Securing medical networks

Ram Dantu, Assistant Professor, University of North Texas
Herman Oosterwijk, President, OTech Inc.
Prakash Kolan, Student, University of North Texas
Husain Husna, Student, University of North Texas

The Health Information Portability and Accountability Act of 1996 (HIPAA) imposes strict regulations on healthcare institutions and commercial vendors to indemnify clinical data against unscrupulous users. Security vulnerabilities concerning hospital information systems not only negatively impact patient healthcare, but may also represent a potential federal violation. For a comprehensive understanding of the security of a radiology communication network, a detailed survey of the Picture Archiving and Communication Systems (PACS) was compiled. In this paper, we present survey results and a set of recommendations for implementing PACS security.

The HIPAA regulations establish national standards on all healthcare systems, including digital medical imaging transactions. They outline a comprehensive risk analysis assisting in investigations of possible security breaches[1]. Such regulations are particularly important to medical imaging because picture archiving and communication systems (PACS), which handle the storage and distribution of medical images, provide easier access to a vast number of confidential records.

The global healthcare system

As PACS become more sophisticated, safeguarding this data has become even more challenging. Access and diagnosis methods require a strong security measures to safeguard patient privacy. We should therefore bring all of the separate medical entities into one global healthcare system to enable the proper flow of information while maintaining strict security policies to prevent unauthorised access[2]. These entities can range from a single medical device (such as a CT scanner) to an entire medical establishment (eg, a hospital).

Among these entities, PACS (which represent a network of image acquisition devices, display devices, storage devices, and imaging servers), plays a vital role in efforts to improve patient healthcare by providing radiologists and physicians with timely access to radiology exams and results.

> "A security threat to PACS may introduce many unforeseen security risks to the remaining network components"

A security threat to PACS may introduce many unforeseen security risks to the remaining network components. In particular, the confidentiality of patient data could be jeopardised. Images sent to doctors' homes after hours must be sent over encrypted communication links. HIPAA specifies encryption requirements in the technical safeguards rules.

The regulations also address the integrity of the data through a requirement for audit trails (also part of the technical safeguards), so that changes can be tracked. Typically, audit trails track any modification of the radiology workstations and archive. Availability is also addressed through a requirement for emergency access procedures. This can be as simple as an internal emergency access number for physicians, enabling them to gain access to any clinical information on the institution's workstations[3].

The PACS architecture survey

Although PACS administrators have made every attempt to restrain external access to these components, most security threats are ultimately generated from internal sources (e.g., viruses, trojans, and sniffers from the physician's workstation) or unexpected entities (e.g., access by vendor for maintenance)[4]. Therefore, as part of a larger effort to identify appropriate solutions to refine current PACS networks, topology, components, and access control, we developed a web-based survey to assess current PACS architectures and usages[5]. In this paper, we present results obtained from our survey and a set of suggestions to implement PACS security. The goals of our work are to obtain a comprehensive understanding of the hospital communication network, and to recommend configurations to implement PACS security.

It is anticipated that the results, observations, and suggestions presented here will provide sufficient information to compare an existing topology with a model topology and to understand the security gaps that may exist in an existing system. We hope that they will also provoke further discussion among the PACS community as we continue to discover strategies to refine the PACS architecture.

Depending on the size in which a HCF (Health Care Facility) operates, unique implementations of PACS and security strategies are essential to maintain the proper flow of clinical information. Larger healthcare institutions require dedicated, well-qualified IT departments, whereas smaller institutions often consist of a few staff with limited training. Therefore, the initial challenge of our research is to determine the general understanding of a typical PACS network configuration and use this understanding as a framework to identify the most critical PACS components.

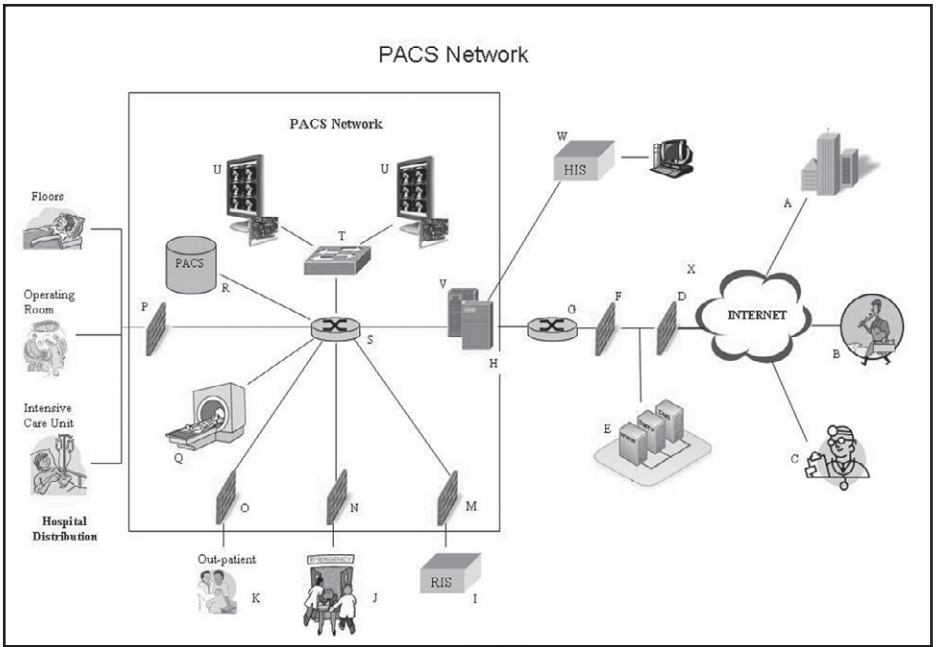

Figure 1: Typical secure PACS network diagram

Our survey included around 90 questions, addressing a wide range of topics in network topology, firewall management, IDS implementation, and remote access policies. These questions helped us to understand current hospital and radiology department parameter control and methods of isolating different segments within the hospitals.

Around 40 healthcare institutions ranging from 100 to 1000 beds with an annual radiology exam number varying between 50,000 to 1,000,000 per year completed the survey. We received responses from variety of experts, including PACS administrators, IT system administrators, radiologists, biomedical equipment repair specialists, and network solution designers. Our initial testing indicated that each participant needed approximately 20 minutes to complete the survey.

Results

After seeking input from experienced PACS administrators and other professionals within the hospital imaging informatics community, we constructed a typical secure PACS network diagram for the survey. Although the necessary resources to support the architecture at a HCF may differ greatly, each HCF has the same components in its PACS network. Table 1 shows the name of the components for every symbol used in our constructed PACS diagram and summarises the survey results. The symbols will be referenced throughout this article. In our survey, we found that 60% of the respondents agree with the network topology that includes layer 2 switches interconnecting the PACS workstations and modalities. In addition, a core router is interconnected with sub networks in the hospitals. Subnets related to outpatient ward, emergency room (ER), and radiology information system (RIS) are connected to the same router.

In addition to our observations on the current PACS network configuration, the process of our development to gather information from numerous sources (including the survey we conducted) significantly assisted us in recognising critical security concerns in the current PACS architecture and novel approaches to refine hospital network security in general[6].

Using NEMA gateway

The National Electrical Manufacturers Association (NEMA), in cooperation with other international standards organisations, proposed the use of a single gateway for remote service access as an entry point for a hospital network[7]. Our survey indicates that more than 60% of the participants have implemented gateways as part of their PACS networks. Among these institutions, many allow commercial vendors to install and have full control over these gateways instead of having their PACS administrator manage the access.

> "A single gateway managed by the hospital will be more efficient, but our survey indicates that only 32% of the respondents use a single gateway"

The effect of vendor-managed gateways is that HCFs often implement several gateways. In many cases, there could be one for each vendor that the hospital may associate with. For example, a HCF that uses devices from three vendors – one for magnetic resonance imaging, one for the special procedures room, and one for ultrasound – will have three or possibly more gateways implemented as part of their PACS networks.

Federal regulations require HCFs to check the audit logs trails on all devices in their networks, especially if any clinical data is accessed[8]. Therefore, having multiple gateways for different vendors will certainly be more expensive (we assume this cost is passed to the HCF) and the management procedures become much more complex. A single gateway managed by the hospital will be more efficient, but our survey indicates that only 32% of the respondents use a single gateway.

Comparing VPN: IPsec or SSL

More than 80% of our participants agreed that VPN technology is predominantly used to support secure remote

Components	Service implementation or management	Sample count	Yes %	No %	Un-Known%
Firewall	Isolating internal hospital network from the internet	38	94	3	3
(D,F,M,N,O,P)	Isolating RIS from the rest of the PACS network	31	0	71	29
	Isolating HIS from the rest of the PACS network	38	26	50	24
	Isolating PACS from the rest of the PACS network	38	24	50	26
	Isolating hospital gateway from the rest of the PACS network	37	41	27	32
	Performing maintenance and policy changes	33			
	Daily	64			
	Weekly	18			
	Monthly or quarterly	18			
Gateway (H,V)	Implementation of gateways	37	62	16	22
	Following NEMA recommendation of single gateway	37	32	14	54
IDS (Y,Z)	Detecting abnormal network activities	38	47	19	34
VPN	Supporting remote connectivity	35	86	8	6
	Supporting remote connectivity with dialup access	33	36	64	
	Using SSL for secure remote connection	29	66	24	10
	Using IPSEC for secure remote connection	29	55	35	10
DMZ (E)	Supporting access request to PACS network	33	6	45	49
VLAN	Supporting VLAN on the router	33	70	12	18
POLICIES	Supporting SNMP to service the network	35	43	14	43
	Supporting single sign-on	35	23	66	11

Table 1: Survey results and symbol guide for model PACS security configuration

access to clinical data. Therefore, to secure the exchange process of this vast amount of confidential data, PACS administrators often implement SSL technology at the transport layer. In addition, we suggest IP security (IPsec) as a more applicable solution in some contexts of the PACS network, whereby a secure "tunnel" is established at the network level. Table 2 shows the major differences between SSL VPN and IPsec VPN in the context of PACS security. The ✓ symbol denotes suitable PACS device/application.

Device/Application	SSL	IPsec
Type of connection	Transient	Fixed
Type of access	Remote physicians, service personnel	Site-to-site
Modalities	✓	
Remote physicians clinic		✓
IT staff	✓	
IT consultants	✓	
Mobile physicians	✓	
Service personnel	✓	
Remote hospitals		✓
Entire subnet with no application remote access		✓
DICOM application	✓	
RIS	✓	
HIS	✓	
PACS archive	✓	
HL7 application	✓	

Table 2: Different VPN implementations for PACS security

> "HIPAA requires that information regarding a patient's identity be removed or encrypted before that information is exchanged"

Recommendations and conclusions

The federal HIPAA requirements state that a U.S. Health Care Facility (HCF) must implement specific privacy and security measures to maintain the confidentiality of clinical data. It requires that information regarding a patient's identity be removed or encrypted before that information is exchanged. In addition, audit trials of system usages, performances, and all other activities must be maintained, as these data are used to identify potential unauthorised access. We suggest that implementation of audit trials should also be consistent and easily available at a consolidated, central location when the necessity arises.

Our findings and proposed suggestions in implementing PACS security provide an overview for further discussion and elaboration. HCFs can prevent the security vulnerabilities described in this publication by using open source or commercial software that has been customised for use in clinical environments. Based on our survey results and prior observations

while visiting institutions and discussing security vulnerabilities with PACS administrators, we present a set of recommendations for implementing PACS security. These extensive recommendations are not exclusive and should not be considered a comprehensive assessment of the HIPAA federal regulations:

- Conduct patient risk analysis while patching vulnerabilities[9,10]
- Work towards PACS-specific virus scanners
- Limit exposure to vulnerabilities with proactive test systems
- Deploy PACS-specific internal firewalls and NEMA gateways
- Protect network-specific patient information[11]
- Secure physician remote access
- Implement HL-7 and DICOM-specific intrusion detection and prevention systems
- Implement PACS monitoring and patient-specific audit logs

Security vulnerabilities in information systems of a healthcare infrastructure not only negatively affect the availability, integrity, and confidentiality of clinical data, but also represent a potential federal violation as stated in HIPAA. The model network diagram produced as a result of our survey does not have all the details of every kind of hospital but represents several important elements of the PACS network. The survey, completed by the IT staff from about 40 hospitals, revealed several important vulnerabilities and their relation to the capacity of the hospital. Based on our findings, we have proposed several recommendations. Further work will include adding more details to the survey and increasing the number of hospitals involved.

Acknowledgements

We would like to thank all our survey participants who spent their valuable time completing the lengthy survey. We would also like to thank Barco for providing the research grant for the survey. This research was also partially supported by NSF grants CNS-0516807 and CNS-0551694.

References

1. Frost and Sullivan, "Effects of HIPAA in U.S. Healthcare Markets", October 2002. January 2007 <www.researchandmarkets.com/reportinfo.asp?report_id=365197>.
2. Networking Health: Prescriptions for the Internet National Research Council, 2003.
3. Revolutionising Health Care through Information Technology, President's Information Technology Advisory Committee Report, June 2004, January 2007 <www.nitrd.gov/pitac/reports/20040721_hit_report.pdf>.
4. M.Loveless, "Internal security threats: Identification and Mitigation", Bind View Corporation, 2005.
5. Medical Security Survey, R. Dantu, University of North Texas, 2004. January 2007 < http://secnet.unt.edu/hospital_survey>.
6. R.Dantu and H.Oosterwijk, "A Blueprint for implementing security in Radiology", AHRA Workshop for PACS Administrators, April 2005.
7. Security and Privacy Requirements for Remote Servicing, Joint NEMA/COCIR/JIRA Security and Privacy committee (SPC), 2001.
8. Security Standards for Health Information, Health Information Portability and Accountability Act (HIPAA), Section 1173 (d), 1996. January 2007 <http://aspe.hhs.gov/admnsimp/pl104191.htm#1173>.
9. R. Dantu, K. Loper, and P. Kolan, "Risk Management using Behavior-based Attack Graphs", IEEE International Conference on Information Technology, April 2004.
10. Defending Medical Information systems against malicious software, Joint NEMA/COCIR/JIRA Security and Privacy committee (SPC), 2003.
11. Patching Off-the Shelf Software Used in Medical Information Systems, Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), NEMA, October 2004. January 2007 <www.nema.org/prod/med/security/upload/Patching_OffTheShelfSoftware_Used_in_MedIS_October_2004.pdf>.

About the authors

Ram Dantu *has 20 years of experience in the networking industry, working for Cisco, Nortel, Alcatel, and Fujitsu. For the last five years, he has been researching the prevention of DoS and spam attacks in VoIP networks. He is currently an assistant professor in the department of computer science and engineering at the University of North Texas (UNT). In addition to more than 70 research papers, he has authored several RFCs related to MPLS, SS7 over IP, and routing. Due to his innovative work, Cisco and Alcatel were granted a total of 12 patents. Another eight are pending.*

Herman Oosterwijk *is president of OTech Inc. (www.otechimg.com) a healthcare technology consulting and training firm, specialising in PACS. Herman has published several textbooks and study guides on the subject of PACS and image and information communication standards and teaches and presents about this subject extensively both on a national and international level.*

Prakash Kolan *is a PhD candidate majoring in computer science at the University of North Texas. He received a Bachelors degree from JNT University, India. His research areas include VoIP security, intrusion detection and artificial intelligence.*

Husain Husna *is presently enrolled in Masters Program majoring in computer science at the University of North Texas. He is a research assistant in the network security lab. His research areas include the detection of spammers and botnets.*