# WIRELESS SECURITY IN HEALTH CARE

Zeeshan Ahmad [1]

[1] School of Computer and Information Science,
The University of South Australia

ABSTRACT: There are different types of Wireless Networking technologies available but the most prominent in health care industry is Wireless Local Area Network (WLAN). If critical and sensitive data is to be transmitted on air, it must be protected and access must be controlled. This research paper will investigate a bare minimum wireless security framework specifying the essential and desired components of wireless security in health care industry.

## INTRODUCTION

Wireless Networking has the potential to solve many problems, specifically linked with hard to move wired terminals, late updates of data and in some cases, data loss. Through mobile data processing devices, medical practitioners can have instant access to patient care data, lab reports, health policies, medical manuals etc. Nurses could access procedures while pharmacists could query database(s) of thousands of drugs. In a healthcare survey conducted in the United States involving 355 hospitals, it was discovered that Wireless technology and hand-held devices would be the most sought after technologies in near future [BAK2003].

Hand-held devices, pagers and mobile phones are already a part and parcel of the IT infrastructure of most modern hospitals. For example in an Australian context, Flinders Medical Centre of South Australia has a system in place, where fatal error(s) in core data processing systems of the hospital result in automatic notifications to the programmers and other stakeholders through pagers and mobile phones. A Commonwealth funded pilot project involving 12 iPAQs is underway to investigate the feasibility of Electronic Data Processing (EDP) applications on hand-held computers. Security is a critical aspect of wireless networking and this paper will investigate the appropriate security infrastructure in healthcare settings. Our main sources of research include review of field literature and interaction with the industry players, specifically in South Australia.

## WIRELESS SECURITY IN HEALTH CARE

### Confidentiality And Integrity: Health Critical Requirements

Breaches of Confidentiality and Integrity are the two biggest issues in health. Both can have serious professional and legal repercussions; not to mention the fact that patients' lives can be at risk [WAE2001]. Patient confidentiality is protected by numerous legislations in Australia. Government of South Australia [NTM2003] has published 'Code of Fair Information Practice' [DHS2001] that contains guidelines about secure data transfer policies. Before vital medical data is transferred in the air, proper security mechanisms should be put in place. Following section points out the major security limitations of wireless security and protocols.

### Security Limitations Of Ubiquitous Devices

Mobile data processing applications running on Personal Data Assistants (PDA) are very attractive in health industry. Unfortunately, today's PDAs and mobile data processing devices lack advanced security features. Contemporary PDA operating systems are not designed for carrying out secure functionality. Privilege access structure, protected memory space, virus protection and Access Control Lists (ACL) based permissions do not exist. Furthermore, hardware limitations prevent usage of strong encryption (computing-intensive algorithms and larger keys) [BAK2003]. Even more powerful desktop and laptop computers suffer due to wrong configuration. Health care IT managers must analyse security requirements and match them with the feature list of the candidate hardware platforms before acquiring a wireless infrastructure.

## Security Vulnerabilities And Risks

Spectrum Analysis: Frequency Hopping Spread Spectrum (FHSS) is de-facto wireless transmission standard; it distributes wireless waves across different frequencies. FHSS signals are prone to spectrum analysis and FHSS de-scrambling equipment is readily available in the market [NTM2003].

Open and Invisible Access Points: An Access Point (AP) links wireless devices to physical network (LAN). Wireless waves can not be physically restricted and can be picked up in the adjacent area of the access point. Later on, this information can be analysed and attacked with statistical methods. Management of hospitals should ensure that quasi-protected critical assets (e.g. web servers, databases) are not connected to the wireless infrastructure [BAK2003]. Periodic scanning can reveal hidden APs installed by the users of wired LAN. It should be a corporate policy to discourage and punish such practices.

Overlapping Access Points: Modern systems (such as Windows XP) claiming ubiquitous computing can automatically negotiate and re-configure when a user accidentally enters a new or stronger wireless zone – without user's knowledge. To prevent such security leaks, wireless devices with critical functionality should be locked to their respective security zones or access points [ibid].

Masquerading Access Points: Any wireless compatible computer equipped with software such as HostAP can act as an AP – it can be used to masquerade other wireless stations. The user names and passwords along with login details (MAC and SSID) can be easily retrieved from wireless stations requesting connections from a rogue AP. Rogue APs can take over the client wireless stations and encryption techniques such as VPN tunneling can be rendered useless [ibid].

MAC & SSID Identification: Access Points are often configured to identify authorised devices based on the unique MAC addresses and common SSID shared in a subnet. This form of security is not fully reliable. If MAC addresses and SSID are weakly encrypted, a hacker can use tools such as Ethereal and Kismet to extract the actual values [ibid].

Flooding and DoS attacks: Jamming, flooding and Denial of Service attacks are possible in WLANs. 'Denial of Service attacks can be launched by configuring a laptop as an AP and then flooding the airwaves with 'disassociate' commands that force all the stations within range to disconnect from the WLAN [ibid]'.

## Wireless Security Protocols And Standards

IEEE 802.11 WEP Security: It uses a challenge/response protocol authentication based on RSA RC4 stream. WEP encryption is weak and breakable and IT managers should not rely solely on WEP to protect critical data and functionality [NIK2001]. WEP cracking software such as WEPCrack and AirSnort are readily available on Internet [BAK2003].

IEEE 802.1x Security: Based on the p[revious standard, 802.11x offers dynamic key exchange facilities and offers Port Based Access Control. Unfortunately, session high-jacking is possible in all 802.1 based standards and 'combination of IEEE 802.1x and 802.1 standards does not provide a sufficient level of security, nor will it ever without significant changes [MAB2002].'

TKIP: Temporal Key Integrity Protocol [TKIP] has been proposed as a replacement for WEP. Using EAP based authentication, it offers stronger cryptographic support. This standard is not yet available on many devices and is prone to the 'Man in the Middle' attacks [MAB2002, BAK2003].

WAP Security: Wireless Application Protocol (WAP) has been designed for carrying out wireless data communications over low performance carrier links. Wired Transport Layer Security (WTLS) is the de-facto security protocol, providing confidentiality, integrity, and authenticity. WAP is susceptible to hacking when wireless data is decrypted inside the WAP gateway before being routed to internet.

## Off The Shelf Solutions

Standard protocols (discussed above) often do not offer the level of reliability desired for critical health care applications. IT managers might like to examine some off the self software. Solutions such as

NetMotion Mobility[NTM2003] and Citrex offer consolidated wireless security services and can be considered as an alternative to in-built security offered by ubiquitous devices.

NetMotion Mobility: An Example

NetMotion Mobility is built on the concept of Virtual Private Networks(s) and comprehensive authentication. A VPN 'connects the components and resources of one network over another network. VPNs accomplish this by allowing the user to tunnel through the wireless network or other public network in such a way that the tunnel participants enjoy at least the same level of confidentiality and features as when they are attached to a private wired network [BIR2001].'

Before a tunnel can be established, cryptographic methods are used to establish the identity of the tunnel participants (authentication). For the duration of the VPN connection, information traversing the tunnel can be encrypted (confidentiality). Authorisation and authentications are based on Windows NT authentication [NTM2003].

## CASE STUDY: FLINDERS MEDICAL CENTRE

### Background

Ubiquitous computing is Holy Grail of health informatics. Flinders Medical Centre (FMC) is spearheading the move towards mobile data processing in South Australia. Departments such as Surgery, Wards, CCMU, Computing, and Endoscopy are actively pursuing data processing applications utilising wireless technology. A team of in house developers is building a decision support system for iPAQ hand held devices called Pathology Ordering Decision Support [PODS]. Strict auditing demands require that highest level of security be maintained to protect critical and confidential data. As the ITS manager Raj Shastri put it, 'ad-hoc wireless installations have put the whole network infrastructure at risk'. Following paragraphs highlight the wireless security situation and the infrastructure designed to cope with it.

### Pathology Ordering Decision Support [PODS]

The PODS is software designed to integrate test protocols and patient pathology data for display on hand-held PDAs [UNT2002, WHI2003]. Patient pathology data is crucial and its integrity and privacy must not be compromised. Such a system would require Application Layer Security APIs for developers and Hardware Level Security Protocols for WLAN.

### FMC Wireless Security Net

Technical specification: iPAQ devices, equipped with wireless Network Interface Card(s) will connect to dual band 80.2.11a/g class APs in Aironet 1200 Network Configuration. This outer WLAN will be treated as a non-trusted Virtual LAN maintained using Cisco Catalyst 6509 router. APs would then connect to the wired infrastructure (trusted LAN) through FMC PIX firewall. This firewall is responsible for filtering all incoming and outgoing packets using a firewall policy already in place for LAN. End to end encrypted sessions will be maintained using Virtual Private Network and Cisco ACS 3.1 Dynamic Key Exchange server. While laptops are capable of running sophisticated VPN clients, the market for hand-held clients is still not mature. Solution may require acquisition of VPN clients for iPAQ PDAs.

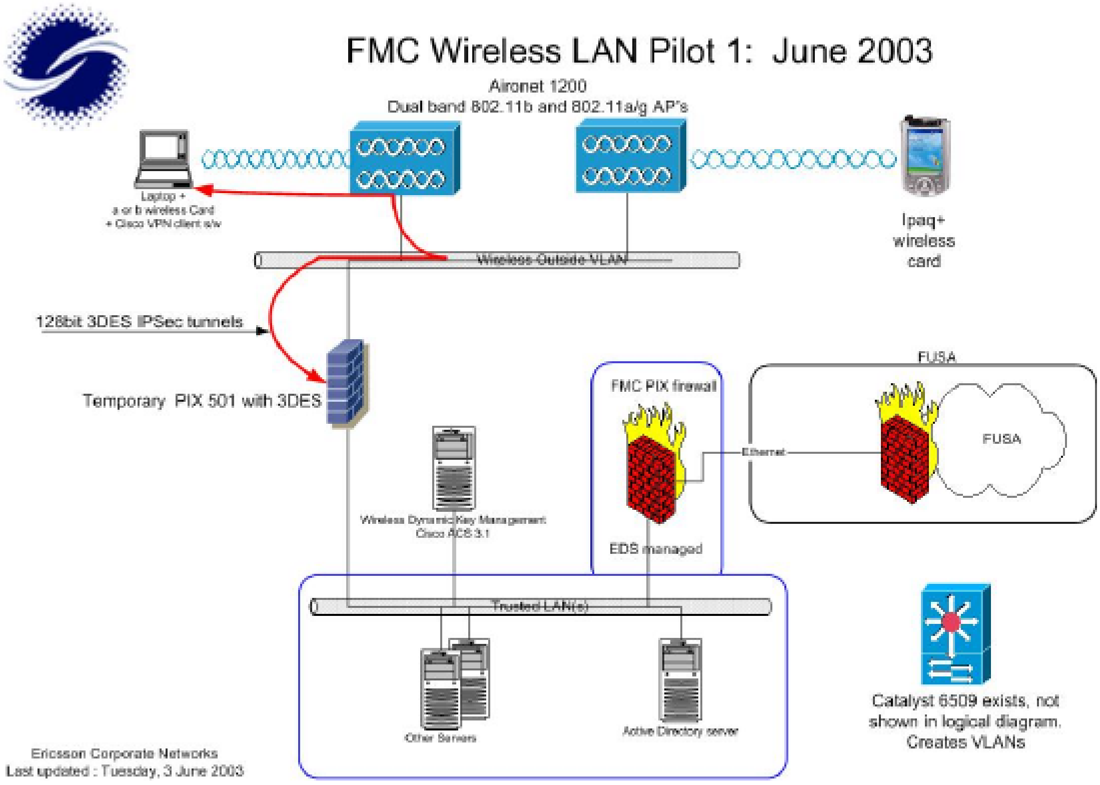
FMC Wireless LAN Pilot 1: June 2003
Aironet 1200
Dual band 802.11b and 802.11a/g AP's
Laptop +
a or b wireless Card
+ Cisco VPN client s/w
Ipaq+
wireless
card
Wireless Outside VLAN
128bit 3DES IPSec tunnels
Temporary PIX 501 with 3DES
FMC PIX firewall
EDS managed
Ethernet
FUSA
FUSA
Wireless Dynamic Key Management
Cisco ACS 3.1
Trusted LAN(s)
Other Servers
Active Directory server
Catalyst 6509 exists, not
shown in logical diagram.
Creates VLANs
Ericsson Corporate Networks
Last updated : Tuesday, 3 June 2003

Figure 1 - © Ericsson Corporate Networks [ERI2003]

Application Boot Procedure

A valid PDA must authenticate itself and establish a secure VPN session before any transaction can take place [UNT2002, ERI2003].

1. On a connection request, AP queries a checklist of valid MAC addresses and if that client MAC is allowed to connect, connection is offered

2. Client user name and password is authenticated against a Remote Access Server running Windows 2003 Server or Cisco ACS – authentication method is PEAP

3. A Virtual Private Network tunnel is established between mobile device and the LAN gateway – Cisco PIX 501 Firewall/VPN and a VPN client running on iPAQs

4. Wireless transactions take place inside the encrypted VPN tunnel

5. Optional: Applications may maintain their own Access Control Lists and control access to different levels of the application. This would provide another layer of security, on cost of performance and simplicity

Future Vision - Biometrics Technology: Biometrics Technology uses fingerprint technology for user authentication. Along with user name/password based security; the use of finger print biometrics technology can add a new layer of security and discourage theft of the device. Biometrics authentication should only be used in conjunction with standard authentication and not as a replacement.

Case Study Analysis

Network design is especially strong in areas such as multi-layer authentication, encryption, use of Virtual Private Network, treating WLAN as an un-trusted VLAN, and protecting crucial LAN infrastructure through a firewall. VPN is the cornerstone of security in this network configuration and the confidence in this technology is well placed. VPN has become the de-facto standard for remote access to critical resources and many IT support personnel at FMC use VPN to access computing resources remotely. Lack of application level security is a weak point in the system but it becomes a non-issue given the fact that data is transferred using a VPN. Initial MAC and SSID authentication is a weak point in system but the overall authentication procedure (involving EAP) is sound and workable. Although the network is still prone to Denial of Service attacks, a properly configured firewall can mitigate this effect by filtering rogue packets. Besides the network configuration, a mature and active security policy is needed to ensure that implementation and enforcement of security procedures (such as key management and encryption) is carried out properly. Continual network surveillance and wireless scanning would be needed to identify rogue and masquerading Access Points. By treating wireless LAN as a (non-trusted) Virtual LAN, critical resources can be protected from malicious attacks.

## CONCLUSION

It is obvious that no ‘out of the box’ wireless security solution provides the level of security desirable in health care area. Following model takes into account the research conducted so far and encapsulates the set of ‘reasonable protection’ technologies for wireless based applications deployed in a health care establishment. Security implementations (third party software packages or off shelf network solutions) based on this framework best meet the health care wireless security needs in current technology context [for further reading: NTM2003, BAK2003, and MOT2002].

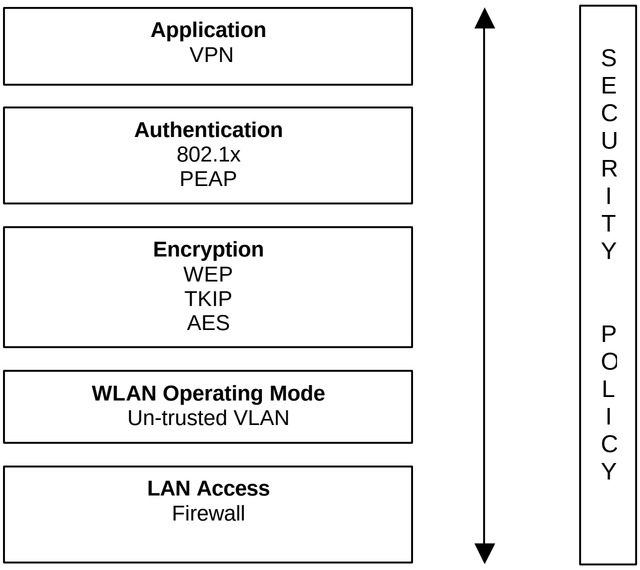

Figure 2 – A Framework

## REFERENCES

[AND2002] Andersson. H et al. 'Protected EAP Protocol (PEAP),' PPPEXT Working Group, 23 February 2002, Available at http://www.globecom.net/ietf/draft/draft-josefsson-pppext-eap-tls-eap-02.html (Last Accessed Thursday, 17 July 2003)

[BIR2001] Virtual Private Networks, Frequently Asked Questions, Compiled by Tina Bird, Moderator, VPN Mailing List, Available at http://vpn.shmoo.com/, Last modified: 19 Aug 2001, (Last Accessed Thursday, 17 July 2003)

[BAK2003] Baker. Dr. Dixie B., 'Wireless (In)Security for Health Care, Version 1.1', HIMSS Advocacy White Paper published by Enterprise & Health Solutions January 10, 2003

[DHS2001] ‘Code of Fair Information Practice’, Department of Human Services, Government of South Australia, 2nd Edition, December 2001

[ERI2003] ‘FMC Wireless LAN Pilot’, Ericsson Corporate Networks, 03 June 2003

[GHO2001] Ghosh, Anup K. and Tara M. Swaminatha, ‘Software Security and Privacy Risks in Mobile e-Commerce,’ Communications of the ACM, Vol. 44, No. 2, Feb 2001, pp 51-57.

[MAB2002] Mishra, Arunesh, and William A. Arbaugh, “An Initial Security Analysis of the IEEE 802.1x Standard,” University of Maryland, Department of Computer Science, Report CS-TR-4328, UNIACS-TR-2002-10, 6 February 2002.

[MOT2002] Mota. Ray, 'Enterprise Wireless LANs - Analyzing the Ramifications of Untethering Your Corporate LAN,' Published by Synergey Research

[NIK2001] Nikita B., Ian G., and David W., ‘Security of the WEP algorithm’, University of California at Berkeley, February 2001.

[NTM2003] ‘NetMotion Mobility HIPAA Compliance’,Available at http://www.netmotionwireless.com/solutions/healthcare/hipaa.asp

[RUB2003] Rubin. Aviel D., ‘Wireless Networking Security,’ Communications of the ACM, May 2003 Volume 46, Number 5

[UNT2002] Unterweger. Zlatko. ‘Pathology ordering decision support’ Overview and initial specification document, 11-Sep-2002, Flinders Medical Centre Information Technology Service

[WAE2003] Waegemann. C. Peter, ‘Confidentiality and Security for e-Health’, Available at http://www.itu.int/itudoc/itu-t/workshop/e-health/s5-05.pdf (Last Accessed Thursday, 17 July 2003)

[WEA2000] Weatherspoon, Sultan. ‘Overview of IEEE 802.11b Security,’ Intel Technology Journal, Q2, 2000.

[WHI2003] White. T., et al, ‘Facilitating Best Practice Pathology Utilisation by the Use of the Hand-Held Decision Support Devices,’ October 2002, Department(s) of Computing Service and Department of Medical Biochemistry, Flinders Medical Centre