보안 에이전트 역할 기반에 기초한 의료정보시스템 소프트웨어 보안아키텍쳐 설계방안★

이대성* · 노시춘**

요 약

의료정보 기술의 빠른 발전과 더불어 새로운 의료정보 서비스 개발에 대한 연구가 많이 진행되고 있다. 의료서비스를 향상시켜 환자들에게 많은 도움을 주는 방법이다. 하지만 정보보안에 대해 대비없이 기술만 발전한다면 의료서비스 체계에 위험과 위협의 요소를 만드는 것이다. 오늘날 현안과제인 공중망을 통한 안정적인 접근문제, Ad hoc을 이용한 센서네트워크 보안, 비통합 의료정보 체계의 보안취약성과 같은 보안의 취약성을 해결하지 않을채 의료정보시스템은 발전과 활용에 큰 제한을 받게 된다.. 서로 다른 보안 정책을 가진 의료정보시스템 환경에서 보안정책이 출동할 경우 해결할 수 있는 매커니즘이 필요하다. context-aware와 융통성있는 정책을 통해 의료정보의 통합성과 비밀성이 보장되어야 한다. 다른 도메인간 원거리 통신시 접근제어 정책이 보호 되어야 한다. 본 논문에서는 의료정보시스템의 접속자가 다양화, 다변화 되는 환경에서 Security agent 역할 기반의 보안시스템 아키텍쳐 설계방안을 제안한다. 제안된 시스템아키텍쳐는 현장에서 설계작업에서 하나의 모델로 활용이 가능할 것으로 기대한다.

A Study of Methodology Based on Role-Based Serucity Agent Medical Information System Security Architecture Design

Daesung Lee* · SiChoon Noh**

Abstract

In addition to the rapid development of health information technology services for the development of new medical information, a lot of research is underway. Improve health care services for patients are many ways to help them. However, no information about the security, if only the technology advances in health care systems will create an element of risk and threat. Today's issues and access issues are stable over a public network. Ad hoc sensor network using secure, non-integrated health information system's security vulnerabilities does not solve the security vulnerabilities. In the development and utilization of health information systems to be subject to greater restrictions. Different security policies in an environment with a medical information system security policy mechanism that can be resolved if people get here are needed. Context-aware and flexible policy of integration and confidential medical information through the resistance should be guaranteed. Other cross-domain access control policy for telecommunications should be protected. In this paper, that the caller's medical information system, diversification, diversification Security agent in the environment, architecture, design, plan, role-based security system are proposed. The proposed system architecture, design work in the field and in the utilization of one model are expected to be.

Key words : Security Agent, Medical Environment, Security Methodology

접수일(2011년 09월 09일), 수정일(1차: 2011년 09월 15일)
게재확정일(2011년 09월 16일)

★ 이 논문은 KCC/MKE/KEIT의 IT R&D 프로그램의 지원을 받아 작성되었습니다. [KI002140, 개인신변 안전보장을 위한 영상보안기술 개발]

* 경기대학교 산업기술보호특화센터
** 남서울대학교 컴퓨터학과 (교신저자)

1. 서 론

의료정보시스템은 의료활동을 지원하는 정보시스템 혹은 정보시스템의 집합이다. 좁은 의미의 의료정보시스템은 병원 내의 EHR (electronic health records)을 중심으로 의료와 직접적으로 관련된 작업들을 지원하는 전산시스템이다. 최근의 의료정보시스템 동향은 무선 네트워크와 다양한 소형 단말기의 발달로 사용자가 컴퓨터나 네트워크를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 유비쿼터스 환경이 모든 분야에서 빠르게 이루어지고 있다. 아직은 유비쿼터스적 접근이 미비하지만, 종이 없는 디지털 병원 및 재택 의료 서비스 등 웹을 통한 의료서비스가 다양하게 시도되고 있다. 환자들은 많은 병원 진찰을 받고, 그 데이터들은 각 병원에 흩어져서 저장된다. 분산된 환자 데이터는 네트워크를 통해 통합되어 의사뿐 아니라 환자도 정보보안 안전성을 확보한 상태에서 조회와 사용이 가능해야 한다. 본 연구는 이와같이 의료정보시스템의 접속자가 다양화, 다변화 되는 환경에서 Security Agent 역할 기반의 의료정보 보안 시스템 아키텍처 설계방안을 제안한다. 논문의 전개순서는 서론, 문제점 진단, 요구사항 도출, 의료보안 소프트웨어아키텍처 설계, 결론의 순서이다.

2. 의료정보시스템 보안 현안

2.1 공중망을 통한 안정적인 접근문제

국가나 기업에 기밀 문서처럼 유출되거나 침해되어서는 안 되는 정보가 있듯, 각 개인의 의료 정보도 절대로 남에게 보여져서는 안 되는 정보이다. 그러므로 의료정보시스템은 악의적인 공격으로부터 철저히 보호되어야 한다. 그러나 아직까지 의료정보시스템의 안정적인 접근제어와 공용 망을 통한 데이터 전송에 대한 보안이 취약하다는 문제점이 있다. 미래는 병원에서 더 많고 다양한 기기들을 이용하여 환자의 정보에 접근 할 것이다. 사무실에서 PC로뿐 아니라, 병원에서 이동하는 동안에도 PDA, 소형 PC, 이동전화기, 스마트폰으로 의료정보에 접근하게 된다. 다양한 정보미디어를 지원하는 다재 다능한 인터페이스가 모바일 환경의 의료정보시스템에 필수적이다. 하지만 아직까지 이런 다양한 인터페이스의 환경의 보안기술 대책은 개발이 미흡하다는 것이 문제이다. 의료정보는 공중망을 통한 안정적인 접근문제로서 기밀성과 응급 상황에서도 대처할 수 있는 가용성을 가져야 하며 철저한 보안을 필요로 한다. 의료정보는 의료진, 환자, 일반인 등 사용자 식별을 통해 진료기록의 접근을 통제하고, 사용 권한에 따라 암호화 수준과 해당 정보에 대한 역할 기반의 접근을 제어하여 보호해야 한다[1][2].

2.2 Ad hoc을 이용한 센서네트워크 보안

센서 네트워크 시스템 환경에서 센서노드는 개별 관리가 어려운 개방된 환경에 배치된다. 무선 네트워크와 다양한 소형 단말기의 발달로 Ad hoc을 이용한 센서네트워크는 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 유비쿼터스 환경을 제공한다. 아직은 유비쿼터스적 접근이 미비하지만, 종이 없는 디지털 병원 및 재택 의료 서비스 등 웹을 통한 의료서비스가 다양하게 시도되고 있다. 이런 특징으로 인해, 공격자는 센서노드를 물리적으로 쉽게 획득(compromising)할 수 있으며 획득한 센서노드(compromised node)를 이용하여 허위보고서를 쉽게 베이스 스테이션으로 보낼 수 있다. 허위보고서는 제한된 에너지 자원을 가진 센서노드의 수명을 단축시킬 뿐만 아니라 베이스스테이션과 관리자의 중요한 결정에 혼란을 유발시킬 수도 있다. 이러한 허위보고서의 피해를 최소화하기 위해서는 허위보고서를 전송 중에 발견하여 걸러내야하며, 보안대책을 마련해야 한다[1][3].

2.3 비통합 의료정보 체계의 보안취약성

현 시점에서 의 대부분의 의료 정보 시스템들은 해당 기관에 속하는 국가나 기관의 특성에 따라 독자적인 시스템 체계를 가지고 있다. 개별적으로 구축된 의료정보시스템은 조직 내에서도 이질적인 모델과 구축 도구 등으로 인해 모델 간의 상호 운영성이 떨어진다. 이런 비 통합적인 체계는 정보의 재사용성과 환자에게 질 좋은 의료 서비스 제공을 저해하는 요소이다. 산재된 의료 정보는 실시간으로 통합할 수 있어야 하고. 의료 정보가 실시간으로 의사나 환자에게 검색되어야 한다. 의료 정보의 교환은 신뢰할 수 있는 데이터 통신이

어야 한다. 의료정보는 복잡하고 용량이 크며 여기저기에 산재해있어 의료진들의 신속한 정보통신을 방해한다. 이런 이질적인 의료 정보를 통합적으로 관리하고 서로 다른 시스템들 사이의 데이터 교환을 원활하게 하기 위한 의료정보 정책이 필요하다[4][5]

3. 제안 보안 구조

서로 다른 보안 정책을 가진 시스템들 간에 보안 정책이 출동할 시에 그것을 해결할 수 있는 매커니즘을 개발한다. 매커니즘은 context-aware 와 융통성 있는 정책을 기반으로 설계한다. 의료정보의 통합성과 비밀성이 보장되면서 원거리 통신시 다른 도메인끼리 접근제어 정책이 보장 되어야 한다. 원거리 통신시 데이터에 접근하여 인증을 받은 사용자는 재접근 시 다시 인증 받지 않토록 한다. 자격이 되는 사용자가 의료 정보에 접근을 하였다 하더라도 통신하는 과정에서 정보를 빼앗길 위험에 대비한다. 의료 데이터가 통합된 DB나 서버측의 시스템 보안. DB나 서버가 WAN으로 나가는 곳, gateway에 의료 정보 시스템에 적절한 접근정책을 설계하여 통합된 정보 매커니즘을 제공해야 한다[5]. 이상의 환경에서 알고리즘 기본구조는 Security agent를 기반으로 하는 보안기능을 기본으로 한다. 각 도메인에 설치한 Security agent는 영역의 보안정책을 책임진다. Security domain으로서 각 구역은 지역적 보안 정책에 의해 통제가 된다. 같은 보안 정책에 의해 통제가 되는 구역을 설계하고 처별화된 보안정책을 적용한다[7].

<표 1> 제안 보안 구조의 아키텍처

Security agent 기반 알고리즘	Security domain	Security agent
Security agent 개념을 기본으로 각 도메인 Security agent는 그 영역의 보안정책을 책임진다.	각 구역은 지역적 보안 정책에 의해 통제가 된다. 같은 보안 정책에 의해 통제가 되는 구역을 security domain으로 설정한다.	Security agent는보안과 관련된 정보를 교환하고 보안 서비스를 위임받아 처리한다.

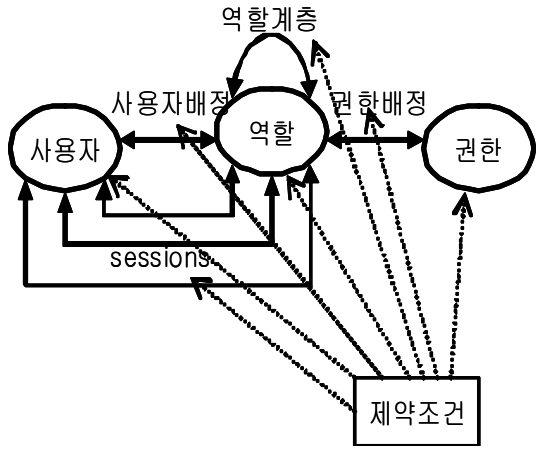
4. 의료정보보안 아키텍처 설계

4.1 역할 기반 소프트웨어 아키텍처

이해관계자는 시스템에 관심(Concern)을 갖는 사람이나 조직이다. 의료정보보안 아키텍처는 의료정보 이해관계자들의 관심을 아키텍처로 수렴한다. 따라서, 아키텍처는 여러 이해관계자들의 관심을 조율하고 절충해서 만족시켜야 한다. 이해관계자들은 아키텍처를 활용해서 상호작용하고 자신의 관심을 만족시킨다. 따라서, 아키텍처 기술서(Architecture Description)를 작성할 때 기본구조는 Security agent를 기반으로 하는 보안기능을 기본으로 한다. 각 도메인에 설치된 Security agent는 그 영역의 보안정책을 책임진다. Security agent는 이해관계자와 이해관계자의 관심을 식별하는 것은 아주 중요한 역할을 수행한다[6].

4.2 역할 기반 Security agent 알고리즘

역할 기반 Security agent알고리즘은 보안 역할에 기반을 두고 사용자의 시스템 자원에 대하 접근을 제어하는 기법이다. 접근권한을 부여하는 단위가 사용자가 아니라 사용자가 속한 분류의 역할이다. 즉, 사용자는 보호가 되는 정보나 자원을 얻기 위해 해당 접근권한이 배정된 역할의 구성원이 되어야 한다. 역할간 계층구조를 통해 하위 역할의 권한이 상위 역할이 사용될 수 있게 권한상속이 된다.



(그림 1) 역할기반 모델

4.3 사용자가 가지는 역할의 속성 결정

역할 기반 Security agent알고리즘에서 사용자가 가지는 역할의 속성들은 다음의 정책에 의해 결정된다.

4.3.1 {UserID, UserName, Domain} 정의

- UserID, UserName: 사용자의 고유한 아이디와 이름
- Domain: 사용자가 속한 그룹과 지위임. 의료진그룹 서브그룹에 속하는 사용자는 상위그룹으로부터 권한을 상속 받는다. 사용자는 최소한 하나 이상의 역할을 가질 수 있다.

4.3.2 relation 관계 정의

이들이 가지는 역할과 권한과의 관계를 다음과 같이 정의되어야 한다.

{ID, r, {operation}, t, constraint(r, t, p)}

- ID:권한 식별자
- r(role) : 해당 권한을 처리하기 위한 역할
- operation : 역할에 의해 처리되는 실제행위
- t(target) : 해당 행위가 실행되어지게 될 개체
- constraint(r, t, p): 해당 권한에 대한 제약조건을 의미하며, role과 target 및 privilege에 의해서 결정

4.3.3 역할의 권한과 privilege를 소유했는지 판단하는 함수

- domain_user(r): 해당 역할을 가지며 도메인에 속해 있는 사용자
- satisfy(p): 해당 privilege를 만족하는 사용자
- belong(r,t): 해당 역할을 가지며 특정 개체에 접근할 수 있는 권한을 소유한 사용자

이때, 환자 정보는 환자 개인의 것이므로, 자신에 정보에 접근할 수 있는 사용자를 환자가 등록할 수 있어야 한다.

4.3.4 역할-권한 브로커

환자는 모든 사용자에 대해 모든 역할과 권한에 대해 제어할 수 있는 것은 아니다. 역할과 권한은 역할-권한 브로커가 수행한다.

- 사용자 식별 및 인증
  해당 시스템이나 리소스에 접근하기 위한 사용자 식별아이디와 암호를 입력 받는 단순 인증과 디지털서명이 있는 인증서에 의한 인증 지원
- 접근 제어 및 권한 부여
  알고리즘에 기반한 권한 부여와 접근제어 모델
  사용자가 어느 특정 리소스에 어떠한 권한을 가지고 무슨 행위를 할 수 있는지 접근제어
- 감사
  모든 보안에 관련된 행위들에 대한 로그 데이터 저장. 비정상적인 접근 패턴 분석

4.4 세션 관리 정립 절차

서비스를 만족하는 사용자의 세션을 관리 접근 방법들은 의료 데이터를 사용하기 원하는 사용자가 권한이 있는 사람인지 아닌지를 판별하여 인증해주는 것이다. 그러나 사용자의 권한 설정과 인증만으로는 의료정보와 같이 중요한 데이터를 보호하는데 한계가 있다.

각 HIS(Hospital Information System)은 객체 타입(진단서,영상, 처방서 등)별로 동일한 환자 데이터 포맷을 가지며, 단일 포맷을 갖는 데이터로 변환이 가능하다고 가정한다.

데이터 전송시 XML로 표기된 공통 데이터 포맷을 사용한다.사용자는 플랫폼에 상관없이 동일한 접근 인터페이스로 각 병원 정보 시스템에 접근한다.장소에 상관없이 병원 정보 시스템에 접근을 보장한다.

4.5 보안 보증기능 설정원칙

각 병원 정보 시스템들은 서로 배타, 독립적이며 오직 접근 제어 agent를 통해서만 접근이 가능하다. 신규 병원 정보 시스템의 추가, 삭제를 단순화하며, 확장성을 보장한다. 정책관리는 기존 내부 사용자와 외부 사용자로 구분된 이중정책을 통해 이뤄진다.

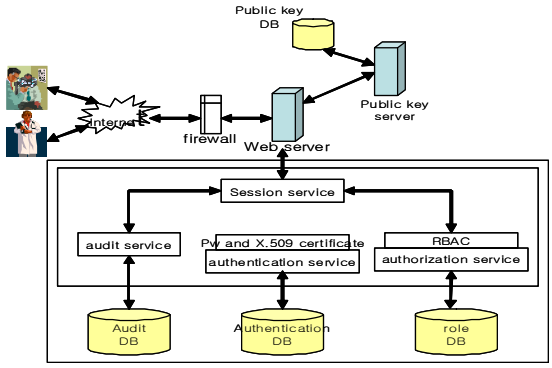
- 기밀성: 민감/기밀 데이터의한 선택적 암호화
- 전자서명: 공개키 기반 공인인증서(X.509v3)를 통해 사용자 인증
- 무결성: 전송되는 데이터에 데이터의 전자서명을 첨부
- 로그정보: 사용자와 병원 정보 시스템간의 모든 트랜잭션의 로그정보를 감사한다.

제안된 시스템 구조

- client application : 접근제어 agent를 통해 다중 병원 정보 시스템에 접근 할 수 있는 단말노드로서 암호화된 데이터의 복호화 기능
- 사용자의 전자 서명 첨가: 모든 사용자는 고유 인증서(X.509v3)를 가지고 있다. 전송 데이터의 무결성 검증과 사용자 인터페이스 제공
- ACC(Access Control Central Agent) :사용자의 인증, 감사 및 HIS의 EMR 데이터 요청에 대한 낮은 수준의 접근제어 유효성(user-role관계)를 검사. 승인된 요청에 대해 HIS의 LAC로 사용자의 요청정보를 전달. LAC를 통해 ACC로 반환된 데이터에 대해 기밀/민간 정보에 따른 선택적 암호화를 한 후, client application에 반환하여 선택적 데이터 보호를 제공
- LAC(Local Access Control Agent) : 사용자의 인증, 감사 및 HIS의 EMR 데이터 요청에 대한 높은 수준의 접근제어 유효성을 검사
- 4.6 User-Role 관계 : HIS의 접근제어 시스템에 의한 Role-Permission 관계 검증: 내부사용자 인지 외부사용자인지 판별 (내부사용자와 외부사용자에 대한 정책이 다르다.)한다. HIS와 ACC간의 데이터 변환 담당: XML 데이터로 변환(요청된 데이터를 ACC로 보낼 시)

센서 네트워크는 네트워크 시스템 중 다수의 센서 노드로 이루어진 네트워크를 말하며, 각각의 센서 노드는 주변 환경을 센싱하여 정보를 수집하게 된다. 이 센서 네트워크는 유비쿼터스 컴퓨팅 환경을 구현하기 위한 기술 중 하나로 인식되고 있으며, 기술의 발전에 따라 그 응용기술이 폭발적으로 개발될 것으로 기대한다. (1)

기존 센서 네트워크는 환경모니터링, 야생동물관찰, 군사감시 등을 주 목적으로 사용, 개발되고 있다.



(그림 2) 제안된 시스템 구조

4.6 Security agent 프러시듀어

Security agent는 시스템으로부터 보안과 관련된 정보를 교환하고 보안 서비스를 받는다. Security agent는 알고리즘의 규칙에 의거하여 사용자 인증, 사용자 권한, Security logging, Security services provide, Security agent 디렉토리 서비스,,인증 규정, 정책 충돌 해결을 다음과 같은 프러시듀어로 7개 영역의 정책을 수행한다.

- 사용자 인증: 사용자는 자신의 인증서를 보여줌으로써 EHR server와 연결을 한다. 그 domain의 agent는 사용자를 인증하고, 인증이 되면 임시적인 세션을 연결한다. 한번 인증이 된 사용자는 다른 domain의 정보를 이용할 때에도 재 인증을 할 필요가 없다.
- 사용자 권한: local security agent는 각각의 원격 security agent에 의해 제공되는 정보를 가지고 있지 않다. 그러므로 사용자 권한은 동적이고 context-specific(문맥이 명확) 해야 한다.
- Security logging: 모든 security agent는 감사에 필요한 모든 로깅정보를 생산하고 저장한다.
- Security services provider : 웹 서비스의 형태로 local agent들에게 보안 서비스를 제공하는 독립적인 시스템이다.
- Security agent 디렉토리 서비스: SSP는 security agent들의 편리한 통신을 위해 모든 security agent들의 디렉토리를 가지고 있다.

- 인증 규정: SSP는 인증기관처럼 서비스 한다. agent 들 서로간의 인증을 위하여 디지털 인증서를 사용한다.
- 정책 충돌 해결: 여러 security domain간의 정책적 충돌이 발생하는데, SSP는 이런 충돌이 해결되도록 서비스를 제공한다.

5. 결 론

역할에 기반을 두고 사용자의 시스템 자원에 대하 접근을 제어하는 기법은 권한을 부여하는 단위가 사용자가 아니라 사용자가 속한 분류의 역할이다. 사용자는 보호가 되는 정보나 자원을 얻기 위해 해당 접근 권한이 배정된 역할의 구성원이 되어야 한다. 역할간 계층구조를 통해 하위 역할의 권한이 상위 역할이 사용될 수 있게 권한상속이 된다. 서로 다른 보안 정책을 가진 시스템들 간에 보안 정책이 출동할 시에 그것을 해결할 수 있는 context-aware와 융통성있는 정책이 필요하다. 이를 위해 의료정보의 통합성과 비밀성이 보장되어야 한다. 다른 도메인끼리 즉, 원거리 통신시 각 도메인의 접근 제어 정책이 보호 되어야 하며 이상으로 제시한 Security Agent 역할 기반에 기초한 의료정보시스템 소프트웨어 보안아키텍쳐 설계방안은 현장의 정보시스템 설계시 활용될 수 있을 것으로 기대한다.

참고문헌

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

[2] Dimitris Gritzalis, Costas Lambrinoudakis, “A security architecture for interconnecting health information systems”, International Journal of Medical Informatics 73, 305~309, 2004.

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

[4] Richard E. Scott, Penny Jennett, Maryann Yeo, “Access and authorisation in a Glocal e-Health Policy context”, International Journal of Medical Informatics 73, 259~266, 2004.

[5] 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.

[6] Wireless Sensor Networks for Emergency Medical Care. Presented at GE Global Research, March 8, 2004

[7]Biomedical telemedicine - CSCI E-170 January 11, 2005

[8]Healthwear:Medical Technology Becomes Wearable - 2004 IEEE

[저 자 소 개]

이 대 성 (Daesung Lee)

1999년 2월 인하대학교
전자계산공학과 학사
2001년 2월 인하대학교
전자계산공학과 석사
2008년 2월 인하대학교
정보공학과 박사

email : xdilemma@naver.com

노 시 춘 (SiChoon 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