



*The Wireless Security Experts*

# SECURITY ANALYSIS

Code Red Systems Ltd.  
21 HaVaad HaLeumi  
POB 16120, Jerusalem, Israel  
T +972-2-642-3401, F +972-2-642-3402  
Email: [info@code-red.biz](mailto:info@code-red.biz)  
Web: <http://www.code-red.biz>

June 2004

## 802.11 Wireless Security & Safety for Healthcare Environments

By,  
Drew Tick  
CEO, Code Red Systems

***"Everybody I talk to says healthcare is one of the biggest opportunities," said Julie Ask, a senior analyst with Jupiter Research. "These vertical applications that are flying under the radar are really the untold story of Wi-Fi."***

(Jerusalem, Israel) Many vertical markets are undergoing major IT overhauls. One of the most blatant is the healthcare sector. An industry based primarily on paper records, there is now a major move to electronic patient records, prescription fulfillment, and medical information.

By definition, doctors and nurses require highly mobile solutions as they go from one patient to another, or from a major hospital to a private clinic. This is the reason for the high penetration rate of wireless LAN technology in healthcare environments.

The purpose of this analysis is to present the main wireless security issues, with emphasis on issues particular to the healthcare industry.

### ***Overview***

According to MedScape, wireless technology will continue to thrive in healthcare, where revenues related to wireless networking are expected to double by 2005 to \$400 million a year. According to a Pico Report on wireless technology in the US healthcare industry, 80% of US physicians accessed patient records using a wireless device in 2003.



*The Wireless Security Experts*

This impressive growth is fueled by the increased penetration of Electronic Patient Records (EPR), which can be found on PDAs, tablets, laptops and PCs. In addition, there are also application specific wireless hardware such as barcode readers and medical devices.

The breadth of applications and market growth indicate clearly that wireless is becoming an important component of the IT infrastructure in clinics and hospitals. This is due to mobility and the improvement it enables for both patient care and productivity.

These advantages, however, also present challenges in terms of how to secure these wireless networks. In addition to wireless security issues which are common to commercial wireless networks, there are also specific legislative and safety concerns which are specific to healthcare applications.

The best wireless security solution should provide the basic elements common to most wireless networks, but should also include features which respond to the specific needs of clinics and hospitals.

***The Problem***

*General Wireless Security Issues*

Wireless LAN is based on radio waves in the 2.4 Mhz frequency. This radio works very much in the same way as a standard FM radio. Anyone in range with the same radio equipment can receive the signal. In fact, once in range, Microsoft's Wireless Zero Configuration will automatically connect a PC to a wireless network without any user intervention.

This means anyone within 500 ft (150 m) radius, including those outside the physical premises, can easily access the network. This poses two immediate threats: The first, is eavesdropping where intruders can capture information sent over the wireless network. The second, is unauthorized access where attackers can gain full entry to both the wireless and wired networks.

Another threat is placement of a rogue access point. This is when an attacker gains access to the physical network and attaches their own wireless access point to the wired network. In a hospital environment with thousands of visitors, this is a real possibility.

***These threats clearly indicate that operating a wireless LAN in Open Mode, without security mechanisms in place, is clearly unacceptable for any healthcare related facility.***



*The Wireless Security Experts*

*Healthcare Specific Wireless Security Issues*

First and foremost among concerns for healthcare facilities are adherence to the 1996 Health Insurance Portability & Accountability Act (HIPAA). One of its major aspects includes a requirement to move medical records online in electronic format. While HIPAA does not refer specifically to wireless networking, there are strict guidelines regarding patient privacy and limitation of access on a need-to-know basis.

Wireless networking is a natural outgrowth of the EMR (Electronic Medical Record) initiative. As information becomes more available, clinics and hospitals are looking for ways to leverage electronic information with the goal of greater efficiency and improved patient care. Considering the high level of mobility required by doctors and nurses, the next logical step in the evolution of electronic information is to allow access via PDAs and laptop computers using wireless networking.

In terms of HIPPA compliance, there are no specific rules for wireless networking. There are, however, data security guidelines which include authentication, access control, encryption, and audit logs.

While the security issues are clear, there are safety related issues which should also be taken into consideration. Wireless LANs operate in the 2.4 Ghz unlicensed radio spectrum. There are also medical devices which operate in this frequency which means potential for interference. While this is not necessarily a data security issue, it is of serious concern for the healthcare industry.

***Therefore, the HIPPA defined data security requirements, mandate that wireless security precautions must be taken, if an organization is to adhere to HIPPA guidelines.***

***The Solution***

*Existing Solutions*

The majority of current wireless security solutions have been geared towards large office environments. This also makes a number of assumptions such as the ability to upgrade to the latest equipment, the possibility of a single vendor solution, and IT intensive solutions.

This explains why 802.1x RADIUS server based solutions are the preferred corporate solution. The leading player in this field is Cisco, but in order to operate properly, it means that every access point, device and the RADIUS server must all be Cisco.

Generic 802.1x solutions are also available using RADIUS servers from companies such as Funk, and installing the 802.1x client on all devices. While this may be a good solution for laptops, it may be difficult for PDAs and other devices.



*The Wireless Security Experts*

Other advancements include WPA (WiFi Protected Access) and AES (Advanced Encryption System). The problem is that these new security standards are only beginning, or are yet to appear in the market and are not compatible with the 100 million or so devices already deployed.

Existing solutions provide encryption and may be enough for HIPPA compliance. The problems are a lack of management, support for multiple vendors and the support for multiple operating systems.

*The AirMarshal Medical Edition*

AirMarshal is a software-only wireless security software solution, which provides authentication, encryption and audit logs for wireless networks. The main features are automation, transparency and redundancy working on multiple vendors over multiple operating systems.

The system automatically operates Wired Equivalent Privacy (WEP) the lowest common denominator of all wireless devices. It is well documented that WEP keys can be compromised over time, so the software automatically changes keys at preset intervals using a key rollover mechanism. Using this method, potential attackers cannot record enough information to reverse the encryption key.

Likewise, authentication is accomplished by allowing access only to those with the AirMarshal software and current encryption key. Otherwise the wireless device cannot associate with the network. This is in addition to the regular network username and password which are also be required.

The management console also keeps track of all devices accessing the network and records entry and exit times. This provides the audit log necessary for HIPPA compliance. Other modules will include Intrusion Detection for finding rogue access points and measurement of power levels to avoid potential conflicts with wireless medical equipment.

From a central management console, administrators will be able to see all access points and connected wireless devices. In terms of security, the dynamic WEP key rollover mechanism will provide both the encryption and authentication required by HIPPA regulations.

***The AirMarshal Medical Edition is a software-only wireless security solution providing authentication, encryption and audit trails for equipment from multiple vendors across multiple operating systems.***



*The Wireless Security Experts*

***Conclusion***

Healthcare related organizations are adopting wireless networks to take advantage of the increased mobility enabled by their move to online electronic patient records. While improving patient care and increasing work flow efficiency, wireless networking also provides a number of challenges, especially in terms of security and safety.

HIPPA provides general data security guidelines, but does not refer specifically to 802.11 or any other wireless protocol. It is believed that inclusion of authentication, encryption and audit logs in a wireless security solution, should mean compliance with HIPPA guidelines.

In addition to general wireless security issues, there are medical specific concerns as well such as patient privacy and interference with medical equipment.

The AirMarshal Medical Edition is wireless security software which offers a full solution for hospital and clinical environments. The system provides authentication, encryption, and audit trails for equipment from multiple vendors over multiple operating systems. Additional modules include medical specific solutions such as HIPPA compliant audit trails and power measurement of wireless equipment.

***With advances in wireless security technology, healthcare facilities can now profit from the benefits of wireless networking without having to compromise HIPPA compliance.***