https://doi.org/10.48009/2_iis_2009_585-591

WIRELESS (IN)SECURITY: AN OVERVIEW IN THE HEALTHCARE INDUSTRY

L. Roger Yin, University of Wisconsin-Whitewater, USA, yinl@uww.edu
Daniel T. Norris, University of South Carolina, USA, dnorris@sc.edu

ABSTRACT

The installment of HIPAA solidifies regulations of protecting patient records, especially private information against unauthorized access. However, the increasingly popular wireless network devices used in healthcare facilities, though convenient and time-saving, exacerbates the administration difficulty of network security. This paper provides an overview and guide to healthcare managers with limited IT Staff yet need to deal with the information security treats through wireless communication.

Keywords: Network Security, Wireless Security, HIPAA, Healthcare Information Management

PROBLEM STATEMENT

Imagine a hospital has deployed the latest health care technology: a state-of-the-art wireless handheld application that lets administrators, physicians and medical staff access records, order lab tests and prescribe medications. It's a hit. Record keeping costs are lowered, patients agree service is more efficient, and fewer errors are made. But what happens when a doctor sits down his PDA – still logged on--and discovers it's missing when he reaches for it again? As the IT staff at Columbus Hospital found securing a wireless network in a hospital setting is a huge tedious task. They allowed the users to get there choice of wireless device to connect to the network, their only requirement was that the users brought the device to IT and get it configured.

A PRACICAL GUIDE OF WIRELESS SECURITY IN HEALTHCARE FACILITIES

The major thing with a wireless network is it will talk to anything within its spectrum [18]. Without employing network security measures any user with a wireless network connection the wireless access point will allow it on. It is not only bad practice to leave you wireless network unprotected but also unethical and against the law to snoop around another peoples' networks [18, 24, 19].

Clayton Dillard was the first man in the nation convicted of a wireless crime. He stole patient records from an Internal Medicine Consultant; although he thought it was an experiment the authorities saw it as a crime [22]. Hospitals and Healthcare institutions are becoming more aware and concerned with the flaws of wireless networks that the network administrators and Internet security officers are dedicating more time to securing the network [21].

Not only is securing the patient data important they also need to think about network bandwidth and email spamming. Both of which can be as harmful to a network as a virus or a hacker. If a user gets on your network and decides to start downloading movie files or music files it's going to take up a considerable amount of bandwidth. This can cause the network to slow to a halt therefore data can't be entered efficiently and users will become frustrated. Worse would be unauthorized use of streaming media, if you've ever watched a network monitor when someone decides to watch a movie online you'll see the tunnel get very tight. These two things can result in poor network response therefore not allowing the doctors and nurses to get the results they are looking for in a timely matter. As seen from Figure 1 [22] the healthcare and pharmaceutical industries are right at the top of the chart meaning they should be top priority to be very secure.

This could pose a big factor when a healthcare facility looks to implement a wireless network. They need to be concerned that security is priority no. 1. If they do any sort of implementing without fully testing their security settings there could be some serious backlashes from the implementation.

<insert Figure 1 here>

Typically a health care organization doesn't put a whole lot of emphasis on the security of their network. When going wireless this lack of security is really going to hurt. According to Gartner Inc., in Stamford, Conn., approximately 30 percent of enterprises last year suffered serious exposures from deploying WLANs without implementing proper security. "Healthcare organizations haven't lagged in [technology] spending, but they've lagged in execution," says Dorenfest, who is CEO of Dorenfest & Associates, a Chicago-based provider of health information technology market data. [16]

The healthcare industry is a huge industry that would greatly benefit from going wireless, if they could execute some of their ideas to go wireless the long run would prove to be very beneficial. Doctors could roam freely using handhelds or laptops and easily enter data while at a patient's bedside. Hospitals are required to meet Health Insurance Portability and Accountability Act regulations (otherwise known as HIPAA). HIPAA requires that all electronic records meet a certain level of security [4]. Due to these requirements imposed by HIPAA network administrators and information security officers determined early on that WEP (Wired Equivalent Privacy) is insufficient to use for their wireless networks. WEP is a very easy security protocol to setup and configure per machines but cracking the encryption is a also a very easy thing to do. Another security hole administrators are seeing are rogue wireless access points, which anyone can setup. This is particularly dangerous because a wireless access point setup incorrectly will allow anyone (not just hackers) onto the network and intercept data, send/receive data, and surf the Internet as if they were plugged into the network with a wire. This is a huge security risk because as the administrator you have no control over the device configuration or users on the network. It's like a race car driver having no control of their car going into a turn, there is no telling what the outcome will be. Unfortunately a rogue access point can be put on the network, intentional or unintentional.

Unintentional rogue access points:

- Physicians in the medical office deploying their own wireless networks so they can access their data from a common medical library on another floor.
- A group of accounting consultants who needed connectivity for several users in a conference room with only one Ethernet jack.
- A mobile cart vendor who left behind an evaluation cart and a wireless access point.

These access points were setup to keep the flow of work flowing smoothly and quickly although they can be very dangerous as anyone could log into these and get on the network and steal data or flood the network with bad data. Users don't usually understand that when they are just trying to do work more efficiently that they are possibly tampering with security.

Intentional rogue access points:

- A radiologist connected two competing hospitals with wireless LANs so he could review films from both hospitals in one office.
- Vendors plugged into an access point to intercept e-mail traffic from purchasing to determine what bids were being offered by competitors.

Although these access points aren't meant to really harm anything they are a prime example of a dangerous rogue access point. In two ways,

1. They are intentionally getting onto a network and stealing data and using it for their benefit and against the hospital.
2. Others can also log onto these access points and get into the hospitals network therefore having the ability to steal data and/or inject bad data.

Rogue access points can also be configured incorrectly by users creating them in ad hoc mode, that is basically just a peer-to-peer access point but still allows for use on the network, this can be potentially dangerous. Each of these examples of rogue access points exposes the network to outsiders that want to intercept data. All are very dangerous to the health and well being of the hospitals wireless network.

There are many software packages that can detect these access points, a few are Mobile Manager Enterprise and a wireless security package from AirDefense Inc. Most of these packages also include intrusion detection software so administrators can monitor their WLAN and be first to detect any unusual behavior on the network. "Hospitals are a little in the dark on their use of wireless technologies," said Wayne Haber, chair of the security special interest group of the Health Information and Management Systems Society (HIMSS). "They're using wireless, but they're sometimes using it in ways that are known to be insecure" [8].

Another security measure administrators are using is requiring users to authenticate once they've logged onto the network. This will ensure that only users that have network logins will be on the network. Of course this philosophy doesn't always hold true, as users tend to write their usernames and passwords on post-its and put them on their monitor or under the keyboard. Another security tactic administrators are using is timing out a user's login session after a certain period of inactivity. This eliminates the problem of leaving workstations, laptops, or PDA's unlocked; therefore, not just anyone with the knowledge of computers can walk up to the station and begin browsing the network.

Other security restrictions would be not allowing users to store information on the actual wireless device, not allowing users to cache ID's or passwords and force users to change passwords every 1 to 3 months. Along with changing their passwords users should have

stringent rules on the types of passwords they can use. These rules need to be strictly enforced and complied by all. All these security measures are the only way a hospital can protect their data and keep wanders out of their network. Patient data is a very touchy subject; some would say getting a hold of this data could be construed as a form of terrorism. Therefore, securing this data is a very important aspect of network administration. Another way to help increase level of security is to install software firewall on all the wireless devices. Windows XP SP 2 and Vista comes with a fairly decent firewall, although a more flexible solution like Zone Alarm can allow for more customization.

An additional concern for hospital administrators is an authorized network user could steal a laptop and log onto the network anywhere in the facility or even outside of the facility. There is nothing stopping a user that has a username and password to log on from anywhere within the range of the access points. A couple things security administrators could look for is inactive connections, connections that are weak, and lots of activity to one computer account. These could all be indications of shady activity. There is not much that can be done to prevent this activity but monitoring the wireless setup could help identifying the problems more quickly. Not allowing users to keep connections after long periods of inactivity or prompting them to re-login once they've hit a certain amount of time but not losing any data on their computer. Users would need to get use to some new security features using wireless as the network is more open and therefore needs to be more secure. No one should be allowed on without a username and password, or without having their pc checked out by a certified IT professional.

WHAT THE HACKERS DON'T WANT YOU TO KNOW

Although network security officers need to look at how to secure their network they also need to look into how Hacker's can still get into the system. No matter how hard you try to secure your network someone somewhere will find a way in if they work hard enough. Therefore network administrators really need to go at it from a different point of view. They need to read up on how hackers typically penetrate a network, and then stay one step ahead.

It is impossible to completely secure your network but you can work to find weak spots in your WLAN and employ intelligence that work to maintain and secure your enterprise wireless network. Securing the wireless network requires a multitude of options that need to be employed. They are encryption, user education, securing all laptops and mobile devices, among other things. [12] You can't prevent hackers from detecting your WLAN's RF signal but you can work to prevent hackers from easily picking up the signal and getting into your network. A couple ways to do this are to redirect your antennas, setting up simple encryption using WEP, WPA, or in the future WPA2, and finally you could setup IPSEC or SSL (which are used in VPN technologies). WEP (Wired Equivalency Protocol) was the first encryption for wireless networks and was hacked within the first couple weeks. The next attempt was WPA (Wi-Fi Protected Access), which made encryption tighter, and now they are working towards WPA2 with 802.11i. WPA2 uses a more advanced encryption type (AES) that is which meets Federal Information Processing Standard 140-S specifications for wireless security, although new hardware may need to be bought to comply with the new AES standard. Finally IPSec and SSL are used to create VPN tunnels between two locations. As long as both ends of the tunnel are secure, VPN will be a tight tunnel and hacker's will be have a hard time getting in. There is a group of general attacks hackers use. These attacks are typically Mac Spoofing, Denial of Service, Malicious associations, and Man-in-the-middle attacks [12]. These are just a few of the attacks network administrators have to be cautious of as hacker's are smart people and are always trying to come up with new ways to get into a system.

Another vulnerability that makes up about a third of the vulnerabilities is internal. This can be again intentional or unintentional; the doctor wants to have his wireless router on the network so he can work without having the cabling. If that router isn't secured well he's going to be a weak link in the network. Another example would be someone that doesn't want to follow the rules and just goes around the information technology department and does what he/she wants. Another vulnerability would be users that work from home or want to take their laptop to a hotspot like Starbucks. These locations are typically not as secure as they should/could be. A hacker could easily be lurking around these points and get right into the users network while they are doing innocent work.

HIPAA REGULATIONS FOR NETWORK SECURITY

Wireless security wasn't even on the table when HIPAA started working on the network security options.

> "There are so many security issues around wireless and the [security] rule gives you no substantial guidance on how to secure wireless," said Marne Gordon, director of

> regulatory affairs at TruSecure Corp., referring to the Health Insurance Portability and Accountability Act of 1996 guidelines on security. "I know a lot of doctors in their own hospitals are looking to see what steps wireless can save them. There are so many security issues around wireless and the rule gives you no substantial guidance on how to secure wireless. A lot of organizations are looking for 'How do I secure that,' because that's the weakest link,' she said." [20]

Even though it's not a standard by HIPAA's regulations WEP should not be an encryption method that hospitals use. It's very easy to crack the WEP encryption just by sniffing the network and figuring out what the combination of the encryption key is and the creating one like it and injecting packets into the network.

BENEFITS OF WIRELESS TECHNOLOGY IN A HOSPITAL OR CLINIC

Table 1 shows how a wireless network will help a hospital or clinic improve its processes. Using wireless pretty much makes the nurses/doctors free to roam, they don't have to be tied down to a terminal to enter/update data, they can take their laptop or PDA to any room and easily and quickly check the status of that patient's lab results or prescription requests.

Reduces Transcription Errors	Letting nurses be able to transcribe notes and order medications right from patients' bedsides improves
Improves Scheduling	Caregivers can bring computing wherever they go. They can more easily arrange and rearrange scheduling tests than if they would have to wait for a terminal to be available.
Physical Restraints	Hospitals are notoriously cramped spaces. Wireless technologies can be installed easily and unobtrusively.
Mobility	Doctors and nurses are always on the go. Wireless gives them the ability to communicate wherever, whenever they wish.

Table 1: Benefits of Wireless Technology in a Hospital

Getting access to real time data is a crucial part of the patient doctor relationship. Sitting behind a big monitor is much less personal than working with a small handheld at the patient's bedside. It allows the doctor/nurse be more personable with the patient, it also makes it more convenient for the caregivers. Using small handheld devices, or laptops also allow the caregiver to do point of care ordering and charting. This is a big improvement, as it will make the information more accurate since the caregiver is entering it as the patient is describing a pain or while the caregiver is taking vitals on a patient. No more writing down the information and then trying to decipher what you wrote later in the day or whenever you get a chance to get it entered into the system. The benefit to using wireless in healthcare is point of care makes a qualitative difference in the quality of care provided to patients.

A FRAMEWORK OF USER TRAINING

Training is a going to be a big factor in getting the wireless network effective in the hospital. All users need to know the risks and ramifications that go with a wireless network. Below is a table of the responsibilities and training necessary for each of the roles in the hospital.

<insert Table 2 here>

CONCLUSION

It is unfortunate that no computer network is completely secure unless they unplug their routers from the outside world. In the words of Eric Cole, "Intrusion is a given, detection is a must." Security in a wireless network is very crucial. Hospitals especially need their environment secure due to all the patient and confidential information that will be transmitted. HIPAA laws would need to be accounted for when setting up for the network.

If the hospital wants to allow it's patients and their guests on the Internet they could setup another network that patients and guests could connect to with personal laptops. A major factor in making wireless work in a hospital would be user education. The users need to be educated on the security risks and how to avoid the problems that go along with those risks. Users need to be aware that they can't just leave usernames and passwords on post it's or tape pieces of paper on their desk drawer. We feel wireless in the healthcare industry could bring some great revelations to the industry; mistakes in personal information would be decreased, double and triple checking of data could be

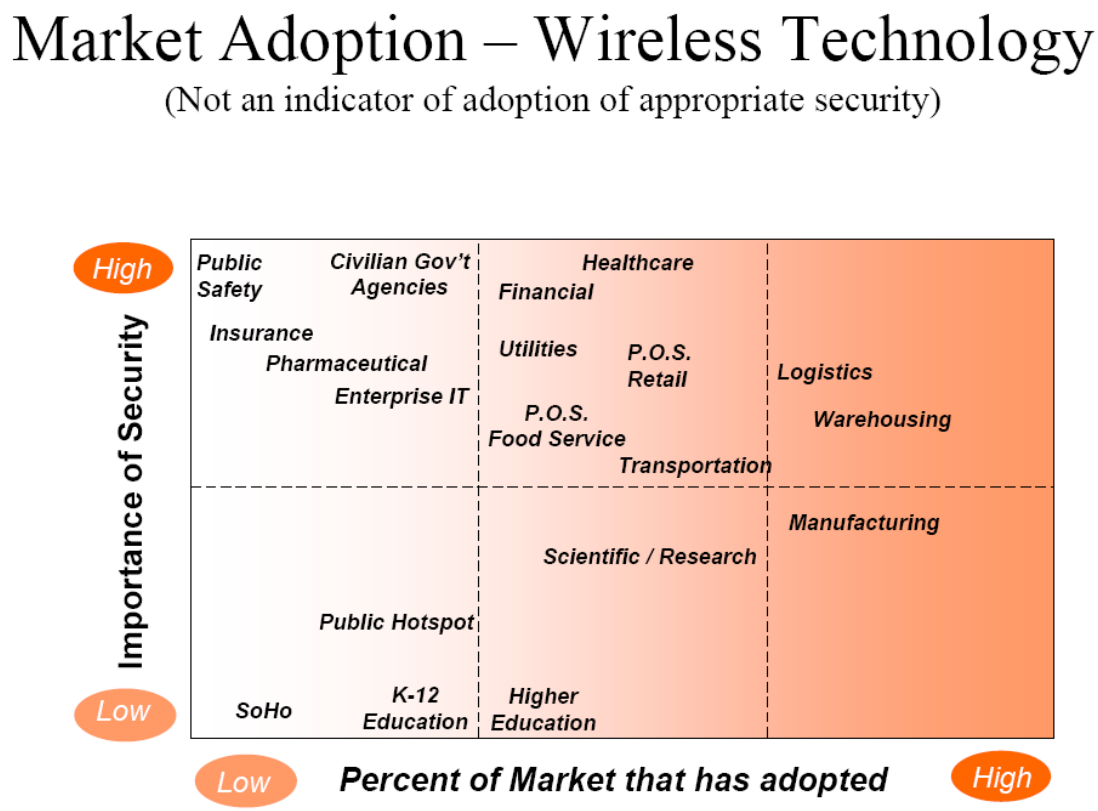
more automated and doctors/nurses could update, monitor, and retrieve important data instantly. If a hospital rolls out a wireless plan properly it could greatly reduce costs for all areas. The big thing they need to keep in mind is the user aspect, how will the users be affected. The cost of going back and patching up user problems after the infrastructure is in can really hurt a company. Users should be involved all along the process to keep human errors to a minimum. As long as security continues to improve and there is always someone on the inside that can be one step ahead of the hacker's (as well as others on the outside), wireless will take off in the healthcare industry.

REFERENCES

1. Barron, R. (2004), Healthy investment for hospitals: wireless nets, Retrieved February 13th 2008 from http://www.bizjournals.com/industries/health_care/hospitals/2004/09/20/eastbay_story7.html
2. Bluesocket (2006), Wireless security and management in healthcare organizations, Retrieved February 19th 2008 from
3. http://www.anidirect.com/downloads/wp/BlueSocket/Healthcare-BluePaper.pdf
4. Chen, A. (2003), Hospital Cures WLAN Insecurity, Retrieved February 16th 2008 from
5. http://www.eweek.com/article2/0,1759,1498376,00.asp
6. Featherly, K. (2004), Wireless Whereabouts, Retrieved February 18th 2008 from
7. http://www.healthcare-informatics.com/issues/2004/07_04/cover.htm
8. Haskin, D. (2004), Hospital WLANs Improve Patient Care But Threaten Security, Compliance, Retrieved February 20th 2008, http://www.compliancepipeline.com/trends/50500087
9. Hulme, G. V. (2004), Columbus Regional Healthcare System, Retrieved February 14th 2008 from
10. http://informationweek.com/story/showArticle.jhtml?articleID=55300433
11. Joch, A. (2002), Wireless Watchdogs, Retrieved February 22nd 2008 from http://www.healthcare-informatics.com/issues/2002/07_02/wireless.htm
12. Keenan, K. (2004), What hackers don't want you to know about your WLAN, Retrieved February 22nd 2008 from http://whitepaper.networkcomputing.com/shared/write/collateral/WTP/51007_80489_56542_AirMagnet_Hacker_WP.pdf?ksi=962831&ksc=1213665319
13. Kellogg. (2003) Kellogg on Technology and Innovation. Wiley, 229-234
14. McCormick, J. (1999), Wireless Hospitals: New Wave in Healthcare Technology - Industry Trend or Event, Retrieved February 14th 2008 from http://www.findarticles.com/p/articles/mi_m0DUD/is_6_20/ai_55182581
15. O'Dorisio, D. (2003), Securing Wireless Networks for HIPAA Compliance, Retrieved February 28th 2008 from http://www.sans.org/rr/whitepapers/awareness/1335.php
16. Powers, V. (2004), Improving IT wellness—Healthcare organizations adopt knowledge-enabled technology, Retrieved February 13th 2008 from
17. http://www.kmworld.com/publications/magazine/index.cfm?action=readarticle&Article_ID=1681&Publication_ID=105
18. Rackley, S. (2007), Wireless Networking Technology: From Principles to Successful Implementation. Newnes Elsevier: Burlington, MA
19. Rubin, A.D. (2003), Wireless Network Security. Communications of ACM. 46(5): 2-3.
20. Sarker, D. (2003), Wireless Security entangles HIPAA, Retrieved February 23rd 2008 from http://www.fcw.com/geb/articles/2003/0616/web-hipaa-06-18-03.asp
21. Shayegani, S. (2008), Reliable Wireless Security: Just What the Doctor Ordered for Networked Medical equipment.
22. Sinnott, D. (n.d.), Wireless InSecurity, Retrieved February 16th 2008 from http://www.e-nc.org/pdf/Sinnot.pdf
23. Simms, B. (2004), Moving from Liability to Viability, Retrieved February 18th 2008 from http://www.healthmgttech.com/archives/0204/h0204viability.htm
24. Vacca, J. (2006), Guide to Wireless Network Security. Springer: New York.

TABLES AND FIGURES

Figure 1: Wireless Security in Markets that Have Adopted It



Source – Wireless Security Vendor to DOD

Table 2: Training Needs of Wireless Security in a Hospital

Role	Responsibility	Training	Benefits
Doctor's	Review Patient Information, Enter new data briefly	Review the risks of having their own access point in their office. Train them how to lock their PC or log off when they are not at their machine.	E-prescribing, checking what symptoms and/or side affects might occur for specific patients, Maintaining patient history and sending and receiving lab tests and results
Nurses	Enter bulk of patient vitals, medication dosage, review what has been done on other shifts	Training on the risks of leaving computers logged in	Monitor the patients from the nurse's stations or offices as necessary, All results, diagnostic information and other relevant information can be transferred to a central server and monitored more accurately,

Patient's	Monitor their own vitals	A handout on how to use the hospital internet access only	Remote monitoring of themselves, major problems could potentially be seen earlier and taken care of, therefore; making the hospitals more efficient and more accurate. Patients could also be monitored from their home therefore saving them and the insurance companies money and freeing up space in the hospital for more urgent issues.
Technical Support Staff	Support Doctor's and nurses when needed, maintain a secure network at all times, make sure all hardware is up and running efficiently at all times.	Wireless Security Conventions, Seminars on Wireless networking, depending on their role in the Technical Support Department they could get Cisco Certified for the wireless hardware offered by Cisco	More mobility as they don't have wires to tie them down, getting new users/computers up and running will be quicker as no wires to run. Once the network is setup very little maintenance with the exception of security and ongoing analysis.
Administrative Staff	Enter patient personal data, monitor that all data either patient or employee is up to date and accurate	Training on the risks of leaving computers logged in	Admitting new patients could be done at the patient's bedside or at a terminal done by the patient and spot verified by an administrative person. Checking patient records could be done more accurately and easily when the patient needs something or wants to update something.
Hospital Visitor's	Vendors and Drug Reps. No access points should be allowed into the hospital. If the visitor has a wireless card they could connect to the hospital's network but with no access to data just internet.	A handout on how to use the hospital internet access only	Could get on the internet to check their email, inventory, past orders.
Patient's Visitor's	No real benefit but the hospital could have hotspots the visitor's could connect too.	A handout on how to use the hospital internet access only	Allow them to get on the internet to allow them to pass the time.