Iatric Systems
Wireless Security Introduction

The information contained in this document is presented for reference purposes only. Information included is current as of this writing. As wireless networking and security are rapidly changing environments, please notify Iatric Systems, Inc. of any inconsistencies or new information, and every effort will be made to update this reference in as timely a manner as possible. All trademarks are property of their respective owners.

Iatric Systems, Inc. has implemented security within the MobilCare product line to work with and enhance the existing security of wireless networks. Recognizing that, many healthcare groups have requested further guidance or reference information for implementing or enhancing their own wireless networks.

Wireless Network Security Overview

Wireless network clients must be authenticated, the communications encrypted and integrity verified in order for the network to be considered secure. This can be accomplished by a variety of methods, such as WEP, WPA, or WPA2. Some methods are more secure, while others offer wider compatibility. In addition, certain components or standards are often part of more than one security method.

Most organizations find standardizing on one solution to meet all needs is a goal that can rarely be met. Legacy clients and required equipment often force compromises. Security can often be described as striking a balance between absolute security (no access for anyone) and complete accessibility (no restrictions for anyone). That balance point should be the point of acceptable risk.

For this reason, no one set of recommendations or guidelines can be written to cover all eventualities. Toward that end, this document is intended to help each organization identify the security measures most suited to their environment.

The primary factors of wireless network security can be expressed as:

1. Authentication – I am allowed to communicate with you, because I've proven who I am.
2. Encryption – Communications will be confidential, and not subject to eavesdropping.
3. Integrity – Communications will be verified complete, with counterfeits or errors ignored.

Choosing the methods used to provide these primary factors can be a challenge. The networking industry and individual vendors have provided a myriad of choices with which to secure a wireless network. However, these choices are often incomplete, in conflict with one another, or do not support a suitable range of devices. Several of the encryption and authentication methods proposed as standards in the past have turned out to be weak or insecure. In addition, many of the currently offered solutions have limitations that prove daunting when an organization attempts to implement a solution.

To further complicate a new implementation, many of the current standards have several complex sub-components which may or may not work with one another. A given device may or may not support, or be certified for, a given standard. There is, however, often additional software which does meet the needs. In fact, many solutions often require the purchase of additional software clients for some or all devices.

1. Authentication

WEP Shared Key – WEP (Wired Equivalent Privacy) has been used in the past with pre-shared keys as a means of simple authentication. Clients must be configured with the same keys in order to connect.

However, once the encryption method was found to be weak in 2000-2001, pre-shared keys quickly became a security risk. While WEP encryption is weak, and can be cracked in a matter of hours using current processors and software, it is better than nothing. Using shared keys however, means that an eavesdropper has only to crack one of the pre-shared keys, and that individual now has access listen to private data of anyone on the network.

WEP Open Authentication – WEP Open Authentication, by contrast, chooses a new key for each new connection. While it offers no authentication, it does offer somewhat better security, because even if one session is cracked, the key obtained is useless for any other session, even to the same access point. This is essentially a trade-off. With open authentication, anyone can join the network and see what they can find. However, the randomized keys make it slightly less likely that private data will be compromised by eavesdropping.

MAC Address Authentication – a MAC (Media Access Control) Address is the address of your network card. This isn't the same as the IP Address, but, rather is usually the address burned into the card at the factory. Some sites may elect to set their MAC Addresses; these are referred to as LAA's (Locally Administered Address).

While a great variety of access controls can be set based on the MAC Address, this has significant weaknesses as a method of authentication. An eavesdropper can find the MAC Address of a valid device in seconds, and can have their system configured to use it (by means of an LAA) in minutes.

Web Authentication - Several systems are available which require users to log in via username and password to a web page. Once authenticated, the system will allow users to access the network. This is especially useful in situations with large numbers of guests; hotels, airports and restaurants in pay-for-access situations, etc.

However, these systems rely on a session being continuous, either in the form of a minimized web page, a java applet, or relatively constant traffic (no pauses of more than X minutes, or you have to log in again). This model doesn't lend itself well however, to devices which: don't have a web browser, are not on all the time, or don't run minimized applications (like handhelds).

802.1x authentication – This provides the most secure wired or wireless authentication. 802.1x is based on EAP (Extensible Authentication Protocol). You may hear it referred to as RADIUS authentication (a RADIUS server is used in most implementations), EAPOL (EAP on LAN), EAPOW (EAP on Wireless), or by one of the many methods used inside of 802.1x. These are covered later in the document.

802.1x authentication is essentially a framework standard, within which many types of authentication can be used. These include, but are not limited to EAP-MD5, EAP-TLS, EAP-TTLS, EAP-LEAP, EAP-PEAP, Kerberos, etc. Most 802.1x clients implement only a subset of these methods. As such, it's very important to choose methods which support most or all of the clients (devices) you plan on using.

2. Encryption

WEP Encryption – WEP encryption, which is based on the RC4 algorithm, has been found to have significant weaknesses. That said, WEP with Open Authentication (so you get the random session keys) with 40 or 64 bit encryption (these are actually variants of the same 40 bit method) is better than nothing. Likewise, 128 bit WEP is better than 64 bit WEP. Beware however, of 256 bit WEP implementations; most clients don't support this.

TKIP Encryption – TKIP (Temporal Key Integration Protocol) is currently considered secure. TKIP still has RC4 at the core. However, as is implied by the name, the key is periodically changed based on time. There are a number of other changes as well to strengthen both the integrity checking, and the encryption.

AES Encryption - AES (Advanced Encryption Standard) is currently the strongest encryption system implemented for wireless devices. The system is actually a block cipher with 128 bit keys, data blocks, and message integrity check values.

WPA – WPA (Wi-Fi Protected Access) is a subset of the IEEE 802.11i standard. While 802.11i was still being ratified, the Wi-Fi Alliance put together WPA as an interim, hopefully forward compatible, solution. It consists of 802.1x Authentication, and TKIP Encryption.

802.11i (WPA2) – IEEE 802.11i specifies security mechanisms for wireless access. Many vendors refer to it as WPA2. While WEP and WPA both use forms of the RC4 algorithm, 802.11i utilizes a 128 bit AES block cipher with various key lengths. The implementation of AES is required by 802.11i, but the standard does provide for optional backward compatibility with TKIP.

3. Integrity

WEP - WEP provides for minimal integrity checking of messages via an ICV (Integrity Check Value) which is a simple CRC (Cyclic Redundancy Check) value encrypted with the packet. Once the encryption is broken, it is a simple matter to change the data, and calculate a new ICV. The integrity of standard WEP is therefore as weak as the encryption.

TKIP - TKIP provides integrity checking in the form of a MIC (Message Integrity Check) value. This value is computed not only from the data, but also from the source and destination, and a seeded MIC key. This ensures that any change of the data, source, destination, etc. will be detected.

AES – AES provides for message integrity by calculating a MIC value based not on the whole message, but rather based on the encrypted cipher text of the first 128 bits, mathematically combined (XOR'd) with each successive 128 bit block, until the entire message is calculated.

I'm using 802.1x/WPA/WPA2, what EAP type should be used?

802.1x Components

There are 3 main components, or roles, in an 802.1x system.

- Authentication Server – This is typically a RADIUS server. It authenticates clients, and passes out network parameters. These can be used to trigger access controls, specify encryption types, etc. This server may contain a list of users/passwords or certificates, but more often checks these against an existing source such as a Microsoft ADS Server, a Certificate Authority, or other system.

- Authenticator – This is usually the wireless access point. It may prompt the client for authentication, but does no authentication itself. It essentially passes the authentication through to the Authentication Server, and acts upon parameters and responses received back from it.
- Supplicant (Client) – The client software responds to authentication challenges, manages encryption parameters, and handles the identification information for a given session. The client software is often provided by operating system vendors, hardware vendors, network card manufacturers, as well as third party software clients.

In order for an 802.1x deployment to function successfully, the authentication server, access points, and clients must all support the same EAP protocols and encryption methods. There are exceptions to this, which will be discussed later. It is crucial to plan the security, choose protocols, and identify authentication methods for all device types in order to avoid surprises.

EAP Types

EAP-MD5: Uses an MD5 hash of the user's password. It is very weak, and not recommended for use in any wireless environment.

EAP-LEAP: Utilizes mutual server and client authentication. It is sufficiently strong for use in wireless environments where there exist only Cisco Access Points, and where passwords longer than 10 characters are used. It is susceptible to some dictionary attacks. Cisco has moved forward with newer methods, but still supports LEAP due to widespread adoption in many organizations.

EAP-TLS: TLS Uses Server and Client side unique certificates for mutual authentication. This has very widespread support due to the simplicity of implementation for access points and clients. However, building and deploying a complete mutual certificate environment is extremely labor intensive on an ongoing basis (certificates expire and must be renewed, system reloads, new clients, etc). In addition, if configured incorrectly, the entire infrastructure becomes vulnerable and will require complete reissues of certificates to recover. Note: Depending on the clients and methods in use, you may be authenticating machines to the network, NOT the users on the machines.

EAP-TTLS: Tunneled TLS. Developed to ease the burden of certificate infrastructures. A certificate on the server is used to establish a secure tunnel. Within the tunnel, username/password or other authentication methods are used. Usually this is used with PAP or MS-CHAPv2 which allow authentication against an existing Microsoft Windows domain. This may not be suitable where usernames or passwords are stored in LDAP or Novell directories without Microsoft style password hashes.

EAP-PEAP: Developed by Cisco and Microsoft, also to ease the burden of certificate infrastructures. Like EAP-TTLS only a server certificate is required. However, only certain types of authentication can be utilized. At this time, only EAP-MSCHAPv2 and EAP-GTC are supported. EAP-MSCHAPv2 is by far the most widely deployed, by virtue of the clients deployed as part of Microsoft operating systems. EAP-PEAP is supported by most other vendors and systems as well. EAP-PEAP is recommended where ease of configuration and integration is desired, and Windows ADS or Domain systems are already installed.

EAP-FAST: EAP-FAST is similar to LEAP, and was developed by Cisco in response to the weaknesses in the LEAP implementation. It is not widely deployed or supported by other vendors as of this writing.

A review of the supported EAP Types by server and client is provided in **Appendix A**, and an example device survey is provided in **Appendix B** to aid sites in choosing the most appropriate implementations for their environment.

Additional Items/Questions

What if not all the devices support 802.1x/WPA/WPA2?
This is not at all uncommon. Many organizations have significant investments in equipment which cannot be cost effectively replaced all at once. While early 802.1x hardware often failed to consider this, current offerings make allowances. For instance, many of the access points available now (and some older systems with firmware upgrades), allow a site to utilize WPA, and also use WEP, and/or MAC based authentication. In most cases, these access points can also be configured to allow different access based on how a device is connected. For instance, a wireless printer without WPA might be authenticated via WEP, but only allow traffic to and from the device and a print server.

I want to use WPA for the staff, but I don't want usernames and passwords for guests!
I want to use WPA and WEP, but I don't want to maintain multiple networks and access points!
As in the previous case, many access points allow for this. Set up 802.1x access, and WEP with Open Authentication. Create access policies which allow access to only the internet for guests. Authenticated 802.1x users can be allowed to the full hospital network, or only portions of it as well. Legacy devices can be configured with MAC authentication, or, set up access to the full network via VPN for example.

This sounds great, but how do I manage all these policies in all these access points?
This can be very complicated in a mixed environment. Fortunately, many vendors offer software, sometimes as part of their purchase, or downloadable from their site, to manage policies and push them out to multiple devices. There are more powerful packages available as well to manage large networks of diverse devices.

What's the Chicken and Egg Problem?
This is a common pitfall of many 802.1x implementations. Consider the following scenario:

Most managed laptops are joined to a domain.
The Microsoft 802.1x client validates to the network after the user logs on to the domain.
If the user has never logged on to the laptop, there are no cached credentials.
Therefore, a new laptop user cannot log on to the laptop by validating to the domain, because the user has not authenticated to the network. However, the user cannot authenticate to the network, because the user cannot log on to the laptop (domain).

Similar situations can exist on handheld (or other) devices if applications are started before the handheld is authenticated to the network. For example, an update-at-startup mechanism that checks with the network when the handheld is powered on. It is not able to reach an auto-update server, because the network is not available. Once authenticated to the network, the update-at-startup has already run, so the device never gets updated.

There are a variety of ways around problems like this:

- GINA replacements, like those in clients available from Aegis or Odyssey can authenticate the user to the network before attempting the domain logon.
- Workstation accounts can be authenticated to the network, then registry settings will cause the 802.1x client to re-validate as the user following logon. There is sometimes a lag for the re-validation, and policies to be applied. In addition, many RADIUS servers don't posses the capability to accomplish this.

- Set up an un-validated wireless VLAN to allow logon attempts to get to the domain/ADS servers. For this method, you'll also need the workstation to be able to reach DNS servers and/or WINS servers. This decision would need to be assessed to determine if it is an acceptable risk.
- Authenticate managed laptops via certificates or MAC address for purposes of connecting to the domain server, and re-validate after logon as the user.
- Many access points and or clients can be set up to authenticate devices to a certain minimal access list with stored credentials, default access, etc.

Other Wireless Considerations

Wireless Surveys

Ensure that wireless surveys are performed where devices will actually be installed. For example, if surveying with a laptop and signal strength meter, or another laptop held on carts, 3.5-4 ft from ground level, a cinderblock wall is 1ft thick. However, put one laptop on the ceiling where the access point would be installed, and hold the other 3.5-4ft high. Now the cinderblock wall is 2ft thick because of the angle the radio waves travel through the wall.

Obtain equipment to perform access point surveys

Experience has shown that policies and training are insufficient to prevent users from deciding to help themselves. Hospital network administrators are sometimes surprised to find that someone with marginal or no network coverage has purchased a $29.95 access point and plugged it in under the desk. Simply equip a laptop with a survey software (Like NetStumbler, Kismet, or AirSnort), and preferably utilize a wireless adapter with an external antenna port and directional antenna (typically under $100). This will allow personnel to make weekly surveys of the facility for rogue access points, and the directional antenna makes finding it much easier. This same small investment will also allow for fairly accurate wireless signal strength surveys when the external antenna is detached.

Antenna Choices

Some access points come with multiple antenna connectors. Be sure to check with the manufacturer for specifications for their use. While some access points are beginning to appear which have MIMO (multiple-in, multiple-out) technology where both are active, most access points use diversity antennas. Diversity antennas switch between the two, choosing the antenna with the best signal from the client. When there are multiple antennas widely spaced, and multiple users, this can sometimes result in users being left without a signal, while the other antenna is in use.

Appendix A
Server and Client Capabilities Reference

EAP Types by Server

EAP Types	Servers							
	Cisco AP Local RADIUS	**Microsoft IAS**	**Cisco ACS**	**Intermec AES**	**Aegis Server[3]**	**Juniper (Funk[2]) SBR or Odyssey**	**Radiator**	**Freeradius**
EAP-TLS		X	X	X	X	X	X	X
EAP-TTLS				X	X	X	X	X
EAP-PEAP		X	X	X	X	X	X	X
LEAP[1]	X		X		X	X	X	X
EAP-FAST	X		X					

[1] Cisco Aironet access points are required for all LEAP implementations
[2] Funk Software is now part of Juniper Networks
[3] Meetinghouse Data Communications owns the Aegis product line

EAP Types by Client

EAP Types	Clients[3,4]						
	Cisco Aironet Client	**Microsoft**	**Juniper (Funk[2]) Odyssey**	**Intermec Smart System Supplicant**	**Aegis Client[5]**	**Apple OSX**	**Open1X XSupplicant**
EAP-TLS	X	X	X	X	X	X	X
EAP-TTLS			X	X	X	X	X
EAP-PEAP	X	X	X	X	X	X	X
LEAP[1]	X		X	X	X	X	X
EAP-FAST	X		X	X			

[1] Cisco Aironet access points are required for all LEAP implementations
[2] Funk Software is now part of Juniper Networks
[3] Not all clients are supported on all operating systems
[4] Clients may support fewer authentication types on some platforms
[5] Cisco has acquired Meetinghouse Data Communications and the Aegis product line. There is currently no replacement client identified for Palm, PPC, Mac, and Linux operating systems

Clients by Platform

Clients	Platform						
	Windows 2K/XP[1]	**Pocket PC 2002**	**Pocket PC 2003**	**Windows Mobile 5**	**Palm[3]**	**Apple OSX**	**Unix/ Linux**
Cisco	X	X	X	X		X	X
Microsoft	X		X	X			
Odyssey[2]	X	X	X	X			
Intermec[4]	X		X	X	X		X
Aegis[5,6]	X	X	X	X	X	X	X
Apple						X	
Open1x							X

[1] Windows 2000 clients do not include all features of Windows XP clients
[2] Odyssey FIPS Client for WPA2 only supported on Windows 2K/XP
[3] Client support for Palm is often limited to specific models
[4] Intermec Smart System Supplicant is distributed only with Intermec Products
[5] Aegis Meetinghouse 2.1.2 is supplied by Symbol for Symbol Mobile Computers
[6] Cisco has acquired Meetinghouse Data Communications and the Aegis product line

Appendix B

Each site considering security upgrades or new implementations should complete a survey with all desired features, for all devices, prior to deciding on a course of action. Identify specifically what clients are planned for use to meet special needs. An example survey is shown below.

Note: Adding Quantity and Cost columns will allow you to delineate which clients come with devices, and which will have to be purchased. This will aid your budgeting by allowing you to clearly see what your total implementation cost for clients will be.

Note: While several devices are shown as examples in the table below, please refer to *Iatric Systems MobiLab Hardware Specifications* for currently recommended devices.

Device Wireless Capability Survey

	EAP Type				Encryption			Client
Device	**TLS**	**TTLS**	**PEAP**	**LEAP**	**WEP**	**WPA**	**WPA2**	**Type(s)**
Intermec CN2B	X	X	X	X	X	X	X	Intermec
Laptops	X		X		X	X	X	Windows
Laptops	X	X	X	X	X	X	X	Aegis
Palm Tungsten C				X	X			Aegis
Symbol PPT8846	X	X	X	X	X	X	X	Aegis
Symbol MC70	X	X	X	X	X	X	X	Aegis
Zebra QL220 Symbol 802.11b Radio				X	X	X		Zebra
Zebra QL220Plus Zebra or Symbol 802.11b Radio	X	X	X	X	X	X		Zebra
Zebra QL220Plus Zebra 802.11g Radio	X	X	X	X	X	X	X	Zebra

Appendix C
Additional References

Companies and Organizations

Cisco Networks
Intermec Inc.
Juniper Networks
Meetinghouse Data Communications
Microsoft
Symbol Technologies
Freeradius
Open1x
Radiator

References and Whitepapers

802.11i (How we got here and where are we headed)
An Overview of 802.11 Wireless Network Security Standards & Mechanisms
Best Practices: Wireless LAN Security
Choosing the Right EAP Type for Wireless LAN Security
Closing the Loop: Extending Wireless LAN Security to Wireless Printers
Compliance and Mobile Computing
FAQ on Cisco Aironet Wireless Security [Wireless, LAN (WLAN)]
Five Ways to Improve Your Wireless Security [Wireless]
Glossary of Security Terms
Information Security Reading Room
Secure Wireless LANs in Mobile Healthcare
Securing Wireless Technology
Selecting an EAP Method for Your Wireless LAN
Wireless security beyond WEP and WPA.
Wireless Security: the IEEE 802.11i Standard