Journal of Signal and Image Processing
ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 2, 2012, pp.-93-96.
Available online at http://www.bioinfo.in/contents.php?id=48

DICOM IMAGE SECURE COMMUNICATIONS WITH INTERNET PROTOCOLS IPv6

THAKARE A.O.

M.E. Computer Science and Engineering Dept., Sant Gadge Baba Amravati University, Sipna C.O.E.T., India.
*Corresponding Author: Email- aothakare@rediff.com

Received: March 15, 2012; Accepted: April 12, 2012

Abstract- Image-data transmission from one site to another through public network is usually characterized in term of privacy, authenticity, and integrity. In this paper, we first describe a general scenario about how image is delivered from one site to another through a wide-area network (WAN) with security features of data privacy, integrity, and authenticity. Second, we give the common implementation method of the digital imaging and communication in medicine (DICOM) image communication software library with IPv6/IPv4 for high-speed broadband Internet by using open-source software. Third, we discuss two major security-transmission methods , the IP security (IPSec) and the secure-socket layer (SSL) or transport-layer security (TLS), being used currently in medical image- data communication with privacy support. Fourth, we describe a test schema of multiple-modality DICOM-image communications through TCP/IPv4 and TCP/IPv6 with different security methods, different security algorithms, and operating systems, and evaluate the test results. We found that there are tradeoff factors between choosing the IPsec and the SSL/TLS-based security implementation of IPv6/IPv4 protocols. If the WAN networks only use IPv6 such as in high-speed broadband Internet, the choice is IPsec-based security. If the networks are IPv4 or the combination of IPv6 and IPv4, it is better to use SSL/TLS security. The Linux platform has more security algorithms implemented than the Windows (XP) platform, and can achieve better performance in most experiments of IPv6 and IPv4-based DICOM-image communications. In teleradiology or enterprise-PACS applications, the Linux operating system may be the better choice as peer security gateways for both the IPsec and the SSL/TLS-based secure DICOM communications cross public networks.

Keywords- Data security, digital imaging and communication in medicine (DICOM) communications, Internet IPv6 and IPv4 protocols, picture archiving and communication system (PACS).

Citation: Thakare A.O. (2012) DICOM Image Secure Communications With Internet Protocols IPv6. Journal of Signal and Image Processing, ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 2, pp.-93-96.

Introduction

A picture archiving and communication system (PACS) requires high-speed networks to transmit large image files between components. In case of intranet, that is, PACS within a healthcare campus, 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 Internet for teleradiology applications or enterprise PACS, image data must be transmitted between hospitals and campuses. There are two important issues that need to be addressed when medical-image transmissions are over public Internet: the first issue is cost effectiveness, and the second is data security. The current 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 communication protocol IPv6 emerges as a potential solution with high-speed networks and acceptable cost for image-data transmission [1]. For security issue, there are certain critical features that need to be addressed in image-data exchanging through WAN between application entities, i.e., data privacy, authentication, and integrity. There are three organization-issued guidelines, mandates, and standards for image/data security.

First, the American College of Radiology (ACR) standard for teleradiology, adopted in 1994, defines guidelines for qualifications of both physician and non physician personnel, equipment specifications, quality improvement, licensure, staff credentialing, and liability the DICOM Standard specifies security profiles and technical means for application entities involved in exchanging information to implement security policies there have not been active systematic research and development efforts in the medical-imaging community to seriously tackle the secure DICOM image communication over the Internet protocols IPv6/IPv4 and evaluate their performance with different secure methods and various algorithms used to encrypt the image data for privacy and authentication.

In this paper, first, we describe a general scenario about how image is delivered from one site to another through a WAN with security features of data privacy, integrity, and authenticity. Second, we describe the implementation method of the DICOMimage-communication-software library with IPv6/IPv4 with open-source software. Third, we discuss two major security transmission methods, the IP security (IPSec) and the secure socket layers (SSL) or transport-layer security (TLS), used in medical image data communication with privacy support. Fourth, we design a test schema of DICOM-image communications Through TCP/IPv4 and TCP/IPv6 with different security channels, different security algorithms, and operating systems, and evaluate the test results. Finally, we discuss the outcome of our research results and clinical applications.

Secured-Image Communication Through Wan

Secure transmission of image data from one site to another through public networks is usually characterized in terms of privacy, authenticity, and integrity. Privacy refers to denial of access to information to unauthorized individuals. Authenticity refers to validating the source of a message, that it was transmitted by a properly identified sender. Integrity refers to the assurance that the data was not modified accidentally or deliberately in transit, by replacement, insertion, or deletion. Fig. 1 shows a data flow of image secure delivering from one site to another through the WAN.

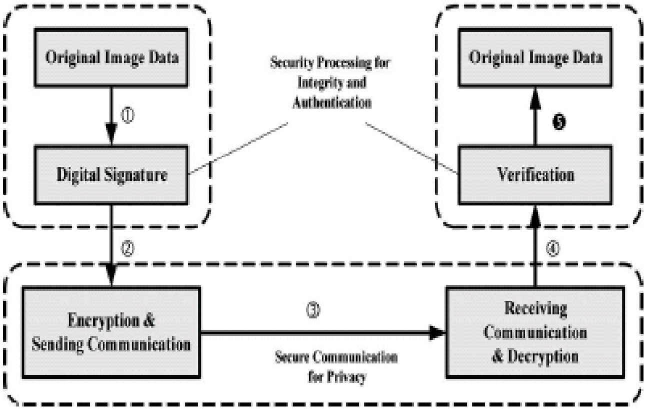
Original Image Data
①
Digital Signature
Security Processing for Integrity and Authentication
Original Image Data
❺
Verification
②
④
Encryption & Sending Communication
③
Secure Communication for Privacy
Receiving Communication & Decryption

Fig. 1- Data flow of medical image secure communication from one site to another through public internet

There are two processing steps to provide 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 [6]; Second, for data privacy, the secured communication channels are provided to transmit the image through networks. For the first secure measure, there are already many papers and books discussing the technical methods and algorithms [7], [8]. In the following sections, we will focus on the second secure measure, which is data privacy, with evaluation results. Currently, there are two methods to provide secure communication channels with TCP/IP protocols: IPSec and SSL/TLS. In Section III, we will discuss the implementation of the TCP/IPv6/IPv4-enabled DICOM-communication library and application software.

IPv6/IPv4 Protocols and Dicom Communication software

A. Basic Architecture of TCP/IP

Most of today's Internet uses IPv4, which is now nearly 20 years old. IPv4 has been remarkably resilient in spite of its age, but it is beginning to have problems. Most importantly, there is a growing shortage of IPv4 addresses, which are needed by all new machines added to the Internet. Most network applications and protocols (Client/Server, Web, http, DICOM, etc.) used in the Internet or intranet are developed based on TCP/IPv4, which is partitioned into three layers according to the ISO (International Standards Organization Open Systems Interconnection, ISO-OSI) definition (International Standards Organization. [Online]. Available: http://www. iso.org), i.e., the application layer, the transport layer, and the IP layer. Due to the oversubscription of Internet addresses and the availability of higher network bandwidth, TCP/IPv4 starts to show certain strains, such as: 1) address shortage; 2) security is not integrated and the IPSec is an add on; 3) problems of multicasting; 4) complicated header; 5) fragmentation/retransmission problems; 6) poor quality of service (QoS); 7) inability to handle large frames; and 8) limited autoconfiguration support (needed by the DHCP).

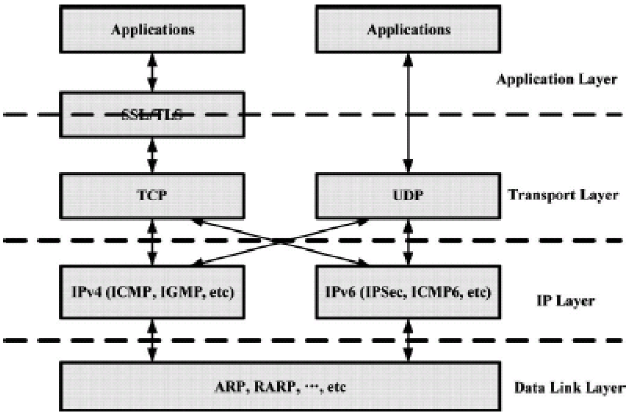

Fig. 2- TCP/IPv4/IPv6 protocols family architecture

IPv6 is a new version of IP, which is designed to be an evolutionary step of IPv4 [9]. IPv6 is designed to run well on high performance networks (e.g., Gigabit Ethernet, OC-12, ATM, etc.) and, at the same time, still be efficient for low-bandwidth networks (e.g., wireless). In addition, it provides a platform for higher speed Internet functionality that will be required in the near future. IPv6 were designed to solve many of the problems of the current version of

IPv4 with regard to address depletion, security, auto configuration, extensibility, etc. IPv6 includes many associated protocols, such as IPSec, ICMPv6, etc. IPv6 has some special features as follows: 1) larger address space; 2) aggregation-based address hierarchy and efficient backbone routing; 3) efficient and extensible IP datagram, such as no fragmentation by routers, 64-b-field alignment, and simpler basic header; 4) autoconfiguration; 5) security; and 6) IP renumbering as part of the protocol. Fig. 2 shows the architecture of TCP/IPv4 and TCP//IPv6, from which we see that the major difference of TCP/IPv4 and TCP/IPv6 is in the IP layer. Also, the IPSec is integrated into IPv6 as default security protocol, whereas SSL was adopted to provide security channel in the application layer in the IPv4-network environment, although IPSec was added on to IPv4 later on.

B. DICOM-Communication Software Over TCP/IPv6

Most medical image communication uses DICOM communication services to transfer the image data or objects between imaging modalities, PACS archiving server, workstations, and other components; as well as between teleradiology systems, and in enterprise PACS environment with WAN interconnection. In DICOM, the open system interconnection (OSI)) basic reference model is used to model the interconnection of medical-imaging equipment, as shown in Fig. 3. DICOM uses the OSI upper-layer service to separate the exchange of DICOM messages or objects at the application layer from the communication support provided by the lower layers. In order to enable medical-image transmission through highspeed broadband networks with IPv6, there is a need to develop the DICOM upper layer for TCP/IPv6 and also make it compatible with IPv4. The implementation was straightforward: for software, it only needs to replace the original TCP/IPv4-socket functions with requests for comments (RFC) standard TCP/IPv6/ v4-compatible socket functions, provided by each operating system, recompile the software, and link it to DICOM applications services. For operating environment, there is a need to install the IPv6-stack software and perform some reconfigurations, such as assigning IP address, configure the tunnel in the specific operating system, such as Windows XP, Linux (e.g., Red Hat version 3.0 or up) and Solaris (version 7 or up), which have already supported the IPv6.

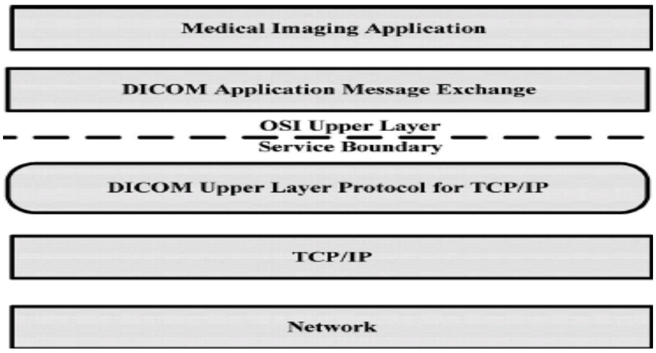
Medical Imaging Application
DICOM Application Message Exchange
OSI Upper Layer
Service Boundary
DICOM Upper Layer Protocol for TCP/IP
TCP/IP
Network

Fig. 3- DICOM network communication protocols architecture.

As a result, we come up with three basic IPv6/IPv4-enabled DICOM-communication services and applications:

1. DICOM Storage (C-Store) service-class user (SCU)) and service-class provider (SCP);
2. DICOM Query (C-Find) SCU and SCP;
3. DICOM Retrieval (C-Move) SCU and SCP.

Implementation of DICOM secure Communication DICOM

DICOM Standard Part provides a standardized method for ensuring secure communication and digital signature verification. The secure communication of IPv6-enabled DICOM-image transmission utilizes IPsec protocol, which is now mostly used in virtual private network (VPN)) applications, and will be widely used in high-speed broadband networks. In this section, we first give the software implementations of IPv6/IPv4-secure DICOM communication with IPsec support, and then discuss the SSL/TLS-based DICOM secure communication.

A. DICOM Communication With IPSec-Based Security Support

From the right-hand side of Fig. 2, we can see that IPSec is a member of the IPv6-protocol family. It provides security to the IP and the upper-layer protocols. IPSec is composed of two protocols: authentication-header (AH) protocol and encapsulating security payload (ESP) protocol. AH is used to ensure the authentication and integrity of the message, while ESP is used to ensure confidentiality. The AH protocol uses hash-message authentication codes (HMAC) to protect integrity. Many algorithms can be used in AH, such as the secure hash algorithm (SHA), Message Digest-5 (MD5), etc. The ESP protocol uses the standard symmetric encryption algorithms to protect confidentiality, such as triple DES (3DES), Advanced Encryption Standard (AES), and 448-b Blowfish encryption algorithm.

There are three steps in IPsec communications. The first is Internet-key exchange (IKE) protocol association. In this step, the Internet security association and key management protocol (ISAKMP)) daemons running in both SCU and SCP sites negotiate the IKE parameters and exchange certificates, which are used for IPSec association. In the second step, the SCU and SCP entities establish DICOM association, which includes the IPSec association. In this step, both sites negotiate IPSec parameters and create a session key, which is used for secure communication of DICOM data. The third is transferring the DICOM data on the secure channel. Since the secure operation is in the IP layer, the IPSec has no effect on DICOM-communication entities, which works in the application layer. To test the performance of DICOM communication with IPSec support, we need to set up a security association (SA) for peer entities to establish the secure channel. During the setup process, we create certificates for both peers and set SA-associated parameters.

B. DICOM-Image Communication With SSL/TLS-Based Security Support

The SSL was originally developed by Netscape Communications to allow secured access of a browser to a Web server. SSL has become the accepted standard for Web security [11]. It provides secure-communication channel between client and server by allowing mutual authentication, which uses digital signatures for integrity, and encryption for privacy. The protocol was designed to support multiple choices of specific algorithms used for cryptography, digests, and signatures. SSL 3.0 is the basis for the TLS protocol, which is still being developed by the Internet engineering task force (IETF) The SSL protocol uses both public-key and symmetric-key encryption. Symmetric-key encryption is much faster than public-key encryption, but public-key encryption provides better authentication techniques. SSL consists of two protocols: the handshake protocol and the SSL-record protocol. The handshake protocol defines how the peer entities exchange associated information, such as, SSL version and ciphers, and authenticates certificate. The SSL-record protocol defines the format of SSL record or message, in which all of the SSL-associated messages or application data should be transferred. The SSL connection is executed in two phases: the first is the handshake, and the second is data transfer.The data flow of the DICOM Storage SCU and SCP entities with SSL/TLS support is shown in Fig. 5. The SSL/TLS works between the TCP layer and the application layer. For IPSec and SSL/TLS-based security communications, we created X.509 certificates for both sites of DICOM C-Store SCU and DICOM C-Store SCP from the same CA attached in the Open SSL toolkit. In order to measure the transmission speed, we need to measure the transmission times of the images, since we already know the total sizes of image data to be transmitted. So, we embedded the APIs (application-program interface) about the Date/Time of the operating system (Linux/Windows XP) at the start and endpoint of the testing program of the DICOM secure communication to get the times of starting transmission and ending transmission, and then calculated the transmission speed.

Experimental Results and Discussion

We evaluated the DICOM-image communications with three different sets of parameters:

1. TCP/IP protocols (IPv6 and IPv4);
2. Security configurations (IPSec and SSL/TLS) and algorithms;
3. PDU sizes;

and three scenarios.

1. We measured the performance of IPv6 DICOM communications of different modality images with different PDU sizes on Linux and Windows XP computer platforms, and compared the results with that of IPv4 without security setting.
2. We measured the performance of IPv6 IPsec-based secure DICOM communications of different modality images with different PDU sizes on Linux and Windows XP computer platforms with different secure algorithms in the Ipsec-secure setting.
3. We measured the performance of IPv4 SSL/TLS-based secure DICOM communications of different modality images with different PDU sizes on Linux and Windows XP computer platform with different security algorithms.

References

[1] Huang H.K. (2004) *PACS and Imaging Informatics*.
[2] James A.E., James E., Johnson B. and James J. (1993) *Legal Med.*, 87-113.
[3] Berger S.B. and Cepelewicz B.B. (1996) *Amer. J. Roentgenol.*, 166, 505-510.
[4] Berlin L. (1998) *Amer. J. Roentgenol.*, 170, 1417-1422.
[5] Kamp G.H. (1996) *Amer. J. Roentgenol.*, 166, 511-512.
[6] Zhou X., Huang H.K. and Lou S.L. (2001) *IEEE Trans. Med. Imag.*, 20 (8), 784-791.
[7] Huitema C. (1999) *IPv6: The New Internet Protocol*.
[8] *Overview of RSNA DICOM Demonstration* [Online], (1997), Radiological Society of North America (RSNA) and Mallinckrodt Institute of Radiology.
[9] Rescorla E. (2001) *SSL and TLS: Designing and Building Secure Systems*.