웹 기반 의료정보시스템 다중 접근제어를 위한 소프트웨어아키텍쳐 설계방법

노시춘* · 황정희*

요 약

웹 기반 의료정보는 많은 편리성을 제공하지만 공개된 네트워크 환경에서 나타나는 보안 취약성을 해결하지 않은 채 정보 노출의 위험속에 사용이 확대되고 있다. 웹 기반 의료정보 접근시 보안문제에 대한 안전한 방법론 강구없이 기술만 발전시키려 한다면 또 다른 위협의 요소를 증가시키는 것이다. 따라서 웹에 기반한 정보활용 보안대책 으로서 웹 기반 의료정보 접근제어 보안 메커니즘 기반 설계가 필요하다. 본 논문은 소프트웨어 아키텍쳐 설계사상을 기반으로 하여 의료정보시스템 접근제어 보안 메커니즘 기반을 설계 하였다. 그 방법론은 새로운 설계절차를 도출하고 아키텍쳐를 설계하며 기능 메커니즘 알고리즘을 구성하는 것 이다. 이를위해서는 웹 기반 다중 환자 정보 접근제어를 위한 보안 아케텍쳐 인프라스트럭가 필요하다. 제안하는 소프트웨어아케텍쳐는 소프트웨어 프레임워크를 도출하고 기능 메커니즘을 구성하는 기반에 관한 구조도를 도출했다. 제안된 시스템를 활용하여 의료정보 어플리케이션을 설계할때 의료정보 사용자는 실시간으로 데이터를 검색하면서도 통합화된 접근제어 알고리즘의 보장하에서 정보관리 안전성을 확보하는 시스템 설계가 가능하다.

A Study of Software Architecture Design Methods for Multiple Access Control under Web-based Medical Information System Environment

Si Choon Noh* · Jeong Hee Hwang*

ABSTRACT

Web-based health information provides a lot of conveniences, however the security vulnerabilities that appear in the network environment without the risk of exposure in the use of information are growing. Web-based medical information security issues when accessing only the technology advances, without attempting to seek a safe methodology are to increase the threat element. So it is required. to take advantage of web-based information security measures as a web-based access control security mechanism-based design. This paper is based on software architecture, design, ideas and health information systems were designed based on access control security mechanism. The methodologies are to derive a new design procedure, to design architecture and algorithms that make the mechanism function. To accomplish this goal, web-based access control for multiple patient information architecture infrastructures is needed. For this software framework to derive features that make the mechanism was derived based on the structure. The proposed system utilizes medical information, medical information when designing an application user retrieves data in real time, while ensuring integration of encrypted information under the access control algorithms, ensuring the safety management system design.

Key words : Software Architecture, Multiple Access Control, Medical Information System

접수일(2011년 08월 22일), 수정일(1차: 2011년 09월 10일)
게재확정일(2011년 09월 11일)

* 남서울대학교 컴퓨터학과

1. 서 론

의료정보시스템은 의료활동을 지원하는 정보시스템의 집합이다. 의료정보시스템 사례는 전자의무기록시스템(EMR), 처방전달시스템(OCS),의료영상전달시스템(PACS), 임상병리시스템(LIS), 일반관리시스템(ERP)을 들 수 있다. 의료정보시스템은 그룹웨어, 홈페이지 등과 함께 가동시켜 진료 및 경영의 효율을 향상시켜 의료진뿐만 아니라 환자와 병원 관계자들의 편의성을 추구한다. 인터넷을 통한 의료정보 교환은 기존의 의료업무의 틀을 유지하면서 인터넷과 IT 기술이라는 새로운 접근 채널이 추가된 형태이다. 때문에 위협요소 (risk factors) 또한 전통적 위험요소를 유지하면서 추가하여 인터넷과 IT 기술에 대하여 그 위험이 확대된다. 의료정보는 복잡하고 용량이 크며 산재해 있어 의료진들의 신속한 정보접근과 정보통신을 어렵게 하는 요인이 되었다. 이에따라 다른 영역의 정보시스템 사례와 같이 의료정보도 웹에 기반을 두고 문제점을 해결하고자 하는 방법론이 다양하게 제시되고 있다. 본 연구는 다양하게 제시되는 의료정보시스템 활용시 웹에 기반한 정보의 경우 보안대책 으로서 웹 기반 정보 접근제어를 위한 보안 메커니즘 기반 설계방법을 소프트웨어아키텍처 설계측면에서 제안한다. 기술 순서는 서론, 의료정보시스템 보안 문제, 접근제어 아케텍처 설계 절차, 결론의 순서이다.

2. 웹 기반 의료정보 보안 문제점

웹 기반 의료정보는 실시간 공유 및 활용되는 특성으로 기밀성 보장, 접근 권한관리, 익명성 확보 등이 취약하다. 진료정보 데이터베이스 시스템에 저장된 각종 개인 의료데이터에 대한 프라이버시 보호와 정보공유 및 활용시 다음과 같은 대표적인 문제가 발생하게 된다[3].

○ 오늘날의 의료정보 이용계층은 PC, 이동 PDA, 소형 PC, 이동전화기, 모바일폰, 스마트폰등 다양한 기기를 사용, 환자정보에 접근하게 되는데 이때 접근통제의 합리적인 기술방법, 규칙이나 제도적 기반이 취약한 상태이다.

○ 유헬스 의료정보 환경은 정보가 무선방식으로 전송되는 비율이 높아지고 의료정보의 이동성이 증가하므로서 무선통신 의료정보에 대한 외부 공격가능성이 증가한다.

○ 웹 기반 의료정보 처리는 전통적으로 폐쇄구조의 망에서 공개구조의 인터넷 망을 사용하게 되므로 네트워크 기반의 중앙집중 시스템에 저장 관리 및 처리된다. 이때 의료정보는 통합관리 되므로서 데이터베이스 접근시 업무 관련자 모두 접근가능하여 접근제어가 보안 문제점으로 대두된다.

3. 의료정보보안아키텍처 설계방법

3.1 아케텍처 설계의 기본 틀

소프트웨어아키텍처는 시스템 설계의 초기 결정사항으로서 초기 결정은 설계, 개발, 테스트, 유지보수에 지속적인 영향을 미친다..프로젝트 개발의 가이드라인 으로서 아케텍처 설계의 기본틀을 다음과 같이 추상화(abstraction)한다[1]

- 의료정보 시스템(System)의 목적 이나 사명(Mission) 수행을 지원해야 한다.
- 의료정보 시스템은 여러 이해관계자 (Stakeholder)들이 사명과 환경을 결정한다.
- 모든 의료정보 시스템은 아키텍처 (Architecture)를 가진다.
- 아키텍처 기술서는 아키텍처를 결정한 근거 (Rationale)를 제시한다.

3.2 의료정보 이해관계자 관심 도출

의료정보시스템의 이해관계자는 의료정보 사용자 (User), 의료정보시스템인수자 (Acquirer), 의료정보시스템 개발자 (Developer) ,의료정보 시스템 유지보수자 (Maintainer)로 구분하며 이해관계자의 관심을 다음과 같이 도출한다[2].

□ 의료정보 사용자 (User)

- 의료정보가 실시간으로 탐지가 되는가?
- 의료정보 결과를 바로 알 수 있는가?

- 의료정보 사용, 설치는 어렵지 않은가?

□ 의료정보시스템 인수자 (Acquirer)
- 의료정보시스템은 목적은 달성할 수 있는가?
- 시스템은 경제성이 있는가?

□ 의료정보시스템 개발자 (Developer)
- 의료정보시스템 접근제어 구현시 방법론
- 높은 사양을 요구하지 않는가?

□ 의료정보시스템 유지보수자 (Maintainer)
- 의료정보업데이트는 편하게 할 수 있는가?
- 시스템을 설치하기에는 쉬운가?

<표 1> 이해관계자 관심 도출

이해관계자	관 심
의료정보사용자 (User)	• 의료정보가 실시간으로 탐지가 되는가? • 의료정보 결과를 바로 알 수 있는가? • 의료정보 사용, 설치는 어렵지 않은가?
의료정보시스템인수자 (Acquirer)	• 의료정보시스템은 목적은 달성할 수 있는가? • 시스템은 경제성이 있는가?
의료정보시스템개발자 (Developer)	• 의료정보시스템을 구현하는데 어려움이 없는가? • 높은 사양을 요구하지 않는가?
의료정보시스템유지보수자 (Maintainer)	• 의료정보업데이트는 편하게 할 수 있는가? • 시스템을 설치하기에는 쉬운가?

3.3 이해관계자 관점 식별

이해관계자와 이해관계자들의 관심을 식별해서 아키텍처 기술서에 명시해야 한다. 아키텍처 기술서는 뷰(view)들로 이루어진다. 관점은 모델(model) 작성 방법을 정의 하고 어떤 모델(Model)의 어떤 부분이 어떤 뷰을 만들 때 꼭 필요한 것인지 정의한다. 관점의 정의에 따라 모델(model)들 가운에 꼭 필요한 부분을 모아서 뷰를 작성한다. 이해관계자 관점을 논리 관점, 프로세스,개발 관점, 물리 관점 기준으로 정리하면 다음과 같은 아키텍처 를 도출할 수 있다[2].

<표 2> 이해관계자 관점 식별

관 점	이해관계자	설 명
논리 뷰 (Logical view)	의료정보시스템개발자, 유지보수자	요구된 기능을 제공하기 위한 시스템의 구조
프로세스 뷰 (Process view)	의료정보시스템개발자, 인수자, 유지보수자	시스템의 동작 관점 (Activity)
개발 뷰 (Deployment view)	의료정보시스템개발자, 유지보수자	시스템을 구성하는 물리적인 배치 관점
유즈케이스 뷰(Usecase view)	의료정보시스템사용자, 인수자	실제 사용하는 사용자 관점 (Use-Case)
물리 뷰 (Physical view)	의료정보시스템개발자, 인수자	시스템의 소프트웨어와 하드웨어를 구현하는 관점

□ Logical View(논리 뷰)

요구된 기능을 제공하기 위한 시스템의 구조로서 의료정보시스템개발자, 유지보수자 관점이다. 서버에서 탐지된 패킷은 데이터 베이스로 탐지된 패킷과 유형을 저장 후 클라이언트에게 신호 전송. 클라이언트는 신호를 받은후 DB에 저장되어 있는 패킷과 유형을 분석 후 관리자에게 보여준다.

□ Process View(프로세스 뷰)

시스템의 동작 (Activity) 뷰로서 의료정보시스템개발자, 인수자, 유지보수자 관점이다. 네트워크에 설치된 IDS 는 패킷을 분석해 위험도를 파악한다. 일정 이상의 위험도는 순위를 패킷과 같이 서버 DB에 저장한다. 위험도가 높은 경우 클라이언트에 신호를 보낸다. 신호를 받은 클라이언트는 DB에 저장된 패킷과 유형을 분석해 대응 방법과 유형을 관리자에게 알린다.

□ Development View(개발 뷰)

개발 뷰는 다음 각 부분 모듈을 필요로 한다.

IDS : 패킷 탐지, 패킷 분석, 패킷 위험도 파악,
DB 저장, Client와의 소켓통신

DB : 데이터 저장, 데이터 삭제, 데이터 갱신,

Client : 패킷 유형 분석, 대응 방법 분석, 관리자 호출, DB SQL(JBDC), IDS와의 소켓통신

□ Cncurrency View(동시처리 뷰)

본 프로그램을 통하여 사용자는 완성된 결과물을 자신의 스마트폰에 저장하며, 주기적 업데이트를 통하여 다양한 데이터를 다운로드 받게 된다. 사용자가 프로그램을 통하여 얻은 결과물을 사용자의 동의에 따라 자신의 트위터 및 페이스북 등 다양한 SNS에 개제하는 결과물을 개발자나 유지보수자가 얻게 되어 프로그램 의 문제점 및 보안해야 할 점을 얻을 수 있다.

3.4 접근제어 기능적 요구사항

이상과 같이 이해관계자의 관심을 도출한 결과를 토대로 요구사항을 분석한다. 요구 사항은 기능적 요구사항과 품질요구사항으로 구분된다. 의료정보 접근제어 기본 메커니즘 설계방법의 첫번째 과제는 의료정보의 다양한 사용자를 파악하고 각계 각층의 사용자 요구사항을 수렴하는 일이다. 이를 위해 각 시스템 간 연계를 위해 개발자 간 조화를 이루는 일이 요구된다. 접근제어를 위한 기능적 요구사항은 다음과 같다[4].

□ CA(Client Application)

- 사용자는 중앙접근제어 agent를 통해 여러 상이한 플랫폼의 병원 정보 시스템에 접근한다
- 장소에 상관없이 병원정보 접근을 보장한다.
- 각 병원정보시스템들은 서로 배타, 독립적이며 오직 접근제어 agent를 통해서만 접근 가능.
- 단말노드는 접근제어 agent를 통해 다중 병원 정보시스템에 접근 기능
- 접근시 데이터의 암호화,복호화 기능
- 사용자의 전자 서명 첨가: 모든 사용자는 고유 인증서(X.509v3)를 가지고 있다.
- 전송 데이터의 무결성 검증
- 편리한 사용자 인터페이스 제공

□ ACC(Access Control Central Agent)

- 사용자의 인증, 감사 및 HIS의 EMR 데이터 요청에 대한 낮은 수준의 접근제어
- 유효성(user-role관계) 검사.
- 승인된 요청에 대해 HIS의 LAC로 사용자의 요청정보 전달.
- LAC를 통해 ACC로 반환된 데이터에 대해 기밀/민간 정보에 따른 선택적 암호화
- client application에 반환하여 선택적 데이터 보호 제공

□ LAC(Local Access Control Agent)

- 사용자의 인증, 감사 및 HIS의 EMR 데이터 요청에 대한 높은 수준의 접근제어 유효성 검사
- User-Role 관계.HIS의 접근제어 시스템에 의한 Role-Permission 관계 검증
- 내부사용자 인지 외부사용자인지 판별
- 내부사용자와 외부사용자에 대한 정책
- HIS와 ACC간의 데이터 변환 담당
- XML로 변환 요청된 데이터를 ACC로 보낸다.

3.5 접근제어 품질 요구사항

시스템은 통합된 접근제어시 상호운용성, 접근성, 확장성, 유연성 요구사항을 만족시켜야 한다[5].

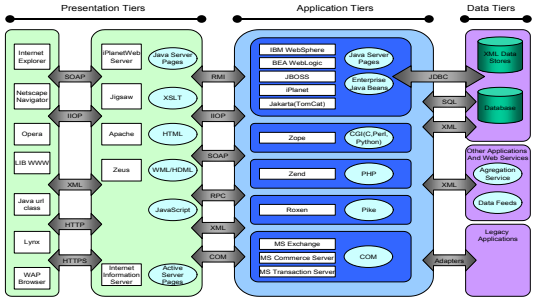
- 각 의료정보시스템은 객체 타입(진단서,영상, 처방서 등)별 동일한 환자 데이터 포맷을 가진다.
- 환자 데이터는 단일 포맷을 갖는 데이터로 변환이 가능해야한다.
- 데이터 전송시 XML로 표기된 공통 데이터 포맷을 사용한다. 사용자는 플랫폼에 상관없이 동일한 접근 인터페이스로 정보시스템에 접근
- 신규 정보 시스템의 추가, 삭제를 단순화하며, 확장성을 보장한다.
- 정책 관리는 기존 내부 사용자와 외부 사용자로 구분된 이중정책을 강구한다.
- 서로 다른 보안 정책을 가진 시스템들 간 보안 정책이 출동할때 해결할 수 있는 매커니즘, context-aware와 융통성 있는 정책이 필요하다. 이를위해 의료정보의 통합성과 비밀성이 보장되어야 한다.
- 다른 도메인끼리 즉, 원거리 통신시 각 도메인의

접근 제어 정책이 보호 되어야 한다.

- 원거리 통신시 데이터에 접근하여 한번 인증을 받은 사용자는 다시 인증 받지 않아도 된다.

4. 웹 애플리케이션 아키텍처 설계

4.1 웹 애플리케이션 아키텍처



(그림 1) Web Application Architecture

웹 어플리케이션은 HTTP 프로토콜을 사용하여 사용자와 다른 시스템과 통신하기 위한 클라이언트/서버 소프트웨어이다. 클라이언트는 대부분Internet Explorer나 Netscape Navigator와 같은 브라우저를 사용하거나 자동화된 브라우저로 동작하는 HTTP 에이전트를 사용한다. 웹 어플리케이션을 위한 제품이 수시로 개발되고 있는 실정으로 웹 어플리케이션 구성을 위한 전체 구조가 많은 상태지만 일반적 3단계 논리 구조를 설계한다[7].

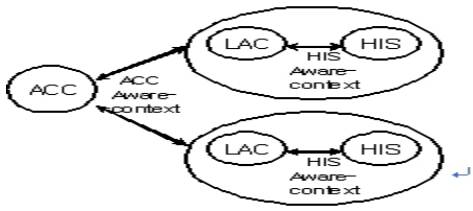
o 표현 계층(Presentation Tier): 사용자나 시스템에게 데이터를 표현하는 것을 담당

o 어플리케이션 계층(Application Tier): 비즈니스 로직, 사용자 입력 처리, 결정 등을 위한 웹 어플리케이션의 엔진에 해당하는 부분

o 데이터 계층(Data Tier): 어플리케이션에서 사용하는 임시 및 영구 저장소 역할을 위한 계층

4.3 애플리케이션 접근제어 알고리즘

네트워크는 동적인 환경으로서 다양하고 새로운 네트워크 위협 공격이 지속적으로 등장하고 있다. 이러한 위협에 대처하기 위한 웹 애플리케이션 접근제어 동작 알고리즘은 의료정보보안 아케텍 설계방법과 웹 애플리케이션 아키텍처 설계방법을 실현하는 접근제어 동작 알고리즘을 설계한다.



(그림 2) 접근제어 알고리즘

기능적 요구사항 CA(Client Application), ACC(Access Control Central Agent),LAC(Local Access Control Agent)의 기능을 만족시킨다. client application, ACC(Access Control Central Agent), LAC(Local Access Control Agent)간 다음의 Step 0에서 Step으로 Step 9 까지 단계적으로 동작한다.

Step 0. LAC (Idle)

Step 1. (Random delay) Node LAC는 상위 ACC layer로부터 transmission을 위한 새로운 packet을 얻은 후 trial counter(num_retries)를 0으로 초기화하고 random delay와 함께 시작

Step 2. (Listen)Random delay 후 listen 기간 동안 carrier sensing

Step 3. If medium = busy and numtrials < maxtrials go Step 4

Else if medium = busy and numtrials = maxtrials packet drop 후 go Step 0

Else if medium = idle go Step 6

Step 4. (Backoff)numtrials++, set timer, timer가 timeout 될 때까지 기다림

Step 5. If timeout Step 2

Step 6. (Await CTS)RTS packet 전송 후 일치하는 CTS packet을 기다림

Step 7. If (none or foreign CTS) and numtrials < maxtrials go Step 4

Else if (none or foreign CTS) and numtrials = maxtrials

packet drop 후 go Step 0
Step 8. (Await ack)Data packet를 보내고 일치하는 acknowledgment를 기다림
Step 9. If Explicit acknowledgment go Step 0
Else if no ack and numtrials < maxtrials go Step 4
Else if no ack and numtrials = maxtrials go Step 0

5. 결 론

웹 기반 어플리케이션은 인터넷 비즈니스의 가장 핵심적 자산 이지만, 보안을 고려하지 않은 시스템 개발시 문제를 검증하지 않고 웹을 운영하는 경우가 많다. 웹 어플리케이션 구현상의 보안 취약점 간과는 해커들로 하여금 고객의 중요한 정보를 훼손하게 됨을 잊지 말아야 한다. 성공적인 의료정보 설계를 위해 보안 아키텍처 설계가 요구된다. 웹 기반 다중 환자 정보저장소 접근을 위한 보안 아케텍처 인프라스트럭처는 새로운 설계사상을 기반으로 하여 프레임워크를 도출하고 기능 메커니즘을 구성했으며, 기반 구조를 설계했다. 제안시스템 에서는 실시간으로 데이터를 통합하며 좀더 안전한 의료정보시스템 설계를 목표로 하였다. 웹 기반 다중 환자 정보저장소 접근을 통하여 정확한 데이터를 주고 받을 수 있는 시스템이 구축되어 진다면 좀더 많은 효율성을 얻을수 있을 것이다.

참고문헌

[1] Architecture From Prehistory to Post-Modernism,르 코르뷔지에, 1923
[2] IEEE Std. 1971 (Recommended Practice for Architectural Description of Software-Intensive Systems),2000.10
[3] Portable, Low-Power, Wireless Two-Lead EKG System, Thaddeus R. F. Fulford-Jones, Gu-Yeon Wei, and Matt Welsh. In Proceedings of the 26th IEEE EMBS Annual International Conference, SanFrancisco, September2004
[4] CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care, David Malan, Thaddeus Fulford-Jones, Matt Welsh, and Steve Moulton. International Workshop on Wearable and Implantable Body Sensor Networks, April 2004.
[5] Biomedical telemedicine - CSCI E-170 January 11, 2005
[6] Healthwear:Medical Technology Becomes Wearable - 2004 IEEE
[7] Vital Positioning System Product Page, Medical Intelligence website, Retrieved December28,2004.
[8] Lifeguard Overview, Stanford Lifeguard Website, Retrieved December 23,2004 URL: http://lifeguard.stanford.edu/lifeguard_flyer.pdf.

[저 자 소 개]

노 시 춘 (Si Choon Noh)

1987년2월 : 고려대학교
경영정보학(석사)
2005년2월 : 경기대학교
정보보호기술(박사)
2002년11월 : KT 시스템보안부장
2004년 12월 : KT 충청전산국장
2005년3월 ~현 재 : 남서울대학교
컴퓨터학과 교수
2011년2월 ~현 재 : 남서울대학교
IT융합연구소 연구위원

email : nsc321@nsu.ac.kr

황 정 희(Jeong Hee Hwang)

2001년8월 : 충북대학교
전자계산학과 (이학석사)
2005년8월 : 충북대학교
전자계산학과 (이학박사)
2001년8월~2006년2월 : 정우씨스템(주)
연구소장
2006년3월~현재: 남서울대학교
컴퓨터학과 교수

email : jhhwang@nsu.ac.kr