# 모바일 환경에서의 MIR 시큐리티 시스템에 관한 연구*

김석수** · 하경재*** · 한군희****

**요 약**

본 논문에서 제시되는 MIR 시스템은 의료정보를 필요로 하는 어느 병원에서나 보건기관에서 즉시 사용할 수 있도록 전국적인 의무기록 정보 시스템을 구축하는 것으로 대부분 보안이 요구되는 자료들이다. 특히, 환자와 의사에 관련된 개인정보, 의료 전문기술 관련정보, 각 병원의 전산적 정보는 사용 빈도가 높고 정보의 변질을 통해 다른 목적으로 이용될 수 있는 가능성이 높다. 따라서 이러한 의료정보 서비스를 효과적으로 제공함과 동시에 정보의 유출을 방지하기 위한 보안대책이 강구된 시스템 개발이 필요하다.

# Design of MIR Security System in Mobile Environment*

Seok-Soo Kim** · Kyung-Jae Ha*** · Kun-Hee Han****

**ABSTRACT**

MIR system is a nationwide medical record information system that makes medical information available to any hospital and health institution at any time, and information in the system mostly requires high security. In particular, personal information related to patients and doctors, medical technology information and each hospital's digital information are used very frequently and are likely to be modified for illegal use. Thus we need to develop a system equipped with security measures to prevent information leakage while providing medical information service effectively.

Key words : MIR, Security, Medical, Record, Telemedicine

* 본 연구는 2005 산학협동 재단 학술연구비 사업지원으로 수행되었음.
** 한남대학교멀티미디어학부
*** 경남대학교컴퓨터공학부
**** 천안대학교정보통신학부

## 1. Introduction

Common Recently many countries are developing and introducing MIR (Medical Information Record) system as a means of effective medical information management. In particular, developed countries including the U.S. are rushing to materialize and apply CRP system with new frame on which a large volume of information is built including personal details and clinical data related to patients, exceeding the contents and uses of medical records in paper documents in the past. In Korea, however, the level of medical information is still low. Most of all, basic technologies and information infrastructure such as remote diagnosis and sharing of medical service information are not sufficient for introducing MIR system.

With increasing interest in mobile technology, however, investments in R&D are growing for medical and communication technologies in order to provide home medical services and other types of services and, as a result, we expect the rapid progress of basic technologies for medical information and specifically the evolution of hospital medical information system from existing EMR (Electronic Medical Record) to MIR system that allows integrated information management.

MIR system is a medical information system developed to make patients' medical information available to any hospital or health institution at any time.

It analyzes the occurrence and flow of medical information related to patients, identifies substantial entities in the process of medical treatments, and builds logical data structure based on relations among the entities. However, because current MIR system provides information in batch mode through collective data management, it has difficulties in active processing of entity relations applied during the processing of medical information. Moreover, MIR system is mostly implemented in the client/server structure in storing and providing information, so it is exposed to the risk of information leakage by system users or unauthorized users. Information leakage may worsen people's perception on medical information system, which is based on patients' trust. Thus the present study examines how to apply the procedure of medical information processing to information effectively and designs the operating environment of MIR system fit for mobile environment. In addition, we propose a security system for creating safe operating environment of MIR system in mobile environment. The proposed MIR system is composed of user authentication system for access control over patient information, data encryption system for the integrity and confidentiality of important data, and encrypted communication system for each system unit for secure communication between servers and clients.

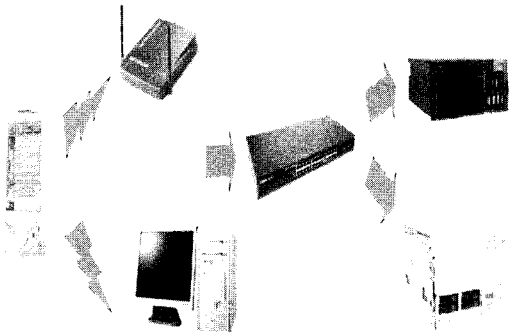
## 2. Medical Information Record System

There are the following types of medical information system.

- EMR (Electronic Medical Record) : This system stores patients' medical information in electronic files, manages systematically and makes it available for viewers.

- OCS (Order Communication System) : Through the system, orders are issued by doctors and delivered to the administration office and other supporting departments.
- PACS (Picture Archiving & Communication System) : The system keeps data such as radiographs, CT and MRI in database and improves their availability and accessibility.
- Telemedicine : Through the system, doctors can diagnose, treat and counsel patients online without face-to-face meeting.
- POC (Point of Care System) : This is a PDA -based system to process patients' clinical information at the place of medical service without the limitation of time and space. This system is regarded as the most effective technology for mobile healthcare. (Figure 1) is a flowchart of mobile medical support solution, showing the process of wireless communication between mobile PDA and the server providing medical information. For the commercialization of mobile medical solution, AP(Access points) should be installed or broadband wireless communication should be available. Currently in Korea, most public facilities and institutions like schools are equipped with wireless communication facilities and this system service can be provided at a low price. Thus, Korea is in a very advantageous position for introducing POC compared to other countries.

Among the medical information system listed above, EMR is most popular in hospitals today. Accordingly, CRP system for mobile environment must be designed in consideration of compatibility withERM system.




(Figure 1) Mobile medical support solution

## 3. Security Policies of MIR system in Mobile Environment

### 3.1 Analysis of the vulnerability of MIR security in mobile environment

Because MIR(Medical Information Record) system in mobile environment was designed to provide information through the wireless Internet and inter operation with each EMR server, there can be elements threatening the security of information while the information is being transmitted. Thus, for the design of a more secure system, we need to analyze the vulnerability of the proposed MIR system in mobile environment.

Security functions include authentication for identifying the senders and receivers of information and the users of information system, access control for preventing unauthorized persons from illegal access to and use of the system, confidentiality for protecting the contents of information from being disclosed to unauthorized

persons who acquired the information illegally, and integrity for protecting information in storage or in transmission from being fabricated or modified in an unauthorized way. In addition, it includes the non-repudiation function that prevents users from denying the sending or receiving of information through the information communication system, and the availability function that guarantees authorized users to send or process data using the system [1-3].

Security risk factors in operating environment identified from the analysis of the vulnerability of MIR system in mobile environment are as follows.

First, when information is exchanged between hospitals, it can be leaked out easily without the process of user authentication.

Second, personal information on patients and doctors can be leaked out as it is managed under DBMS without security tool. Particularly when the information system for managing clients such as EMR is integrated with database, various data on clients are exposed to a high risk of disclosure.

Third, when patients' information is viewed by relevant staffs or departments in the hospital, there is no clear standard for the extent of disclosure and this may increase the risk that patients' security and privacy may be intruded. Moreover, there is no policy defined clearly for the standard of disclosure of medical information according to viewer.

Fourth, because medical information is exchanged between hospital servers through TCP/IP network communication, network packets are exposed to the risk of tapping and modification. Particularly as the system is extended to mobile environment, this risk is getting higher due to information transmission among wireless network equipments.

Fifth, as the system components of each hospital server are directly connected to the network, they are exposed to aggressive users, unauthorized access and DOS attacks.

Security policies are established in relation to authentication/access control, tapping/modification of network packets, and vulnerability in network security as analyzed in the operating environment.

### 3.2 Establishing security policies of MIR system in mobile environment

MIR system is a global trend, and the Internet and medical information sharing system such as remote diagnosis are prevailing throughout the medical world. In this situation, various types of sensitive patient information can spread in a moment to the world. That is, due the possibility of the abuse of medical information, each country is tightening information security and several legal issues are rising [4].

Thus, in response to the vulnerability of security analyzed in the previous section, MIR system requires the establishment of security policies concerning the following aspects : Authentication/access control, Confidentiality/integrity, Non-repudi ation, Availability.

In response to risk factors threatening security as presented in the previous section, we need technical security measures as follows.

First, user authentication system should be introduced. User authentication mechanism can be implemented using ID/password, one-time password, two-factor authentication, open key

certificate, etc. MIR should intensify its authentication system using ID and password for protecting information of personal mobile terminal users in mobile environment. Information service through the wireless Internet is exposed to various security risks compared to wired service [5]. In this study, we use two-factor authentication for stricter authentication. Two-factor authentication provides intensified user authentication by adding the authentication of equipment or device such as PC, laptop or portable device (cellular phone, PDA) in addition to ID and password.

Second, XML is used as recommended by HL7 (Health Level 7) to share information among heterogeneous EMR systems and build integrated environment for protecting information [6]. For convenient exchange of information among systems, transformed medical information documents are developed fittingly to Web environment. Moreover, security for XML documents using XML encryption algorithm SOAP (Simple Object Access Protocol) and network security using SSL (Secure Sockets Layer) are applied together.

Third, security level is defined for user information, and XML documents are partially encrypted to restrict the disclosure of the documents according to users.

Fourth, in order to complement/monitor vulnerability in the integrity and confidentiality of data exchanged between MIR systems, each user's access to and use of information is logged and analyzed.

Fifth, intrusion detection and prevention system is introduced in preparation against hackers' intrusions and DOS attacks.

In order to implement security policies listed above, we defined security level as in <Table 2> as a standard for evaluating the security of MIR system.

〈Table 1〉 Security level of MIR system

| Level | Level 1<br>User authentication | Level 2<br>Access control | Level 3<br>System monitoring |
|---|---|---|---|
| Sub-level | 1-1<br>ID/password | 2-1<br>Set data access right for each user | 3-1<br>Log each user's data access |
| | 1-2<br>Two-factor authentication | 2-2<br>Set access right for parts of XML documents | 3-2<br>Analyze system log |
| | 1-3<br>Transmit SOAP protocol through XML document encryption | | 3-3<br>Analyze log using intrusion detection and prevention system |

## 4. Structure of MIR Security System in Mobile Environment

This chapter designs MIR security system to provide independent security service in various MIR application program environments based on the security policies of MIR system in mobile environment as established in Chapter 3.

A patient or a carer accesses a hospital server using his/her mobile terminal. The hospital server uses two-factor authentication to identify the user. That is, user authentication is carried out with ID/password and device authentication and

then the user's level is confirmed. If authentication is completed properly, the server and the user send/receive information. All information is exchanged in XML and is encrypted through XML security algorithm and SOAP according to user level. In addition, network security is provided through SSL. In information exchange between the user and other hospital servers and between hospital servers, two-factor authentication is applied first and then security for information itself is applied. The process of information request and provision between a hospital server and a patient and between two hospital servers is monitored by the intrusion detection and prevention system and the data is used in log analysis for each user and system.

### 4.1 XML security for user authentication

In addition to two-factor authentication system, we need a security system to encrypt XML documents and provide them differently according to user level. For the encryption of XML documents, a module should be designed based on XML signature standard [7, 8] and XML encryption standard[9, 10]. The purpose of module design is to remove the problem that the accuracy of the operation of XML security on domestic standard algorithms and encryption libraries has not been proved. Basic technologies for XML-based security are as in <Table 2>.

XML can protect documents using standardized methods as in <Table 2>. Depending on necessity, XML security technologies can encrypt information partially. XML documents can be encrypted differently according to the importance of information or whether the information is open or confidential and the whole document can be encrypted by the user's request. In this way, XML security encrypts and decrypts information selectively and this improves system performance and can meet user's requirements.

〈Table 2〉 XML-based security technologies

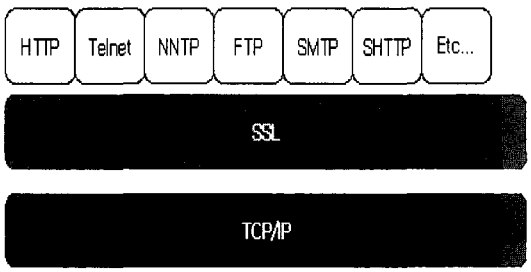
| Function | XML-based security technology |
|---|---|
| Authentication | XML digital signature, SAML, XACML |
| Authorization | XACML |
| Integrity | XML digital signature, XKMS |
| Confidentiality | XML encryption |
| Non-repudiation | XML digital signature |

### 4.2 Network security system

Network security system provides encrypted communication among EMR servers, network servers, relay servers for communication with wireless network, and clients. Encrypted communication security protocol may design and implement a separate security protocol but such a protocol is hard to design and implement and its stability is not reliable [11].

Accordingly, it is more effective to use established common protocols. One of widely used security protocols proved in the Internet is SSL, which is implemented on TCP layers and provides functions such as authentication, integrity and confidentiality. The protocol shows very reliability stability [12]. Thus, the present study recommends SSL considering for smooth services of established systems. SSL protocol uses a transport protocol like TCP to exchange data and runs under upper

protocols such as HTTP and IMAP. It is easy to identify a user with SSL because it contains functions to verify the user's certificate, public ID, whether the certificate was used by an officially approved institution, etc. SSL can be applied easily to established systems and is suitable for intensifying their security. (Figure 2) shows the location of SSL protocol implemented.




(Figure 2) The location of SSL protocol implemented

## 5. Conclusions

MIR system is a nationwide medical record information system that makes medical information available to any hospital and health institution at any time, and information in the system mostly requires high security. In particular, personal information related to patients and doctors, medical technology information and each hospital's digital information are used very frequently and are likely to be modified for illegal use. Thus we need to develop a system equipped with security measures to prevent information leakage while providing medical information service effectively.

The present study designed a MIRsystem and, for the development of a security system, established security policies for the MIR system through analyzing the operating environment and vulnerability in security and designed a security system implementing the policies. The security system supporting MIR system is composed of authentication system, XML documentation and encryption of medical information and network security system.

## References

[1] Matt Bishop, "Computer Security : Art and Science", Pearson Education, 2003.

[2] Ben Galbraith, et. al., "Professional Web Services Security", Wrox, 2002.

[3] Charles P.prleeger and Shari Lawrence Pfleeger, "ecurity in Computing", 3rd ed. Pearson Education, 2003.

[4] Jeong hyeon cheol, "medical information system of security", Communications of the Korea Information Science Society, Vol. 16, No. 12, 1998.

[5] A. Mishra, and W. rbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", February, 2002.

[6] HL7, http://www.hl7.org/Press/ 20040427b. pdf

[7] IETF/W3C, "XML-Signature Requirements (Working Draft)", Oct. 1999. http://www.w3.org/TR/1999/WD-xmldsig-requirements-19991014.html

[8] IETF/W3C, XML-Signature Syntax and Processing(Working Draft), Oct. 2000. http://www.w3.org/TR/2000/WD1-xmldsig-core -20001012/

[9] W3C XML Encryption WG, "XML Encryption Charter", http://www.w3.org, 2001.

[10] xml-encrytion@w3.org Mail Archives,

http://lists.w3.org/Archives/Public/xml-encryption/

[11] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, 2003.

[12] AlAN O.Freier, Phillip Karlton, Paul C. Kocker, "The SSL Protocol version 3.0", Netscape, 1996.

**김 석 수**

1991년 성균관대학교 대학원 정보공학과 공학석사
1991년~1996년 정풍물산(주) 중앙연구소 주임연구원
1997년~1998년 (주)한국탑웨어 책임연구원
2002년 성균관대학교 대학원 공학박사
1998년~2000년 경남도립거창전문대학 교수
2000년~2003년 동양대학교 컴퓨터공학부 교수
2003년~현재 한남대학교 멀티미디어학과 교수

**하 경 재**

1980년 성균관대학교 전기공학과 학사
1982년 성균관대학교 대학원 전기공학과 석사
1989년 성균관대학교 대학원 전기공학과 박사
1997년 미국 Wayne 주립대학 visiting scholar
1984년~현재 경남대학교 컴퓨터공학부 교수

**한 군 희**

1989년 충북대학교 컴퓨터 공학과(공학사)
1994년 경남대학교 컴퓨터 공학(공학석사)
2000년 충북대학교 컴퓨터 공학과(공학박사)
1989년~1994년 대우정보시스템 연구
1995년~2000년 대천대학 전기전자 컴퓨터학부 교수