Global Information Assurance Certification Paper

Daniel O'Dorisio

Securing Wireless Networks for HIPAA Compliance
GIAC GSEC Practical Assignment
Version 1.4 Option 2 (Case Study)
Submitted 12/23/2003

Abstract

The intent of this paper is to discuss wireless networks and why it is useful to organizations, namely healthcare organizations. Once we have established the foundation for why we need wireless, we will cover the vulnerabilities and problems with wireless networks. We will then take a tour of recent laws that govern healthcare organizations, and how these laws affect wireless networks. After this overview a more thorough interpretation of the laws will be presented with details on what each part means in relation to wireless.

Our next step, will be to take a network and work through any current problems. We will then apply different technologies and configuration changes to that network in order to provide security that will meet the requirements set forth previously. We will then examine briefly a snapshot of the network after our security implementation. Finally we will sum up the paper with a conclusion of what we have found through this case study.

Why Wireless Is Important

Wireless is one of the latest advancements in technology, the expansion of which has enabled users to become disconnected and connected at the same time. We are now able to access information almost anywhere over wireless frequency ranges, which in a healthcare environment is a great advantage. Providers can use hand-held devices in the course of making rounds in a hospital, or performing office visits. This provides a great deal of data to the physician right at his or her fingertips so they can more accurately and efficiently make decisions on the treatment of a given patient. No longer does a provider have to carry charts or have staff search for documents for a patient, they are all available immediately thanks to the use of wireless networks. There are many software developers utilizing this technology to develop solutions to provide physicians with the type of mobility and power to access data as mentioned earlier[1].

The benefits of wireless—like most other technologies—come with their share of downfalls in security. Wireless as the name implies uses air rather then wires at the physical layer. This opens the network up for the world to see much easier. An attacker can just be in range of the access point (AP) and obtain access to the network. In the following sections we will discuss the technical issues that are related to wireless networks.

Wireless Technical Issues

Since wireless networks use radio frequencies to communicate, any device that is 802.11x compliant will be able to receive these transmissions. It's a

great challenge to protect the data that is passed through the frequencies used by 802.11x. This challenge is actually tougher then it is to protect traditional wired networks from sniffing. There are methods of installing aluminum in the walls of buildings to keep the radio waves from penetrating to the outside world[2]. However, this is quite costly and requires major renovations to the physical structure. In an effort to address these issues, included in the 802.11x protocol suite is Wired Equivalent Privacy (WEP). There have been many flaws discovered in the protocol such as the improper implementation of cryptographic methods[3]. No longer should WEP be considered a secure protocol, especially so in a healthcare environment where we are dealing with Protected Health Information (PHI). Media Access Control (MAC) filtering is another method built into 802.11x devices; it works by blocking any traffic that is not originating from a wireless network card that has a trusted MAC address. This attempt at securing who can gain access to the wireless network can also be thwarted rather easily. Since MAC addresses can be spoofed, an attacker can discover one that is allowed by the AP's and gain access by changing the MAC address on their system[4].

Wired networks are harder to sniff since all the transmissions are over a wire, and would require a physical wiretap. IP Security (IPsec) has been designed well for wired networks since it encrypts the original IP header so that less information can be gathered. The only information that is publicly viewable is MAC addresses, which are not of great value on a wired network since MAC addresses are only of value on the segment in which they are located. That layer (Logical Link) of the Open Systems Interconnect (OSI) Protocol stack is not routable. Applying IPsec Virtual Private Networks (VPN's) to wireless networks is the best option available right now for encryption. The problems with it are none of Layer 2 traffic is encrypted by IPSec. This leaves all MAC addresses and Service Set ID's (SSID's) un-encrypted. This in turn allows an attacker to gather more information about the network. Gathering information is the first thing that attackers do when they begin an attack. Regardless of what is done, auditing is a must! In the words of Eric Cole, "intrusion is a given, detection is a must." We must have auditing measures in place so we can detect what happens. A good practice is to ask this question "if an attacker broke in and modified a piece of data, would we have the intelligence to know what was changed."

Brief Overview of HIPAA:

Technological advances have enabled healthcare providers and insurance agencies to more effectively and efficiently communicate PHI, and provide for the patients care. Being stored on electronic media, and transmitted over wire and eventually through the air, the communication and storage of PHI could no longer be considered secure. Until the Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996 [5], no governing standards were in place for insuring the safety of PHI. Healthcare institutions were left to secure transmissions and storage on their own. The public began demanding that security measures be put in place to maintain their privacy.

August 12, 1998, a proposed rule for HIPAA was published. After all the details had been worked out, HIPAA finalized on February 20, 2003[6]. These regulations went into effect April 21, 2003. The rule states that institutions have until April 21, 2005 to be compliant, one exception being that small health institutions are provided with one more year to become compliant[6].

HIPAA Standards

While the Final HIPAA rules do not necessarily deal directly with wireless, the regulations cover many separate areas that deal with PHI. In summary the document deals with 3 major areas:

1. Administrative Safeguards
2. Physical Safeguards
3. Technical Safeguards.

The Administrative Safeguards section (164.308) provides regulation for the management of healthcare organizations. Secondly, Physical safeguards (section 164.310) regulate how physically secure the facility should be. Finally Technical Safeguards (section 164.312) provide regulations for access control to the network, security and integrity of data/transmissions, auditing and authentication. This section is most relevant to our situation.

In order to provide the highest security to a wireless network, the relevant regulations need to be extracted from the HIPAA document and interpreted for use in the scenario presented. The following is a brief summary of the standards that relate to our wireless scenario.

1. Access control (164.312(a)(1)) is simply what the name implies, controlling who is granted access to the organization's resources.
2. Auditing (164.312(b)) is maintaining logs of who accessed a given resource at what time and where so that in the event of a security compromise there will be an audit trail.
3. Integrity (164.312(c)(1)) consists of making sure that PHI is not modified in any way by an un authorized user during transmission or storage.
4. Person authentication (164.312(d)) is authenticating that the person the computer says they are is really the correct person. This could be argued that it should be done at the server, but I think we can take it a step further and authorize the user when they transition from the wireless to the wired network.
5. Transmission security (164.312(e)(1)) is ensuring that the network transmissions are kept private and since the media is the air this is a high priority in wireless environments.

In the next section, we will cover these 5 regulations and apply the interpretation of them to our scenario.

Implementation of the Standards

For the standards that are found to be relevant to a wireless network, we need to find the implementation specifications for those standards and lay out a foundation for how the specific issues with wireless will be addressed. In the

following paragraphs we will map out overall implementation specifications for our standards. Most of the issues raised by these standards are addressed with the use of stronger encryption and auditing tools.

First we need to have unique user identification and automatic logoff. In a Virtual Private Network (VPN) situation, the user will be required to authenticate with the firewall in order to gain access to the corporate network (CN) and all the data contained in it. This access will be terminated upon 15 minutes of inactivity so that the sessions are harder to hijack. Next we need to have auditing, our VPN will store all the information on traffic entering the CN from the Wireless LAN (WLAN), these logs will provide us with one audit trail. We also need to have an Intrusion Detection System (IDS) on the network to detect specific attack trends. We will also need to check the integrity of the data, the VPN will have integrity checks to ensure that the data was not changed during transmission and that the data that ends on the device, is the same data that originated on the server. Person/entity authentication is more of a server issue, but as mentioned earlier the VPN will add one more authentication point to make sure the user is who they say they are coming onto the VPN. Finally we need encryption, by its nature this is the classic job of a VPN to encrypt. The VPN will use strong encryption to keep the data private. This will not stop sniffing, but it will render sniffed packets useless.

With this comes an understanding of why wireless networks are vital to healthcare networks, and the problems associated with them. We will use our translated HIPAA specifications to analyze a network and secure it according to those specifications.

Case Study

In the next few sections we will analyze a network and discover problems and solutions for those problems. Then we will go back and test to see how our fixes worked on the problems that we found. As mentioned earlier in HIPAA Standards, we will use our list of relevant regulations as a guideline for security.

Before Security

Access Control, this is simply controlling who/what is granted access. Wireless networks have a single built in method for controlling who is granted access to the network, this being MAC filtering as discussed in a previous section. MAC addresses can be modified rather easily, and usually this can be done with full support from the manufacturer via a driver property page. An attacker would need to just set up a sniffer on the network and watch to gather IP addresses and MAC addresses from users that are authorized to use the network. The attacker then could issue a Denial of Service (DoS) attack against one of the authorized users. Once the user was flooded and no longer able to communicate on the network, the attacker could then change his settings to reflect the authenticated user and gain access. This completely fools the access control lists (ACL's) on the AP, since it thinks that the attacker is really an authenticated user. More detail on this type of attack including TCP dumps and

screen prints can be found in Joshua Wright's paper located at http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf.

SSID's can also be used for access control, AP's should be configured to keep the SSID private and not broadcast it. This keeps the network at a lower profile and will prevent a casual looker to find the network and gain access. This doesn't mean that if you set the SSID to a string that resembles a password and you don't broadcast it you are safe. SSID's can still be sniffed, it just requires a device on the network re re-authenticate with the AP[7].

WEP keys are another form of access control, since the AP can be configured to require data encryption, therefore the AP will not accept traffic unless that traffic has been encrypted with the correct key. This is also a weak form of access control since WEP is vulnerable to cracking and the keys can be discovered easily.

The site under review was not utilizing MAC filtering, but did have a rather secure SSID and it was not broadcasted. This benefited the company in the fact that it would be harder for a casual war driver to find the network. The network was not secured enough in order to meet the requirements of the HIPAA regulations. Anyone with a minimal skill set could use sniffing tools and detect the SSID and gain access to the network. They were using data encryption, but had a weak WEP key, Which was in fact weaker then the SSID.

Auditing. Going back to the phrase from Cole, "intrusion is a given, detection is a must." No site will ever be 100% secure unless they unplug their routers from the outside world. This leaves administrators with the job of making sure that an intrusion can be detected early enough to prevent a great deal of damage. Wireless networks should adhere to the same recommendations for wired networks; they need to have auditing tools in place on the wireless subnet to monitor the traffic. Ideally there would be one IDS for each AP. This would let us capture the early warnings of MAC address related attacks.[4] However as we all know there is no perfect world. At the minimum there should be at least one IDS on the segment so it can view all the traffic that passes to the gateway. This idea will be covered in more depth in following sections.

Once again the site that was under review had no forms of auditing in place on the network. There was no true way of knowing what was happening on that network.

Integrity. It is key to any network that the data that is entered by the user is the same data that is viewed at a later time. Without this key quality, networks would be useless since they could not be trusted. Wireless networks open up holes to the network that can aid an attacker in compromising the network and thus giving him the ability to change the data that has been stored on the network. Another problem with the integrity of wireless is that, In theory, an attacker could issue a DoS attack against a wireless AP intercept traffic destined for it, modify it, and then pass that traffic on to the AP, or vice versa. The 802.11x protocols have WEP to address this issue, but as we have mentioned previously, WEP is not to be considered secure as it can be cracked easily[8]. Since WEP isn't

secure there are no other options available in the protocol suite to address this problem of data integrity.

Rather then trying to use WEP a better solution would be to put a more robust algorithm in place at a higher layer of the OSI stack. A good choice would be IPSec or another similar VPN architecture that has been battle proven.

The site in review had only WEP in place, with a weak key so this was not in any way secured to the standard that was needed. Even an amateur hacker could break the security.

Person/Entity Authentication. This is authenticating that the person or entity that is believed to be accessing a given resource truly is that person they claim to be. There are several problems with this in a computing environment, the first being that it requires a secure channel to communicate. If the channel isn't secured, the authentication tokens can be sniffed by an attacker and replayed to the server and the attacker can be authenticated. This is obviously a undesirable as the attacker shouldn't have access to the data. It is possible to sniff on wired networks, but even easier on wireless networks since the medium is the air. On wired networks, network administrators have learned their lessons and are utilizing VPN technologies to keep the channels secured. Wireless networks however, are being treated as if they are just another leg of the CN and they are not utilizing strong encryption. Wireless should be treated just as it was a public network. WEP is not strong enough to secure the communications.

The reviewed site had WEP enabled which has already been deemed insecure. All the physicians were utilizing the wireless networks to access patient data. If the login information was sniffed by an attacker and replayed, the attacker could have full access to the PHI on the servers.

Transmission Security. This deals with keeping the transmissions private and protected from un authorized users. As was covered in the previous section, keeping transmissions secure enables a site to securely communicate data between parties. Secure communications are vital to keeping PHI protected. It is also vital to ensuring that login credentials are not snooped, and the security of the systems compromised. Transmission security is provided by encryption algorithms. The 802.11x protocols have WEP built in as an attempt to secure the transmissions. This protocol can no longer be deemed secure as we have covered previously. That leaves network administrators with the problem of implementing a stronger encryption algorithm over top of the wireless protocol. Practical applications of encryption on top of the wireless protocol suite are VPN's. As mentioned earlier it is best to think of wireless networks as public domain since the media and path of the packets can not be confined to the wires running through the building. VPN's work well to encrypt the transmissions. The problems with VPN's are that they don't encrypt the whole packet. This allows SSID's and MAC addresses to be sniffed.

We will look at the IPSec protocol for example. When a packet is encrypted with IPSec it encrypts all the way out to the IP header, so IP addresses are encrypted. However, that is as far as it goes. It doesn't encrypt at

layer 2 of the OSI model. This means that all the SSID's and MAC addresses are broadcasted in plain view of any attackers that are sniffing the network. This data can be used to the advantage of an attacker in an attack[4].

Once again the reviewed site was only utilizing WEP with a very weak key. There were no other encryption methods in place to protecting data.

How Vulnerabilities Were Addressed

Access Control

It is tough and close to impossible to lock down who is granted access to view the packets on the network. The only true way is to line the building with aluminum. This is very costly and quite cumbersome. Rather, it is better to use directional antennas so that the wireless field will not penetrate well beyond the reaches of the building. This narrows down the locations that an attacker can gain access from[2]. A secure SSID had already been chosen for the site, and the broadcast feature of the access points had been turned off already at the site in review. This is a small wall that helps to keep exposure down at a lower level. At this specific site the budget didn't allow for replacing the wireless antennas to narrow down the broadcast footprint. This would be the next step to locking down access. MAC filtering was considered to put up another small defensive measure, but the manageability and ease of breaking it outweighed the benefits. The AP's were placed on a separate subnet logically and physically. This provided us with the means to filter all traffic coming into the CN. This is where our access control was effective. We put the wireless network on its own DeMilitarized Zone (DMZ) off the firewall, and then configured the firewall in such a way as to require the user to authenticate in order to send packets anywhere including the internet. This gave us a more robust means to controlling access, however, we still were unable to keep attackers from gaining access to our packets, and never will be able to. This did secure the network to a point in which unauthorized users could not utilize the wireless network to access any other networks.

Auditing

Since we placed the wireless network on its own subnet, we were able to place an IDS on the net to monitor the traffic. We used a higher end switch that allowed us to monitor all the switched network over one port. The sniffer had only the recieve wires connected to the network so that it would be very difficult if not impossible for an attacker to gain access to this box. This still works for sniffing since the network interface is only receiving packets and doesn't need to be set up with an IP address or any other configuration options. This will monitor all the traffic on the network. We also have a point in which all the traffic will pass when it is leaving the wireless network, which is the firewall. The firewall was configured to log all the traffic coming from the wireless network, as well as logging all the authentication attempts. We now have a great deal of information available about the traffic on our network. There is one other problem with the

network, which is the problem of rogue AP's being put in place by attackers. An attacker could get users to login to his rogue network and steal authentication information. With this information he could easily bypass all our security measures and would appear as if he was a legitimate user on the network. We can counter hack this problem by placing wireless sniffers in such a way that they cover the floor plan of the building. These wireless IDS's could consist of a small pc running Linux with a built in wireless NIC. They would sniff everything and pass it back to a central logging server. This logging server would analyze for any symptoms of a rogue AP attack. Reference Josh's paper. It is a good point to note that even organizations that are not utilizing wireless networks should think about installing wireless sniffers to guard against un-allowed wireless traffic. This rogue AP sniffer would be similar to the architecture developed by AirDefense in their wireless IDS system [9].

Integrity

Integrity of the network was provided by the use of a VPN, when we set the wireless network on its own network segment we also forced the packets to go to the firewall before getting to the corporate network. At this point the firewall requires a VPN connection from the user in order to allow them though. We now have required that all packets going anywhere but the local network be encrypted with a strong VPN encryption scheme. There is still one problem, packets that are staying on the wireless network. These packets will be transmitted without being encrypted. At the present time, the devices on the wireless network don't need to communicate between each other, it is strictly client server so this helps us. But in the future should the devices need to communicate amongst their selves this will need to be addressed again. The other problem with integrity that our VPN solution solves is that an attacker will need to circumvent the firewall to gain access to the CN. While no system is 100% safe, it is harder to break a well configured firewall then to just breeze through an AP. This helps to ensure that the integrity of the data inside the network remains true.

Person/Entity Authentication

This function is primarily accomplished by the server that is providing the resource. However in order for the authentication to be secure and successful the communication channel needs to be secured, this channel being the wireless network. Once again the VPN setup took care of this. It also added an authentication point in which any person/entity that needs to access resources on the CN must authenticate with the firewall. Currently with the amount of users that we have, we utilized the builtin functionality of the Checkpoint firewall rather than a RADIUS server or some other authentication source. With the users of the wireless networks being physicians and needing to have quick access, we set the authentication scheme to be certificates, and configured the firewall to timeout after 10 minutes of inactivity.

Transmission Security

This is covered by the VPN that we put in place. We are using 3DES encryption and MD5 for the hash algorithm. All the transmissions between the devices and the CN and between the internet are encrypted up to the point that they reach the firewall. The key to keeping this secure though, is having strong authentication at the firewall. As mentioned earlier we configured the VPN to use certificates and they must be changed every 3 months. While our packets are still out in the open they are virtually useless to an attacker since the cyphertext is too difficult to crack.

After Security

Access Control

After our changes, hackers would still be able to access our wireless network; however it will be less obvious due to the configuration changes regarding broadcasting the SSID. Now with a lower profile, if an attacker connected to our wireless network, they would only be able to sniff traffic on that network, and it would all be encrypted and useless to them. They no longer can communicate past the AP's since the firewall requires VPN strength authentication.

Auditing

With our new logging measures we have 24/7 logs of the traffic on our networks, this gives us both proactive monitoring and the ability to research what has happened in the past. The Wireless IDS's will alert us of unwanted wireless activity, such as rogue AP's or MAC attacks.

Integrity

After our VPN implementation was in place, the packets going back and forth were encrypted and checked with MD5 to ensure integrity. The VPN also tightened down attackers gaining access to the corporate network via the wireless network. This helped with the problem of attackers using the wireless network as means to change data within our CN.

Person/Entity Authentication

We were able to secure the communications channel by using the VPN, so that the back end servers are now able to effectively communicate the authentication information and enable secure logons. We also added a second authentication point to keep more load off the back end servers. A user must get past the firewall before they can access the back end servers.

Transmission Security

With the VPN all transmissions to and from the wireless devices and the CN are encrypted with strong encryption. This has secured the communications so that the only sniffable data is cyphertext and is useless to an attacker.

Conclusion

Wireless will never be one hundred percent secure, nothing will ever be one hundred percent secure. This is why we must be able to detect the early signs of an attack, and try to prevent substantial damage. We started with configuring the AP's in the correct manner. Then we put the VPN as a major piece for locking down the network, and this gave us much more security. Finally IDSs were implemented in place in order to provide us with more detailed auditing logs. The network is now more secure and able to effectively protect patient data as specified in the HIPAA guidelines.

A further step that can be preformed but the budget did not allow for is physically placing aluminum panels in the walls of the building in order to stop any wireless transmission from coming in or going out. As network technology changes this network will need to be constantly maintained and evaluated to keep it secured to the HIPAA standards. As a security professional once said, "Security is a process not a product." While there are humans in the world and networks to be hacked, no system will be secure without constant evaluation and patching.

Reference Material

1. "Moving Mountains With Mobile Computing, Wireless Technologies IN Healthcare" URL:
   http://www.medicalmanager.com/graphics/hci_ultia_article.pdf

2. Miller, Stewart S. WiFi Security McGraw-Hill 2003
   pg 87-88 Fortress of solitude (wirelessly speaking)

3. "(IN)Security of the WEP Algorithm" URL:
   http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

4. "Detecting Wireless LAN MAC Address Spoofing" URL:
   http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

5. "Public Law 104-191" URL:
   http://aspe.hhs.gov/admnsimp/pl104191.htm

6. "Federal Register Document 03-3877" URL:
   http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-3877.htm

7. "Minimizing WLAN Security Threats" URL:
   http://www.wi-fiplanet.com/tutorials/print.php/1457211

8. "AT&T Labs Technical Report TD-4ZCPZZ" URL:
   http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

9. "Wireless Intrusion Detection and Response" URL:
   http://www.airdefense.net/products/intrusion_detection.shtm

Appendix A

3DES An encryption algorithm based on the DES algorithm that is stronger and more robust then the previous.

802.11x This is the wireless protocols, 802.11a 802.11b and 802.11g. The latest version is 802.11g, 802.11a came out after 802.11b, the reason being that the 802.11b standard was approved before the 802.11a standard. The most popular of these are 802.11b and g.

ACL Access Control Lists, these are lists that are kept on a device to provide basic filtering based on one value that is provided to the device. They are generally static in nature meaning that they must be modified by hand.

AP Access Point, This is the device that bridges the wireless network to the wired network. It is basically 2 NIC's, one wireless and one wired. This allows wireless devices to communicate with wired networks.

CN Corporate Network, this consists of the private networks of an organization, the goal of the security administrators is to protect this network.

Cyphertext This is the text that is generated from plaintext when passed through an encryption algorithm. The difficulty of cracking this is based on how strong the encryption algorithm and key are.

DMZ DeMilitarized Zone, this is the network that public servers are placed on. They often have less security built into them so that outside users can access the company's public information.

DoS Denial of Service, this is an attack in which the attacker floods a user or server with so many packets that it causes that device to no longer be able to communicate on the network.

HIPAA Health Insurance Portability and Accountability Act, this is the act that was signed to law in 1996 to provide a governing standard for protecting healthcare networks, and patient information in general (PHI).

IDS Intrusion Detection System, This is a device or server that it attached to the network and gathers network data and analyzes that data for attack signatures and alerts the network administrator of the problem.

IP Internet Protocol, this is the network layer protocol used by TCP, it is connectionless, and routeable.

IPSec IP Security, this is a protocol that was drawn up for securing packets all the way out to the IP headers.

LAN Local Area Network, this is similar to the CN, it consists of the local segment that a device is on. While the CN can consist of multiple segments all that are internal to the company.

MAC Media Access Control, this is the protocol that runs at the data link layer of the OSI stack, it provides an interface between the logical link and physical layers.

MD5 MD5 is a one way hash algorithm that generates a hash of a file. If the file is changed the hash will be different.

NIC Network Interface Card, this is the physical device that allows a computer to communicate on a network.

OSI Open Systems Interconnection, this is a network architecture model with a suite of protocols to go with it. It was developed by the International Standards Organization.

PHI Protected Health Information, this is defined by the HIPAA regs as data about a patient that is private and should be protected.

RADIUS is an enterprise logon server that is able to serve many logins, it is more powerful and robust then most OS login systems.

Sniffing This is the practice of gathering data off of a network that is not destined for you.

SSID Service Set IDentifier, this is a string that is assigned to a particular wireless network, this is how wireless devices know what network to communicate with.

TCP Transmission Control Protocol, this is a communication protocol widely used on the internet to move data between devices on the network. It is reliable and connection oriented.

VPN Virtual Private Network, this is an architecture for creating private network over the internet. It utilizes the internet infrastructure but employs encryption to simulate it as being private.

WEP Wired Equivalency Privacy, this is the encryption protocol that was built into the 802.11x protocols to try and provide privacy similar to what is on local wired networks.

WLAN Wireless Local Area Network, This is essentially the same as a Local Area Network, but it is all wireless devices.