



Wireless Security

Uday Ali Pabrai, CISSP, CHSS

The security of defending today's health care information infrastructure is largely based on protocols and technologies that support a wired infrastructure. The proliferation of mobile devices and wireless communication is introducing new security gaps that must be addressed. As the saying goes, security is only as good as your weakest link, and wireless systems are the weak links in the health care information infrastructure. Security practitioners need to better understand wireless technologies, protocols and standards and develop a policy to address wireless security to ensure that these technologies are not the "gaps" exploited by hackers.

Acronyms

SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
WAP	Wireless Application Protocol
WEP	Wired Equivalent Protocol
Wi-Fi	Wireless Fidelity
WML	Wireless Markup Language
WPA	Wi-Fi Protected Access

Wireless Network Standards

The IEEE has defined 802.11 standards for wireless networks. These wireless networks are basically Ethernet networks without cables. The following is a summary of the IEEE 802 wireless standards:

- 802.1x: Framework for stronger authentication for 802.11 WLANs.
- 802.11a: Physical layer standard in the 5 GHz radio band. Maximum link rate is 54 Mbps per channel.

- 802.11b: Physical layer standard in the 2.4 GHz radio band. Maximum link rate is 11 Mbps per channel.
- 802.11d: Supplementary to MAC layer in 802.11. Supports use of 802.11 WLANs.
- 802.11e: Provides QOS and multi-media capability
- 802.11f: Defines the registration of access points within a network and exchange of information between access points when a user is handed over from one access point to another.
- 802.11g: Physical layer standard for WLANs in the 2.4 GHz and 5 GHz radio band. Maximum link rate is 54 Mbps per channel.
- 802.11h: Supplementary to MAC layer to comply with EU regulations for 5 GHz WLANs.
- 802.11i: Supplementary to MAC layer to improve security. Alternative to WEP with new encryption methods and authentication procedures.
- 802.16a: Extends the range of 802.11 to several miles. Provides enhanced security and supports high quality phone calls.
- 802.20: Extends the range of 802.11 to several miles and is being designed to support high-speed links in cars and trains traveling at speeds exceeding 120 miles per hour.

Glossary

Access Point: An interface between the wireless network and a wired network.

Bluetooth: Considered a wireless Personal Area Network (PAN). A standard for 1 Mbps data rates in the 2.4GHz frequency band at relatively short distances.

Service Set Identifier (SSID): A configurable identification that allows wireless clients to communicate with the appropriate access point.

Wired Equivalent Privacy (WEP): A wireless standard for encrypting data in transmission. The standard supports 40-bit and 128-bit keys for encryption.

Wireless Fidelity (Wi-Fi): A standard for interoperability sponsored by the Wireless Ethernet Compatibility Alliance (WECA). The "Wi-Fi" brand signifies compatibility with other Wi-Fi products.

Wi-Fi Protected Access (WPA): Is a security standard to address known deficiencies in WEP. It combines 802.1x authentication with a stronger encryption element from the 802.11i draft called Temporal Key Integrity Protocol (TKIP).

Wireless Network Components

IEEE 802.11 wireless LANs include the following components:

- Wireless Network Interface Card: May be PC, USB or PCI cards that interfaces between the client computer and the communications medium. It converts digital data to and from radio waves.
- Client System: May be a laptop, PDA or a desktop system.
- Communications Medium: Consists of radio waves in the 2.4 GHz or 5 GHz radio frequency band. The frequency band is broken up into channels.
- Access Point: Is a hardware device that provides several channels to connect client systems to the wired LAN.

The components may be connected in one of two types of operating modes. The IEEE 802.11 standard defines two specific operating modes:

- Ad-Hoc
- Infrastructure

In the Ad-Hoc mode, two or more client systems create a peer-to-peer network with each other's wireless NICs through a mesh network. This network is typically formed on a temporary basis.

In the Infrastructure mode, client systems connect to an access point. The access point is connected to the wired network. Client systems communicate with each other through the access point.

Before a client system can connect to an access point, the system must provide a Service Set Identifier (SSID). The SSID is an alphanumeric code that is configured on both the wireless NIC and the access point. SSIDs identify wireless networks.

Wireless Security Challenges

Lack of user authentication, weak encryption, and poor network address management are some examples of security challenges of wireless networks. For example, an access point can authenticate hardware based on MAC or IP addresses and not require user authentication. Further, while the Wired Equivalent Protocol (WEP) may be used to encrypt wireless transmission, the encryption is weak and not difficult for hackers to break. Hackers can also monitor transmissions to determine SSIDs – these are not encrypted. SSIDs provide information on the name and availability of a wireless network.

Wireless networks are also vulnerable to attacks such as:

- Man-in-the-middle attack
- Rogue access points
- Session hijacking
- Denial of Service

In a wireless infrastructure it is the access point that authenticates the client and authorizes the connection. The client does not authenticate the access point. It is thus possible for an attacker to set up a rogue access point with the same SSID and a stronger signal – this rogue access point then “traps” all information from the client to the authorized access point. It essentially is an example of a “man-in-the-middle” attack. The client does not know that the communication is being received by the rogue access point.

Another example of an attack is session hijacking. Here the attacker sends a “dissociation” message to the client and thus drops the client from the connection to the access point. The attacker then spoofs the access point with identification information of the client and continues the communication.

In a denial of service attack, the attacker emulates the access point and continuously sends de-authentication and disassociation messages to the client systems. The clients are unable to connect to the access point and are not able to establish a connection. The attacker can also jam radio signals by generating enough radio noise in the frequency range used. This again prevents clients and access points from communicating.

Wireless Security Protocols

Several standards and protocols have been defined to better secure wireless networks. These include:

- Wired Equivalent Privacy (WEP)
- IEEE 802.1x User Authentication
- Extensible Authentication Protocol (EAP)
- Lightweight Extensible Authentication Protocol (LEAP)
- Wi-Fi Protected Access (WPA)

Let us take a closer look at each of these wireless security-related specifications.

Wired Equivalent Privacy (WEP)

This is the standard 802.11 wireless security protocol for data encryption. It uses a key to encrypt wireless data transmitted through the radio waves. It supports a 40-bit key and a 128-bit key. Attackers have been able to compromise both WEP key lengths.

IEEE 802.1x User Authentication

802.1x is an IEEE standard that works with WEP to provide the framework for strong authentication. The IEEE 802.1x consists of three components:

1. **Supplicant:** This is the client system trying to access the wireless network
2. **Authenticator:** This provides the physical port to the network, such as an access point or a switch
3. **Authentication Server:** This verifies user credentials and provides key management – may be a RADIUS server, LDAP directory, Windows NT Domain or an Active Directory

Extensible Authentication Protocol (EAP)

This is an authentication protocol used by 802.1x components to allow users to authenticate to a central server. Once the server authenticates the client, keys are sent to both the authenticator – the access point and the supplicant – the client.

Lightweight Extensible Authentication Protocol (LEAP)

This was developed by Cisco and is also referred to as the Cisco Wireless EAP.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is the emerging standard in wireless security to address the weaknesses in the WEP algorithms. WPA addresses two areas of security: authentication and encryption. It combines the 802.1x authentication with a stronger encryption. The encryption is based on the IEEE 802.11i draft, referred to as the Temporal Key Integrity Protocol (TKIP). Note that the 802.11i draft also includes the specification, Counter Mode with CBC-MAC Protocol (CCMP). CCMP uses the Advanced Encryption Standard (AES) – thus, providing very strong encryption capability.

Getting Started: Wireless Security Policy

Security practitioners should get started by first developing a policy for securing wireless devices and transmissions. The scope of this policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the organization's networks. This includes any form of wireless communication device capable of transmitting packet data.

This policy should include specific recommendations such as:

- Wireless implementations must maintain point to point hardware encryption of at least 128 bits
- Wireless devices must maintain a hardware address that can be registered and tracked, i.e., a MAC address
- Wireless devices must support strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar
- Laptop/PDA users can select strong passwords and must have anti-virus software installed with automatic updates
- Screen savers must be activated if 2 -3 minutes of idle time
- Encryption must be used to store sensitive information on laptops

Designing a Wireless Infrastructure

The core objective in the design of the wireless network must be to minimize the number of access points, as each of these represents a potential point of vulnerability. Further, the access points should be installed away from exterior walls so that the strength of the signal is reduced for access from outside of the physical facility. The access point should not be installed on the same network as other network resources. The key here is to

understand the risk to the infrastructure if the access point is compromised. It should typically be separated from the wired network and the design should require communication to go through a firewall system.

Summary

Sensitive and confidential information transmitted over wireless networks are typically not encrypted and lack proper authentication. A vulnerable wireless infrastructure is a significant risk to business. It exposes the health care organization's sensitive information such as electronic Protected Health Information (ePHI) to liabilities that may be legal, HIPAA compliance violations, or others. Security practitioners must understand wireless technologies and standards and create a security policy that addresses risks associated with a wireless infrastructure. The deployment of wireless technology components must follow policy requirements to ensure consistency and security. The critical elements of user authentication as well as encryption must be addressed to secure confidential business information.

The design of the perimeter must be reviewed to address wireless entry and exit points between internal and external (Internet) networks. End users should be better educated on wireless policies so that they use their mobile devices securely to access the network. The bottom line, do not make your wireless infrastructure the weak link in your environment.

Author Bio

Uday O. Ali Pabrai is a highly sought after InfoSec and regulatory compliance expert. Based on his hands-on consulting experiences, he developed a unique security methodology, BizShield™: *The Seven Steps to Enterprise Security*. BizShield™ today provides the framework for many security initiatives. Mr. Pabrai is the author of the forthcoming book, *The Art of Information Security* - a strategic blueprint document for security practitioners. He has also developed specialized InfoSec security policy templates that can easily be tailored to address enterprise requirements.



Mr. Pabrai was the creator of the first program on Internet skills certification, CIW. CIW is today one of the leading vendor neutral certification programs in the world. Mr. Pabrai also established the first and highly respected healthcare transactions, privacy, and security certification program, Certified HIPAA Professional™ (CHP) and Certified HIPAA Security Specialist™ (CHSS). The CHP and CHSS programs have been attended by several agencies of the United States Armed Forces, state and county governments, hospitals, insurance companies and IT as well as legal professionals.

Mr. Pabrai's clients have included Blue Cross Blue Shield Affiliates, State of Illinois, Iowa, Oregon, Microsoft, U.S. Defense Intelligence Agency, U.S. Naval Surface Warfare Center, HCR ManorCare, VitalWorks, Florida Department of Law Enforcement, Kemin Industries, Marsh and many others.

His hands-on, field accomplishments include leading a team of ten instructors to deliver customized regulatory compliance training to over 10,000 employees at the State of Oregon DHS. He was the lead architect for several risk analysis and vulnerability assessment (penetration testing) engagements across the United States.

Mr. Pabrai has delivered keynote and other sessions at numerous conferences worldwide including the ISSA Conference, HIPAA Summit, National Council for Prescription Drug Programs (NCPDP) National HIPAA conference, VitalWorks, COMDEX, COMNET, Internet World and DCI's Internet Expo.

Mr. Pabrai is the author of several leading industry texts that are all available at the ecfirst.com e-store. He has published extensively on the subjects of enterprise security and regulatory compliance including articles in PharmaVoice, Certification, Business Advisor, InetCE and several others.