid connecting to fake honeypot APs. In this context, 802.1x is sometimes referred to as dynamic WEP. Delivering these services requires 802.1x implementations to use one of several authentication protocols called extensible authentication protocol (EAP) types. EAP is responsible for establishing how the authentication process should be carried out and the rules so both client and AP know the rules and appropriate responses for a successful authentication. The most popular EAP types are TLS, PEAP, TTLS and Cisco’s FAST. HP recommends Juniper’s Steel-belted RADIUS (SBR) and the Tunneled Transport Layer Security (TTLS) EAP protocol when the Odyssey client is used.

Another important tool is known as a “shared secret,” which is a text string that serves as a password and creates a trusted relationship between an autonomous AP or wireless LAN controller and the RADIUS server. To protect the RADIUS server and AP/controller clients from brute force computer

attacks, long, randomized shared secret text strings of more than 15 characters should be used. Every standalone AP or controller should have a unique shared secret.

HP also recommends the use of matched (client-to-server) authentication solutions (such as Juniper Odyssey client to Juniper Steel-belted RADIUS Server, Microsoft wireless client to Microsoft IAS). Mismatched client and server solutions will require specialized equipment and expertise for testing. Untested or partially tested solutions will bring unexpected and unsupported results. Matched client- and server-authentication solutions optimize wireless features, functionalities, and support.

Simply because 802.1x is a necessary part of a strong security solution, it does not exclude other security measures. While 802.1x will address authentication, it must also be coupled with an encryption strategy. For example, 802.1x is used as a component of WEP, WPA, and 802.11i, but not as an alternative.

- **Use strong encryption**—Two major hurdles hamper WLAN deployment: WEP and the complexity of add-on security solutions that often prevent IT managers from enjoying the benefits of WLAN security enhancements. The HP WLAN V3.0 bundles security components into a simple policy manager that customizes systemwide security policies on a per-WLAN basis. To enable easy client connectivity, manufacturers typically don't configure access points for over-the-air encryption. Unfortunately, after deployment, many IT managers fail to configure a method for over-the-air security, opening the door most commonly used by hackers.

To stop unauthorized use, remember to configure for over-the-air encryption before the radio is enabled.

Whenever possible, HP recommends that enterprises use the most secure over-the-air encryption tools, either WPA with TKIP/MIC or AES with CCMP.

When client devices force the use of less secure encryption methodologies (like WEP), supplement the solution with 802.1x authentication and configure the server to automatically deliver new encryption keys at 15-minute intervals or less. As WEP cracking tools improve, this interval may need to be decreased. HP recommends companies plan now for the refresh of these devices so that their solutions will support more secure encryption techniques and protocols.

For government agencies, FIPS compliance eases security concerns and will spur the adoption of wireless networks in the federal, state, and local government. FIPS certification and compliance with DoD Directive 8100.2 wireless policy provides government customers with the ability to use wireless more expansively, including deployment of advanced wireless services for nonclassified information, such as asset tracking, voice, and security for guest networking. FIPS compliance requires a lengthy certification process for client and infrastructure devices and mandates the use of IEEE 802.11i, the IEEE standard for implementing wireless security. The HP V3.0 WLAN infrastructure and Juniper's Odyssey client solutions are both certified as FIPS 140/2 compliant.

- **Comply with WLAN regulations and standards**—Comply with and maintain all city, state, government/federal agency, and industry regulations governing the use of WLANs.

PCI DSS, for example, is the payment-card industry data-security standard to protect credit card numbers and cardholder information against loss or theft. The exposure of 45.7 million credit and debit card numbers in the TJX data theft should serve as a wakeup call to retailers who risk losing money and credibility when they fail to protect sensitive customer data. Payment Card Industry Data Security Standard (PCI DSS) compliance mandates an ongoing approach that includes vulnerability assessment and audits to ensure the privacy and security of consumer data. All retailers or service providers that handle, transmit, store, or process consumer credit-card information are required to be PCI DSS compliant, which is to the credit card industry what Sarbanes-Oxley (SOX) has been to publicly held companies. Those who don't comply can be heavily fined or barred from issuing or accepting cards from any council members. And, because the council consists of a consortium of five powerful card companies—Visa, MasterCard, American Express, Discover and JCB—not complying can effectively ban a bank from issuing cards or a merchant from accepting them. PCI DSS compliance mandates a minimum level of security measures as well as ongoing vulnerability assessments and audits to ensure data integrity and security.

- **Use identity networking**—Various user families need access to the WLAN network to access different types of information, and wireless networks must securely accommodate them, regardless of location. For example, order administrators require access to order entry and shipping systems; accounting and finance staff require access to accounts receivable and payable and other financial systems; and marketing and sales teams require access to sales

performance data. The HP WLAN V3.0 supports identity networking and assigns and enforces WLAN policies based upon a wireless client's identity, rather than a physical location. Identity networking authenticates wireless devices only once in a WLAN system. Context information follows the devices as they roam to ensure transparent mobility. If a WLAN is associated with a specific Virtual Large Area Network (VLAN), users can gain entry only to network resources on that VLAN. For example, personnel in shipping and receiving could access the wireless network using the SSID "receiving" for VLAN access only to email and enterprise resource planning (ERP) systems. All SSIDs support strong 802.11i or WPA encryption.

Many corporations use barcode scanners to track inventory in shipping and receiving or mobile printers on the manufacturing floor. As Wi-Fi phones becoming more prevalent, voice-over-WLAN is gaining popularity. These two devices often do not support today's strong 802.11i or WPA security, but they do accommodate the less-secure WEP encryption. Still, they can be segregated on a specific SSID supporting WEP that routes traffic to a VLAN allowing access only to the specific related database or application. Such a setup, augmented by dynamic encryption key rotations and MAC address control lists, mitigates potential security risks.

Administrators should use strong administrative passwords that are difficult to guess or an authentication methodology such as TACACS. In addition, administrators should ensure that all passwords are changed on a regular basis to minimize the risk of an unauthorized user gaining access by guessing or cracking administrative passwords.

Finally, many guests to an organization require on-site Internet access. A wireless guest network allows such access while eliminating the necessity for IT personnel to authorize individual users. The HP V3.0 WLAN solution enables guest networks through an open security method segregated on a specific SSID. The ID, which is broadcast so that guests can find it without assistance, routes traffic to a VLAN or physically isolates the access only to the public Internet. Users enter login ID and passwords through a captive portal Web page that audits usage and requires acceptance of terms and conditions prior to usage. HP recommends changing long-term guest passwords every 90 days.

- **Protect management ports**—Hackers can—and do—reconfigure the access point through the management port to illegally penetrate a corporate network. To prevent this, the management interfaces of the WLAN system should support secure, authenticated methods of management. The HP WLAN V3.0 supports simple network management protocol version 3 (SNMPv3), secure shell (SSH) protocol (secure web), and SSL (secure telnet) interfaces to the wireless control system (WCS). HP discourages the use of SNMP version 1 and 2 due to inadequate security controls and encryption. Furthermore, the WCS is configurable to prevent management over the air (recommended). The management system should reside in a firewalled-client compartment and be supported by a separate management VLAN that only allows stations on a specific VLAN to modify the WLAN network settings. Such user authentication mechanisms as TACACS should also be enabled to ensure that only authenticated users are allowed access to the management interfaces of an AP, controller, or management system.

- **802.11 FHSS radios**—In some instances, legacy devices might be based on frequency hopping spread spectrum (FHSS) WLAN technology operating in the 2.4-GHz range. Sometimes, these deployments are part of pre-existing wireless networks or recommended to clients for apparent security reasons. Obtaining these types of radios and putting them into a promiscuous mode is more difficult than with standards-based 802.11 scenarios. However, it is not impossible to do, but they should be avoided to adequately secure a WLAN. In most instances, these radios do not have an inherent equivalent security scheme comparable to WPA and 802.11i. HP recommends that these radios be migrated to an autonomous and/or LWAP solution as quickly as possible.

- **Use lightweight access points**—The lightweight access points within the WLAN controller-based solution that HP uses do not store encryption or other security information locally, so the network cannot be compromised if an access point is stolen. In addition, a X.509 certificate automatically authenticates all access points to prevent the addition of nonauthorized access points to the network. To prevent unplanned changes to RF coverage, access points should be secured against tampering. When possible, deploy them out of sight above a suspended ceiling, with only the antenna visible. To facilitate this type of deployment, the lightweight access points should support a Kensington lock interface and connected antennas.

- **Monitor the external site**—Access-point signals extend beyond the perimeters of most buildings. If security patrols or video surveillance are already in place, security personnel should watch for vehicles or people loitering in nearby parking lots or across the street.

- **Select strategy alternatives**—For those companies that cannot use 802.11i, WPA2 (AES) or WPA because the client does not support the encryption and authentication types due to age or lack of driver compatibility, a VPN is the next best solution for securing the over-the-air client connection. A VPN combined with network segmentation using multiple SSIDs and VLANs provide a robust solution for networks with varied clients. IP Security (IPSec) and Secure Sockets Layer (SSL) VPNs provide a similar level of security as 802.11i and WPA. There are drawbacks to VPN solutions, however. They add overhead, impede roaming, are more expensive, and don't scale well in large WLAN architectures.

- If none of these methods are possible, consider configuring WEP with an 802.1x (RADIUS) solution. If a higher level EAP protocol, such as TTLS or Protected Extensible Authentication Protocol (PEAP), is not possible—often the case with many older, handheld devices—use Cisco LEAP with strong, nondictionary passwords. Configure the RADIUS server to automatically deliver new keys at less than 15-minute intervals. As WEP-cracking tools improve, the interval may need to be decreased. Because LEAP is not acceptable for enterprise laptops, use the wireless client to disable permission for the weaker LEAP and MD5 protocols. Now is the time to plan the refresh to improved devices that will support more secure encryption techniques and protocols.

Static WEP is widely known to be easily compromised by tools available on the Internet. It only provides a deterrent to casual snoopers and is no longer acceptable for enterprise WLANs. HP recommends adopting an 802.1x solution and a stronger encryption methodology, such as WPA or AES.

WPA or AES pre-shared keys (PSK) are typically intended for small-office implementations or home use. WPA and AES-PSK are normally not an adequate encryption methodology for use in the corporate enterprise, largely due to the inability to physically or logically secure the static keys within the infrastructure or device configurations. Pre-shared keys for home use or when devices can be secured in an enterprise environment should always be longer than 20 characters (a maximum of 63 random ASCII characters is possible) and never use dictionary terms. Access to PSK-encrypted devices must be strictly controlled so the keys and configuration are not compromised. Keys should be rotated on a regular basis (monthly to yearly depending on information criticality) or whenever a compromise has occurred.

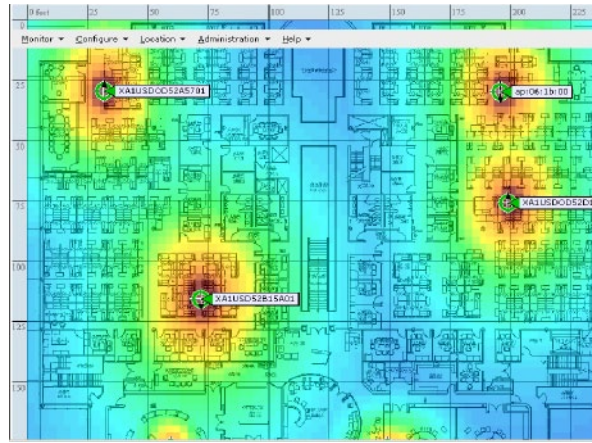
## Use intrusion detection, protection, and containment

Next, consider intrusion detection, protection, and containment for both wireless and wired networks. Simply alerting employees to threats is insufficient. For example, antivirus policies typically don't prevent users from opening contaminated attachments. More stringent measures are required to avoid enterprisewide damage, significant downtime, and lost productivity, particularly with potential violations of regulatory controls and legal statutes at stake. Even a "no Wi-Fi" policy offers no guarantee against potential threats. Employees can unwittingly introduce rogue access points, and laptops with embedded Wi-Fi can connect to neighboring networks. Both vulnerabilities are as contagious as viruses, worms, and spam—and equally as harmful. Such traditional wired security methods as firewalls and VPNs fail to detect these threats as they occur over the air. But the HP V3.0 Wireless LAN is designed to actively monitor and detect these occurrences.

With the HP V3.0 WLAN, access points can act as monitor-only rogue detectors to support a "no Wi-Fi" policy," supplement autonomous AP solutions or simultaneously act as air monitors and data-forwarding devices. This arrangement allows access points to communicate real-time information about the wireless domain—including potential security threats to wireless LAN controllers—without interrupting most data services. Security threats are rapidly identified and presented to network administrators through the wireless control system (WCS), which accommodates accurate analysis and corrective action.

Companies with a "no Wi-Fi" policy can initially deploy the HP V3.0 WLAN as a standalone wireless intrusion detection, location, and containment solution. Later, they can reconfigure it to add WLAN data, voice, mesh, and enhanced location services. This phased approach allows network managers to create a defense shield around radio frequency (RF) domains and prevent unauthorized wireless activity until the organization is ready to deploy WLAN services. HP provides a WLAN system that offers simultaneous wireless protection and WLAN service delivery, helping ensure complete WLAN protection without unnecessary overlay equipment costs or extra "throw-away" monitoring devices.

**Figure 2.** Location tracking of rogue access points and clients



Permanently removing the wireless threat involves physically removing the rogue device. If an autonomous or stand-alone system has been deployed, a laptop or handheld analyzer using AirMagnet or equivalent software can detect rogue devices in the general area. This approach, however, can be ineffective and become time-consuming, particularly for multi-floor sites, because wireless propagation can extend quite far. In addition, the results are only accurate for the time the area is scanned. HP recommends using the WLAN v3.0 with its WCS management system [and future location server] to track rogues and Wi-Fi enabled devices. The locations of rogues can be tracked across an entire campus, a single building, a floor, or a room (see Figure 2). With tracking capabilities, IT or security administrators can instantly receive alerts of rogue access points and clients, as well as their locations within a few meters, depending upon the density of AP deployment.

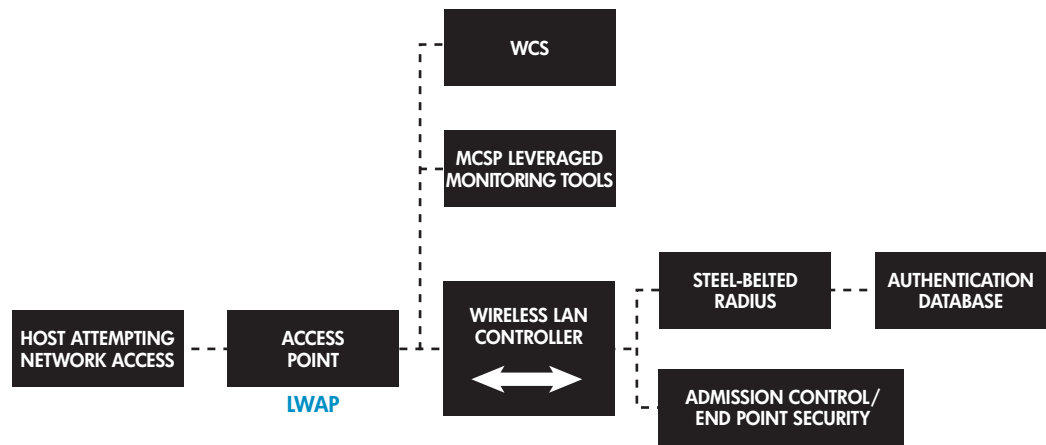
## Protection from external threats

In today's corporate environment, companies have no single perimeter as mobile computing extends boundaries and complicates the protection of networks from security threats. Patching network vulnerabilities is no longer an option. Policy and compliance management is becoming increasingly important in HP network strategy of proactively monitoring and quarantining malware to maintain network integrity. A compliance program looks for system and network policy violations. Without this, IT administrators are blind to security policy infractions.

## Policy management and compliance

Laptop computers require the same protections as do company networks. Firewalls, virtual-private networks (VPNs), and antivirus software help protect laptops from threats when they're connected to the Internet. Such tools as security agents consolidate endpoint security functions like firewall, intrusion prevention, spyware, and adware protection, among others, into a single agent. Because the agent analyzes behavior rather than seeking signature matching, it requires no updates to stop a new attack. This "zero-update" architecture provides adequate protection with reduced operational costs. Security agents allow organizations to enforce security policies on individual endpoints.

**Figure 3.** WLAN architecture with admission control and end point security



User authentication for access control and data encryption can significantly strengthen laptop security measures. User authentication can be performed through passwords, USB tokens, or smart cards. Although generally effective, these methods will not prevent someone from removing a hard disk to access sensitive data. As a result, encryption should be a consideration; however, it must be automatic and transparent to users. Requiring users to enable encryption for individual files is an unreliable method. HP recommends using PointSec for laptop hard-drive encryption.

### Ensure policy compliance

The HP future solution for endpoint visibility and admission control will help ensure that all wired and wireless devices attempting to access a network meet corporate security policies. Infected or vulnerable endpoints will be automatically detected, isolated, and cleaned.

HP admission control offers both appliance- and architecture-based approaches, meeting the functional and operational needs of any organization. The admission control works for a simple security policy requirement, as well as for a complex security implementation involving numerous security vendors and a corporate desktop management solution. Admission control is a set of technologies and solutions that use the network infrastructure to enforce security policy compliance on all devices

seeking to access network computing resources and limits damage from emerging security threats, such as viruses, worms, and spyware. Customers using admission control can allow network access only to compliant and trusted endpoint devices and restrict—or prevent—the access of noncompliant devices. Figure 3 illustrates a wireless host attempting access via a WLAN architecture with admission control and endpoint security controls.

## Conclusion

Corporate enterprises are no longer defined domains within buildings. Mobile devices and technologies have permanently removed traditional boundaries, expanding connectivity zones to homes, airports, hotels, coffee shops, and other Wi-Fi hotspots. But with this freedom comes a price: the introduction of multiple vulnerabilities to corporate networks. Security concerns are now front-page news as wireless signals penetrate walls, and mobile devices connect outside the relative safety of a corporate environment.

Fortunately, security solutions exist that meet the needs of Wi-Fi users, and although every company has different requirements, most find that a comprehensive security solution requires all of these steps, working in unison to mitigate WLAN threats.

Whether your company has a no-WLAN policy or plans to implement WLAN on a global basis, begin by assessing the wireless threats that could have an impact on your business. Determine your requirements along with where the technology should be used to support your business needs. Examine all elements for the WLAN solution to determine how they could be misused or hacked to gain access to your corporate resources.

Next, perform a WLAN security assessment and risk analysis to determine the measures and costs necessary to mitigate risks with the most impact. Now you can design a security policy to mitigate the high priority risks and then continue with the multi-layered approach and recommended best practices as outlined in this paper.

Even if no WLAN is currently planned, companies must still thwart such wireless threats as rogue access points and clients. These threats, illustrated in the TJX example, typically open holes in a network, exposing confidential information to hackers and theft. An unsecured network can—and most likely will—damage a company's reputation and increase the likelihood of financial and legal penalties. Initially, the HP WLAN V3.0 can be securely deployed as a wireless IPS solution or as a supplement to an existing

autonomous solution and then migrated to lightweight WLAN service later. In this age of Wi-Fi and ubiquitous mobile computing, applying the security practices described in this paper can help you protect the integrity of your infrastructure and its corporate applications and resources.

## Why HP?

- HP designs, implements, monitors, and manages thousands of wireless and WLAN devices for multiple clients, across multiple industry groups, on a global basis.
- HP detects and quarantines 940,000 viruses annually.
- HP examines and stops 63 million spam messages monthly.
- HP manages and monitors more than 2,500 firewalls and 3,000 intrusion-detection systems for threats and vulnerabilities.
- HP employs over 2,000 security and privacy professionals worldwide.
- HP prevents 550 million confirmed junk mail messages from ever reaching our employees' and our clients' e-mail environments each month.

# Checklist of recommended practices for WLAN security

The following table provides a WLAN security assessment checklist. The table presents guidelines and recommendations for creating and maintaining a secure 802.11 wireless network. For each

recommendation or guideline, three columns are provided. The first column, the “Recommended Practice” column, if checked, means the recommendation is for all enterprises. The second column, the “Should Consider” column, if checked, means the recommendation is an option that an enterprise should consider, weighing the risks, costs, and benefits. The last column, the “Status” column, allows the enterprise to use this table as a checklist to indicate whether this recommendation has been taken.

**Table 1.** Security recommendations

Security recommendations	Checklist		
	Recommended practice	Should consider	Status
<b>Management recommendations</b>			
1. Document a security policy that defines standards that must be met when wireless communications equipment is connected to the client network.	x		
2. Develop a security awareness program to educate users and establish good security practices for WLAN use on an annual basis or as vulnerabilities present themselves.	x		
3. Perform annual security assessments and inventory audits to check lost or stolen devices and security posture and to determine corrective action.	x		
4. Ensure that users are knowledgeable of software and documentation, including technical data, that are subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and which may be subject to export or import regulations in other countries. Strict compliance is necessary with all such regulations, and the solution or service owner acknowledges that it has the responsibility to obtain licenses to export, re-export, or import software and documentation.	x		
5. Comply with and maintain all city, state, and government/federal agency regulations governing the use of WLANs.	x		
6. Perform rigorous testing of all security features and vfunctionalities in a Model Office [test] lab for the network and/or devices to be introduced, then Pilot at select site(s) with scaling to capacity prior to deployment and full production.	x		
7. Perform site surveys to determine the proper placement of APs and antennas and the minimum power levels required.	x		
8. Physically secure all wireless infrastructure devices and/or place them in out-of-reach places.	x		
<b>Technical recommendations</b>			
1. Manage laptop and handheld [wireless] hardware and software in a consistent office environment.	x		
2. Use SMS for Windows or an equivalent automated solution to push enterprisewide OS, firmware, and drivers as required.	x		
3. Use a wireless client or supplicant that encrypts critical (registry) information or use disk encryption to protect the entire system.	x		
4. Use Internal PCI wireless adapters and restrict use of external wireless cards on laptops as these can retain critical WLAN information.		x	
5. Use wireless clients that have configurations that can be preconfigured, self-installed, and easily updated.		x	
6. Use clients with wireless configurations that can be administratively secured through a client permissions editor or equivalent administrative controls.	x		

**Table 1.** Security recommendations (continued)

Security recommendations		Checklist		
		Recommended practice	Should consider	Status
<b>Technical recommendations (continued)</b>				
7.	Use wireless clients that have a wireless suppression capability to prevent bridging of wired and wireless networks.	x		
8.	Use clients that can maintain multiple SSIDs. Change SSIDs regionally and for different industry or service applications.	x		
9.	Of the two mechanisms, open and shared, open association mode should be used. Open association is a basic authentication mechanism but should not be used as a replacement of encryption or 802.1x for user authentication or equivalent. Shared association is subject to man-in-the-middle attacks.	x		
10.	Work with COE administrators to disable, or migrate to a client that can disable, ad hoc connections, which create an opening for hackers to gain access to users' laptops and corporate networks.	x		
11.	Use laptops and other wireless devices that have up-to-date firewall, anti-virus, and VPN capabilities to connect to corporate resources outside of the enterprise.	x		
12.	Do not share user IDs and passwords on handhelds. Use separate strong user IDs and passwords to authenticate on a per device basis.	x		
13.	PDA devices with access to corporate resources should incorporate a firewall, anti-virus, two factors of authentication, 802.1x, and be capable of WPA or AES encryption.	x		
14.	No broadcast of SSIDs except for properly configured guest hotspot.	x		
15.	Default SSIDs (tsunami, ...), firewall ports (1645/1646), community strings (public, private, ...), and other well-known defaults should be changed at installation to mitigate risk of exposure.	x		
16.	If encrypted at Layer 3, use VPN w/ IPSEC, SSL, or equivalent.  If encrypted at Layer 2 use a dynamic encryption solution with frequent rekey. WPA or AES is preferred. If dynamic WEP, use a key rotation of <15minutes as an interim solution. If static WEP is used, immediate action should be taken as static WEP has been broken in ~5 minutes.  Use FIPS 140/2 or equivalent for unclassified data at state, government, or military entities. Use Type 1 or equivalent encryption for classified data.	x		
17.	Establish policy or guidelines for a minimum of static WEP encryption on home WLANs and preferably WPA-PSK encryption or better.		x	
18.	There are special considerations for enterprise use of WPA or AES with PSK; they include devices and configurations that must be physically and logically monitored and protected 24/7; a minimum of 63 random ASCII characters (alpha, numeric, and special characters) in the encryption key; and the encryption key is changed on a periodic basis (<= 1 year). This is not a solution for devices that could be lost or stolen.	x		
19.	Use an authentication standard such as 802.1x or equivalent and use TLS, PEAP, TTLS, or equivalent protocols. Use multiple factors of authentication such as machine authentication, smart cards, secure token, x.509 certificates, or equivalent.  Use a protocol that encrypts both the user ID and password in the authentication process. EAP protocols - TLS, TTLS, Cisco PEAP, and FAST to provide privacy.	x		
20.	Use MS-CHAPv2 w/ certificates or other mechanisms to encrypt the ID/password exchange.  Use client or administrative options to force validation of the client certificate to the Radius server.	x		
21.	Do not use FHSS radios as security through obscurity; migrate to current technology radios as soon as possible.	x		
22.	Use password amplifiers or equivalent to generate strong shared secrets greater >= 15 characters. Shared secrets should be unique for each device.	x		

**Table 1.** Security recommendations (continued)

Security recommendations		Checklist		
		Recommended practice	Should consider	Status
<b>Technical recommendations (continued)</b>				
23.	Use standards certified and matched wireless clients and Radius servers to optimize security features, functionality, and support in 802.1x solutions.	x		
24.	Use Layer 2 encrypted solutions for global implementations of WLANs. Layer 3 VPN solution for WLAN is typically manageable and secure in small implementations; however, it tends to add overhead, impede roaming, add cost, and does not scale well in large or global deployments.		x	
25.	Use SSIDs and VLANs for separation of wireless data, voice, multimedia, and guest hotspot applications from wired traffic. Guest hotspots may require physical network isolation in some instances.	x		
26.	The wireless architecture should be logically designed to put management traffic on a different subnet (VLAN) to protect management traffic, interfaces, and passwords.	x		
27.	On guest hotspots, use one-time passwords or generate secure ID/passwords for authentication and user tracking. Password changes for long-term guest users should be no greater than 90 days. Open guest hotspots increase liability to the corporation when users cannot be held accountable for their actions.	x		
<b>Operational recommendations</b>				
1.	Monitor the external perimeter of buildings with security patrols, video monitoring, or equivalent solution to protect against attacks on the wireless solution.		x	
2.	Use firewalls to protect management systems from unauthorized access. Use SNMPv3, HTTPS, SSL, or SSH for connectivity to management systems and infrastructure components. Do not allow over-the-air management.	x		
3.	Use advanced network management or equivalent to monitor all wireless infrastructure configuration profiles for changes on a real-time basis. Alarms or events should be generated when unauthorized configurations changes are made.	x		
4.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.		x	
5.	Monitor/poll all wireless infrastructure components on a consistent basis (<=15 minutes) and have a solution for their management.	x		
6.	Administrative password should not be based on dictionary terms or easy to guess. Use of eight alpha, numerals, and special characters are recommended. TACACS or equivalent solutions will also minimize the risk of unauthorized users gaining administrative access.	x		
7.	Have a policy or guidelines to clear wireless device configurations before disposing or returning these devices for maintenance (RMA) to prevent the disclosure of network configuration, keys, passwords, etc.	x		
8.	Use an advanced management system or equivalent to collect and save events, traps, and alarms with accurate time-stamps. Administrative user actions are also logged for accountability.	x		
9.	A management solution should be in place to effectively implement OS software and firmware upgrades based on newly discovered vulnerabilities or on a yearly basis otherwise.	x		
10.	Designate an individual to track the progress of 802.11 security products and standards (IEEE, IETF, etc.) and the threats and vulnerabilities with the technology.		x	
11.	Use stand-alone or hybrid wireless intrusion detection and prevention systems for real-time monitoring, location, and containment of threats in the wired and wireless networks. These can be a combination of wired and wireless solutions.	x		
12.	Use end point and network access controls to ensure user devices meet security and COE policies and are compliant prior to granting entry to the corporate network.		x	

**Table 2.** The Wi-Fi hacker's dictionary

<b>The Wi-Fi Hacker's Dictionary</b>	
Ad hoc peers	Many mobile users never think to change their service set identifier (SSID) when leaving the office or home. Because they don't reset this router/access point SSID from what they normally use (such as Linksys), they can be attacked at an airport, for instance, by another computer mimicking their home network.
Evil twins	In this wireless version of phishing, users believe they've connected to a hot spot, but instead they've linked to a malicious server that then goes after, for example, their banking information.
Honeypots	This anti-hacker measure involves attaching a server to the Internet to act as a decoy for hackers so that how they work and get into a system can be studied. The hacker's access is limited to the monitoring server, and, if done well, hackers don't realize they're being duped and watched.

**Table 3.** Terms definitions

<b>Terms Definitions</b>	
802.11	A set of Wireless LAN/WLAN standards developed by the IEEE LAN/MAN standards committee (IEEE 802). Also commonly referred to as "Wi-Fi."
802.11i	An amendment to the IEEE 802.11 standard specifying security mechanisms for wireless networks.
802.1x	A framework for link-layer authentication specified by the IEEE.
AES-CCM	Advanced Encryption Standard-Counter with CBC-MAC. A wireless encryption protocol specified by IEEE 802.11i. Currently regarded as the strongest form of wireless encryption.
EAP Extensible Authentication Protocol	A series of authentication methods used inside 802.1x to achieve wireless authentication.
IEEE Institute of Electrical and Electronics Engineers	An international professional organization dedicated to the advancement of technology related to electricity. The IEEE is one of the main standards bodies associated with networking technology.
IETF Internet Engineering Task Force	Develops and promotes Internet standards, in particular those of the TCP/IP protocol suite.
IPSEC IP Security	An IETF standard for protecting IP communication by encrypting or authenticating all packets.
LEAP Lightweight Extensible Authentication Protocol	A proprietary protocol supported by Cisco Systems that acts as an EAP method within 802.1x. LEAP was proven insecure in 2003 and does not comply with current security standards.
PEAP Protected Extensible Authentication Protocol	A tunneled EAP method that uses a server-side digital certificate for server authentication and a user name/password for client authentication.
Stateful Packet Inspection	A filtering or firewall technology that keeps track of the state of network connections, such as TCP streams, traveling across it. Only packets that match a known connection state will be allowed, while others are rejected.
VPN Virtual Private Network	A method of building private networks on top of public networks such that the private network is protected and separate.
WEP Wired Equivalent Privacy	This is the encryption protocol specified in the original version of IEEE 802.11. It is now deprecated and does not meet current security standards.
Wi-Fi	A set of product compatibility standards for wireless LANs based on IEEE 802.11. The Wi-Fi term is managed by the Wi-Fi Alliance. Products carrying Wi-Fi certification have passed a series of compatibility tests.
WLAN/Wireless LAN	A type of wireless system based on the IEEE 802.11 series of protocols.
WPA Wi-Fi Protected Access	WPA implements the majority of the IEEE 802.11i standard and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards. Products displaying the WPA logo have passed a certification program run by the Wi-Fi Alliance.
WPA2 Wi-Fi Protected Access version 2	WPA2 implements the full IEEE 802.11i standard but will not work with some older network cards. Products displaying the WPA2 logo have passed a certification program run by the Wi-Fi Alliance.

## About the author

### **Ric Hall**

Ric is a systems architect in the HP Network Architecture, Global Network Engineering organization, where he is the lead architect for the global development of Wireless LAN services for Client HP and Portfolio Services. He has 31 years' experience in the telecommunications industry, with an emphasis on satellite and wireless technologies. Ric is the author of a weekly news brief on wireless and mobility developments. He owns several patents and white papers and is developing services through proof of concepts to further improve HP development and delivery of wireless services.



## Technology for better business outcomes

To learn more, visit [www.hp.com](http://www.hp.com)

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA2-9255ENW, December 2009

