의료정보보안 기반 소프트웨어 아키텍처 설계방법

김점구* · 노시춘**

요 약

의료정보 보안에 대한 대안은 무엇보다 의료정보의 안전한 보존과 각종의 보안 위협으로부터 안전성을 강구하는 소프트웨어 설계로부터 시작되어야 한다. 의료정보시스템은 산재된 의료정보를 실시간으로 통합할 수 있어야 하고 의료정보의 교환은 신뢰할 수 있는 데이터 통신이어야 한다. 의료정보시스템의 소프트웨어 아키텍처 설계는 의료정보 공유상 보안 문제를 파악하고 의사소통을 통해 사용자 요구사항을 파악하여 소프트웨어 설계에 반영한다. 소프트웨어 프레임워크 설계, 메시지 표준 설계, 웹기반 프로세스간 통신절차 설계, 접근제어 알고리즘 설계, 아키텍처 기술서 작성, 아키텍처 평가의 제반 절차를 정립한다. 소프트웨어 아키텍처 초기 결정은 설계, 개발, 테스트, 유지보수에 지속적인 영향을 미친다. 또한 프로젝트상의 세부적 의사결정 근거가 된다. 의료정보보안 기반 소프트웨어 아키텍처 설계방법은 오늘날 중요한 과제가 되고 있는 의료정보 보안의 기본틀을 제공할 수 있을 것이다.

A Study for Security-Based Medical Information Software Architecture Design Methodology

Jeom goo Kim* · SiChoon Noh**

ABSTRACT

What is an alternative to medical information security of medical information more secure preservation and safety of various types of security threats should be taken, starting from the software design. Interspersed with medical information systems medical information to be able to integrate the real-time exchange of medical information must be reliable data communication. The software architecture design of medical information systems and sharing of medical information security issues and communication phase allows the user to identify the requirements reflected in the software design. Software framework design, message standard design, design a web-based inter-process communication procedures, access control algorithm design, architecture, writing descriptions, evaluation of various will procedure the establishing architecture. The initial decision is a software architecture design, development, testing, maintenance, ongoing impact. In addition, the project will be based on the decision in detail. Medical information security method based on the design software architecture of today's medical information security has become an important task of the framework will be able to provide.

Key words : Software Architecture, Design Methods, Health Information, Information Sharing

접수일(2013년 12월 4일), 수정일(1차: 2013년 12월 16일), 게재확정일(2013년 12월 23일)

* 남서울대학교 컴퓨터학과
** 남서울대학교 컴퓨터학과

1. 서 론

의료정보 단말노드인 스마트폰에서부터 인터넷 접속 환경, 그리고 PC와 서버에 침투하는 각종 보안 위협은 날로 새로운 피해를 발생시키다. 이에 대한 대안은 무엇보다 의료정보의 안전한 보존과 각종 보안 위협으로부터 안전성을 강구하는 소프트웨어 설계이다. 의료정보의 표준으로 활용되는 HL7은 정보의 표현 형식을 표준화하여 국제적으로 사용되고 있다. 그러나 HL7이 정보교환 시 발생하는 모든 문제를 해결하는 것은 아니며 그 자체가 모든 상황을 완벽하게 대비했다고 보기는 어렵다. 본 연구는 의료정보 공유상 보안문제 해결방안으로 의료정보 보안 소프트웨어 아키텍처 설계방법을 제안한다. 의료정보보안을 위하여 소프트웨어 아키텍처가 개발되어야 하는 이유는 시스템 구축 후 문제점을 수정하기보다 설계, 개발단계에서 보안을 고려하여 개발되는 것이 바람직하다. 의료 정보 표준을 채용 하더라도 표준만으로 해결 되지 못하는 현안문제를 소프트웨어 구조 측면에서 설계할 필요가 있다. 본 연구 기술순서는 의료정보 공유환경을 진단하고 의료정보 공유상의 문제를 토대로 소프트웨어 아키텍처 설계를 진행하며 마지막으로 결론을 내렸다.

2. 의료정보 공유상 보안 문제

2.1 정보보안 침해 공격 패턴

정보전송 계층에서는 네트워킹 과정에서 공격자는 Scanning을 사용하여 공격표적에 대한 진행 서비스를 점검한다. 해당지역에 활동 중인 Host 확인, 공격하려는 Host의 Open port 등 정보를 수집한다. 포트스캔(port scan)은 웹 서비스를 운영 하는데 관련된 서버들의 불필요한 포트 접근 여부를 점검한다. 텔넷, SSH등 FTP 서비스 등에 접근할 수 있는 계정을 사용하거나 익명계정 등을 허용한다면 공격을 허용하게 될 수도 있다. 포트 스캐닝 도구 중 가장 많이 사용되는 Nmap은 윈도 우, 유닉스 계열 모두 사용가능하며 Console 명령 및 GUI 환경을 제공한다. Enumeration은 스캐닝 을 통해 수집된 정보를 바탕으로 시스템의 자원 공유를 정리, 수집하는 단계이다. User, Group 정보, OS, Routing Table, SNMP 정보 등을 수집할 수 있다. 리눅스에서는 etc/issue.net을 통해 배너를 수집할 수 있으며, etc/motd를 통해 로그인할 때 메시지를 출력할 수 있다. 스캐닝을 통하여 해당 호스트가 SMTP 서비스를 제공할 때, Telnet을 통하여 SMTP 서버에 접속하여 사용자 계정정보를 목록화 할 수 있다[6].

2.2 의료정보에 대한 XSS 공격 과정

웹 시스템 환경에서 가장 위험성이 높은 공격 기법은 XSS(Cross Site Script)이다. 공격자는 보안 취약점이 존재하는 웹 페이지 사용자 입력으로 “test”와 같이 정상적인 스트링을 입력하는 것이 아니라 <script>로 시작하는 악성 스크립트 코드를 입력한다. 웹 서버는 공격자가 입력한 악성 스크립트코드가 포함된 웹 페이지를 생성하여 클라이언트에게 되돌려 준다. 웹 페이지에 포함된 스크립트 코드는 클라이언트 측 브라우저상에서 실행된다. 공격자는 웹 메일이나 게시판 등을 이용 하여 리턴되는 웹페이지를 공격목표가 되는 일반 사용자에게 전달한다. 공격자는 웹 메일에 악성 스크립트 코드를 포함하여 전달하거나 게시판에 악성 스크립트 코드가 포함된 글을 포스팅 후 읽도록 한다[4][5].

3. 보안프레임워크의 역할

보안 프레임워크는 프레임워크 구성요소, 각 구성요소가 다루는 내용과 갖춰야 할 형식, 구성 요소 사이의 관계, 사용 예제를 담고 있어야한다. 프레임워크의 실체는 다루는 대상의 추상화 수준에 따라 달라진다. 프레임워크는 비슷한 문제를 해결 할 때 계속 재사용할 수 있어야 한다. 프레임워크 가 제공하는 재사용 범위는 개별문제를 해결하는 재사용이 아니라 전체 문제를 해결할 수 있는 재사용이기 때문에 패턴언어의 인스턴스로 프레임워크의 재사용 수준도 프레임워크가 다루는 대상의 추상화 수준에 따라 달라진다. 아키텍처 프레임워크는 아키텍처 기술서를 사용하여 사용자들이 원하는 형식으로 아키텍처에 관한 지식을

전달한다. IEEE 1471 같은 표준과 비교해서 본 연구에서 제시하는 아키텍처 프레임워크는 다음의 사항을 정립한다[1][2][7].

- ○ 처리표현 : 유스케이스. 객체 모델링 관점
- ○ 정보표현 : 데이터 흐름 다이어그램, 엔터티 , 객체 모델 다이어그램 같이 시스템이 다루는 정보를 설명할 수 있는 관점.
- ○ 처리구조 : 컴포넌트 다이어그램 같이 시스템 구성요소와 구성요소들 사이의 관계를 설명할 수 있는 관점.

4. 소프트웨어 아키텍처 설계

4.1 설계목표

소프트웨어 아키텍처는 시스템설계의 초기 결정 사항으로 초기결정은 설계, 개발, 테스트, 유지보수에 지속적인 영향을 미친다. 프로젝트 개발의 가이드라인으로서 아키텍처 설계의 기본틀을 다음 과 같이 추상화(abstraction) 목표를 설정한다.

- 의료정보 시스템의 목적이나 사명(mission) 수행을 지원할 소프트웨어아키텍처를 설계한다.
- 의료정보 시스템 설계를 통해 여러 이해관계자(stakeholder)들의 요구사항을 반영한다.
- 모든 의료정보 시스템은 아키텍처를 통해 설계의 청사진(blue print)을 제시한다.
- 아키텍처 기술서는 아키텍처를 결정한 근거(rationale)를 제시하여 문서화한다.

4.2 3단계의 요구사항 분석

의료정보시스템 이해 관계자는 의료정보사용자 (user), 의료정보 시스템인수자(acquirer), 의료 정보 시스템 개발자(developer), 의료정보시스템 유지보수자로 구분하며 이해관계자 의 관심을 도출한다. 의료정보 사용자는 병원, 장기요양 기관, 건강클리닉 등 의료서비스 공급자, 검사실, 약국, 의료 관련기관/부서, 의료분야 소프트웨어 벤더, 의료정보 컨설턴트 등 이다. 의료정보시스템 아키텍처 설계를 위해 이해관계자 관심 도출결과를 토대로 대상 시스템에 대한 요구사항 분석이 시행된다. 의료정보 시스템간 정보연동 문제와 보안성 문제 도출하였고 도출된 문제에 대한 요구사항은 다음과 같이 3개영역으로 정리된다.

< 표1 > 의료정보 이해관계자 유형

이해관계자	기본 관심사항
의료정보사용자	사용과 확장성의 편리함, 신속함과 보안성
의료정보개발자	시스템의 구현, 성능과 보안성, 사용자의 신속한 인증, 저장성
의료정보유지보수자	시스템의 유지보수, 확장성의 용이함과 보안성

< 표2 > 의료정보이 해관계자 관점

이해 관계자	이해 관계자 관점
의료정보사용자 (user)	• 의료정보가 실시간으로 탐지여부 • 시스템을 많이 점유하지는 않는가? • 의료정보 결과를 바로 알 수 있는가? • 의료정보 사용, 설치의 편리성
의료정보시스템 인수자 (acquirer)	• 의료정보시스템은 목적은 달성할 수 있는가? • 시스템은 경제성이 있는가?
의료정보시스템 개발자 (developer)	• 의료정보시스템을 구현하는데 어려움이 없는가? • 높은 사양을 요구하지 않는가?
의료정보시스템 유지보수자 (maintainer)	• 의료정보업데이트는 편하게 할 수 있는가? • 시스템을 설치하기에는 쉬운가?

< 표3 > 의료정보 요구사항 분석

목 표	목 표 내 용		
달성 목표	의료정보시스템의 사용성	기기 사용시의 편리함	사용자, 개발자, 유지보수자
	의료정보시스템의 성능성	기능 작동 시의 신속함	사용자, 개발자
	의료정보시스템의 보안성	기기 작동 중의 보안성	사용자, 개발자, 유지보수자
	의료정보시스템의 확장성	기기 확장(추가)의 용이함	사용자, 유지보수자

4.3 소프트웨어 4개 계층구조 설계

시스템 요구사항에서 도출된 시스템 보안성, 가용성, 유지관리 및 재사용성을 위해 소프트웨어 프레임워크를 구성한다. 아키텍처 기반으로 SDLC 전반 설계로 개발단계는 물론, 애플리케이션의 변화 관리, 형상관리. 운영 시 까지 대처 한다. 의료정보보안 기반 소프트웨어 아키텍처 계층구조를 다음과 같이 Presentation Layer, Foundation Layer, Business Layer, DataStore Layer 4개구조로 설계한다.

ㅇ Presentation Layer

웹상에서 정보를 출력을 담당하는 계층으로 HTML5 SCRIPT를 이용하여 구성된다. 모든 디스플레이를 이 컴포넌트에 하나로 묶어 통합하여 관리하며, 클라이언트 요청을 받아 서버에 전달한다.

ㅇ Foundation Layer

이 시스템 전반에 걸쳐서 공통으로 사용되어지고, 공통 된 클래스들을 모아 놓은 계층이다. 객체 스타일의 자료 구조와 처리기능은 Foundation Layer에서 기반이 되는 중심기능 이 구성된다.

ㅇ Business Layer

비즈니스 로직을 처리하는 컴포넌트로 구성된 계층이다. 이 계층의 컴포넌트는 주요 기능인 카테고리 관련 컴포넌트와 데이터검색 컴포넌트, 데이터관리 컴포넌트, 유저 상태 에이전트가 있다,

ㅇ Data Store Layer

객체타입의 데이터를 저장하기 위한 저장소 및 SQL을 관리하는 계층이다. 관련 데이터를 수집 하여 저장하고 필요할 대마다 정보가 제공되는 기능이다.

4.4 메시지 표준 설계

의료정보 아키텍처 설계를 위한 첫 번째 과제로서 의료정보 메시지 표준을 정립한다. 메시 지 구조는 메시지 의 추상적 정의(abstract message definition)이며 코딩 규칙(encoding rules)은 전송을 위한 메시지의 표현, 트리거 이벤트(trigger events)는 메시지를 촉발하는 애플리케이션 이벤트로써 실세계에 서의 이벤트는 두 시스템 간 정보의 교환을 촉발 시키다. 웹서비스 소프트웨어 아키텍처 환경에서 HL7에 기초하여 표준화 대상으로 명세화 한다. 메시지 표준은 HL7 사용으로 비표준 연동 환경 에서 요구 되었던 데이터의 형식 과 전송방식을 표준화하고 데이터 포맷 타입은 XML객체를 사용한다. Data format은 XML, URL encoding 으로 하며 Data format definition은 XML Schema Wire format, XML Protocol을 사용 한다. 정보표현 기술로서 정보를 구조화하고 의미를 공유, 전달하기 위해 개발된 XML 포맷이 필요 하며 환자 데이터는 단일 포맷 을 갖는 데이터로 변환이 가능하도록 데이터 전송 시 XML로 표기된 공통 데이터 포맷을 사용한다.

< 표4 > 의료정보 메시지 표준 설계 항목

항 목	설계사항
Data format	XML, URL encoding
Data format definition	XML Schema Wire format
ML Protocol	XML-RPC, SOAP

4.5 웹기반 프로세스간 통신절차 설계

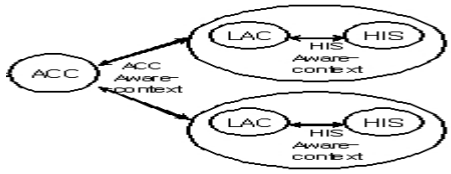
의료정보 공유를 위한 HL7은 Open System Connectivity로 A시스템에서 B시스템으로 메시지를 전송 시 발신시스템의 응용계측(제7계층) 동작을 발생시켜 수신 시스템의 제 7계층과 동등 수준의 관계를 구축한다. 수신시스템은 제7계층의 애플리케이션 프로토콜을 사용하며, 어플리케이션 프로토콜은 수신측에서는 하위계층 제6계층에서 제공하는 여러 서비스를 필요로 한다. 각 하위 각 계층에서도 동일한 과정이 반복되고 마지막으로 제1계층인 물리계층까지 적용된다. 각 시스템 간 연계를 위해 웹서비스 기반의 프로세스간 통신 절차를 다음과 같이 정립한다. ① 서비스 제공자 는 제공 서비스의 상세정보를 서비스 중개자의 UDDI 레지스트리에 등록(Publish)한다. ② 서비스 요청자는 자신이 원하는 서비스를 누가 제공 하는지 알기위해 서비스 중개자의 UDDI 레지스트리 에서 서비스를 검색(Find)한다.③ 서비스 요청자는 서비스 제공자의 WSDL 파일을 다운로드 한다. ④ 서비스의 인터페이스에 맞게 SOAP 전송 프로토콜을 사용

하여 서비스를 요청한다. ⑤ 서비스 제공자는 요청결과를 제공(Bind)한다.

4.6 접근제어 알고리즘 설계

의료정보 프로세스간 접근제어 구조는 CA (Client Application), ACC(Access Control Central Agent), LAC(Local Access Control Agent)이다. CA(Client Application)는 사용자는 중앙 접근제어 agent를 통해 여러 상이한 플랫폼 의 병원 정보 시스템에 접근한다. 접근 시 데이터의 암호화, 복호화 기능을 사용한다. 모든 사용자는 고유 인증서(X.509v3)를 가지고 있고 ACC 는 사용자 인증, 감사 및 HIS의 EMR 데이터 요청에 대한 낮은 수준의 접근제어를 한다. 승인된 요청에 대해 HIS의 LAC로 사용자의 요청정보 전달한다. LAC를 통해 ACC로 반환된 데이터에 대해 기밀정보에 따른 선택적 암호화하고 LAC는 사용자의 인증, 감사 및 HIS의 EMR 데이터 요청에 대한 접근제어 유효성을 검사한다. 접근제어 구조의 사용자 역할은 아래와 같은 속성들에 의해 결정된다.

- 사용자 인증 : 사용자는 자신의 인증서를 보여 줌으로써 EHR server와 연결한다. domain의 agent는 사용자를 인증하고, 인증되면 임시적 세션을 연결한다.
- Security logging : 모든 security agent는 감사에 필요한 모든 로깅정보를 생산, 저장 한다.
- Security agent 디렉토리 서비스: security agent들의 편리한 통신을 위해 모든 security agent가 디렉토리를 가진다.
- 인증 규정 : SSP는 인증기관처럼 서비스 한다. agent들 서로간의 인증을 위하여 디지털 인증서를 사용한다.
- 역할과 권한 : 사용자가 속한 그룹과 지위 ex) 의료진그룹. 서브그룹에 속하는 사용자는 상위 그룹으로부터 권한을 상속받는다. 사용자는 최소 한 하나 이상의 역할을 가질 수 있고 이들의 역할 과 권한의 관계를 정의해야 한다.



(그림1) 접근제어 구조

4.7 아키텍처 기술서 작성

연구는 IEEE 1471의 아키텍처 기술서 작성 공정순서를 참조하여 다음과 같이 6개 단계를 제시한다. 1. 아키텍처 기술서 정보를 작성한다. 2. 이해관계자와 관심을 식별한다. 3. 관점을 선택 한다.4. 관점에 대한 설명을 작성한다. 5. 뷰를 작성한다. 6. 전체 뷰를 작성한다. 이해관계자 관점을 논리, 프로세스, 개발, 물리 기준으로 정리 하면 다음의 아키텍처를 도출할 수 있다.

< 표5 > 기술서에 표시할 뷰 작성 기준

관점	설명
논리 뷰(Logical view)	요구된 기능을 제공하기 위한 시스템의 구조
프로세스 뷰 (Process view)	시스템의 동작 관점 (Activity)
개발 뷰 (Deployment view)	시스템을 구성하는 물리적인 배치 관점
유즈케이스 뷰 (Usecase view)	실제 사용하는 사용자 관점 (Use-Case)
물리 뷰(Physical view)	시스템의 소프트웨어와 하드웨어를 구현하는 관점

4.8 아키텍처 평가체계

4.8.1 3단계 평가항목 구조

의료정보 보안 소프트웨어 아키텍처 평가는 아키텍처 자체에 대한 기본평가와 본 제안에서 제시한 평가, 보안기능평가가 필요하다. 일반적인 아키텍처가 시스템과 프로젝트의 위험요소를 찾아 제거할 수 있는 평가가 되어야한다. 1차 평가 항목은 요구사항 분석을 토대로 성능, 신뢰성, 가용성, 보안성, 기능성, 유연성을 도출한다. 6개 항목을 도출한 이유는 정보공유 기능 요구사항 평가를 산출하고 그 추이를 분석하여 종

합 평가가 가능하기 위해 6개항목이 체크되어야 하기 때문이다. 2차 평가는 본 연구에서 설계한 의료정보 평가에 맞춰 소프트웨어 프레임워크, 메시지 표준, 프로세스간 통신, 접근제어로 설정한다. 3차 평가는 보안성에 대한 구체적인 평가로 아키텍처가 보안목적을 달성할 수 있는 기반을 구비하는지 평가한다.

< 표6 > 아키텍처 공통평가 항목

평가항목	평가내용
성능 (Performance)	시스템 자체가 성능적인 요구사항을 달성하는가.
신뢰성 (reliability)	시스템이 오류발생으로 부터 얼마나 안전한가를 평가
가용성 (Availability)	사용자가 원하는 시간, 장소에서 시스템 사용
보안성 (Security)	보안에 대한 기본적인 요구사항이 달성되는가.
기능성 (functionality)	사용자가 원하는 필수기능이 달성되는지에 대한 평가
유연성 (Variability)	유지보수 중 시스템의 추가 및 제거가 용이한가.

<표7 > 의료정보 아키텍처 평가 항목

평가항목	평가내용
소프트웨어 프레임워크	Presentation Layer, Foundation Layer, Business Layer, Data Store Layer 평가
메시지 표준	정보표현 ,정보 구조화, 정보의미 공유, 전달기능 평가
프로세스간 통신	서비스 제공, 서비스 중개 서비스 요청, 서비스를 검색, 서비스 인터페이스 평가
접근제어	사용자 인증, 인증 규정, 역할과 권한

< 표8 > 아키텍처 보안성 평가항목

영역	세부항목		
기밀성, 암호화	1.암호알고리즘	2.암호 키 관리	3.암호 응용기술
인증 및 접근 제어	1.일반적인 사용자 인증	2.네트워크 상의 사용자 인증	3.기업 환경의 사용자 인증
데이터 무결성	1.PKI	2.전자서명	3.SHA
가용성 및 복구	1.고장 감내성(Fault-Tolerance)	2.데이터 복구(Recovery)	3.DRS(Disaster Recovery System)
4개영역	4개항목	4개항목	4개항목

4.8.2 평가방법

평가는 아키텍처 생명주기 어느 때나 할 수 있지만 위험은 빨리 찾을수록 유리하므로 이른 평가 방식을 선택한다. 이른 평가는 아키텍처가 완성을 기다릴 필요없이 이미 내린 결정과 고려하는 결정 을 아키텍처 구축 과정 어느 때나 평가한다. 본 연구는 실제상황이 아니므로 평가방법 모델을 제시 하고 본 모델을 업무에서 활용토록 방법을 제시한다. 구현하고자 하는 기능을 통해 소프트웨어 아키텍처 요구 성능이 충족되도록 방법론을 통하여 구체 적으로 분석되고 구현 및 테스트 방안이 기술되는지 평가한다. 측정 체크리스트는 1차,2차,3차 품질 파라메터별 측정기준을 설정한다. 소프트웨어 아키텍처 품질 만족도는 세부적으로 측정점수, 가중 점수, 평가 점수로 집계한다. 평가점수는 5단계 등급으로 분류되며 미흡, 기초, 보통, 정상, 성숙 단계로서 각각 1-100까지 분포를 가진다. 평가점수를 목표와 비교하여 달성도를 분석하고 미진분야를 발췌하여 원인분석 및 개선작업에 활용한다. 평가지표의 동일 분류 내 척도를 산출한 후 각 지표의 중요도를 평가하여 중요도 별 가중값을 부여한다.

5. 결 론

프레임워크는 단계적 대응방안으로서 보안 목표를 완벽하게 달성하지 못하지만 보안품질을 어느 정도 보장해 준다. 소프트웨어는 통합된 접근제어 시 상호운용성, 접근성, 확장성, 유연성 요구사항 을 만족시켜야 한다. 서로 다른 보안정책을 가진 시스템들 간 보안정책 충돌 시 해결 매커니즘, context-aware와 융통성 있는 정책이 필요하다. 사용자는 보호되는 정보나 자원을 얻기 위해 권한이 배정된 역할의 구성원이 되어야 한다. 의료정보 사용자에게는 실시간으로 데이터를 검색하면서도 통합화된 접근제어 알고리즘 메커

니즘이 적용되어야한다. 웹 기반 환경에서 보안 아키텍처는 설계사상을 기반으로 프레임워크를 도출하고 기능 메커니즘을 구성하며, 알고리즘을 설계한다. 각 의료정보시스템은 객체타입(진단서, 영상, 처방서 등) 별로 동일한 환자 데이터 포맷을 가지며, 단일 포맷을 갖는 데이터로 변환이 가능하게 데이터 전송 시 공통 데이터 포맷을 사용한다. 본 연구에서 제시한 의료정보 보안 기반 소프트웨어 아키텍처 설계방법이 의료정보 공유 활용에 도움 되기를 희망한다.

참고문헌

[1] IEEE Std. 1971 (Recommended Practice for Architectural Description of Software-Intensive Systems), 2000.10

[2] Technical Report CMR/ SEI-95-Tr-021, 1995

[3] David Gourley and Brian Totty, “HTTP: The Definitive Guide”, O'Reilly Media, 2002.

[4]http://www.owasp.org/index.php/ Cross-Site _Request_Forgery

[5]http://www.owasp.org/index.php/CSRF_GuardOWASP,CSRFGuard,

[6] Sichoon,Noh,"A Securing Method of Multispectral Protection Infrastructure for Malicious Traffic in Intrne System", DCS, 2006.02

[7] R. H. Dolin, L. Alschuler, S. Boyer, C. Beebe,F. M. Behlen, et al(2005), “HL7 Clinical Document Architecture, release 2,” J. Am. Med. Inform.Assoc., 13(1), 30-39

[8] Bernd Blobe(2004), “Authorisation and access control for electronic health record systems”, International Journal of Medical Informatics 73, 251~257.

[9] J.W. Choi, S.Y. Yoo, H.Y. Park, J.H. Chun(2005), “Design and Implementation of HL7-based Real-time Data Communication for Mobile Clinical Information System”, J. Biomed. Eng.Res.Vol.26, No2,65-71.

[저자소개]

김 점 구 (Jeom goo Kim)

1990년 2월 광운대학교 전자계산학과 이학사
1997년 8월 광운대학교 전자계산학과 석사
2000년 8월 한남대학교 컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교 컴퓨터학과 교수
IT융합연구소장

email : jgoo@nsu.ac.kr

노 시 춘 (SiChoon Noh)

1987년 : 고려대학교 경영정보학(석사)
2005년 : 경기대학교 정보보호기술(박사)
2002년 : KT 시스템보안부장
2004년 : KT 충청전산국장
2005년~현 재 : 남서울대학교 컴퓨터학과 교수
2011년~현 재 : 남서울대학교 IT융합연구소 연구위원

email : nsc321@nsu.ac.kr