

Considerations on Implementing A Wireless Network in the Healthcare Environment

**Prepared by the
NCHICA Security Workgroup**

January 2005

Table of Contents

<i>Levels of Security</i> _____	3
Administrative Requirements _____	3
Physical Planning _____	4
<i>Wireless Technology Geographical Coverage</i> _____	4
<i>Access Points</i> _____	5
<i>Wireless Voice over IP</i> _____	6
Technical Considerations _____	6
Technical Considerations (continued) _____	7
Technical Considerations (continued) _____	8
Rogue Network Devices _____	8
<i>Conclusion</i> _____	8
About NCHICA _____	9
Glossary _____	9

Disclaimer

This document is for informational purposes only. Legal, financial or other professional advice may be appropriate or required in addition to competent and qualified technical services. No portion of this document should be construed as legal advice. Contact your attorney for specific guidance on state and federal policies and procedures that best fit your needs and environment.

Introduction

Future improvements to patient care will require smarter use of information technology (IT). IT has been the cornerstone of better information flow between physicians and nurses who make the strategic and tactical patient care decisions and the supporting services which have critical information. Historically, the delivery of information has been limited by the tether of wired networks. This condition has often deprived the primary care team access to the latest patient information. While it has always been possible to retrieve the latest laboratory or radiology results before a visit to each bedside, the logistical constraints of the rounding physician, normally preclude a trip to the local workstation before a visit to each new patient. The reality of the situation is that the information in printed charts drive the decisions.

For many hospitals, wireless systems offer an affordable solution to the stale information problem by providing the means to deliver the most current information to the care team at the bedside. Wireless systems also provide the ability for coordinated data sharing without requiring cables and wires. Wireless systems can also provide the technological foundation to record patient information real-time at the point of care, present vital information upon demand, and ultimately improve the patient's healthcare experience.

The introduction of wireless systems does not come without risks. With wired networks, hospitals can control the information paths, and thus offer a layer of physical security to sensitive information. A strong benefit of wireless systems is the mobility, but this can result in loss of physical security. Hackers have an easier chance of detecting and capturing sensitive information without detection in a wireless environment. This creates additional security challenges and requires effective safeguards to protect patient information.

Levels of Security

From a HIPAA compliance perspective, different levels of security can effectively be used. In addition to the administrative, physical and technical safeguards, technical mechanisms exist at the application level or within the software functionality users should also consider:

- Device level – security via a password or code controlled by the device's software
- Session level – security via the communication protocols used within a network, i.e., encryption or proprietary protocols
- Transport level – security via and within the technology's medium, i.e., CDMA vs. 802.11 vs. cable vs. wire line

Most device manufacturers include security measures for their devices. This paper discusses the administrative, physical and technical considerations for wireless networks including the necessary safeguards to address HIPAA security standards. Technical security mechanism levels are also addressed so the benefits specifically related to 802.11 wireless networks can be leveraged.

Administrative Requirements

Wireless networks offer covered entities the ability to deploy core computing power to areas normally reserved to standalone devices. It also allows for the movement of these assets and opens the door to a paperless workflow. Unfortunately, wireless also opens the door to risks that if managed improperly, may result in a breach of sensitive information or provide an avenue for attack. Wireless networks have inherent weaknesses that require multiple layers of safeguards to reduce the risk of unauthorized access, interception, or compromise of data.

To reduce these risks, any wireless network should be considered an untrusted extension of your internal network, or treated as a network completely external to the traditional wired network. Organizational policies governing the access to wireless networks should mirror those security policies already in place to govern remote access, including:

- Policies defining classes of users and/or systems that are authorized to use the wireless network,
- Policies limiting the types and locations of data access,
- Policies defining the authentication methods,
- Policies to ensure only authorized personnel can reset access points and avoid the use of default settings,
- Policies to disable access points during non-usage periods when possible,
- Policies to assign strong passwords and establish periodic change intervals,
- Policies to continuously evaluate and monitor for conformance to security procedures,
- And finally, policies defining an exception process for classes of users or systems who may have an authorized requirement to use the network but do not have authorization to access the covered entity’s information, e.g., patients and visitors who may be within your facility and desire to have outside access.

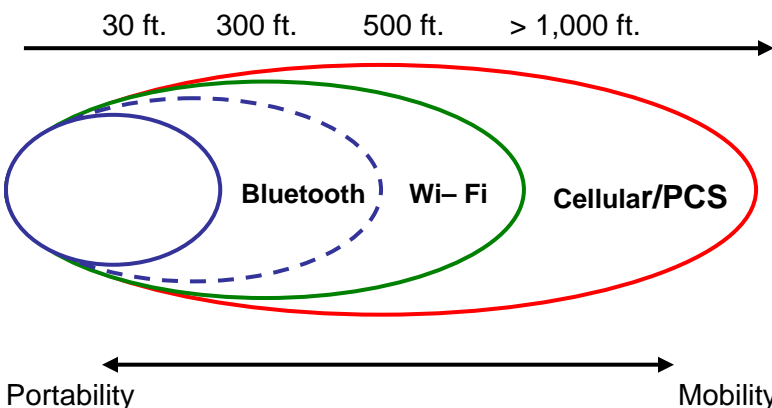
Prior to implementing a wireless network, it is recommended to create and/or amend administrative policies and procedures to deploy, manage and maintain the wireless environment.

Physical Planning

There are two modes of wireless technologies: mobile and portable. Mobile wireless technologies are transient, with a wide signal coverage range such as those used by cellular and personal communications systems (PCS). This technology employs cell-like infrastructure that allows the end user to move about from cell to cell within an expanded metropolitan area with an in-progress application.

Security concerns within mobile wireless technologies are different from those in the portable wireless technologies mode. Portable wireless technologies are somewhat stationary hotspots such as Wi-Fi (802.11) and Bluetooth. These allow in-progress application continuity within a smaller wireless local area network (WLAN). The geographical wireless graphic and table below, identify the distance and frequency ranges to assist you to evaluate the appropriate wireless technology to support your requirements..

Wireless Technology Geographical Coverage



Technology	Cellular	PCS	Wi-Fi	Bluetooth
Frequency	800 Mhz	1.8 Ghz	2.4 Ghz	2.4 Ghz
			5Ghz	

This paper will focus only on the Wi-Fi aspect and security consideration for a wireless network in the healthcare environment. Wireless networks provide their connectivity through the use of radio signals much like those used by cordless telephones. Walls, fluorescent lights, electrical power distribution, medical devices, and other items common to buildings can interfere with the radio signal of the wireless network. These same radio signals can also broadcast further or in a different direction than expected. A poorly planned wireless network may provide coverage to an entire parking lot while failing to completely cover the office area.

Antenna type (unidirectional, bidirectional, and omni-directional), placement and signal strength will determine where the radio signal travels and the quality of the signal. In a campus environment, where more than one antenna might cover an area, it is recommended that careful consideration be taken selecting different varieties of antennas in order to reduce the chance of signal reflection (a common nuisance when several radios are in close proximity). All antennas in publicly accessible locations should be secured to prevent tampering, allowing a signal traveling to undesired location. A wireless survey should be completed to determine the topology of the wireless network to correct any coverage issues. These surveys should be done periodically (because of environmental changes can affect radio signals) as well as immediately after moving equipment or structural changes are completed near an antenna.

Access Points

A critical success factor when deploying a wireless network is to properly install and define all access points. When choosing the locations for wireless access points:

- Choose locations closer to the center of the building rather than locations near the building's exterior walls.
- Consider that each access point may provide coverage to an area that extends in all directions. If you place your access points on a building plan you can draw a circle around that access point to illustrate the area possibly covered; with the most common wireless protocol (802.11b) this circle should be at least 300 feet in diameter.
- Plan the coverage area in 3 dimensions. The circle drawn to illustrate the coverage area should also extend up and down to the other floors in the building. Depending on the construction of the building this area may also vary, but anticipate the radio signal extending at least two floors up and two floors down.
- Consider using a wireless discovery tool, such as the free tool Network Stumbler. A site survey will provide a clear understanding of the radio coverage from the wireless access points. The radio coverage may not be uniform and may not end where anticipated. The objective is to reduce the propagation of radio waves outside your facility.
- If installing multiple access points, the site survey will also help to limit any radio interference between the access points. Each access point has different radio frequencies (or channels) on which it can be configured to broadcast. With the most common wireless protocol (802.11b) there are three radio channels available: 1, 6, and 11. The strength and quality of the radio signal will diminish in locations further from the access point; often access points are installed to provide overlapping coverage to the areas between two installations. In the case of overlapping coverage, different radio channels should be used on each overlapping access point.
- Most 802.11b access points default to channel 6. If there are other offices in the building providing wireless access, then changing the channel may improve performance. Use of a wireless discovery tool may show other access points and the channels in use.
- Consider that, much like other electronic equipment, wireless access points are vulnerable to theft and vandalism. Environmental conditions, such as rain and lightning, can damage access points. Commercial enclosures are available to protect wireless access points from theft or other environmental challenges.

Wireless Voice over IP

Wireless Voice over Internet Protocol (VoIP) phones allow small businesses, corporate and university campuses to use their existing 802.11b (as well as 802.11a or 802.11g) wireless networks and provide virtual cell phone coverage while in range of their wireless network(s). These solutions can greatly reduce the costs of communication when the use of such devices are required within a predetermined area. In order to provide nominal quality for this type of communication the Access Points must support a separate VLAN for voice and data by applying Quality of Service (QoS). The following are minimum recommended QoS parameters to look for in an Access Point to provide nominal phone quality for these solutions (all parameters measuring a delay, the shorter the delay, the better the service):

- Connection Establishment Delay - the amount of time elapsing between a request being sent and the confirmation being received.
- Connection Establishment Failure Probability - the chance of a connection not being established within the maximum establishment delay time - due to network congestion, or other internal problems.
- Throughput Parameters - measures the number of bytes of user data transferred per second, measured over some time interval.
- Transit delay - measures the time between a message being sent by the source and its being received at the destination.
- Residual Error Ratio - measures the number of corrupted messages as a fraction of the total sent.
- Protection - provides a way to specify the transport layer to provide protection against unauthorized third parties reading or modifying the transmitted data.
- Priority - provides a way to indicate that some of its connections are more important than other ones (Voice would be a higher priority than say Data). In the event of congestion the high-priority connections get serviced before the low-priority ones.
- Resilience - gives the probability of spontaneously terminating a connection due to internal problems or congestion.

Technical Considerations

The wireless network and any data transmitted over the wireless network, employ radio signals and broadcasts. These radio signals extend in all directions and can be intercepted without any indication to the network or the end user that this interception is taking place. The possibilities for signal interception, and ease with which an unidentified user with commonly available equipment can access the wireless network, dictate that additional safeguards are necessary to protect any data transmitted and to prevent unauthorized access or use of the wireless network.

- Almost all wireless networks must be considered an untrusted point of entry into the regular network. Access points should be separated from the wired network through the use of VLANs or additional network infrastructure such as firewalls or WLAN Gateways with built-in firewalls (e.g., Bluesocket). Connecting the wireless network through a logically or physically separate firewall, DMZ, or gateway device will provide a means of separation.
- Given that the wireless network is considered an untrusted point of entry, similar to the Internet, it is strongly recommended that a Virtual Private Network (VPN) concentrator be located between the wireless and wired networks or at the point where the wireless network enters the regular network. This will provide several benefits:
 - Serve as a network gateway to separate the wireless network.
 - Authentication from the wireless clients.
 - Provide strong, high performance encryption for the wireless data transmissions.

Copyright (c) 2005 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/> and which is available from NCHICA upon request.

Technical Considerations (continued)

- Consider implementation of personal firewalls and disable file sharing for all folders in Microsoft Windows® operating systems so that user devices associated with an access point on the same wireless network cannot be easily accessed by a hacker.
- Consider deploying access controllers such as ReefEdge, Bluesocket or Nomadix. These devices offer tough access control to the network while interfacing with authentication servers.
- Clients permitted to communicate on the wireless network should be known and registered unless they are guest clients. Utilize static IP addresses for clients and access points. Network addresses or DHCP leases for access should only be provided to recognized clients. DHCP services should not be configured on the individual access points. Using a central DHCP server to provide leases to wireless clients will allow ease of management and accountability. (Note: If a firewall or gateway device is used to separate the wireless and wired networks, centralized DHCP may not work as anticipated.)
- Wireless access points broadcast a radio message known as the Station Set Identifier or SSID. The SSID is the message new clients look for when searching for a network to join. Wireless access points come with a default SSID configured by the manufacturer. The use of default SSIDs and the discovery of SSID broadcasts are two things that increase the exposure of the network to attack. If the wireless network is not intended for full or partial public use, both of the following are strongly recommended:
 - Changing the SSID to something other than the factory default.
 - Configuring the access points to not broadcast the SSID announcements.
 - Ensure access point firmware is up-to-date. Vendors often implement patches that fix security issues. Upgrade the firmware for the access point prior to deployment and regularly check that all devices have the most recent firmware release updates.
- Wired Equivalency Protocol (WEP) using static keys was the means of data encryption provided through the original wireless specifications. WEP uses unchanging encryption keys to encrypt data. These keys are a shared secret between the access points and the clients connected to the wireless network. The weaknesses of the shared secret model and additional weaknesses discovered in the encryption algorithm have resulted in WEP being judged an ineffective means of data protection. Use of WEP on a wireless network will discourage the casual attacker, but WEP can also introduce performance degradation and can be difficult to configure and support on many clients. While WEP will provide limited security benefits, it should never be considered a complete means of protection for wireless transmissions.
- Wireless encryption methods beyond WEP have been developed, such as Wi-Fi Protected Access (WPA) that is partially based on the new 802.11i standards. Individual vendors have also provided proprietary methods, such as Cisco's LEAP, to protect wireless networks. Many of these vendors' proprietary methods will not interoperate with all wireless clients and many of these proprietary methods been shown to have significant weaknesses. At the time of this writing, wireless equipment providing WPA is new to the marketplace; the performance and quality of protection provided is still uncertain. These new standards, such as AES, do offer strong encryption, however, your results may vary.
- To install and configure WPA correctly, vendors suggest using it in combination with 802.1x authentication. The benefit of this approach is that a per-session WPA key is generated which makes breaking the encryption extremely difficult. A Radius server that supports PEAP/MSCHAPv2 authentication must be installed to take authentication requests from the access point and forward them to the internal authentication server. However, this is not as easy as it sounds and introduces a single point of failure into the authentication scheme.
- Performance and data throughput of the wireless network will be slower than the speeds experienced on most modern wired switched networks. Virus-infected clients or clients using high traffic programs such as music file sharing programs can have a dramatic impact on the performance of the wireless network. Mandating current virus protection and eliminating the use of programs not required for business

Technical Considerations (continued)

- operations will improve the performance of the wireless network. Many VPN concentrators and other gateway devices can be configured to check for the presence of virus protection.
- Depending on the physical location of the access points and the construction of the building involved, the wireless radio signal may spill over to areas that should not be covered, such as parking lots, while in other areas the radio signal may not be as strong as desired. To control this radio signal there are after market antennas available from several manufacturers. These include panel antennas that can be used to direct the radio signal largely in a single direction from the access points, as opposed to the factory stock antennas that are normally omni-directional (sending the radio signal in all directions.)
- Finally, wireless access points are intelligent devices that are managed remotely. Since many of the features of these devices are security-related, it is not desirable to allow management from another wireless device. System administrators should configure each wireless access point so that all administration must occur through the wired side, thus preventing administration from the wireless side. Additionally, all management features should be password protected with something other than the factory default. These added level of technical protections ensure that the configuration of the wireless network cannot be compromised by an unauthorized wireless user.

Rogue Network Devices

The introduction of a wireless network requires advance planning. Some impatient users deploy rogue wireless devices unbeknownst to the IT staff. With the price of many Wireless Access Points, or WAPs, rapidly approaching the cost of a good dinner, these devices will find their way into even the smallest of organizations. There is a very high risk that these devices will be deployed with only the standard security or with no security at all.

It is also possible that vendors hired by the covered entity may deploy devices without the same level of security or with the vendor's own security configuration. Since wireless network deployments may support non-IT systems, organizations should have a strong risk management process in place to ensure that vendors and other covered entities operating within your facility do not create security risks.

As a wireless network infrastructure grows, so does the importance of using technology that will detect and shut down rogue access points. One possible method to control the installation of rogue access points is through the use of a feature such as Bridge Protocol Data Unit (BPDU) guard on your wired network. Most wireless access points act as "Bridge Devices", so using the available technology on a wired network (to which any wireless access points must be connected) may allow for the automatic shutdown of these devices. The vendor of your wired switches can help you to determine how to implement this feature.

This is also an area that should be covered by the security policy of the organization. People need to understand the ramifications of installing these devices without the knowledge and support of the IT staff. It is a good practice to maintain a list of authorized radio NIC and access point MAC addresses so your organization has a basis for identifying rogue access points.

Conclusion

Wireless network technology is evolving and adoption can provide benefits that enhance the access, delivery, and exchange of valuable information. Wireless adoption requires security considerations to protect sensitive information and avoid compromise of those resources. While there is widespread discussion of 'wireless insecurity', a multi-layered approach including implementation of effective administrative, physical and technical safeguards can mitigate wireless network risks. As wireless network technology matures and adoption increases, security protection will become better managed.

Contributing Authors

- Douglas Brown, GSEC, CISSP – University of North Carolina at Chapel Hill
- Clyde Hewitt, MS – CTG Information Security Solutions
- Lisa Olson – SEC Associates
- Michele Reynolds, CHP – Epic rd Consulting, LLC
- Tory Russo, CHP, CHSS, President, ComXperts, Inc.
- David Sinnott – Prosecure
- Steve Skibinski – Intel
- Andre Smith - North Carolina Department of Health & Human Services (DHHS)

About NCHICA

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is a nonprofit consortium of over 250 organizations dedicated to improving healthcare by accelerating the adoption of information technology. This white paper was produced by members of the NCHICA Security Workgroup that meets regularly on the third Thursday of each month. Information about NCHICA, its mission and members can be found at <http://www.nchica.org>.

Glossary

[Wireless] Access Points (AP) - a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. AP's are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.

(Source: <http://www.webopedia.com/TERM/A/AP.html>)

CDMA (Code-Division Multiple Access) – A general type of digital cellular technology and often associated with the IS-95 implementation for mobile telephones. CDMA is a "spread spectrum" technology which means that it spreads the information contained in a particular signal of interest over a much greater bandwidth than the original signal. CDMA has no hard limit for the number of users who may share one base station (tower). Instead, with CDMA, additional users can connect until the base station determines that (call) quality would suffer beyond a set limit.

(Source: <http://www.phonescoop.com/glossary/term.php?gid=8>)

Demilitarized Zone (DMZ) - A part of the network that is neither part of the internal network nor directly part of the Internet - basically a network sitting between two networks.

(Source: <http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html>)

DHCP (Dynamic Host Configuration Protocol) Lease - A communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

(Source: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213894,00.html)

Glossary – continued

Firewall - A set of related programs located at a network gateway server that protect the resources of a private network from users of other networks. Basically, a firewall working closely with a router program filters all network packets to determine whether to forward them toward their destination. A firewall is often installed away from the rest of the network so that no incoming request can get directly at private network resources. There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain names and IP addresses. For mobile users, firewalls allow remote access into the private network by the use of secure logon procedures and authentication certificates. (Source: <http://www.stallion.com/html/support/glossary.html>)

Firmware - Software that is embedded in a hardware device that allows reading and executing the software but does not allow modification, e.g., writing or deleting data by an end user. Note 1: An example of firmware is a computer program in a read-only memory (ROM) integrated circuit chip. A hardware configuration is usually used to represent the software. Note 2: Another example of firmware is a program embedded in an erasable programmable read-only memory (EPROM) chip, which program may be modified by special external hardware, but not by an application program. (Source: <http://www.bandwidthmarket.com/resources/glossary/F3.html>)

PEAP (Protected Extensible Authentication Protocol) - A protocol developed jointly by Microsoft, RSA Security and Cisco for transmitting authentication data including passwords over 802.11 wireless networks. EAP authenticates wireless LAN clients using only server-side digital certificates by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange. (Source: <http://wi-fiplanet.webopedia.com/TERM/P/PEAP.html>)

QoS (Quality of Service) Throughput Level. One of the biggest advantages of ATM over competing technologies such as Frame Relay and Fast Ethernet, is that it supports QoS levels. This allows ATM providers to guarantee to their customers that end-to-end latency will not exceed a specified level. This is necessary to guarantee the quality needed for a Voice over IP (VoIP) call. (Source: <http://wi-fiplanet.webopedia.com/TERM/q/QoS.html>)

SSID (Service Set Identifier) - A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the Basic Service Set (a set of wireless stations). The SSID differentiates one WLAN from another so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. (Source: <http://isp.webopedia.com/TERM/S/SSID.html>)

VLAN (Virtual Local Area Network) - a logical, not physical, group of devices, defined by software. VLANs allow network administrators to re-segment their networks without physically rearranging the devices or network connections. (Source: <http://www.puredata.com/manual/backboneswiches/appendix/glossary.html>)

VPN (Virtual Private Network) - A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. (Source: <http://isp.webopedia.com/TERM/V/VPN.html>)

Copyright (c) 2005 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/> and which is available from NCHICA upon request.

Glossary – continued

WEP (Wired Equivalent Privacy) - A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physical nature of their structure, having some or all parts of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

(Source: <http://wi-fiplanet.webopedia.com/TERM/W/WEP.html>)

Wireless Application Protocol (WAP) - A secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smartphones and communicators. WAP supports most wireless networks, all operating systems and ones particularly engineered for handheld devices. Because WAP is fairly new, it is not a formal standard yet.

(Source: <http://www.webopedia.com/TERM/W/WAP.html>)

Workflow is an IT technology that uses electronic systems to manage and monitor business processes. It allows the flow of work between individuals and/or departments to be defined and tracked.

(Source: <http://www.documentmanagement.org.uk/>)

WPA (Wi-Fi Protected Access) - a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP (i.e., as a software upgrade to existing hardware), the technology includes two improvements over WEP: 1) Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a ehashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. 2) User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network. *It should be noted that WPA is an interim standard that will be replaced with the IEEE's 802.11i standard – the full IEEE 802.11i standard is commonly known as WPA2.*

(Source: <http://wi-fiplanet.webopedia.com/TERM/W/WPA.html>)