SECURITY HANDLER FOR A HL/7 ELECTRONIC DATA INTERCHANGE

T.S. Chen[a], B.S. Liao[b], M.G. Lin[a]

[a]Department of Engineering Science, National Cheng Kung University, Taiwan, ROC
[b]Department of Electrical Engineering, ChengShiu Institute of Technology
E-mail: tsch@mail.ncku.edu.tw

ABSTRACT

The promotion of medical treatment quality is very important to the healthcare providers as well as patients. It needs to combine the different hospitals' medical resources to realize the goal of sharing medical information to reduce the unnecessary wastes. Computer-based patient record is one of the best consideration methods to accomplish the patient's clinical data interchange. The Health Level/Seven (HL/7) format is used to achieve the clinical data interchange for healthcare requirements, since it has been supported by many healthcare providers and becomes a standard reference. The security of clinical data interchange is a serious issue for people using computer by internet communication. Therefore, several international well-developed security algorithms, models and secure policies are adopted to design a security handler for a HL/7 architecture. The main goal is to establish a safety delivering channel for a HL/7 electronic data interchange. A suitable security environment is implemented to improve some shortcomings of clinical data interchange.

1.INTRODUCTION

The interchange of clinical data sometimes can reduce the medical cost [1]. Traditional methods for clinical data interchange are primarily with hand-writing forms, manpower delivery or fax machine [2]. As the availability of the internet and the computerized medical information, people can easily communicate and operate with personal computer or workstation. We can send or receive information from medical information systems in various way to meet the requirements for the clinical data interchange if it has an E-mail security handler.

The HL/7 organization is trying to popularize its format as a standard for clinical data interchange [3]. It was established in 1987, and the primary objective is to build up an international common standard for clinical data interchange. The HL/7 protocols are defined and located at the application layer of ISO/OSI reference model. The medical message components, sub-components and related types of message events are the primary goals of HL/7 protocols. Meanwhile, the patient management system, doctor's advice recording system, examine & diagnosis report system and financial management system are all the contents of the HL/7 protocols. Healthcare providers and hospitals in Taiwan are very interesting to develop the HL/7 protocols as a common standard of clinical data interchange.

After running the hospital information systems well, the healthcare providers try to emphasize the clinical data interchange and data access control inside or between hospitals [4]. Since patients take care their privacy rights, it is quite important to prevent threatens from the inner part of the hospital's medical information system or during the communication between hospitals. Therefore, the security issues are required to handle during the clinical data interchange. Though the dedicated line or value-added network can be used for inter-hospital communication, we prefer to use the availability and accessibility of the Internet to realize the goal of clinical data interchange to promote the whole medical treatment quality and to achieve the shared care.

The security requirements of medical information delivery are typically the same as those of the communication systems. Since the personal privacy has been emphasized, it is required to have more strictly security level in medical information system. Thus, we need to construct a safety data delivery channel and for protecting the clinical data. The related security algorithms and mechanisms we adopted in the system will be discussed [5]. We hope to promote the reliability and the applicability of the HL/7 protocols and to satisfy the requirements of secure level of clinical data interchange [6].

2.SYSTEM SECURITY

Combining HL/7 protocols with the Internet to apply in the interchange of clinical data, we realize that the benefit of the Internet is available to all people, but it is also a dangerous problem for threatening data. Message delivery on the Internet is public, shared, unrestricted, while the interchanges of clinical data require confidentiality, authorization, and strict securities. The usage of the Internet for clinical data interchange or telemedicine used by authorities or hospitals will encounter the same security issue. We have to balance the availability of the Internet and the confidentiality of clinical data. Firstly, six security requirements are addressed to construct the security system [7][8][9].

(1) Integrity: Protecting the delivered clinical data in communication channel without changing or lost by any kind of attack.

Table 1.Medical information security requirements, threatens and security mechanisms.

Security requirements	Threatens	Security mechanisms
1.Integrity	Fiddling, reply, lost	Digital envelope, digital signature, message integrity check.
2.Data origin authentication	To assume another's name to deliver the fake data.	Digital signature.
3.Authorization	System is invaded by illegal user.	Digital signature.
4.Confidentiality	Eavesdropping, disclosure.	Digital envelope, digital certification.
5.Non-repudiation	To make a denial of data delivering.	Digital envelope, digital signature, receipt.
6.Accountability	Illegal actions of users.	Audit, Log.

(2) Data origin authentication: Deciding the correctness of data source.

(3) Authorization: Users have different access control level to access data.

(4) Confidentiality: Assuring the content of the delivered clinical data will not be disclosed by malicious people.

(5) Non-repudiation: Senders and receivers can't make a denial of data that they have ever sent or received.

(6) Accountability: Monitoring the action log of users and taking responsibility about their behavior.

In order to satisfy the above six security requirements, we adopt three kinds of security mechanisms and two kinds of security models for cryptography [10]. They are described and introduced as below.

(1) Message integrity check: This algorithm uses one way hash function on the delivered message to bring message digest which is attached to the original message. The receiver can compare the message digest with the original message to ensure its integrity.

(2) Symmetric cipher: This algorithm uses the same key to encrypt and decrypt the delivered message. It can fulfill the security requirements of authorization and confidentiality.

(3) Asymmetric cipher: We use a key pair to encrypt and decrypt the delivered message. It will encrypt with one key and decrypt with the other key. It can make the security requirements of data origin authentication, non-repudiation and accountability.

It is hard to confirm all security requirements by just using any of the above mentioned three mechanisms. Therefore, we use two security models which are constructed with many security mechanisms to establish the security architecture of the system.

(1) Digital signature: Cooperating message integrity, asymmetric cipher and digital signature algorithm to achieve the security requirements of non-repudiation, data origin authentication, authorization, integrity and accountability.

(2) Digital envelope: Combining symmetric cipher, asymmetric cipher and random generator to achieve the security requirements of confidentiality, non-repudiation and accountability

These two security models are combined to satisfy the system's six security requirements. Table 1 is the summary of the comparison among security requirements, threatens and security mechanisms. It can be realized to protect the clinical data from different threatens with the proper security mechanisms.

3.SYSTEM ARCHITECTURE

This aim of the system is to protect the communication channel between the peers of the communication when medical information system using HL/7 protocols to carry out the end-to-end communication. The architecture of the system can be discussed in two portions: (1) System control: Including access control and audit control which based on Role-based mechanism can handle identification of sender and data origin authentication to protect the safety of the system operation. (2) Transmission channel: Combining the well-developed security algorithms by message integrity, symmetric cipher ,asymmetric cipher with security models such as digital signature and digital envelope to meet the security requirements of message delivery, integrity and confidentiality etc. The acceptable formats in heterogeneous systems during the communication channel have also considered. We can use Base-64 or Quoted Printable algorithm to produce the canonical form to perform clinical data interchange.

The format of the delivered data in this paper is the specification of the Pretty Good Privacy/Multipurpose Internet Mail Extension(PGP/MINE)[11][12]. We adopted algorithms specified in PGP [13], Secure Hashing Algorithm 1(SHA1) in message integrity check, Carlisle Adams and Stafford Tavares (CAST) in symmetric cipher, Digital Signature Standard/Differ-Hellman (DSS/DH) in asymmetric cipher and Digital Signature Algorithm (DSA) in digital signature algorithm.

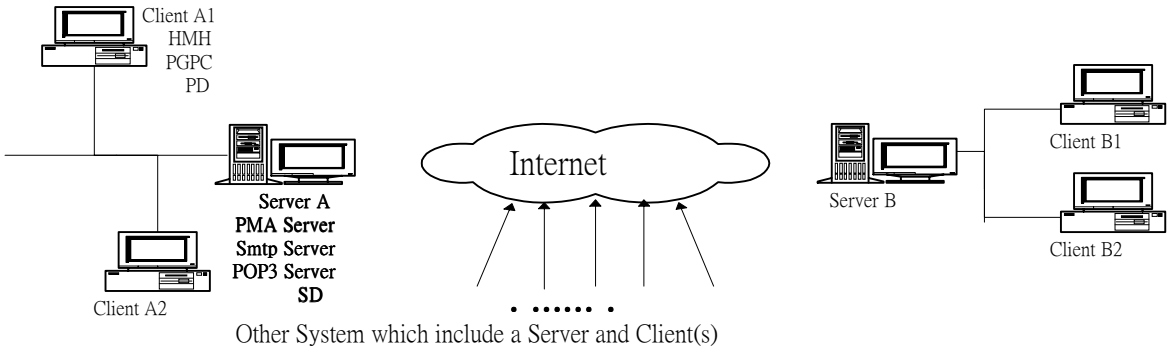

Figure 1. System's experiment architecture.

The whole system's experiment architecture is shown in Figure 1. The system is composed by a server and clients which are attached to an internetwork. The security transmission environment of medical information system is made up by server A, clients A1 and A2. When client A1 wants to communicate with client A2, client A1 have to go through server A. When client A1 intends to communicate with client B1 outside the hospital or the department, server A and server B must be the intermediary between client A1 and client B1.

The designed functional model for medical information security system is shown in Figure 2. The system's functions are based on the cooperation of both server and clients. The HL/7 Message Handling (HMH) in client side is in charge of the message handling, canonical form of message producing and encapsulation of MIME-EDI header. The PGP client (PGPC) uses the user's private key and the receiver's public key to produce digital signature, digital envelope, and send the result to the server.

When PGPC gets the encrypted and signed medical information from server, it decrypts the digital envelope first and then authenticates the digital signature by sender's public key and the receiver's private key. Besides, PGPC has also coupled to the system's security policies, such as the processing of reply message, storing of medical information and user's personal data.

A Personal Database (PD) is to collect and store the specified data including delivered clinical data, sender's personal data, sending time and the receiver's personal data for the evidence and the control of access to sensitive data.

In the server, it is composed of Policy Manipulation Agent (PMA) Server, Simple Mail Transfer Protocol (SMTP) Server, Post Office Protocol 3 (POP3) Server and System Database (SD). SMTP and POP3 are the common parts of a mail server, which provide the functions of mail delivered. PMA is the core security of server side. It's main functions provide the related security policy with generation and authentication of digital signature in server-side, digital envelope and reply message processing, storage of clinical data and management of public keys. These functions also need to cooperate with PGPC in client-side to construct the security policy for the whole system.

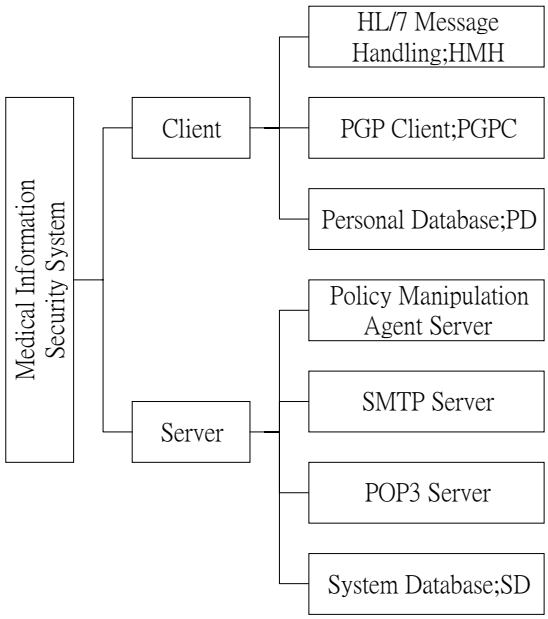

Figure 2. Functional model for medical information security system.

Main functions of SD are similar to those of PD, because both of them are storing the related clinical data for the evidence of possible contention in the future. It should have public key management function to provide highly confidence and highly extensibility.

4.SYSTEM MANIPULATION

An illustration for a simple work flow of transforming and receiving HL/7 message for clinical data interchange is shown in Figure 3. A1 is located in the edi.Mysystem.com.tw and will communicate with A2 in the edi.Othersystem.com.tw. First of all, A1 gets the clinical data of HL/7 format from HL/7 medical information system and transform the clinical data into canonical form with Base-64 or Quoted Printable algorithm and encapsulation with MIME-EDI header. Then it

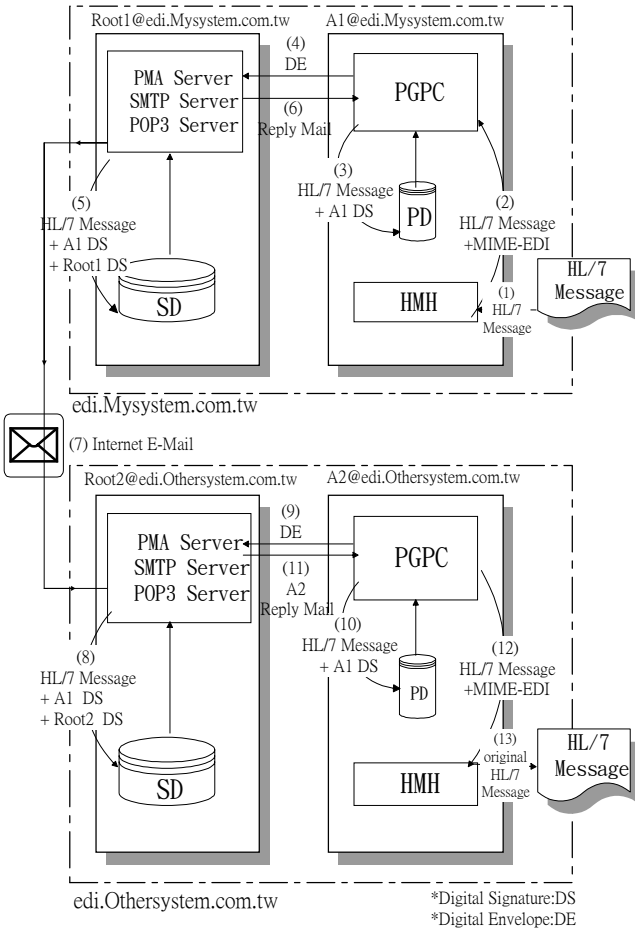

Figure 3.Work flow of transforming and receiving HL/7 message.

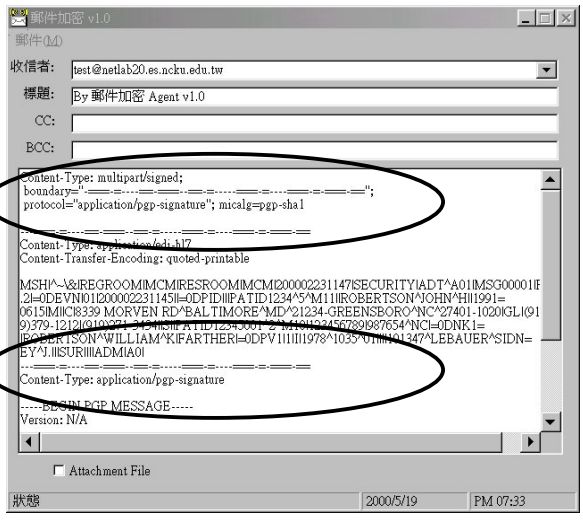

Figure 4. Example of digital signature content.

generates digital signature with A1 user's private key and stores the related data into the PD. These processes are followed from step (1) to (3).

After processing step (3), PGPC is ready to transmit clinical data attached with digital signature to the server side. It converts the delivered clinical data into digital envelope by server's public key and transmits the result to the server. When server Root1 receives the mail, it immediately decrypts the digital envelope and authenticates the correctness of the digital signature. Meanwhile, it stores the clinical data and the attached digital signature into SD for the usage of evidence in the future. Later the reply message sends back to the client A1 in the encrypted from with digital signature. They are shown in Figure 3 from step (4) to stop (6).

Through the step (1) to (6) we mentioned above, PMA gets ready to transfer the clinical data to the user A2 in edi.Othersystem.com.tw. In step (7), PMA uses Root1's private key of server side for clinical data to produce digital signature, and two copies of digital signatures. Root1 uses Root2's public key of receiving side to yield digital envelope and send to the Internet.

When Root2 of server side in edi.Othersystem.com.tw receives the e-mail, it must use the private key to decrypt the digital envelope and use the Root1's public key of sending side to authenticate the digital signature. In step (8), it stores the related information into the SD.

When client A2 detects a new arrived e-mail in server Root2, it will download the e-mail first. At this time Root2 uses the private key to yield the digital envelope and deliver to the client A2. When client A2 receives the e-mail, it uses the private key to decrypt the digital envelope and authenticates the correctness of the digital signature with the public key of server Root2. Finally, Root1 delivers the reply message to the Root2 in server side and stores the received clinical data into the PD. These processes are shown in step (9)-(11).

At the end of process, the PGPC in client A2 will transform the format of the received clinical data into local format, and removes the MIME-EDI header information of clinical data. The clinical data of Hl/7 format is successfully sent by user A1. Figure 4 shows an example of the content of digital signature which is yielded by sender.

5.CONCLUSIONS

The major aim of the designed security system is to provide safety protection in clinical data interchange. It has been run HL/7-based Outpatient Referral system for clinical data interchange between National Cheng Kung University Hospital and Shin-Lo Hospital in Tainan area with satisfaction [1]. We realize the system's security covers all directions which cooperates with many security policies to build up well-form security system. Two architectures of security model are constructed by three basic security algorithms with six security requirements of clinical data interchange including integrity, data origin authentication, authorization, confidentiality, accountability and non-repudiation.

The asymmetric cipher in this study is adopted to fulfill the requirements of data origin authentication, non-repudiation

and accountability. The management of public key is very important to promote the system's extensibility and trustworthy by constructing the authority certification [14]. In the future, we hope to join the system with the specification of S/MIME version 3.0 [15] to lift up the system's compatibility and availability. Additionally we also hope to give some benefits to promote the computer-based patient records in Healthcare Information Network(HIN)2.0, telemedicine as well as personnel computer-based patient record.

6.REFERENCES

[1] T.S.Chen, B.S.Liao, L.Z.Yu. "HL/7 Message Handler for an outpatient Referral System," Medical Informatics Symposium 2000, pp.64-68, Oct. 2000.

[2] Kleijhorst A., Van der velde E.T., Baljon M. H., Gerritsen M. J. G. M.,Oon H."Secure and Cost-Effiective Exchange of Cardiac Images over the Electronic Highway in the Netherlands,"Computers in Cardiology vol24, IEEE, 1997.

[3] "HL7 Health Level Seven . An application protocol for electronic data exchange in healthcare environments. Health Level Seven . Version 2.3 ,"Ann Arbor. MI.1997.

[4] Anderson R."A Security Policy Model for Clinical Information System," IEEE Symposium on Security and Privacy, 1996.

[5] Schneier B. "Applied Cryptography . Protocol, Algorithm and Source Code in C, Addison-Wesley.

[6] Baum Waidner B., Blobel B., Ottes F., Louwerse K., Krohn R., Bleumer G."Security Requirements of a HIS Architecture ,"ISHTAR Project HC 1028, Deliverable 23(Draft), September 1997.

[7] Yahya Y.Al-Salqan. "Security and Confidentiality in Healthcare Information ,"IEEE,pp.371-375,1998.

[8] Bernd, B., Volker, S., Peter, P., Kjeld, E., Rolf,K." Health Level Seven Security Services Framework Part 1: Basics of HL7 Security,"HL7 Secure Transactions Special Internet Group ,July 1999.

[9] Bernd, B., Volker, S., Peter, P., Kjeld, E., Rolf,K." Standard Guide for EDI(HL7) Communication Security . Version 1.1," HL7 consortium,July 1999.

[10] Stallings, William. " Network and international security: principles and practice," Prentice-Hall, 1995.

[11] Galvin,J.,Murphy, S., Crocker, S., Freed, N." Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted," RFC 1847, Trusted Information Systems, CyberCash Inc., Innosoft International, October 1995.

[12] Elkins, Michael." MIME Security with Pretty Good Privacy(PGP)," RFC 2015, Aerospace Corporation, October 1996.

[13] Garfinkel,S." PGP: Pretty Good Privacy. O'Reilly and Association," 1995.

[14] ITU, "CCITT Recommendation X.509 The Directory Authentication Framework," Consultation Committee, International Telephone and Telegraph, International telecommunication Union.

[15] Ramsdell, B." S/MIME Version 3 Message Specification," RFC 2633, June 1999.