팍스 그리드를 위한 신뢰 관리 모델

조현숙, 이봉환
대전대학교 정보통신공학과 컴퓨터네트워크 연구실
{chojo, blee}@dju.ac.kr

Trust Management Model for PACS-Grid

Hyun-Suk Cho and Bong-Hwan Lee
Dept. of Information & Commun. Eng., Daejeon University

요 약

본 논문에서는 인터넷 상에서 서로 신뢰할 수 없는 제3자들 사이에서 디지털 인증서를 교환하여 신뢰를 구축하는 방법인 신뢰 관리 시스템을 소개하고, KeyNote 방식의 인증서에 권한을 추가하는 방식을 팍스 그리드 도메인에 적용할 수 있는 모델을 제안하였다. 기존의 그리드 상의 보안 메커니즘을 활용하여 추가적인 오버헤드를 줄였으며, 인증서를 XML로 변환하여 그리드 시스템과의 연동 및 웹에서 사용 가능하도록 확장성도 고려하였다.

1. 서론

수억 명의 인터넷 사용자들 사이에서 대부분의 교류는 제3자(stranger)들 사이에서 발생한다. 즉, 각 엔티티들은 미리 알려진 관계도 아니며 일반적인 보안 도메인을 공유하는 것도 아니다. 제3자들은 민감한 교류를 가지기 전에 충분한 수준의 상호 신뢰를 형성해야만 한다. 이런 목적을 위하여 참여자들의 아이디(사회보장번호, 지문, 세금ID 등)를 사용하는 방법은 그들에 대한 신뢰 여부를 부적절하게 판단할 소지가 있으며, 대신에 참여자들의 속성(고용 상태, 시민권, 단체 맴버쉽 등)을 이용하는 것이 적절할 것이다.

전통적인 시큐리티 접근방법은 아이디에 기초한 방법으로 제3자에게 로컬 자원에 접근하는 것을 허가하기 이전에 로컬 로그인이나 인증서 등의 로컬 보안 도메인 내의 아이디를 얻게 하는 것이었다. 이와 같은 문제는 온라인상에서도 제3자에게 도메인 내의 특정 종류의 아이디를 얻을 자격이 있는지의 문제로 귀결되었다[1].

이에 대한 해결책으로 제3자들은 디지털 인증서를 교환함으로써 신뢰를 구축할 수 있고, 디지털 인증서는 인증서 발행자의 개인키를 사용하여 서명되는 형태이고, 발행자의 공개키를 사용하여 검증될 수 있다. 전통적으로 디지털 인증서는 특정 엔티티가 소유하고 있는 속성들을 포함하고 있다. 보통은 속성 이름/값의 쌍으로 표현된다. 디지털 인증서는 X.509 인증서[2]를 사용하여 구현될 수 있다.

어떤 자원은 모두에게 자유롭게 공개되지만 많은 인증되지 않은 접근으로부터의 보호가 필요하다. 접근 제어 정책들은 URL을 통해 접근되는 서비스, 역할 기반의 액세스 컨트롤 시스템, 능력(capability) 기반의 시스템 등 많은 종류의 자원을 보호하는데 사용될 수 있다. 여기서 중요한 것은 서비스 요구 주체의 역할 또는 속성이다. 따라서 대용량 분산시스템에서는 속성(attribute) 및 역할(role)에 기반한 새로운 신뢰모델[3]이 요구되고 있다.

본 논문에서는 속성 기반 신뢰 모델에 대해서 소개하고, 이를 팍스그리드 도메인에 적용하는 방안을 제안하고자 한다.

2. 관련연구

2.1 신뢰 관리 시스템

속성에 기반하여 신뢰 문제를 해결하기 위한 시스템을 신뢰 관리시스템 (trust management system)[4]이라 한다. 신뢰구축의 접근법에서 "신뢰"는 반복적으로 인증서를 교환하고 인증서를 요청하는, 일명 신뢰 협상 (trust negotiation)의 과정으로 구축된다. 인증서 기반의 인증과 권한검증 시스템은 다음의 세 그룹으로 분류된다.

- ✓ Identity-based
- ✓ Property-based
- ✓ Capability-based

원래 공개키 인증서들, 예를 들어 X.509 그리고 PGP[5]는 단순히 키와 이름을 바인딩하는 방법을 사용하였으며, X.509v3 인증서는 이후 일반적인 속성에 키를 바인딩하는 방식으로 확장되었다.

- Trust Establishment Project: IBM Haifa 연구소는 공개키 인증서의 내용에 강제사항을 특성화한 정책에 따라 제3자들 사이에서 신뢰를 구축하는 시스템을 개발하였다.
- Capability-based system : 이 시스템은 특정 응용에 대한 권한의 위임을 관리하는 시스템이다. 능력기반의 시스템들은 제3자들 사이에서 신뢰를 구축하기 위해 디자인된 것이 아니라 클라이언트는 응용 서버에 특정 액션들에 대한 권한을 대표하는 인증서들을 소유하고 있다고 가정한다. 능력기반인 KeyNote 시스템[6]에서 인증서에 하나의 원칙적인 권한들은 요구되어진 다른 원칙들에 어떻게 행동하는지에 관한 조건을 명시하였다.
- Simple Public Key Infrastructure : 직접적으로 인증서에 권한을 끼워 넣는 식의 KeyNote의 접근과 유사한 방식을 사용한다.
- Bonatti and Smarati : 이들은 인터넷 상에서 정보를 배출하거나 규칙적인 서비스에 접근하기 위해 표준 프레임워크와 모델을 소개한다.
- Delegation : 분산 신뢰 관리 시스템에서 중요한 역할을 하며 위임 언어들은 명백히 신뢰 구축 세계에서 한 부분을 차지할 것이다. 그러나 현재의 위임 정책 언어와 신뢰 협상에 있어서 기초로는 적당하지 않은 컴플라이언스 체커라는 두 가지 이슈가 대립될 것으로 보인다.

초기의 신뢰 협상 전략은 가능한 한 빨리 잠금을 해제하고 인증서를 노출하고, 임의의 전략은 각 측이 상대측의 정책을 살펴보고, 신뢰가 성립될 수 있다고 결정한 후에 바로 인증서를 노출할 뿐 아니라 정책 정보 없이도 노출한다는 순수한 전략만을 내포하도록 제안되었다. 그러나 본 논문의 도메인인 팍스 영역에서는 각 자원에 대한 정책에 따른 접근 권한 여부를 결정하는 것이 중요한 문제이며, 따라서 제안하는 모델에서는 정책 기반의 접근권한을 사용한다. 또한 구현방법에 있어서는 Keynote의 인증서에 권한을 삽입하는 방식을 차용하였으며, Single-Sign-On을 가능하게 하는 프록시 인증서를 활용하여 팍스 자원에 접근할 수 있는 모델을 제안한다.

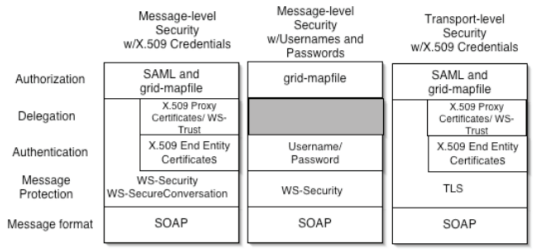
2.2 팍스 그리드

PACS-Grid란 지리적으로 분산된 PACS(Picture Archiving and Communication System, 의료영상저장전송시스템)를 그리드 기술로 통합하여 서로 연동한 거대한 가상의 단일 시스템 혹은 이를 지원하는 서비스들을 제공하는 프레임워크를 칭한다.

PACS-Grid는 지금까지의 PACS에서 요구되어 왔던 스토리지의 안전성과 확장성을 보장하고 원격 이미지 파일 전송 및 협업, 원격진단, 가상병원과 같은 향상된 의료정보기능을 지원한다. PACS는 각 컴포넌트 간 통신을 위해 DICOM(digital imaging and communication in medicine)이라는 표준 프로토콜을 사용한다. DICOM은 소켓 통신 기반의 프로토콜로써 TCP/IP 네트워크 내에서 통신이 자유롭지만, 자료의 보안 및 시스템의 안전을 위해 대부분의 PACS는 병원 내 사설망으로 구축되며 방화벽과 같은 다양한 안전장치로 인해 외부와 단절되어 있다. PACS 및 보관된 자료를 외부의 위험요소로부터 지키면서 특정 외부의 컴포넌트들과는 필요에 따라 통신하기 위하여 WebPACS 및 TelePACS 등의 형태로 진화되어 왔다.

GSI(Grid Security Infrastructure)[7]는 서로 간에 이미 신뢰 가능한 사용자에 의해 발행된 프락시 인증서를 가진 두 개의 임의의 엔티티들에 대한 정책을 가지고 있다. 이 정책은 사용자가 협업을 원하는 어떤 서비스에 대해서 프락시 인증서를 발행함으로서 동적으로 신뢰 도메인을 생성할 수 있게 해준다. 그림1에 나타낸 바와 같이 GSI는 메시지 보호(message protection), 인증(authentication), 권한위임(delegation), 그리고 권한부여(authorization) 등 4개의 구별되는 기능들로 구성되어 있음을 볼 수 있다. TLS (transport-level) 또는 WS-Security 및 WS-SecureConversation (message level)은 SOAP과 연결하기 위한 메시지 보호 메커니즘으로 사용된다. X.509 End Entity Certificates 또는 User name

과 Password 가 X.509 프락시 인증서의 인증을 위해 사용되며, X.509 프락시 인증서들과 WS-Trust가 권한부여를 위해 사용되는 권한 위임(delegation)에, SAML 선언이 권한 검증을 위해 사용된다.

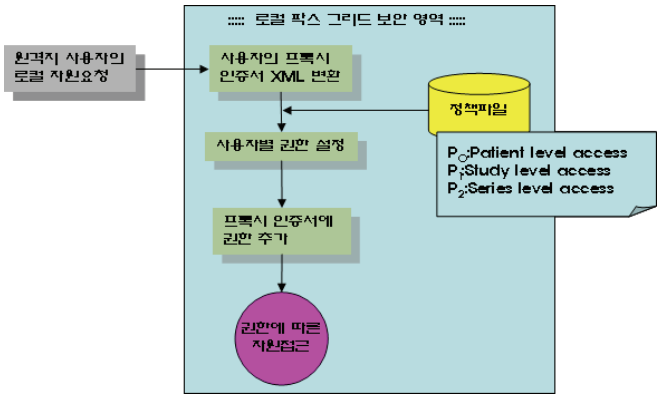


(그림 1) GT4 그리드 보안 하부구조와 서로 다른 기능을 위해 사용되는 표준들

그림1에서 좌측의 두 개의 구조는 X.509 인증서와 사용자이름/패스워드 인증을 가지고 있는 메시지 레벨 보안을 나타내며, 나머지 오른쪽의 구조가 X.509 인증서를 사용하는 전송-레벨 보안을 나타낸다.

3. 팍스 그리드 신뢰관리 모델

팍스 그리드에서는 자원에 대한 사용권한이 가장 중요하며, 그리드의 장점을 수용하기 위해 팍스를 그리드와 접목시키는 만큼 그리드 시스템에서의 권한 관리를 이해하고, 이를 적용하는 것이 필요하다. 본 논문에서 제안하는 팍스 그리드를 위한 신뢰 관리 모델에서는 그리드의 프록시 인증서를 확장하여 권한을 추가하고 자원에 접근하는 방식을 사용한다. 제안하는 모델의 순서도를 도식화하면 그림2와 같다.



(그림 2) 팍스 그리드 신뢰 관리 모델

팍스 그리드 내의 원격지 사용자는 그리드 인증방식을 통하여 그리드 노드 인증(사용자 인증서, 프록시 인증서)을 받은 후, 로컬의 팍스 그리드 노드에 자원을 요청하게 된다. 그리드 상에서 위임의 문제를 해결하려면, 서로 다른 도메인에서 인증 서버(CA)가 다르므로 로컬의 팍스 그리드로부터 프록시 인증서를 통하여 인증을 받아야만 한다. 로컬의 호스트는 원격지 사용자의 프록시 인증서를 받아 XML문서로 변환하는 작업을 거쳐 인증서에 권한을 추가할 준비를 한다.

그림 3의 좌측은 사용자의 프록시 인증서이고, 우측은 이를 XML로 변환한 파일이다.

(그림 3) 프록시 인증서의 XML변환

정책 파일에 따라 자원의 접근 여부를 결정한 이후 권한을 부여받게 되는데, 팍스 데이터베이스의 구조는 정책 결정에 중요한 요소가 된다. 본 논문에서는 테스트를 위하여 세 가지 정책 파일을 적용하였으며, 이후 실용화를 위해서는 정책 파일을 상세화할 필요가 있다. 팍스의 데이터베이스는 patient->study->series 의 순서로, 환자 1인에 대한 상세 병증을 레벨에 따라 접근여부를 결정하도록 정책을 설정하였다.

접근권한을 추가한 후 원격지 사용자는 권한에 따른 자원 접근이 허용된다. 현재 그리드 시스템에서는 로컬의 계정을 원격지의 사용자에게 할당하여, 원격지 사용자는 위임받은 로컬의 계정이 가지고 있는 권한과 동일한 권한으로 자원에 접근하도록 설계되어 있다. 그러나 팍스를 도메인으로 하는 그리드 시스템에서는 개별적인 권한보다는 의사나 간호사 또는 환자 등의 사용자 그룹이 중요하다.

(그림 4) 프록시 인증서의 XML 변환

따라서 그룹별 사용자 계정을 관리하는 문제를 고려할 필요가 있다. 또한 로컬 그리드 영역의 단일 계정에 대한 원격지 사용자의 중복 연결이 가능하도록 현재 그리드의 보안 메커니즘은 구성되어 있으나, 이에 관한 내용 또한 팍스 그리드에서는 자원에 대한 접근여부를 확인하는 등이 시스템 사용에서 중요하게 대두될 수 있는 문제이므로 1:1 매핑 문제를 해결할 필요가 있다. 현재, 에이전트 서버를 구축하여 두 가지 모두를 해결할 방안을 모색하고 있다.

4. 결론 및 향후 연구 내용

본 논문에서는 능력 기반의 신뢰 관리 시스템인 KeyNote와 유사한 방법으로 인증서에 원칙적인 권한을 명시하되, 팍스의 데이터베이스에 맞는 정책 파일을 참고하여 사용자마다 다른 접근 권한을 가지고 로컬 자원에 접근하는 모델을 제안하였다.

그리드 파일과의 연동문제나 웹상으로 확장할 경우에도 문제가 되지 않도록 XML 문서로 프록시 인증서를 변환한 후 확장하여 권한을 추가하였다. 또한 팍스에 알맞은 정책 파일에 따라 사용자의 액세스 권한을 제한하였다. 본 논문에서 제안하는 모델의 장점은 기존의 그리드 인증서를 사용함으로써 로컬 호스트 입장에서는 별도의 인증서를 추가하거나 새로운 보안 메커니즘을 이용하지 않고도, 안전하게 팍스 그리드의 원격지 사용자에게 접근 권한을 부여할 수 있다는 것이다. 또한 사용자 입장에서는 팍스 영역의 사용자가 그리드 노드이기만 하면 별도로 기능을 추가하지 않아도 된다.

향후 연구 내용으로 현재 인증 서버가 다른 그리드 도메인 상에서 자원에 접근하기 위하여 grid-mapfile을 사용하는데, 팍스 사용자가 병원 환경이라는 점을 감안할 때, 이를 자동으로 수행하는 방법이 고안되어야 할 것이며, 실용화를 위해서는 각 자원에 대한 정책을 상세화하는 작업이 중요할 것으로 판단된다.

ACKNOWLEDGMENT

본 연구는 정보통신부의 대학 IT연구센터 지원사업 (IITA-2006-(C1090-0603-0014)) 및 산업자원부의 지역혁신 인력양성사업 지원으로 수행되었음.

참고문헌

[1] Marianne Winslett, et.al, “Negotiating Trust on the Web,” IEEE Internet Computing, 2002.

[2] Sean Turner, Alfred Arsenault “X.509 Public Key Infrastructure” IETF 2002.

[3] Elisa Bertino, Elena Ferrari, Anna Squicciarini, "Trust Negotiations: Concepts, Systems, and Languages," IEEE Web Engineering, July/Aug 2004.

[4] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The Role of Trust Management in Distributed Systems," in Secure Internet Programming, LNCS vol. 1603, Springer, Berlin, 1999, pp. 185-210.

[5] P.Zimmermann, PGP User's Guide, MIT Press Cambridge, 1994.

[6] Matt Blaze, Joan Feigenbaum, Jack Lacy et al, RFC 2704, The KeyNote Trust-Management System Version 2, Sept, 1999.

[7] The Grid Security Infrastructure (GSI), http://www.globus.org/toolkit/docs/3.2/gsi/key/index.html