

Running Head: Wired Network Security: Hospital Best Practices

Wired Network Security: Hospital Best Practices

Jody Barnes

East Carolina University

## Abstract

With an ever increasing amount of information in hospitals transmitted electronically, it is important that security be considered in every phase of network design and maintenance. Although much emphasis has been placed on such things as wireless networks and remote access, it is imperative that the core network not be overlooked. Because the wired network is the “nervous system” of a hospital’s Information Systems, great care must be taken to properly secure it. Also, with legislation such as the Health Insurance Portability and Accountability Act (HIPAA) requiring security measures in healthcare environments, securing the network infrastructure has become mandatory to ensure compliance.

This paper begins by looking at HIPAA and it’s implications for the wired network infrastructure security. A look is then taken at an organizations first line of defense, perimeter security. Although many think that as long as the perimeter is secure the job is done, perimeter security is only a small piece of overall security. Next, network segmentation and traffic isolation will be discussed. By using segmentation and isolation, there is the increased opportunity for security boundaries. Another concept that will be discussed is the security of the network equipment. The network is only functional if the core equipment is operational, so securing equipment is an important part of any security strategy. To conclude, restriction of network access will be investigated and an organizational approach will be discussed. Because more and more users need access to network resources, there must be a way to identify and restrict who is allowed on the network and what access they are granted. In wired network infrastructure security, hospitals must remember they are only as secure as their weakest point. By carefully

considering the various aspects of the network security during design, these weak points can be reduced and the overall security of the network increased. Although it is impossible to be 100% secure and still be functional, by using some general guidelines to secure the wired network, many threats to the network can be reduced if not eliminated.

## Introduction

In today's hospital environment, the wired network infrastructure is the "nervous system" of daily operations and must be secured to insure normal operations. This security must be considered in every phase of network design, implementation, and maintenance. Although much emphasis is placed on parts of the network such as wireless and remote access when security is considered, it is imperative that the core wired network not be overlooked. In the past, if the wired network were to be attacked and go down, all that was lost was access to email and maybe a few other insignificant activities. If the wired network in today's hospital environment is compromised and becomes inaccessible, every aspect of hospital operations is at risk and patient lives may be in jeopardy. Although all areas of the network must be considered in the context of security, we must ensure that we do not overlook the core wired network infrastructure.

Protecting the wired network in a hospital environment is no longer optional due to legislation requiring the security Patient Health Information (PHI). Since the Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996, hospitals and other healthcare entities are required to take necessary measures to ensure that PHI is safeguarded to ensure confidentiality. Part of this security includes protecting the medium on which this information travels including the wired network infrastructure. Not only does it make good business sense to protect such a valuable part of the hospital as the wired network, HIPAA has made it mandatory.

## HIPAA and It's Impact on the Wired Infrastructure Security

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect health information by establishing transaction standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable health information. Entities directly impacted by this act are health plans, health clearinghouses and healthcare providers (*TLC HIPAA Overview*, n.d.).

Even there are other rules incorporated in HIPAA, the Security Rule has the most direct impact on the hospital's wired network infrastructure. This rule addresses security measures such as user authentication, access controls, audit trails, controls of external communication links, and physical security. With increasingly more information being stored and transmitted electronically, the Security Rule works to identify and regulate these activities (Gue, n.d.).

April 2005, was the date for healthcare organizations to be HIPAA compliant. The only exception to the rule is for small institutions with less than \$5 million in revenue. These institutions have been given one additional year to become compliant. Those not in compliance with HIPAA face violations which can carry up to a \$250,000 fine and jail time up to 10 years (Mercuri, 2004). Now is the time to ensure that the wired network infrastructure security is at or above the mark established by HIPAA.

#### Steps to Secure the Wired Network Infrastructure and Meet HIPAA Standards

As with any security strategy, securing the wired network infrastructure must be done in layers. The use of layers provides the hospital multiple lines of defense as well as helping eliminate single points of security failure. The way network security is designed

and implemented is shifting due to increased needs and new security vulnerabilities inside of the organization. It was long thought that all that was needed was a hard external shell and a soft internal network. In today's environment, this couldn't be further from the truth. We must continue to harden the perimeter while increasing the security inside of the trusted network to help mitigate internal security threats (Alomary and Jamil, 2004). As stated by Rabinovitch (2003), "network security can be protected through a combination of high-availability network architecture and an integrated set of security access control and monitoring mechanisms" (pg. 589). In the following sections, a look will be taken at some general steps that can be taken to help achieve this layered security integration approach to the wired network security. Because each section of this paper could be the primary topic of many papers, a broad approach will be taken giving general practices and concepts. So although a detailed demonstration of the techniques needed to accomplish the security goals for a hospital will not be covered, design concepts and best practices will help to ensure that the correct security path is taken.

### Perimeter Security

When securing a hospital network, a secure perimeter is the first step in overall network security. As stated by Sood (n.d.), "when one connects the enterprise network to the Internet, one is connecting its network to the thousands of networks that are unknown thus giving millions of people the opportunity to access your assets"(pg. 1). Because the perimeter is vulnerable to attacks from the Internet and so much is at stake, great care must be taken to ensure that it is secure.

When considering perimeter security, a look must be taken at the devices that will

be used. In many organizations, various types of firewalls and remote access devices are deployed for perimeter protection. Although this is a solid practice, we must ensure that these devices are configured correctly to provide the security for which they were designed. As stated by Kincaid (2004), “an improperly located, configured, or monitored firewall can give a false sense of security for an organization” (pg.1). It is imperative that the utmost attention to detail be taken with the design and implementation of perimeter security devices.

There are many types of firewall that can be used in today’s networks. Initially a decision must be made on the type of firewall to be used at the perimeter. Firewalls can be categorized into the following types: packet filtering, proxy, and stateful firewalls. In many cases, the organizational and network structure will dictate which type of firewall is deployed. In a hospital environment, a stateful firewall is typically the firewall of choice. This is because the stateful firewall keeps track of actual communications state tables which can be useful for IDS and various types of communications required in a hospital environment. Moreover, its ability to track connectionless protocols such as User Datagram Protocol (UDP) makes it a prime candidate for deployment at a hospital’s perimeter (Stauber, 2004). Although there are many types of firewalls deployed today, the stateful firewall is often best suited for the hospital security due to its ability to track communications and the use of continuously updated state tables.

Once the type of firewall has been chosen for the hospital perimeter, we must ensure that it is configured correctly so it performs the security that is expected. The first and most important step in securing the firewall is to turn off all unneeded services. These unused services could be exploited and therefore are an easy step to increase the

security at the perimeter. Another best practice which is often overlooked is changing the default settings. Default settings on things such as passwords, Simple Network Management Protocol (SNMP), services, and http are a few things if not changed can be exploited. Often a firewall is put in place with many of the default settings which makes it an easy target for potential hackers. Another important step in configuring the perimeter firewall for security is to disallow device management from the outside or un-trusted interface. By not allowing the device to be managed from outside of the network, we help to protect the device from being compromised and reconfigured. Security must be considered during the initial configuration of the perimeter firewall to help secure the hospital network.

When considering the perimeter security of the hospital, network architecture is key. One mechanism that should be considered during the design for the network perimeter is the use of Network Address Translation (NAT). Although there is no security in obscurity, by using NAT at the perimeter we help hide the internal network therefore increasing security at some levels (Convey, n.d.). Also, don't allow communications to be initiated from the outside or un-trusted interface. If it is necessary to make servers and devices available from outside, it is recommended that a Demilitarized Zone (DMZ) network be deployed or secure tunnels be used for these devices. The use of a DMZ network gives the ability to access devices without allowing outside devices onto the enterprise network. With this being done, if a device on the DMZ network is compromised, its effects on the hospital's core network are contained (Wilson, 2002). Although this is by no means an exhausted look at the perimeter design in a hospital, it is a look at a few steps that will help increase security.



An additional aspect of the perimeter firewall that must not be overlooked is Intrusion Detection Systems (IDS) and monitoring. Although many firewalls today offer integrated IDS, they are often underutilized or not used at all. If an IDS is integrated in the perimeter firewall, it must be properly configured to be effective. Sufficient time must be taken to ensure that this mechanism is working. Once the IDS is properly configured, it must be monitored. Often an IDS is put in place and never thought about again. An IDS is only effective if it is properly monitored and the data collected is analyzed, so we must implement procedures for this monitoring. With today's firewalls offering integrated IDS, it must be properly utilized and monitored to help secure the hospital perimeter.

An additional aspect of hospital perimeter security which must be considered is Remote Access. In today's hospital, remote access is a critical part of daily operations so steps must be taken to secure this access while still allowing for normal operation. Various devices that are included in this remote access are things such as Virtual Private Network (VPN) concentrators, VPN routers, Dial-In Servers, and many others. Because these remote access devices are acting as a gateway to our network, we must ensure that they are secure (Convey, n.d.).

There are many aspects that must be taken into consideration when securing remote access gateways. Many of the principles and practices used to secure perimeter firewalls must also be applied to remote access devices. Some differences in firewall and remote access security consideration given to access control and auditing must. Because the traffic is coming from different sources outside of the hospital, great detail must be taken to ensure that the users are authenticated and this access is audited (*TLC, HIPAA Overview*, n.d.).

One way to help with remote access authentication and auditing is to centralize administration. By using a centralized source for authenticating and logging, processes are streamlined and become more efficient. If users only have to be added in one place and logs can be viewed in a single place, administration of remote access is made easier and less likely to security vulnerabilities due to missed configuration or unviewed logs. One way this could be done is with a device such as Cisco Access Control server. This server gives the ability to do Authentication, Authorization, and Accounting for remote access in one central location. So although many of the security concerns addressed with firewalls can also be used with remote access devices, due to HIPAA as well as general security practices, great care must be taken when authenticating, authorizing, and accounting for remote access (*Cisco Secure Access Control*, n.d.).

In today's hospitals, things such as Internet connectivity and Remote Access are vital to daily operations. This importance along with the vulnerability of these devices require that they must be configured, placed, and monitored properly to help ensure they do not become a security liability to the hospital. Also, when designing security at the perimeter, consideration must also be given to things such as fault-tolerance and attack postures (Lundell, 2001). Although it has often been thought in the past that if a firewall is placed at the perimeter the hospital is secure, other aspects must be considered when designing, implementing, and maintaining a secure hospital perimeter.

### Network Segmentation

Often network segmentation is only considered in the hospital network when designing the network for efficiency and not security. Network segmentation can play a

huge role in the security of the hospital wired infrastructure. By using segmentation, security can be achieved through things such as path isolation and increased number of security boundaries. So although segmentation is necessary for an efficient network infrastructure, it can also be used to help secure the network.

Once thought of only as ways to isolate broadcast and to increase network efficiency and resiliency, Virtual Local Area Networks (VLANs) can be used to help secure the wired network infrastructure. By segmenting devices into separate VLANs on the hospital switches, the opportunity for security boundaries is increased. While devices on the same VLAN may have unrestricted access to each other, things such as Access Control Lists (ACLs) and firewalls can be put on the edge of the VLANs to restrict access to other VLANs therefore giving the opportunity for more security (*Network Segmentation*, n.d.). With this type of segmentation, things such as different departments, equipment, data centers, etc. can be restricted at the edge of the VLAN creating security boundaries. One area of a hospital that requires this type of Layer 2 isolation is Radiology equipment. Much of this equipment lacks the ability for protection at the endpoint so the network segment on which it resides must be secure. The use of VLAN segmentation allows for the restrictions to be applied closer to the source, therefore being more effective (*Virtual LAN Security*, n.d.).

Another aspect that must be considered when designing network segmentation to increase security is path isolation. Often traffic is segmented on the Layer 2 network through the use of VLANs but is often mixed together once it passes through a layer 3 device such as a router. Care must be taken to ensure that certain traffic is isolated on both the Layer 2 and 3 network segments. One case in where this would be necessary

would be “guest access”. This traffic should be segmented and completely isolated from hospital traffic throughout the network to ensure security. At no point in the network should this type of traffic be inter-mixed with hospital traffic. This can be achieved through design strategies such as network virtualization. By using network virtualization, complete traffic isolation can be achieved at both Layer 2 and Layer 3 network segments. By using traffic isolation throughout the hospital network, another layer is built into the wired network security architecture.

Although things such as network segmentation and isolation are often burdensome to design and implement, they can prove to be a great asset in the wired network security of any hospital. As stated by Olzak (2006), “at a minimum, network segmentation should result in a production segment and a restricted access segment” (pg. 1). As networks and the devices that they contain become more complex and diverse, great efforts must be taken to segment, isolate, and secure different traffic as it traverses the wired network.

### Network Access Control

In many hospital environments, great care is taken to design security at the perimeter while network access control on the internal network is often overlooked. Network access (or admission) control is allowing or denying network access based on predetermined criteria. This type of access control is often only considered in the context of things such as wireless networks and remote access. It is not until recently that network access control is becoming popular on the switch port level within the hospital’s wired infrastructure.

The most well-known and implemented piece of network access control is Identity Based Network Services (IBNS) and 802.1x. The IEEE (2004) offers the following description for network access control and 802.1x standard:

Port-based network access control makes use of the physical access characteristics of IEEE 802 Local Area Networks (LAN) infrastructure in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics and of preventing access to that port in cases in which the authentication and authorization process fails. (pg. 1)

So 802.1x gives the ability to allow network access based on credentials supplied by either the user or the device. This offers the ability to allow network access only to legitimate users at the front line, the switch port. Often, in many environments, everyone is allowed access to the network and access control is placed on devices such as servers. By pushing this access control to the port-level on the network, the security of the overall networking environment is increased because only authenticated devices or users are allowed access to the network (Meador, n.d.). With much of today's security threats coming from inside of the network, this type of access control gives the ability to authenticate users on the front line and help to increase the overall security of the core network.

Another aspect of network access control which must be considered is the security posture of the device connecting to the network. Often it is not enough to just verify who is accessing the network but what is accessing the network. With systems such as Cisco Network Access Control and Juniper Universal Clean Access, a device can be verified for

network access. This verification process can include checks for such things as Anti-virus, patches, and other security aspects (Lippis, 2006). By using such systems for network access, the device that is accessing the network can be tested for security compliance as well as the user. This ability to scan the device allows for compromised and un-secure devices to be denied at the edge of the network before affecting the entire infrastructure.

In many cases network access control is a very tedious task to deploy throughout a hospital but it can prove to be a major asset in infrastructure security. By authenticating and authorizing users and devices at the port level, potential security threats are eliminated before given the ability to impact the network infrastructure. As stated by Guo and Wang (2005),

LAN connections, traditionally considered trusted networks now also require higher levels of security. In fact, internal threats are ten times more financially damaging than external threats. (pg. 281)

With many of today's security threats coming from inside of the organization, this ability is becoming a necessary part of network security and also helping with HIPAA compliance.

### Network Infrastructure Equipment Security

A network infrastructure is only as secure as the equipment on which it runs. In securing a hospital's network infrastructure, equipment security must not be overlooked. If the equipment that runs the network is compromised, the entire hospital and the data which it contains is left vulnerable, so it is a major piece of the security puzzle.

The first thing that must be considered when looking at securing network equipment is access. Who and how access to the network equipment is controlled. HIPAA requires that equipment be housed in a secure location so put the equipment in locked environments wherever possible (*TLC HIPAA Overview*, n.d.). Also authentication and authorization must also be required for access and management of the network equipment. This is best done through a centralized authentication server such as Radius or TACACS+. Great care must also be taken to secure how the equipment is accessed. Wherever possible, eliminate insecure protocols such as telnet and http and use protocols such as Secure Shell (SSH) and HTTPS. Also, restrict access to only known device IP addresses through access control list. Many network segments and subnets have no need to manage network equipment so deny access from these networks. Wherever possible, use out-of-band management so that normal traffic and management traffic are not on the same segments (Convey, n.d.). Network equipment access security in management is critical to the overall security posture of the network infrastructure.

As mentioned earlier with perimeter firewalls unused services must be disabled to help secure network devices. Unused services on network devices are a potential security risk and should be disabled. If the services aren't used, no functionality is lost but security is gained if the services are disabled. These services will vary depending on the type and manufacturer of the device, but most manufactures document services to disable if not needed. So a good rule of thumb is to know your equipment and what it does and turn off everything else. Also, disable unused ports. An unused port that is enabled can potentially become an entry point for an attacker. So to help ensure the security of the network equipment as well as the overall network, disable all unused services and ports

on the network devices (Convey, n.d.).

### Conclusion

In today's hospital, increased reliance on the wired network infrastructure has made security a major part of every aspect of design, installation, and maintenance. Every effort must be made to secure the various levels of the network. In the past, network security was an afterthought. In today's network, it must be a major factor in every part of the network (*Cisco Medical Grade Network*, n.d.). This paper has given a birds-eye view of some practices to be considered when it comes to the hospital's wired network infrastructure. As this, or no other single document, is not be considered the key to hospital network security, it offers concepts to serve as guide to increase security and help insure HIPAA compliance.



References

\*Alomary, A.Y., Jamil, M.S., (2004, April). New trends on security infrastructure for Computer networks. *Proceedings of the IEEE on Information and Communication Technologies: From Theory to Applications, 2004, April 19-23, 2004 pp.19-23.*

Retrieved June 17,2006 from

<http://ieeexplore.ieee.org/ie15/9145/29024/01307620.pdf?isnumber=2902>

[4&prod=STD&arnumber=1307620&arnumber=1307620&ared=+73&ared=+74&ar](http://ieeexplore.ieee.org/ie15/9145/29024/01307620.pdf?isnumber=2902&prod=STD&arnumber=1307620&arnumber=1307620&ared=+73&ared=+74&ar)

[Author=Alomary%2C+A.Y.%3B+Jamil%2C+M.S.](http://ieeexplore.ieee.org/ie15/9145/29024/01307620.pdf?isnumber=2902&prod=STD&arnumber=1307620&arnumber=1307620&ared=+73&ared=+74&ar)

\*Convey, S., Trudel, B. (n.d.). *SAFE: A Security Blueprint for Enterprise Networks.*

Retrieved June 21, 2006, from

[http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe\\_wp.pdf](http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.pdf)

*Cisco Medical Grade Network Reference Architecture for Healthcare Enviroments.* (2005, December). Retrived June 22, 2006, from

[http://www.cisco.com/web/strategy/docs/healthcare/MGN\\_Architecture.pdf](http://www.cisco.com/web/strategy/docs/healthcare/MGN_Architecture.pdf)

*Cisco Secure Access Control Server for Windows.* (n.d.) Retrieved June 19, 2006 from

<http://www.cisco.com/en/US/customer/products/sw/secursw/ps2086/index.html>

\*Guo, Y., Wang, C. (2005, March). Autonomous decentralized network security systems.

*Proceedings of the IEEE on Networking Sensing and Control, 2005., March 19-22, 2005 pp.279-283.* Retrieved June 19, 2006 from

<http://ieeexplore.ieee.org/ie15/9887/31421/01461201.pdf?isnumber=31421&prod=>

STD&arnumber=1461201&arnumber=1461201&arSt=+279&ared=+282&arAuthor=Yanhui+Guo%2B+Cong+Wang

Gue, D. (n.d.). The HIPAA Security Rule (NPRM): Overview. Retrieved October 18, 2005, from <http://www.hipaadvisory.com/regs/securityoverview.htm>

*\*IEEE standard for local and metropolitan area networks - Port-based network access Control* (2004). Retrieved June 13, 2006 from [http://ieeexplore.ieee.org/ie15/9828/30983/01438730.pdf?isnumber=30983&prod=STD&arnumber=1438730&arnumber=1438730&arSt=+0\\_1&ared=+169&arAuthor](http://ieeexplore.ieee.org/ie15/9828/30983/01438730.pdf?isnumber=30983&prod=STD&arnumber=1438730&arnumber=1438730&arSt=+0_1&ared=+169&arAuthor)

Kincaid, Paul. (2004, August 14). *Protection at the Perimeter – One Link in the Defense-in-Depth Chain*. Retrieved June 17, 2006, from <http://www.infosecwriters.com/texts.php?op=display&id=212>

Lippis, N. (2006, May). *The Lippis Report Issue 59: Cisco's Network Access Control Troubles*. Retrieved June 12, 2006 from [http://www.lippis.com/index.php?/news/welcome\\_to\\_the\\_lippis\\_report/lr\\_59](http://www.lippis.com/index.php?/news/welcome_to_the_lippis_report/lr_59)

Lundell, J. (2001). A fault-tolerant approach to network security. *IEEE International Symposium on Network Computing and Applications, 2001*, pp.227. Retrieved June, 14, 2006 from <http://ieeexplore.ieee.org/ie15/7617/20766/00962536.pdf?isnumber=20766&prod=STD&arnumber=962536&arnumber=96253&arSt=227&ared=&arAuthor=Lundell%2C+J>.

Meador, W.J. (n.d.). *Port-based authentication with IEEE Standard 802.1x*. Retrieved June 15, 2006 from [http://www.infosecwriters.com/text\\_resources/pdf/802.1x.pdf](http://www.infosecwriters.com/text_resources/pdf/802.1x.pdf)

Mercuri, R.T. (2004). The HIPAA-potamus in Health Care Data Security. Association for Computing Machinery. *Communications of the ACM*, 47(7), 25-28. Retrieved , from ABI/INFORM Global database. (Document ID: 654995981).

*Network Segmentation*. (n.d.). Retrieved June 20, 2006 from [http://www.juniper.net/products/intergrated/network\\_segmentation.pdf](http://www.juniper.net/products/intergrated/network_segmentation.pdf)

Olzak, Tom. (2006, May 9). *Strengthen Data Protection with Network Access Controls*. Retrieved June 12, 2006, from <http://www.infosecwriters.com/texts.php?op=display&id=440>

\*Rabinovitch, E. (2003, August). Maintaining a secure networking infrastructure. *International Conference on Information Technology: Research and education 2003, August 11-13, 2003 pp.587-589*. Retrieved June 12, 2006 from <http://ieeexplore.ieee.org/ie15/8953/28360/01270687.pdf?isnumber=28360&prod=STD&arnumber=1270687&arnumber=1270687&arSt=+587&ared=+589&arAuthor=Rabinovitch%2C+E>.

Sood, A. (n.d.). *Perimeter Router Security*. Retrieved June 15, 2006 from [http://www.infosecwriters.com/text\\_resources/pdf/PRS.pdf](http://www.infosecwriters.com/text_resources/pdf/PRS.pdf)

Stauber, R. (2004, May). *Defense in Depth*. Retrived June 15, 2006 from <http://www.infosecwriters.com/texts.php?op=display&id=170>

*TLC HIPAA Overview*. (n.d.). Retreived November 1, 2005, from <http://www.mmctlc.com/hipaa.htm>

*Virtual LAN Security Best Practices*. (n.d.). Retrieved June 20, 2006, from [http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp\\_wp.pdf](http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.pdf)

\*Wilson, S.B. (2002, September 5). *What is a Firewall? A high level explanation of Firewall technologies and their features*. Retrieved June 20, 2006, from <http://www.infosecwriters.com/texts.php?op=display&id=12>