REPORT

WIRELESS SECURITY AT BARWON HEALTH

BY VERITY CARNEY
WIRELESS PROJECT OFFICER
DEAKIN IBL STUDENT

TABLE OF CONTENTS

Executive Summary

- It is important that wireless security policy be formulated in line with existing hospital policy and Australian Privacy law to protect the confidentiality, integrity and security of all personal patient information held on the hospitals databases.

- It is also recommend that Barwon Health deploy several layers of defence across the wireless network to mitigate against intrusion and associated breaches of security.

- As an organisation that entrusts mission-critical data to the WLAN network, Barwon Health must invest in a robust, enterprise-class WLAN security solution.

- The Cisco Wireless Security Suite is an enhanced security solution that provides full support for WPA and its building blocks of 802.1X and TKIP.

- Access Control Lists are the most practical solution to ensuring only authorised access to the wireless network.

- To regulate access control, a Radius server can be used to enable centralised authentication and authorisation of not just individuals but also the wireless computers or devices that are permitted access to the network.

- Network Administration at Barwon Health IT Operations should continue to conduct routine and ad hoc audits of network access for intrusion detection.

Wireless Security at Barwon Health

Introduction

Wireless security provides end users with freedom and mobility without offering intruder's access to the WLAN or the information sent and received on the wireless network.

With a WLAN, transmitted data is broadcast over the air using radio waves that travel between client devices, or stations, and access points—the WLAN endpoints on the Ethernet network that link stations to the network. This means that any WLAN client device within an access point service area can receive data transmitted to or from the access point.

With a WLAN, the boundary for the network has moved. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, including in the parking lot.

IT Operations at Barwon Health need reassurance that solutions are available to protect the health services wireless network from these vulnerabilities and that WLANs can provide the same level of security, manageability, and scalability offered by wired LANs.

Background to the Security Imperative

Currently the wireless network at Barwon Hospital is without access controls other than authentication (username/password). In the not too distant future all sites of Barwon Health will be linked via a WiMAX wireless tower that transmits radio frequency to connect point-to-multipoint over a 50 km radius.

At this stage Barwon Health has trialed the use of 16 wireless tablet PCs that may access the network throughout the Geelong Hospital. Over time, however, the wireless technology will become a more widely used and accessed transmission medium.

To comply with law on the privacy, security and integrity of personal information it is essential that Barwon Health IT implement more rigorous access controls to the wireless network. The methods used to secure the network against unauthorised access must be selected and implemented at the level of configuration (security settings) as well as at the physical level of access control (MAC addresses).

Need For Review

Although there have been no known security breaches at Barwon Health it is necessary to outline policy and ensure the appropriate technical measures are taken to secure the network and patient records therein from unauthorised access and tampering. This is particularly relevant given that the wireless network will increasingly be accessed after the network infrastructure is expanded to integrate all sites and facilities of the health service (WiMAX).

It is important that that appropriate controls are placed on access to the network and that policy is developed to ensure legal protection and compliance in the new environment of an increasingly ubiquitous network.

It is often the case that technology develops faster that the principles and practices used to regulate and control its effect and impact. Existing law and policy is a guideline to how the technology should be implemented to ensure compliance with these already agreed to standards and principles and points of law.

The main Act that the wireless network must adhere to is the Privacy law covered in the Privacy Act 1988 (Cth) which incorporates the amendments made to it by the Privacy Amendment (Private Sector) Act 2000 (Cth). in regard to the following principles:

- Storage and security of personal information.
- Access to records containing personal information.
- Alteration of records containing personal information.
- Personal information to be used only for relevant purposes.
- Limits on use of personal information.
- Limits on disclosure of personal information.

The rationale for the adherence to this law is that databases recording personal details, financial accounts and medical records contain private, sensitive and legally protected information.

In addition a wireless network opens new backdoors to malicious hacking and attack, which must be protected against.

The function of a wireless network

The wireless network is an integration of already existing IEEE 802.11 (WiFi) which has been implemented and trailed at the Geelong Hospital with the future extension of IEEE 802.16 (WiMAX) which will link up all sites of Barwon Health into a ubiquitous point-to-multipoint network within a 50 km radius of the radio tower that is to be installed at the Hospital.

The advantage of the network is that it enables full mobility to doctors, nurses and other clinicians throughout the area health service. Patient records and test results may be accessed, referenced and updated at the bedside or during a home visit. The wireless network will thus allow all Health Professionals of Barwon Health to perform their roles within the Area Health Service much more efficiently and effectively due to the availability of network access regardless of location. More detailed notes may be taken at the bedside and patients may benefit from increased quality of service that can be provided by ubiquitous access to patient treatment and care plans as well as test results.

The touch screen tablet computers that have been introduced as part of the wireless trial have additional features that further enhance the benefits of the ubiquitous network. The units allow the user to make notes by writing with a stylus on the screen. These handwritten notes and annotations may be stored and sent electronically – enabling ad hoc and non pro-forma communication between health professionals within the service and thereby facilitating greater collaboration.

Future evolution of the capability may some day soon enable voice recognition applications for doctors and mobile clinicians to enter verbal notes at a patient bedside. In addition the potential for accessing and viewing x-rays and CT scans etc may in the future be possible as medical imaging is digitised and stored within the computer databases of Barwon Health.

WLAN fit into Strategic Objectives

The wireless network enhances the flexibility and scalability of the computer infrastructure at Barwon Health. At the same time doctors, nurses and other clinicians are offered a new level of mobility to ensure best practice in patient care in the hospital and soon throughout the whole area health service. With the ability to access patient care plans, medical records and test results at the patient bedside, doctors will be able to provide better information based consultations with hospital patients and their families. Greater access to information at the point of care will improve the level of service and enhance informed choices in medical treatment and care. These benefits are just the tip of the iceberg for what will in future be a revolution in best practice with the convergence of information and technology in the face-to-face treatment of the sick and disabled throughout Barwon Health.

Wireless Network Threats

Attackers target Wireless networks since about 95% of all networks are completely unprotected. The current standard (802.11b) grants bandwidth of up to 11 MBps. If a Wireless network uses default settings there will be no cap set on bandwidth, which means the attacker can have complete access to the capacity.

Security Risks and Vulnerabilities:

- Spectrum Analysis
- Open and Invisible Access Points
- Overlapping Access Points
- Masquerading Access Points
- Man-In-The-Middle Attack
- MAC & SSID Identification
- Flooding and DoS attacks

It is not possible to anticipate the motivation for such attacks. Some may be just the effect of recreational (illegal) hacking that may at some extreme take the form of a malicious attack. Other scenarios could possibly involve (unprofessional) private investigators in insurance cases breaking into the system to obtain medical records for some particular case. It is possible also that attempts may be made by vested interests to alter or delete particular medical records. It is also possible that in an unsecured network curious people may simply try to see what information they might obtain.

Whatever the reason or the method of intrusion into the wireless network an occurrence of such an attack is a fundamental compromise of information security that threatens the integrity of records and the privacy of patient details. In addition such an attack is a contravention of law on the part of the attacker as well as the Health Service for not ensuring proper security controls.

Prevention is always the best and most effective way to mitigate against such risks. Prevention is ensured by the development, dissemination and implementation of correct security policy in line with legal requirements. In addition, after careful consideration of possible risks and systems requirements, the optimum configuration of Access Points and wireless devices are required. Last but not least is the use of rigorous authentication and authorisation mechanism that then allow network administrators to conduct routine and ad hoc audits of network access.

Security Policy - Legal Requirements

Through mobile data processing devices, medical practitioners can have instant access to:

- Patient care data
- Lab reports
- Health policies
- Medical manuals
- Procedure policy and instructions
- Pharmaceutical databases
- Communication (pagers, email)

Data traversing a wireless environment is vulnerable to corruption, eavesdropping, and unauthorized access.

Confidentiality and Integrity are the two biggest issues in health care (with professional and legal repercussions).

Patient pathology data is crucial and its integrity and privacy must not be compromised.

Australian Commonwealth Privacy law protects individual patient records from unlawful access, disclosure, use and alteration. In addition new developments in the law provide protection of human genetic information[1].

Section 6 of the Privacy Act defines 'health service' as an activity performed in relation to an individual:

- To assess, record, maintain or improve the individual's health; or
- To diagnose the individual's illness or disability; or
- To treat the individual's illness or disability or suspected illness or disability; or
- The dispensing of a prescription drug or medicinal preparation by a pharmacist.

The Privacy Act applies to all public and private sector organisations that deliver these types of services, including all small health services that hold health information. The types of health services covered include traditional health service providers such as hospitals and day surgeries, medical practitioners, pharmacists, and allied health professionals such as counsellors, as well as complementary therapists, gyms, weight loss clinics and many others.

From 21 December 2001 amendments to the *Privacy Act 1988* (Cth) became operative. The new provisions provide for ten National Privacy Principles (NPPs), found in Schedule 3 of the Act, which apply to health service providers. These principles include:

- Principle 1 - Collection
- Principle 2 - Use and disclosure
- Principle 3 - Data quality
- Principle 4 - Data security
- Principle 5 - Openness
- Principle 6 - Access and correction

[1] Protection of Human Genetic Information, as prescribed by law
http://www.austlii.edu.au/au/other/alrc/publications/reports/96/

- Principle 7 - Identifiers
- Principle 8 - Anonymity
- Principle 9 - Trans border data flows
- Principle10 - Sensitive information

Four other significant areas that are monitored by the Commissioner and affect parts of the health sector are in relation to:

- The storage, use, disclosure and retention of individuals' claims information under the Pharmaceutical Benefits Scheme and the Medicare program;
- Privacy standards in the conduct of human medical research in Australia;
- The collection, use and disclosure of personal medical information in relation to the conduct of research, compilation and analysis of statistics relevant to public health, safety or health service management activities; and
- The collection, storage, use and security of personal tax file numbers by organisations that are authorised or approved to record such information under taxation, assistance agency or superannuation law.

The wireless network must comply with Privacy Law in regard to the storage and security of personal information. Access to records containing personal information must be restricted to only those authorised to access them through network access controls and existing authentication procedures (username/password). Before vital medical data is transferred in the air, proper security mechanisms should be put in place[2].

[2] There exist accepted Australian (SA) guidelines about secure data transfer policies http://www.familiesandcommunities.sa.gov.au/Default.aspx?tabid=98

Wireless Security Policy

1. Purpose

In accordance with State and Federal Law all reasonable measures shall be taken to protect personal health information from unauthorised access, disclosure, improper use, and improper alteration. This policy outlines the security safeguards and guidelines for Barwon Health (BH) Staff using the wireless network.

2. Scope

- The network administrator(s) of Barwon Health I.T.
- All persons and entities – including staff, clients and their families, visitors, members of the public and external organisations.

3. Responsibility

- **Staff** who use the network to store and retrieve information on patient care data and lab reports via wireless equipment.
- **IT Operations** conduct routine and ad hoc audits of access, email and password usage for intrusion detection and to ensure compliance to law.
- **Network Administrator** to undertake proper architectural design and configuration of the WLAN to mitigate risk and ensure consistent security settings and to control access to the wireless network.

4. General Policy

- The highest standards of information security are expected within Barwon (See BH Security Policy). The wireless network requires compliance with these already existing policies.

- Base stations and Access Points are to be configured in accordance with the most current security settings to protect against unauthorised access to the network by computers and devices that are not issued by or registered at BHIT operations.

- Personal patient details and records as well as mission critical data are not to be stored on the hard-drive of a wireless computer.

- Standard procedures for requesting and granting new network connections are to be followed and documented.

- Passwords for all information systems are to be kept secure. Staff are responsible for any access to secure information systems using their password.

5. Policies for Network Administration

- Identification of who may use WLAN within Barwon Health
    - Doctors nurses and mobile clinicians in general

- Identification of who can install Access Points
    - B.H.I.T Networking Department

- Security and attack mitigation
    - Routine and ad hoc audit of network access (Intrusion detection for critical resources and subnets).
    - Rotation of encryption key – every three months

- Authentication and authorisation of users to network resources
    - Username / password
    - Valid MAC address and correct encryption key

- Limitations on the location of and physical security of APs
    - APs should be installed out of reach and possibly out of sight – accessible yet secure. Ideally they should be located high on a wall in busy wards at nursing stations where staff are constantly around.

- Registration of new APs and wireless devices.
    - All wireless devices (PC, TC, PDA) used at Barwon Health must be registered at IT Operations – for set up and to record MAC address to enable access. Unit numbers and barcode must be entered into the helpdesk system.

- Reporting the loss of APs and security incidents
    - See hardware department for existing policy and procedure for lost / stolen equipment

- Disabling of unauthorised wireless devices.
    - Remove MAC address from Radius Server

- Frequency of the security assessments.
    - Review every six months

- Access Point (AP) Administration
    - Administration of APs should be done over the wired LAN or via the COM ports to avoid sniffing and packet interception over the WLAN.
    - Only administrators should have access to the LAN key distribution program for the distribution of the encryption keys to ensure their integrity

6. Baseline Configuration Policy

Safeguards

The following are the minimum safeguards, which should be implemented in order to adequately secure the Access Point (AP). These safeguards address the policy aspects of security, as well as the technical configuration and standards for encryption and authentication.

AP Configuration

The following configuration settings will help remove many of the APs vulnerabilities.

Updating Default Passwords: APs generally come with a factory default administrator password, if left unchanged unauthorised users can gain access because these default passwords are common knowledge and widely available.

- All passwords should be updated throughout the AP.
- Passwords should consist of alphanumeric and special characters and be a minimum of eight characters long.
- Passwords should expire after a specified period of time according to the security policy set.

Enable Encryption: Encryption should be turned on and set to the strongest encryption scheme available.

Use MAC ACL: MAC address Access Control Lists (ACLs) allow the AP to grant or deny access to the network based on the users NIC physical address. This provides a strong deterrent against casual attackers.

Change Default SSID, Disable SSID Broadcast, Lengthen Beacon Interval:

- The SSID should be changed from its factory default values, which are published and widely known.
- The SSID should be undescriptive so an adversary can not tell the location of the WLAN.
- The beacon interval[3] should be set to the largest possible time so it does not transmit the SSID as frequently making it more difficult for adversaries to passively find the network.
- The broadcast SSID feature should be disabled[4] in order to ensure active scanning which is probing with a specific SSID.

Change Default Cryptographic Keys: The default keys provided by the manufacturer to enable shared-key authentication should be changed as many vendors use the same shared keys in their factory settings.

Use SNMPv3, Not SNMPv1 and SNMPv2 (Optional): Wireless APs which support SNMP agents allow management software tools to monitor the status of the APs and clients. The first two versions of SNMP support only trivial authentication based on plain-text community strings and thus are fundamentally insecure and should not be used.

- If SNMP is required on the network, version 3 should be used which includes mechanisms to provide strong security. Also,
- The default SNMP community string is commonly known and should be changed as often as necessary to a strong community string.

Change Default Frequency Channel: If two or more APs located near each other use the same default channel and are not on the same network a DoS can result from the radio interference. If radio interference occurs the channels should be changed so that no AP in range is within five channels of the network.

---

[3] The Beacon frames are transmitted at regular intervals to allow a client station to identify and match configuration settings in order to join a wireless network

[4] When searching for a network to join, a client triggers a response from all APs within the area through the use of the broadcast Probe Request message which gets a response from the AP. Disabling the Broadcast SSID feature in the AP ensures the AP doesn't respond to the Probe Request message

Don't Use DHCP, Use Static IP Addresses, Change APs Default IP Addresses:
Wireless devices which join the network automatically use a DHCP server in order to assign themselves IP addresses.

- DHCP should not be used as adversaries could easily gain unauthorised access because DCHP will not necessarily know which devices have access and will automatically assign the adversary a valid IP address
- Static IP addresses should be used on the network to ensure only valid users have the correct IP addresses and can connect to the network.
- The APs default IP address should be changed to prevent unauthorised administration of the AP over the network.

Protect COM Ports, Disable Unnecessary Services:

- The built in COM ports of the AP should be disabled or password protected to protect against unauthorised use.
- All unnecessary ports and services should be disabled

Load Balancing (Optional)

Administrators should consider implementing load balancing across multiple APs to protect the WLAN against flooding.

This would dramatically remove the potential for DoS attacks to occur and be successful on the WLAN

Use Wi-Fi Protected Access (WPA)

Wi-Fi Protect Access (WPA) should be used for authentication and encryption on the wireless network[5].

WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption and utilises 802.1X and EAP for user authentication

TKIP provides per packet mixing functions, a message integrity check (MIC), an extended Initialisation Vector (IV) with sequencing rules and a re-keying mechanism.

The 802.1X and EAP technologies used for authentication utilise a central authentication server such as RADIUS which authenticates each user joining the network.

[5] WPA is available as a firmware upgrade to WEP, and was developed as an interim replacement, which fixes all known problems before the new 802.11i standard becomes available

Access Control using a RADIUS Server

The Remote Authentication Dial In User Service (RADIUS) protocol (RFC 2865) was originally defined to enable centralized authentication, authorization, and access control (AAA) for SLIP and PPP dial-up sessions.

This architecture made it possible to create a central user database, consolidating decision-making at a single point, while allowing calls to be supported by a large, physically distributed set of Network Access Servers.

Applying RADIUS to Wireless LANs

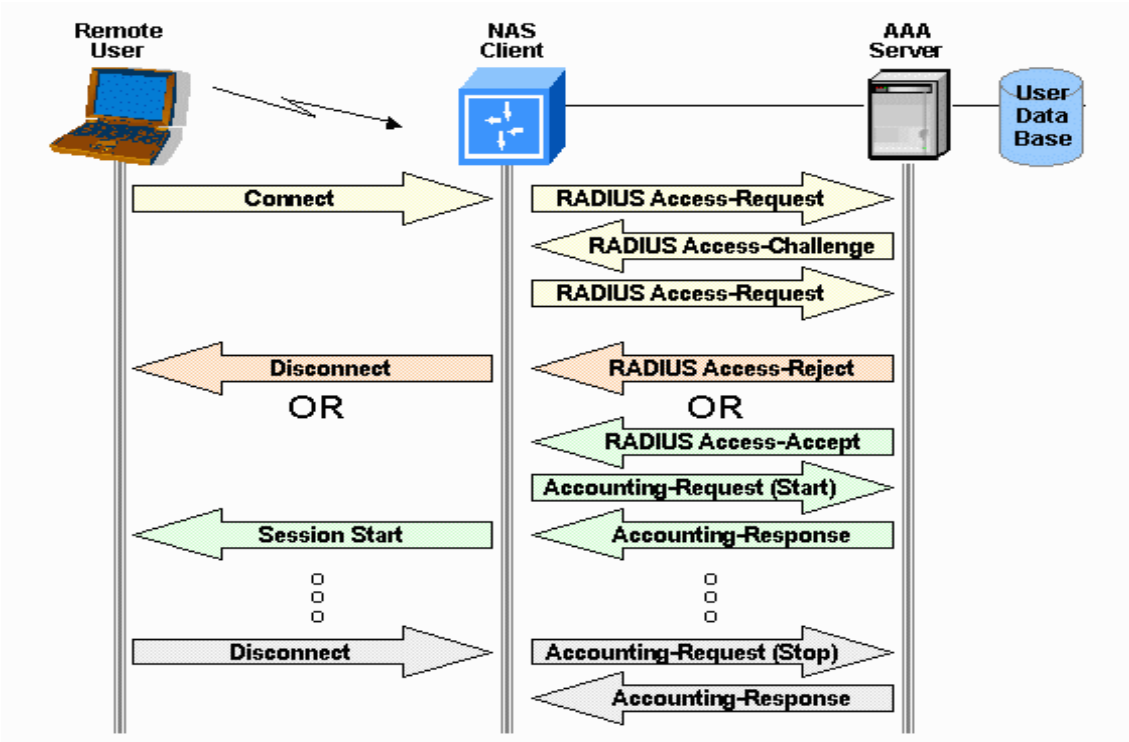
In a wireless network that uses 802.1X Port Access Control, the wireless station plays the role of the Remote User and the wireless AP plays the role of the Network Access Server.

Once associated, the wireless station sends an EAP-Start message to the AP. The AP requests the station's identity and relays it to an AAA Server inside the RADIUS Access-Request User-Name attribute.

The AAA Server and wireless station complete the authentication process by relaying RADIUS Access-Challenge and Access-Request messages through the AP.

If the AAA Server issues an Access-Accept message, the AP and wireless station complete a handshake to generate session keys used by WEP or TKIP to encrypt data. At that point, the AP unblocks the port and the wireless station can send data and receive data to and from the attached network.

If the AAA Server issues an Access-Reject message, the AP disassociates the station. The failed station can try to authenticate again, but the AP prevents the station from actually sending data through the AP into the adjacent network.



Cisco Wireless Security Suite □Aironet Series

The Cisco Wireless Security Suite for the Cisco Aironet Series provides a robust wireless security services that closely parallels the security available in a wired LAN.

This enterprise WLAN security solution integrates quality of service (□oS) and mobility into its framework. Mitigating against sophisticated passive and active WLAN attacks while providing reliable, scalable, centralized security management with support.

Central to this wireless security suite is a Radius Server using 802.1X Authentication and the Extensible Authentication Protocol

The IEEE has adopted 802.1X as a standard for authentication on wired and wireless networks. This standard provides WLANs with strong, mutual authentication between a client and an authentication server.

In addition, 802.1X provides dynamic per-user, per-session encryption keys, removing the administrative burden and security issues surrounding static encryption keys. With 802.1X, the credentials used for authentication, such as logon passwords, are never transmitted in the clear, or without encryption, over the wireless medium.

Another benefit of 802.1X authentication is centralized management for WLAN user groups, including policy-based key rotation, dynamic key assignment, dynamic VLAN assignment, and SSID restriction. These features rotate the encryption keys. They also assign users to specific VLANs to ensure that users are only allowed access to specific resources.

After mutual authentication has been successfully completed, the client and RADIUS server each derive the same encryption key, which is used to encrypt all data exchanged.

Using a secure channel on the wired LAN, the RADIUS server sends the key to the access point, which stores it for the client. The result is per-user, per-session encryption keys, with the length of a session determined by a policy defined on the RADIUS server. When a session expires or the client roams from one access point to another, a re-authentication occurs and generates a new session key. The re-authentication is transparent to the user.

□uture Evolution of the Wireless Network

Wi□A□

In early 2005 Barwon Health IT will be installing a WiMAX tower to connect all sites of the Area Health Service to the wireless network.

WiMAX is standards based wireless technology that provides high-throughput broadband connections over long distances.

It is designed as a complementary technology to Wi-Fi and Bluetooth.

One of the most compelling aspects of Broadband wireless access technology is that Networks can be created in just weeks by deploying a small number of base stations on buildings or poles to create high-capacity wireless access systems.

WiMAX will be the most significant technology to date in making wireless access ubiquitous and, as more free-spectrum is opened up, in creating a major shake-up of the traditional shape of the wireless and mobile communications sector.

Features

- WiMAX uses a radio spectrum frequency range from 10 to 66 GHz, with additional frequency band available between 2 and 11 GHz (802.16a) – supporting licensed and unlicensed bands.
- Provides a 31-mile linear service area range (50 kilometres) with a Cell radius 4 – 6 miles.
- Non Line-Of-Sight connectivity – using point-to-multipoint (PMP) applications and is based on Collision Sense Multiple Access with Collision Avoidance (CSMA/CA)

Transmission Rates□

- High capacity links on both the uplink and downlink of up to 75 megabits per second (Mbps) data transfer rates on a single channel.
- Obtains these speeds in the 2 to 11 GHz range by using OFDM
    - Channels can be bonded together to provide higher bandwidths. eg six channels can be used to provide an effective bandwidth of 250 to 350 Mbps
- By using a robust modulation scheme, IEEE 802.16 delivers high throughput at long ranges with a high level of spectral efficiency that is also tolerant of spectral reflections.

Interoperability

- The 802.16 standard ensures the compatibility and interoperability of broadband wireless access equipment

Security

The 802.16 specifications also include robust security features – privacy and encryption features to support secure transmissions and provide authentication and data encryption. Including:

- Privacy Key Management (PKM) for MAC layer security. PKM version 2 incorporates support for Extensible Authentication Protocol (EAP).
- Terminal authentication by exchanging certificates to prevent rogue devices.
- Data encryption using the data encryption standard (DES) or advanced encryption standard (AES) both much more robust than the Wireless Equivalent Privacy (WEP) initially used by WLAN.
- The architecture supports Subscriber Station (SS) authorisation, strong bilateral user authentication based on a variety of authentication mechanisms such as username/password, X.509 certificates, Subscriber Identity Module (SIM), Universal SIM (USIM), Removable User Identity Module (RUIM), and provides services such as data integrity, data replay protection, data confidentiality, and non-repudiation using maximum key lengths.

□*uality of Service*

WiMAX is characterised by Quality of Service (QoS) features that are needed to enable and support voice (VoIP) and video transmission.

Benefits□

WiMAX has key benefits for operators. By choosing interoperable, standards-based equipment, the operator reduces the risk of deploying broadband wireless access systems.

- Having a standard in place opens the door to volume component suppliers that will allow equipment vendors to focus on system design, versus having to develop the whole end-to-end solution.
- Ultimately operators will benefit from lower cost and high performance equipment, as equipment manufactures rapidly create product innovations based on a common, standards-based platform.
- The standard accommodates voice, video, and other data transmissions by using appropriate features in the MAC layer, which is more efficient than doing so in layers of control overlaid on the MAC.
- Operators are not locked in to a single vendor because base stations will interoperate with subscriber stations from different manufacturers

The wireless tablet capability

Features

The Compaq TC1000 wireless computer tablets currently being trialed at Barwon Health have many distinguishing features. In particular the computer tablets offer simplified computing by adding the convenience of writing using the stylus on the screen.

The unit allows the user to write and store information, sketch pictures and mark up documents with handwritten comments ('digital ink'). Handwritten journal notes (observations) may be made at the patient bedside. These handwritten notes and annotations may be stored and/or sent, enabling ad hoc and non pro-forma communication and facilitating greater collaboration.

Text recognition (automatic transcription) of handwritten journal notes is also a feature of the tablet computer. At the same time using writing the Pad Input Panel can speed up Internet navigation by handwriting a URL and search terms onto the screen.

It is recommended that tablet computer users take the in-built tutorial on using the Journal to ensure that maximum use of this text recognition feature.

Potential Future Applications

It has been suggested by Doctors involved in the tablet trial that Voice recognition applications could be run on the computers and thus allow doctors and other clinicians to enter verbal notes at patient bedside.

It is also possible that in future the wireless tablet computers might be used for accessing and viewing x-rays and CT scans. Currently x-rays (and images) are not stored digitally within the computer database at Barwon Health. In addition many doctors prefer to view x-rays on a light box (increases visibility and thus reliable diagnosis). In future however, the technology may allow zooming (magnification) and greater contrast control to assist doctors in using the technology to assist them in reading these images.

Next Generation - TC1100

HP has given the PC TC1100 a much-needed component boost, resulting in this significantly faster and longer-lasting tablet.

Features include:

- 1GHz Pentium M or an 800MHz Celeron processor;
- A 32MB Nvidia GeForce4 420 Go graphics chip;
- A 30GB or 40GB hard drive;
- And from 256MB to 2GB of fast 333MHz DDR SDRAM.
- With Intel's 855PM chipset and PRO/Wireless 802.11b mini-PCI card,
- The TC1100 qualifies as an official Centrino system.

The test configuration, featuring a 1GHz Pentium M, 512MB of memory, and a 40GB hard drive, performed more than twice as fast as the previous model did in tests.

The Pentium M's power-saving capabilities also lent a hand with the battery life, helping it last 34 minutes longer than its predecessor.

Thanks to its 11.1V, 3,600mAh (40WHr) battery, the TC1100 achieved very long life, clocking in at nearly 4 hours

Wireless LAN Security Assessments Steps

These assessment steps are a valuable guideline for Network Administrators as they conduct checks and reviews of the wireless network to mitigate against security threats. The network security should be assessed every six months.

1. Review existing security policies
2. Review the system architecture and configurations
3. Review operational support tool and procedures
4. Interview users
5. Verify configuration of wireless devices
6. Investigate physical installation of access points
7. Identify rogue access points
8. Perform penetration tests
9. Analyse security gaps
10. Recommend improvements

Recommendations

- Barwon Health should deploy several layers of defence across the network to mitigate threats. Additional security components might include firewalls, intrusion-detection systems (IDSs), and virtual LANs (VLANs).

- Access Control Lists are the most practical solution to the issue of authorised access to the wireless network. This form of control is implemented at the physical/data link level by filtering MAC addresses – granting access only to registered wireless computers and devices (PDAs).

- To regulate access control, Radius servers can be used to enable centralised authentication, authorisation and access control (AAA)- in addition to implementing Light Extensible Authentication Protocol (LEAP) in a wireless network.

- As an organisation that entrusts mission-critical data to the WLAN network, Barwon Health must invest in a robust, enterprise-class WLAN security solution.

- The Cisco Wireless Security Suite is an enhanced security solution that provides full support for WPA and its building blocks of 802.1X and TKIP. The following features are part of the Cisco Wireless Security Suite:

    - 802.1X for strong, mutual authentication and dynamic per-user, per-session encryption keys

    - TKIP for enhancements to RC4-based encryption such as key hashing (per-packet keying), message integrity check (MIC), initialisation vector (IV) changes, and broadcast key rotation

- In addition policy must be formulated and approved in line with existing hospital policy and law that regulates the confidentiality, integrity and security of all personal patient information held on the hospitals databases.

- Network Administration at Barwon Health IT should continue to conduct routine and ad hoc audits of access for intrusion detection.