International Journal of Future Generation Communication and Networking
Vol. 7, No. 6 (2014), pp. 241-250
http://dx.doi.org/10.14257/ijfgcn.2014.7.6.22

Security Threats among DICOM Imaging Communications in Public Networks

Feng Zhou[1], Zhongqi Zhang[2], Jin Wang[1], Bin Li[1] and Jeong-Uk Kim[3]

[1]College of Information Engineering, Yangzhou University, Yangzhou 225009, China
[2] School of Computer & Software, Nanjing University of information science & technology, Nanjing 210044, China
[3] Department of Energy Grid, Sangmyung University, Seoul 110-743, Korea

Abstract

Picture archiving and communication systems (PACS) require high-speed networks to transmit large image files between components. Image-data transmission from one site to another through public network is usually characterized in term of privacy, authenticity, and integrity. However, public network's security issues had always been the significant problems. Recent years, IPv6 brings significant improvements in mechanisms for assuring a higher level of security and confidentiality of the transmitted information. Thus, it is still necessary to take care of some particular aspects. In this paper, we first analyzes how actual security threats and different types of attacks affect IPv6 networks while transmitting Digital Imaging and Communications in Medicine (DICOM) files through the public Internet. Second, illustrate some shortcomings of IPv6 and IPv6's traffic loads. Finally, some possible solutions against a number of security threats in IPv6 DICOM files transmitting networks have been given.

Keywords: *DICOM, security, IPv6, possible solutions*

1. Introduction

Digital Imaging and Communications in Medicine (DICOM) is a standard for handling, storing, printing, and transmitting information in medical imaging. DICOM includes a file format definition and a network communications protocol. The communication protocol is an application protocol that uses TCP/IP to communicate between systems, and the National Electrical Manufacturers Association (NEMA) holds the copyright to this standard [1-2].

Optimal patient care requires timely access to all relevant patients' clinical information. Despite the advanced state of technology, heterogeneous systems gather and store patient information and yet do not communicate effectively [3-4].

In case of network inside the hospital or institution, that is, PACS within a hospital or institution, Gb/s switches with Mb/s connections to workstations are mostly adequate and is a standard in most hospital and university network infrastructures. Their transmission rates, even for large-image files, are acceptable for clinical operation.

However, in case of using the public networks for teleradiology applications or enterprise PACS, image data must be transmitted from hospitals to hospitals or campuses to campuses. In this case, there are two important issues that need to be discussed when DICOM file transmissions are over public networks: the first issue is the cost efficiency, and the second one is data security. Up to now, low-cost commercial wide-area network (WAN) is too slow for medical-imaging application, whereas high-speed WAN is too expensive for cost-effective use.

To solve the first problem, the broadband high-speed Internet technology with new

ISSN: 2233-7857 IJFGCN
Copyright ⓒ 2014 SERSC

communication protocol IPv6 emerges as a potential solution with high-speed networks and acceptable cost for image-data transmission [5].

However, the security of IPv6 protocol is therefore of fundamental significance within the framework of the critical infrastructure protection. We can conclude the reasons as: first, for now the picture archiving and communication system (PACS) infrastructure is founded on IPv6; second, the supervisory control and data acquisition capabilities for industrial control and monitoring systems would increasingly depend upon the PACS infrastructure; third, IPv6 is the basis for vital services such as the picture communications, the voice and video collaboration, and sharing of data such as the surveillance and reconnaissance data [6].

In this paper, first, we describe a general scenario about how image is delivered from one site to another through public networks with security features of data privacy, integrity, and authenticity. Second, we discuss the security layer which contains the application security, service security, and infrastructure security. Third, we illustrate some shortcomings of IPv6 and IPv6's traffic loads. And finally, we will discuss some problems in real world implementation with some possible solutions. Hopefully, at the end of our paper, you can acquire a good knowledge of the security issues about DICOM file transmitting among public networks, and some knowledge about how IPv6 protocol handles the potential threats and some possible solutions.

Organization of the paper: The main content of this paper is constructed in 5 sections as follows: Section 2 gives an overview about general scenario about how image is delivered from one site to another through public networks. Section 3 describes the security layer which contains the application security, service security, and infrastructure security, besides Section 3 describes some shortcomings of IPv6 and IPv6's traffic loads. Section 4 discusses some possible solutions to the real world implementation DICOM communication networks. Finally, Section 5 concludes our work.

2. Research status

DICOM Image Information Model is based on assumptions about the way in which information from different modalities is related; see Figure 1[7]. The four levels of this information model are Patient, Study, Series and Image.

Each of the DICOM image have Patient Register information such as Patient Name, Patient ID, such as unique id generated for a hospital, Patient Date Of Birth, Sex, Age and insert time stamp information. Besides, some Patient Administration information is also needed, such as study information or series images number. All these information are used for DICOM Search operation. When any DICOM image is being archived, it extracts using DICOM tag and stores in the database for the search operation in the PACS system.

Figure 2 shows a data flow of image secure delivering from one site to another through the WAN [8]. There are two main functions to process steps for providing secure measures on the delivered images: First, for the data integrity and authenticity, the digest (or hash computing on data) and digital signature, as well as decoding signature and comparing digest, on the images before and after transferring are performed at both the sending and the receiving sites. Secondly, for data privacy, the secured communication channels are provided to transmit the image through networks.

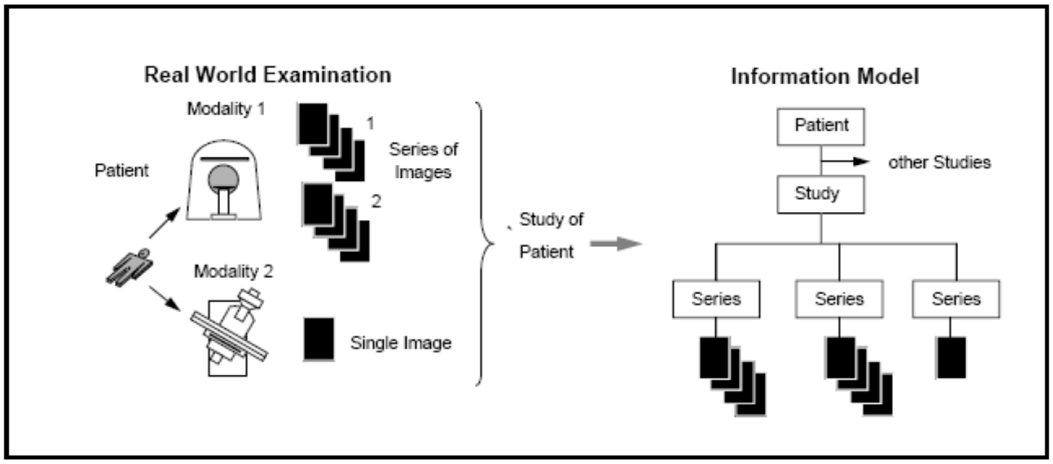


Figure 1. Mapping Real World Examination to Information Model

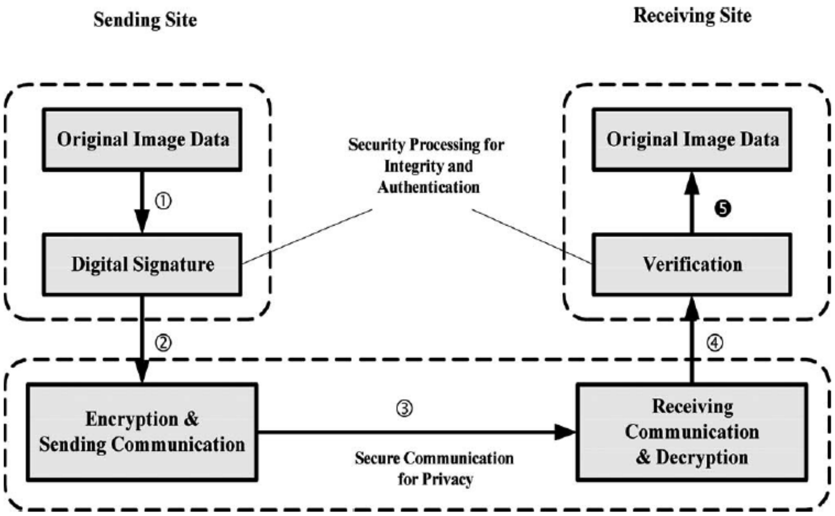

Sending Site
Receiving Site
Original Image Data
①
Digital Signature
Security Processing for Integrity and Authentication
Original Image Data
❺
Verification
②
④
Encryption & Sending Communication
③
Secure Communication for Privacy
Receiving Communication & Decryption

Figure 2. Data flow of medical image secure communication from one site to another through public Internet

To provide comprehensive, end-to-end security solutions, Lucent Networks came up with the concept of security layer which consists of services that customers receive from service providers [9]. These services range from basic transport and basic Internet connectivity (*e.g.*, Internet access), IP service enablers such as authentication, authorization, and accounting (AAA) services, dynamic host configuration services, and domain name services to value-added services such as voice over IP, quality of service (QoS), virtual private networks(VPNs), location services, 800-services, and instant messaging (IM). Note that at this layer the end users as well as the service provider itself are potential targets of security threats. For example, an attacker may attempt to deny the service provider’s ability to offer the service, or the attacker may attempt to disrupt service for an individual customer of the service provider.

Figure 3 [9] depicts the security layers as a series of enablers for secure network solutions: the infrastructure layer enables the services layer, and the services layer enables the

Copyright ⓒ 2014 SERSC

applications layer. In addition, the Network Security Framework recognizes that each layer has unique security vulnerabilities, which result in potential security threats and attacks if they are not addressed. It should be noted that our network security layers represent a separate category that is orthogonal to the layers of the Open Systems Interconnection (OSI) reference model [10].

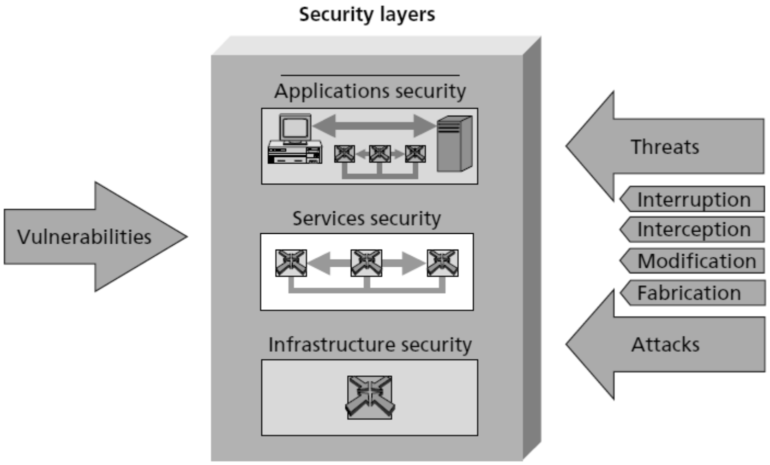


Figure 3. Security layers as a series of enablers for secure network solutions

However, there are still some problems that Lucent Networks dose not taken cares of, for instance, peer-by-peer options, auto configuration, multiple addresses, and IPv6 filtering [6]. In the following paragraphs we will illustrated them in detail.

Peer-by-peer Options: The peer-by-peer options header can have any number of peer-by-peer options, and any option can appear multiple times. An attacker can deliberately use inconsistent option values or invalid options in a peer-by-peer option header. In such situations Parameter Problem ICMPv6 error messages are issued to the sender. An attacker can burden the routers by flooding with such maliciously crafted packets, causing a DoS attack.

There is another vulnerability related to the options in a peer-by-peer options header. The header uses Pad1 and PadN options and these padding bytes must be zero filled. However there is no requirement for the receivers or the routers to verify the correct implementation of that. The options in a peer-by-peer options header may therefore serve as a covert communication channel. This can happen via non zero fill padding bytes. It can also happen because of the pattern in which padding and other options are used. Such a pattern may itself communicate covert channel information. For example, using multiple Pad1's instead of a single PadN, or a PadN followed by a Pad1 may communicate information.

Auto Configuration: State-Less Address Auto Configuration [11] is a distinguishing feature of IPv6. However, state-less address auto configuration also raises serious security concerns. One of the concerns about SLAAC is its trust model with respect to the network trusting a node that auto configures itself [12]. A node can acquire a link-local address and subsequently a globally routable address without any approval or control. A new IPv6 node that auto configures itself is allowed an unchecked access to the link. This unchecked access is not limited to the local link because a node can subsequently acquire a global prefix using solicitation and advertisementICMPv6 messages for Neighbor Discovery (ND) [13].

Copyright ⓒ 2014 SERSC

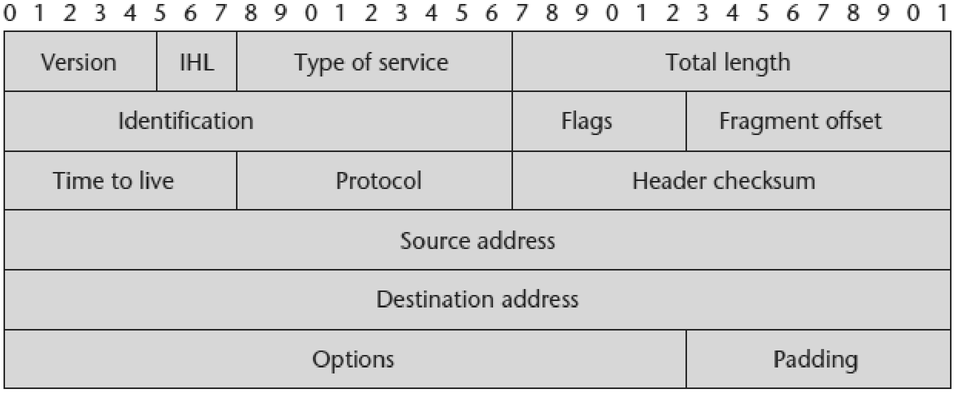
Combining the global prefix with the link local address, the node can construct a globally routable address and start using it without any approval or control. This trust model introduces serious security vulnerabilities and possibilities of attacks [12]. As discussed in this reference, there are about a dozen types of attacks that are possible on the auto configuration feature of IPv6. A variety of approaches are required to mitigate these risks: the on-link ND messages should be filtered at the boundary [14]; the SEND protocol [15] should be used to avoid attacks that use address spoofing; and other filtering mechanisms [16, 17] can be applied.

Multiple Addresses: IPv6 assigns multiple addresses to an interface which challenges the filtering rules in the firewalls and access control lists. This is because, unlike IPv4, address based filtering is no longer feasible when these addresses are auto configured, and when privacy addresses are used (privacy addresses change periodically). In such cases, a firewall will need to learn all the addresses dynamically and the filtering rules will need to be automatically generate-able using sophisticated policy rule sets. Such capabilities are not available. Therefore simpler formalisms must be employed that use some kind of identification tokens instead of addresses in order to identify a host or an interface. No such identification mechanism is currently defined at OSI layer.

ICMPv6 Filtering: The use of ICMPv4 messages in IPv4 is optional. It is not required for normal network operation. Many IPv4 network security administrators block all ICMPv4 messages. This blanket blocking is not possible for IPv6 networks because basicIPv6 network operation require the use of ICMPv6 messages. Therefore specific ICMPv6 traffic must be allowed and theIPv6 firewalls must not apply a blanket blocking of ICMPv6messages. Firewalls with the needed IPv6 filtering capabilities are not yet available. Since some ICMPv6 traffic must be allowed, an attacker can use deliberately malformed ICMPv6 packets to cause error responses that spuriously utilize network resources. IPv6 sends the ICMPv6 messages also to multicast addresses, which offers a potential for DoS attack through packet amplification.

Network traffic loads is another significant problem in our discussion. To analyze network traffic, we need a basic understanding of its composition. In this regard, networking people often speak of flows and formats. Flow is a laconic reference to networking protocols and the messages that travel back and forth between their endpoints. Format refers to the structure of the cells, frames, packets, datagrams, and segments that comprise the flow. The vast majority of network traffic today uses the Internet Protocol (IP) as its network-layer protocol. IP addresses represent sources and destinations, and IP routers work together to forward traffic between them. Link-layer protocols such as Ethernet, token ring, frame relay, and asynchronous transfer mode (ATM) forward IP packets, called datagrams, across many types of links. Fig. 3 shows the format for an IP datagram; Fig. 4 shows the format for a TCP segment, which is the protocol data unit associated with the TCP protocol. These formats are essential for understanding network traffic composition and something of the methods that can be send to corrupt them. TCP/IP traffic accounts for much of the traffic on the Internet.

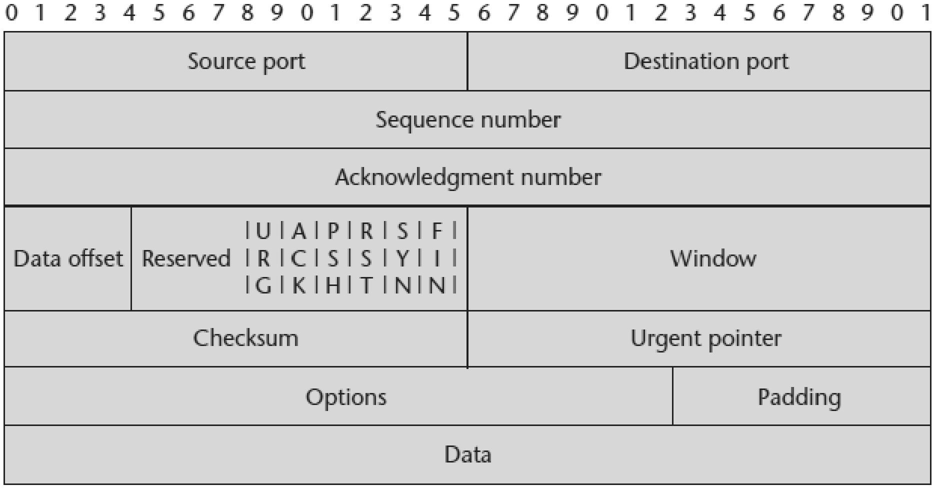
We now have a fairly representative picture of the traffic flowing across the Internet. It consists of IP datagrams (which can be carried inside link-layer frames, for example) carrying higher-layer information, often including TCP segments. Those with malicious intent could misuse any of the fields shown in Figure 4 and Figure 5 [18]. The attackers would know the protocol’s intent and the rules to use to interpret the associated formats and flows. They can create a networking attack by changing values in any of the fields—any ensuing problems constitute attacks on the network. Spoofing, or changing the source address, lets an attacker disguise malicious traffic’s origin.



0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Version	IHL	Type of service	Total length
Identification		Flags	Fragment offset
Time to live	Protocol	Header checksum	
Source address			
Destination address			
Options			Padding

Figure 4. Internet datagram header format. As defined in RFC 791, Internet datagrams running under version 4 of the Internet Protocol (IPv4) carry most of today’s Internet traffic, although a newer version has been defined as IPv6. (The numbers across the top indicate bit positions.)



0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Source port			Destination port
Sequence number			
Acknowledgment number			
Data offset	Reserved	U A P R S F R C S S Y I G K H T N N	Window
Checksum			Urgent pointer
Options			Padding
Data			

Figure 5. Transport Control Protocol header format. As defined in RFC 793, TCP provides a reliable end-to-end transport service across the unreliable Internet

3. Problem in DICOM Image Transmission

Hospitals and Institutions are usually equipped with a computer room; there are some computers which can directly access to the campus computer network in this room, doctors and faculty are usually available to use these computes to access to internet to get information and learn online. However, the lack of unified management software and system for monitoring and logging, these computer rooms can't be essential in the management state. Most rooms have serious flaws in registration and management system, so the internet user’s identity cannot be recognized. Its very convenience for us to use functions provided by the hospital network, but it also has become a quick way to transfer the virus. Network virus

Copyright ⓒ 2014 SERSC

outbreaks can led directly to the user's privacy and important data leaks. Network virus is also a great consumption of network resources, resulting in a sharp decline in network performance, even can severely bring down the network performance.

In the hospital network, attacks, intrusion the machines, theft of another account, the illegal use of the network, illegal access to unauthorized files, harassment by mail and other incidents often occur, and so on, indicating the users' safety consciousness in the hospital network are very unimpressive. Most serious problem is the shortage of funds for the network construction in college or university, limited funds are mainly invested in network equipment, systematic input for construction and management of network security has not been taken into account seriously. Because of lack of the awareness in major hospitals, management institutions are not perfect, administration system is imperfect, management technology is not advanced; these factors make the hospital's network management center can't take any measures and preventive measures for information security. Meanwhile, countries do not have well-developed and rigorous network security system, there is no strict implementation of standards for the hospitals network security management; this is an important reason forth proliferation of network security.

By the analysis above, the hospitals network security issues is mainly in the following areas: Password disclosure can result in data leakage. A variety of database systems is running on-line in the hospitals network, such as teaching management system, student achievement management system, hospitals employee card management system, test bank and so on. The user personal misconduct or negligence of safety measures can lead to these database password be lost, the data may be illegally removed or replicated, resulting in information disclosure, in serious circumstance, may result in serious illegal deletion of data. Therefore, setting password is also very important.

Hospitals networks can connect with the internet with routers; of course, internet users can enjoy the convenience of fast and unlimited resources of this platform, but also have to face to the risk of an attack. There is a considerable security risk within the hospitals network, internal users are relatively understand more about the network structures and applications of models than the external users, therefore the internal security threats are the main threats. At present, hacking tools flooded in the Internet, hackers use network protocols, server and operating system security vulnerabilities and management oversight to illegally access to network resources, deletion of data, damage the system, these attacks caused to the adverse effects of the campus network of and the damage to the reputation of the school.

4. Possible solutions

As can be seen in Figure 6 [9], a security program which consists of policies and procedures in addition to technology, progresses through three phases, the definition and planning phase, the implementation phase, and the maintenance phase over the course of its lifetime. The Network Security Framework can be applied to security policies and procedures, as well as to technology, across all three phases of a security program.

The Lucent Network Security Framework can guide the development of comprehensive security policy definitions, incident response and recovery plans, and technology architectures by taking into account each security dimension at each security layer and plane during the definition and planning phase. The Network Security Framework can also be used as the basis of a security assessment that would examine how the implementation of the security program addresses the security dimensions, layers, and planes as policies and procedures are rolled out and technology is deployed. Once a security program has been deployed, it must be maintained to keep current in the ever-changing security environment. The Network Security Framework can assist in the management of security policies and procedures, incident response and recovery plans, and technology architectures by ensuring that modifications to the security program address each security dimension at each security layer and plane.

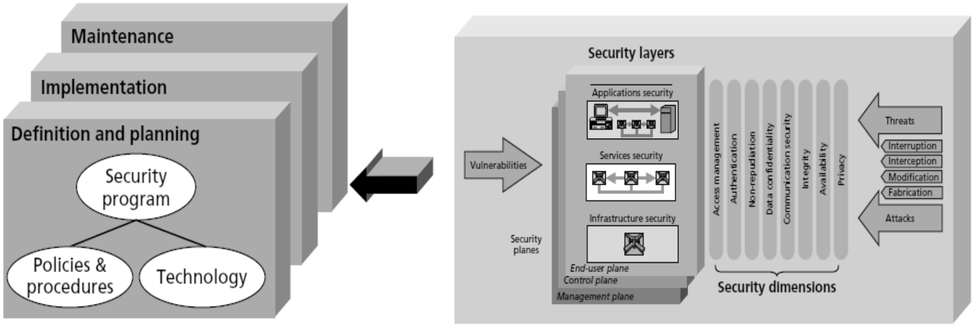


Figure 6. Applying the Network Security Framework to security programs

Another possible solution is intrusion detection in ipv6 networks. Intrusion Detection System (IDS) is a hardware or software system for supervision and analysis of different events occurring in the network or on the particular host. The purpose of the IDS system is to find potential security problems and to detect an unauthorized intrusion and misuse of network resources.

There are two main types of IDS systems: Host-Based IDS systems (HIDS) and Network-Based IDS systems (NIDS). The NIDS system captures and analyzes network traffic on a whole local network or a network segment protecting many hosts simultaneously. The HIDS system protects a single host. For achieving maximum level of protection it is recommended to install the HIDS system at every host in local network networks. The NIDS system should be implemented on every segment (subnet) of local network networks or at least between local network networks and the Internet. Such placement of HIDS and NIDS systems enables detection of outside attacks such as unauthorized activities of local users.

For IPv4 networks exists some open source IDS systems. By using software IDS systems in IPv4 networks, procedure of intrusion detection can be automated. In that case intrusion attempt will be recognized and logged by IDS system and user will be warned. Unfortunately, the situation considering IPv6 support by non-commercial IDS systems is not so good. There are several commercial IDS systems with IPv6 support, but no freeware known to authors (November 2005).

Since there is no freeware IDS software for IPv6 networks, we considered a possible method for intrusion detection by using packet capturing tool (network analyzer). By using this method, an intrusion detection procedure will not occur automatically (unlike automated intrusion detection in IPv4 networks with appropriate IDS tools). This method of intrusion detection will require an educated administrator who will be able to recognize attempt of intrusion from captured pattern of network traffic.

IPv6 supporting the IDS system must consider some new things typical of the IPv6protocol. IPv6 defines a new header format that the IDS system must properly recognize. In order to simplify the main header, IPv6 introduces extension headers (such as Hop-by-hop, Routing, Fragment, Destination Options, Authentication, and Encapsulation Security Payload). A Next Header format also allows new types of IPv6 extension headers to be defined and implemented. The IDS system must implement support for these types of headers. A proper header order is also defined, thus it is

Copyright ⓒ 2014 SERSC

desirable for IDS to check the order of extension headers. It is recommended for IDS to discard a packet with an undefined "Next Header" value and to record this as incident.

5. Conclusions

In this paper, we introduce and analyze a lot of factors and potential factors which intimidate the security of hospitals network’s transmission of DICOM files, and gives advices on how to build up the systems of campus networks from management and techniques. As lots of hospitals and institutions construct their own local networks to transmit DICOM files, and the application of local networks becomes more and more widely, information security is an inevitable factor to ensure the networks running smoothly and maximize its functions. Providing a well informational environment is the strong backup of model hospital works and hospitals networks is the hardware guarantee of the environment. Hence, how to make the campus networks running with high efficiency is an important issue in our future work.

Acknowledgements

This work was supported by the Industrial Strategic Technology Development Program (10041740) funded by the Ministry of Trade, Industry and Energy (MOTIE) Korea. It was also supported by the National Natural Science Foundation of China (61402234). Prof. Jeong-Uk Kim is the corresponding author.

References

[1] http://en.wikipedia.org/wiki/DICOM#Port_numbers_over_IP

[2] S. C. Horii and W. D. Bidgood, DICOM: a standard for medical imaging, in Proc. SPIE Int. Soc. Optical Engineering, (**1992**) Sep 8, USA.

[3] R. Noumeir, DICOM Structured report document type definition, IEEE Transactions on Information Technology In Biomedicine, Vol. 7, No. 4, December (**2003**)

[4] Supplement 23: Structured Reporting, DICOM (Digital Imaging and Communications in Medicine). (2000). ftp://medical.nema.org/medical/ dicom/final/ sup23_ft.pdf [Online]

[5] H. K. Huang, Communications and networking, in PACS and imaging informatics. Hoboken, NJ: Wiley-Liss, (**2004**).

[6] A.R. Choudhary, A. Sekelsky, Securing IPv6 network infrastructure: A New Security Model, Technologies for Homeland Security, IEEE International Conference on, (**2010**) Nov. 8-10,Waltham, MA

[7] B.K. Sahu, R. Verma, DICOM search in medical image archive solution e-sushrut chhavi, the 3rd International Conference on Electronics Computer Technology, (**2011**) April 8-10, Kanyakumari, India

[8] J.G. Zhang, F.H. Yu, J.Y Sun, and Y.Y. Yang, DICOM image secure communications with internet protocols IPv6 and IPv4, IEEE Transactions on Information Technology In Biomedicine, 11, 1, (**2007**)

[9] A.R. McGee, S.R. Vasireddy, C. Xie, D.D. Picklesimer, U. Chandrashekhar, and S.H. Richman, A framework for ensuring network security, Bell Labs Technical Journal, 8, 4, (**2004**)

[10] International Organization for Standardization, “Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model,” ISO/IEC Standard 7498-1, (**1994**) <http:// www.iso.org>.

[11] IETF RFC 4862, IPv6 Stateless Address Auto configuration, (**2007**)

[12] IETF RFC 3756, IPv6 Neighbor Discovery (ND) Trust Models and Threats, (**2004**)

[13] IETF RFC 4861, Neighbor Discovery for IP version 6 (IPv6), (**2007**)

[14] IETF RFC 4890, Recommendations for Filtering ICMPv6 Messages in Firewalls, (**2007**)

[15] IETF RFC 3971, Secure Neighbor Discovery (SEND), (**2005**)

[16] IETF Internet Draft draft-nward-ipv6-autoconfig-filtering-ethernet-00, (**2009**)

[17] O. McGann, IPv6 Packet Filtering, a Master’s Thesis at Department of Electrical Engineering, National University of Ireland Maynooth, Supervised by David Malone, (**2005**)

[18] M. Howard, A. Whittaker, Network Security Basics, IEEE COMPUTER SOCIETY, (**2005**)

Authors

Feng Zhou He obtained his B.S. degree in the computer science and technology major from Jiangsu University of Science And Technology in 2002. He is now an experimentalist in College of Information Engineering, Yangzhou University. His current research interests are in wireless networks, and hardware design and implementation.

Zhongqi Zhang He obtained his B.S. degree in the Eletronic and Information Engineering from Nanjing University of Information Science and technology, China in 2012. Now, he is working toward the M.S. degree in the Computer and Software Institute. His current research interests are in performance evaluation for wireless sensor networks, and healthcare with wireless body area networks. He is a student member of ACM and CCF.

Jin Wang He received his B.S. and M.S. degree from Nanjing University of Posts and Telecommunications, China in 2002 and 2005, respectively. He received Ph.D. degree from Kyung Hee University Korea in 2010. Now, he is a professor in the College of Information Engineering, Yangzhou University. His research interests mainly include routing protocol and algorithm design, network performance evaluation and optimization for wireless ad hoc and sensor networks. He is a member of the IEEE and ACM.

Bin Li He received the B.S. degree in Computer Software from Fudan University, China in 1986, M.S. and Ph.D. degrees in Computer Application Technology from Najing University of Aeronautics & Astronautics, China in 1993 and 2001 respectively. He is now a professor in the College of Information Engineering, Yangzhou University. He has published more than 100 journal and conference papers. His main research interests include artificial intelligence, multi-agent system and service oriented computing. He is a member of the IEEE and ACM.

Jeong-Uk Kim He received his B.S. degree in Control and Instrumentation Engineering from Seoul National University in 1987, M.S. and Ph.D. degrees in Electrical Engineering from Korea Advanced Institute of Science and Technology in 1989, and 1993, respectively. He is a professor in SangMyung University in Seoul. His research interests include smart grid demand response, building automation system, and renewable energy.

Copyright ⓒ 2014 SERSC