



WHITEPAPER

**Wireless LAN Security for
Healthcare and HIPAA Compliance**

Wireless LAN Security for Healthcare and HIPAA Compliance

Wireless deployments in healthcare institutions have accelerated as mobility has proven to play a vital role in care delivery – especially in the acute hospital setting. This situation raises concerns relative to the upcoming healthcare privacy and security regulations. This paper will provide insights into this dilemma and offer solutions that can help ensure the security of wireless data in order to meet the demanding needs of the healthcare environment.

Wireless LAN Security

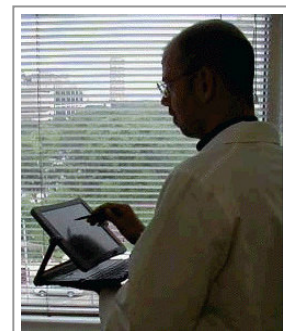
For many healthcare institutions, wireless LANs (WLANs) have become a key component of the IT infrastructure. WLANs have moved into mainstream use by providing greater efficiency and accuracy to users of such mission-critical applications as bedside medication administration, emergency registration, order entry, physician rounding and clinical documentation. As the paper chart gives way to computer-based patient records, mobile devices are becoming the primary point of clinical communications.

Inherent security weaknesses in the architecture of 802.11 wireless local-area networks (WLANs) have received a great deal of publicity in recent months. As the user base grows and mobile applications become increasingly mission-critical, the need for effective security and management of these networks becomes a top priority. This situation raises concerns relative to the upcoming healthcare privacy and security regulations. This paper will provide insights into this dilemma and offer solutions that can help ensure the security of wireless data in order to meet the demanding needs of the healthcare environment. Wireless LANs are challenging from a security standpoint for several reasons, including:

1. Rogue Wireless Deployments
2. Malicious Hackers
3. Performance Management & Troubleshooting
4. Meeting HIPAA Security Requirements

Challenge #1: Rogue Wireless Deployments

Unauthorized rogue access points are the most daunting challenge created by WLAN technology. A rogue access point provides easy access to the entire network infrastructure—and not just for a serious hacker, but for anyone with a wireless network adapter and an antenna within several miles of the rogue access point. Rogues may be introduced by well-intentioned employees, physicians, consultants, or contractors who install their own access points without regard to proper security configuration requirements.



Rogues also can be created accidentally during deployment or maintenance of the wireless network by failing to properly configure an access point. Users also can create rogues by using the “ad hoc” wireless configuration feature that allows a PC to act as an access point. PCs can create a rogue situation by connecting unknowingly to neighboring networks, a process known as “accidental association”. The problem of rogues is so common that several websites, such as www.WIGLE.net, actually catalog thousands of open wireless networks. Stopping rogue deployment is a must for healthcare organizations.

Challenge #2: Malicious Hackers

Wireless networks provide anonymity and ease of access to the enterprise network. Unlike Internet hacking, the anonymous nature of WLAN hacking means that it is nearly impossible to track down a hacker’s origin. This has made WLANs a popular entry point for stealing intellectual property or obtaining demographic and credit card information for identity theft or credit card fraud. Wireless hacking also provides a wealth of unwitting sources for e-mail spamming or malicious hacking into others networks.

WLAN technology uses a notoriously weak encryption scheme inappropriately called Wired Equivalent Privacy (WEP). On a busy network, WEP can be cracked in a matter of hours. Wireless vendors have responded with more advanced solutions such as Microsoft’s 802.1x/EAP and Cisco’s Lightweight Extensible Authentication Protocol (LEAP). Many new products are available that protect the WLAN through the use of virtual private network (VPN) solutions. Although these technologies are a crucial part of any secure wireless deployment, they provide only part of the required security infrastructure. Even when using WEP, LEAP or VPN technologies, all traffic at OSI layers 1 and 2 are available to the hacker along with crucial management frames. There is no authentication involved at layers 1 and 2, so any hacker can pretend to be an access point or any legitimate network user. This has made it easy to create software to perform wireless Denial of Service attacks. Because the hacker can see both sides of any conversation, “man-in-the-middle” attacks—which are difficult to execute on the Internet— are an easy task in the wireless realm.

All wireless stations are at risk to the malicious hacker. Any PC with a wireless radio in it can be easily coaxed into associating with a hacker’s PC, making any files on the PC readily available, regardless of any enterprise encryption or authentication scheme. A hacker can take advantage of this vulnerability to browse through the contents of a PC in a hospital—or on board an airliner. Although the likelihood of a malicious hack may be low, the risks are high because of the difficulty in detecting and thwarting an attack.

Challenge #3: Performance Management and Troubleshooting

Wireless networks can be challenging to manage. Overall wireless performance is very limited when compared to wired LANs, and user performance varies based on environmental conditions such as distance, user load and interference. Interference can come from other access points on the same channel, either part of the same network or from neighboring networks. It can also come from outside sources: microwave ovens, telemetry systems, cordless phones and imaging systems. Any occurrence of users being disconnected or experiencing poor performance can be caused by poor coverage, improper channel configuration, outside interference, access point or radio degradation, or network utilization,

among other factors. The challenge is gathering enough useful information to determine where performance issues are coming from and rapidly responding. As applications become more mission-critical, not only are patient safety and clinical productivity at risk, but so is the adoption of the entire software investment.

Challenge #4: Meeting HIPAA Security Requirements

Because of the scope of these vulnerabilities, wireless networks in healthcare institutions will come under greater scrutiny with approval of the final Health Insurance Portability and Accountability Act (HIPAA) Security Rules. Although the exact impact of the security rules are undetermined, if they remain consistent with the current draft proposal, wireless LANs are expected to be classified as “open” networks. As such, wireless LAN installations would require a documented security policy, the use of data encryption, verification of ongoing policy enforcement, and security incident reporting procedures.



Before outlining the proposed rule’s relationship to wireless LANs, it is important to remember that if reasonable safeguards are implemented and a malicious hacker uses extraordinary effort to compromise the network, the situation would unlikely be considered a violation of HIPAA rules. However, the existing vulnerabilities in wireless LANs can inadvertently create an open pathway for anyone – not just an experienced hacker – to gain access to the greater enterprise network. If this scenario occurs and data is compromised, the fault will likely be considered to be that of the institution, and HIPAA penalties may be levied. *Wireless LANs in healthcare must address these known wireless LAN vulnerabilities with encryption, security management and incident reporting.*

Data Encryption - Because data is transmitted in the open air, wireless LAN traffic must be encrypted. Encryption using the Wired Equivalent Privacy (WEP) protocol, which is part of the wireless 802.11b standard, is likely to be considered sufficient for HIPAA purposes despite WEP’s inherent weaknesses that are proven to be easily exploitable. More advanced protocols, such as Cisco’s Lightweight Extensible Authentication Protocol (LEAP), would likely be considered to exceed HIPAA requirements.

Security Management Process and Certification - Beyond encryption, the next requirement is to establish a security management process and apply it to the wireless LAN. The rule requires that a policy, such as the use of WEP or LEAP, be defined and that equipment inventory and vulnerability assessments be performed to ensure the proper configuration of all access points.

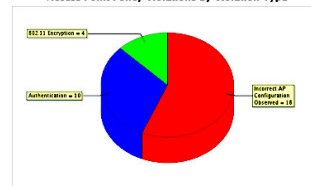


System Name: AirDefense
Location: Atlanta, GA
Generated: 2007-03-26 16:10:20
Version: 7.2.0-95

Security Access Point Policy Violations

from 2007-03-24 16:08:00 to 2007-03-26 16:08:00

Access Point Policy Violations By Violation Type



Count	Category	Subcategory	Type
10	Policy Compliance	Authentication	AP Authentication Mode Violation
4	Policy Compliance	802.11 Encryption	AP Encryption Mode Violation
8	Policy Compliance	Incorrect AP Configuration Observed	AP Adversarial Data Rate Violation
3	Policy Compliance	Incorrect AP Configuration Observed	AP Incorrect Channel
7	Policy Compliance	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon

Security Configuration Management - The proposed rule also calls for a security configuration management process. This process requires that verification and documentation of the security configuration be performed on a regular basis to ensure that additions and changes to the network do not adversely affect security.

Incident Reporting Procedures - The rule also includes a requirement for tracking security incidents when they occur. This would necessitate a means of incident detection, alarm creation, and event reporting when an alarm occurs. Documentation of the timeliness and efficacy of the response to the alarm would also need to be documented.

Risks Unique to WLANs - WEP, LEAP, and VPNs will all satisfy the HIPAA requirements for encryption and authentication, but wireless LAN face new risks that originate from the open nature of a wireless network. Unauthorized rogue access point, and devices configured for ad hoc networking must be identified. Wireless LAN traffic must be analyzed for accidental association. The ongoing integrity of a wireless LAN must be maintained by alerting all configuration changes. Malicious intrusions and denial of service attacks must be detected and thwarted. HIPAA rules dictate that healthcare organizations document these occurrences and the corresponding response.

Regardless of HIPAA requirements, network administrators must consider a wireless LAN's vulnerability to attacks that compromise the enterprise network. Healthcare administrators must consider the public relations issues that would result from the wireless LAN being used as a launching pad for attacks against other networks.

A thorough wireless LAN security deployment can safeguard wireless LANs from these issues. Wireless LANs must first be configured outside the firewall, as its own segment or VLAN. Access points should be deployed in such a manner as not to broadcast signals far outside of the facility. The Service Set Identifier (SSID) for the access points should not beacon or advertise the name of the organization. Filtering of MAC addresses provides basic authorization for sanctioned devices. Encryption technology such as WEP, LEAP, or a VPN must be deployed. Finally, healthcare organizations must monitor their wireless LANs 24x7 to identify network vulnerabilities and detect new threats in real time.

Mitigating Wireless Risks & Complying with HIPAA Requirements: The AirDefense Solution

Because encryption is not enough to guard a network against rogue access points, insecure configurations, and many attacks, AirDefense provides the final layer of security that only can be provided with 24x7 monitoring of the network. AirDefense complements WEP, LEAP and VPNs to address the weaknesses of wireless LANs. To recap, this layered approach to security includes:

1. Locking down the wireless LAN's perimeter (both access points & wireless-enabled stations)
2. Securing communication across the wireless LAN (authentication, encryption & VPNs)
3. 24x 7 Real-time Monitoring of Network Traffic (using AirDefense)

Perimeter control for the wireless LAN starts with deploying personal firewalls on every laptop and deployment of enterprise-class access points that offer advanced security and management capabilities. All access points should be completely locked down and reconfigured from their default settings. The SSIDs of the access points should be changed from their default names. To secure mobile users at hotspots etc, organizations can deploy the **AirDefense Personal** product. Residing on mobile users' computers, AirDefense Personal quietly monitors for malicious or accidental wireless activities and wireless misconfigurations that may cause security exposures or policy violations thereby providing complete protection, regardless of the location.

Organizations should deploy strong encryption and authentication standards (for e.g.: WEP, PEAP, WPA, LEAP etc.) and install VPNs to secure communication across the wireless networks.

Like a video camera that monitors all activity in a secure building 24 hours a day, a critical layer of wireless LAN security requires continuous monitoring of the network to identify rogue WLANs, detect intruders and impending threats, terminate and locate unauthorized connections and enforce WLAN security policies. **AirDefense Enterprise** provides the most advanced solution for control of the airwaves, security, policy and operational support for wireless networks. Using patent-pending technology to correlate and analyze the monitored data, AirDefense Enterprise provides the industry's most accurate intrusion prevention for wireless networks.

The AirDefense system provides a means of addressing them in a manner that eases HIPAA certification and documentation requirements:

Security Management and Certification - AirDefense continually monitors the airwaves throughout the enterprise for internal security violations including rogue access points and stations, ad hoc networks, improper configurations and accidental associations. AirDefense provides a continuous review of security policy and vulnerability assessment.

Security Configuration Management - AirDefense monitors access points to provide real time equipment inventory and verify that additions or changes to the network do not violate configuration policy.

Incident Reporting Procedures - AirDefense immediately detects intruders and alerts security managers of malicious acts, such as NetStumbler scans, spoofed MAC addresses, and "man-in-the-middle" hacking attempts. The alarm can be routed to an email address, pager, or cell phone. Response to the event is logged to track the timeliness and outcome of the event resolution. AirDefense has created a report that is specifically designed to assess compliance of wireless devices and networks with the HIPAA requirements (For report sample, please see Appendix 1). Dozens of healthcare institutions are already taking advantage of AirDefense to ensure proper network security and peace of mind.

Conclusion

AirDefense can help healthcare organizations secure their wireless LANs in a comprehensive fashion and provide the security management and incident reporting capabilities necessary to meet the requirements of HIPAA in an organized and laborsaving manner. Most importantly, AirDefense ensures the highest possible level of security to address the unique vulnerabilities of wireless networks.



HIPAA Compliance Report

from 2007-03-24 16:01:00 to 2007-03-26 16:01:00

System Name: AirDefense
 Location: Atlanta HQ
 Generated: 2007-03-28 16:02:38
 Version: 7.2.0-35

HIPAA Requirement Summary

The HIPAA Security Rule requires that Protected Health Information (PHI) that is transmitted over public networks be encrypted by a commercially acceptable encryption mechanism. Because the very nature of wireless LANs requires that they broadcast data in the air, they should be considered public networks and must meet the encryption requirement to maintain HIPAA compliance per Section 164.312(e)(1) of the HIPAA Security Rule 45 CFR Subpart C.

This report details the policies of this institution regarding encryption requirements for each wireless access point. It also indicates where violations may occur: due to mis-configurations of access points, deployments of improperly configured unauthorized or "rogue" access points, user stations roaming to unsecure neighboring networks without the user's knowledge and other scenarios that would undermine the required encryption policy.

This report is based on real-time monitoring of the airwaves throughout this institution and includes all violations to policy as well as how timely a response is given to policy violations per Section 164.308(a)(6). Because monitoring is done constantly, this report also reflects the discovery and vulnerability assessment requirements of the HIPAA rule in regards to maintaining a security management process per Section 164.308(a)(1).

Policy Compliance Summary

APs without Proper Authentication:	10
APs without Proper Encryption:	4
Rogue Access Points:	11
Rogue Stations:	5
Unauthorized Roaming between APs:	1
After-Hours Activity:	0
Severe and Critical Alarm Count:	45
Severe and Critical Uncleared Alarms:	45

Specific Policy Violations (Up to 50 Listed)

Total Policy Violations								40
Device	Device MAC	Sub-Category	Alarm	Start Time	Location	Group	Cleared	
Airdefense:10:00:09(a,b)	00:16:5d:10:00:09	Incorrect AP Configuration Observed	AP Incorrect Channel	3/7/07 10:37 AM	Atlanta HQ	1st Floor	No	
Airdefense:10:00:09(a,b)	00:16:5d:10:00:09	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	3/7/07 10:37 AM	Atlanta HQ	M510 Group	No	
Airdefense:10:00:09(a,b)	00:16:5d:10:00:09	Authentication	AP Authentication Mode Violation	3/7/07 10:37 AM	Atlanta HQ	M510 Group	No	
Airdefense:10:00:09(a,b)	00:16:5d:10:00:09	Incorrect AP Configuration Observed	AP Advertised Data Rate Violation	3/7/07 10:37 AM	Atlanta HQ	M510 Group	No	
Airdefense:10:00:08(a,b,g)	00:16:5d:10:00:08	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	3/7/07 10:37 AM	Atlanta HQ	M510 Group	No	
Airdefense:10:00:08(a,b,g)	00:16:5d:10:00:08	Authentication	AP Authentication Mode Violation	3/7/07 10:37 AM	Atlanta HQ	M510 Group	No	
Airdefense:10:00:08(a,b,g)	00:16:5d:10:00:08	Incorrect AP Configuration Observed	AP Advertised Data Rate Violation	3/7/07 10:37 AM	Atlanta HQ	M510 Group	No	
Cisco:35:37:a0(b,e)	00:11:20:35:37:a0	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	2/21/07 3:46 PM	Atlanta HQ	M510 Group	No	
Cisco:35:37:a0(b,e)	00:11:20:35:37:a0	Authentication	AP Authentication Mode Violation	2/21/07 3:46 PM	Atlanta HQ	M510 Group	No	
Cisco:35:37:a0(b,e)	00:11:20:35:37:a0	Incorrect AP Configuration Observed	AP Advertised Data Rate Violation	2/21/07 3:46 PM	Atlanta HQ	M510 Group	No	
Airdefense:10:00:3d(a,b,g)	00:16:5d:10:00:3d	Incorrect AP Configuration Observed	AP Incorrect Channel	2/21/07 3:46 PM	Atlanta HQ	1st Floor	No	
Airdefense:10:00:3d(a,b,g)	00:16:5d:10:00:3d	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	2/21/07 3:46 PM	Atlanta HQ	1st Floor	No	
Airdefense:10:00:3d(a,b,g)	00:16:5d:10:00:3d	Authentication	AP Authentication Mode Violation	2/21/07 3:46 PM	Atlanta HQ	1st Floor	No	

Appendix 1: AirDefense HIPAA Compliance Report

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring's* Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

AirDefense Enterprise, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

AirDefense Personal, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact info@airdefense.net or call us at 770.663.8115. **All trademarks are the property of their respective owners.**