공공기관을 위한 XML기반의 접근제어 모델에 관한 연구

정성우°, 박제원*,강철오**,원종진**,이남용*
*숭실대학교 컴퓨터학과
**국가보안기술연구소
e-mail:{swjeong°,jwpark}@ssu.ac.kr
{cyberkan,wonjj}@etri.re.kr
Nylee@Computing.ssu.ac.kr

A Study of the XML-based Access Control Model for the public organization

Sung-Woo Jeong°, Jae-Won Park*,
Cheol-Oh Kang**,Jong-Jin Won**,Nam-Yong Lee*
*Department of Computing Graduate School,
SoongSil University
**National Security Research Institute

요 약

국내 공공기관에서는 사이버 행정환경의 기밀성, 무결성, 신원확인, 부인방지등을 보장하기 위하여 행정전자서명인증체계(GPKI:Government Public Key Infrastructure)의 구축과 함께 모든 문서를 XML형태로 표준화하여 공공기관간의 문서를 통합하기 위한 시도를 하고 있다. 하지만 행정전자서명인증체계에서 사용하는 공개키기반(PKI)을 연동한 인증체계는 단순한 사용자 인증만을 제공하여, 공공기관의 응용업무 환경에서 요구되는 다양한 사용자의 직위, 직무, 역할정보 등의 관리가 어려우며 XML형태의 공공문서에 대한 상세한 접근제어를 지원하지 못하는 한계점이 있다. 이러한 한계점을 해결하기 위하여 본 논문에서는 공공기관에서 사용하는 인증 및 접근제어 시스템의 가상시나리오를 통하여 보안문제점을 도출하고 분석한 후에 이를 근거로 공공기관의 보안 문제점을 해결할 수 있는 보안기술인 PMI(Privilege Management Infrastructure)와 XACML(eXtensible Access Control Markup Language)을 연동한 접근제어모델을 제안하였다..

I. 서론

1.1 연구의 배경

국내공공기관의 인증 및 접근제어 시스템은 사용자관리 및 접근권한관리 정책이 기관별, 업무별로 구성되었으며, 이를 각 기관에서 분산되어 운영하고 있다. 이러한 시스템의 사용자들이 업무를 수행하기 위해서는 접근제어시스템의 인증을 거쳐 정보시스템 내부의 접근권한관리 정책에 의해 접근할 수 있도록 사용자 인증 및 접근권한을 부여 받아야 한다. 최근에는 공개키 기반의 인증시스템이 범용적으로 사용됨에 따라 공공기관에서는 인증 및 접근제어 시스템을 공개키기반의 행정전자서명인증체계(GPKI: Government Public Key Infrastructure)와 연동하여 인증을 시행하고 있다. 하지만 행정전자서명인증체계는 신원확인을 위한 간단한 사용자 인증 수준에 머물고 있어 다양한 행정업무 환경에서 요구되는 접근권한, 역할정보 등을 효율적으로 관리하기에는 부족한 실정이다. 이러한 한계점을 해결하기 위하여 정부 및 연구기관에서는 조직의 임무, 지위, 역할 등 다양한 속성정보에 대한 인증을 제공하는 X.509 속성인증서를 이용하는 PMI의 도입과 공공기관의 인증 및 접근제어시의 보안문제점을 해결하기 위한 표준 인증기술과 접근제어기술에 관한 연구가 진행 중이다. 하지만, 공공기관에 적합한 PMI기술과 XACML과 두 기술의 연동에 관한 연구가 미흡한 상태이기 때문에 이에 대한 추가적인 연구가 필요한 상황이다.

본 논문에서는 공공기관의 안전한 접근제어를 위하여 공공기관의 프로젝트 수행 시 발생할 수 있는 시나리오를 작성하고 그 내용을 바탕으로 공공기관에서 발생할 수 있는 인증 및 접근제어 문제점을 도출하였다. 그리고 이러한 문제점의 해결을 위하여 공공기관의 특성을 고려하여 X.509 속성인증서와 표준 인증 및 접근제어기술인 SAML과 XACML을 연동한 PMI기반의 XML접근제어 모델을 제시하였다.

1.2 관련연구

1.2.1 PMI(Privilege Management Infrastructure)

PMI는 인증서 구조에 사용자에 대한 속성 정보를 제공하여 권한 관리가 가능하도록 하는 속성 인증서 기술과 속성 인증서를 발급, 저장, 유통을 제어하는 기반구조이다. PKI는 단순한 사용자의 신원확인만을 제공하는 여권이라면 PMI는 사용자의 속성정보를 통해 다양한 접근제어가 가능한 비자와 같은 역할을 수행한다.

1.2.2 XACML(eXtensible Access Control Markup Language)

SAML과 함께 주로 사용되며, XML기반으로 되어있어 다양한 시스템 사이에서 접근제어정책(Access Control Policy)을 기술하는 표준이다. XACML은 개발자들이 웹을 통해 어떤 사용자들이 접근할 수 있는 지를 결정하는 정책을 기술할 수 있도록 접근제어언어와 요구/응답 언어를 포함하고 있다.

II. 공공기관의 인증 및 접근제어시스템의 보안 문제점 도출

현재 공공기관에서 사용되고 있는 인증 및 접근제어기술의 문제점을 도출하기 위하여 공공기관의 부처간 EA(Enterprise Architecture)구축 프로젝트의 시나리오를 작성하였으며 이를 바탕으로 공공기관의 인증 및 접근제어 시 주요 보안문제점을 분석하고 각각의 문제점이 해결될 수 있는 방법을 제시하였다.

2.1 시나리오를 통한 보안 문제점 도출

다음은 공공기관에서 일어날 수 있는 다음과 같은 예제 상황으로 인증 및 접근제어 관점에서 발생될 수 있는 문제점을 도출해 보고자 한다.

2.1.1 시나리오 작성

[시나리오 1] 팀장에 대한 권한 할당

프로젝트의 프레임워크 구축의 일부인 데이터참조모델(DRM)을 설계하기 위한 팀장급들은 조직의 업무와 시스템을 구성하는 데이터 및 정보를 종합적인 관점에서 표현하기 위해 각 기관의 모든 데이터 및 정보가 필요하게 되었다. 하지만, 행정자치부 및 정보통신부에는 각 부처의 모든 정보 및 파일에 대한 권한할당을 주기에는 국가 보안상 어려움이 있어,

필요한 요청이 올 때마다 데이터 및 정보를 보내주기로 하였다. 하지만 신속히 DRM을 설계하기 위해 필요한 자료를 얻기 위한 문제로 프로젝트를 진행하는 시간이 지연 되었다.

[시나리오 2] 외부 전문가 도입

EA 구축 컨설팅 전문가인 이 교수는 정보통신부의 요청에 의해 이 프로젝트에 참여하게 되었다. 이 교수는 컨설팅을 하기 위해 필요한 자료와, 기술현황 및 사용 장비에 대한 권한이 필요하여 이를 정보통신부와, 행정자치부에 요청하게 되었고, 이러한 요청에 따라 각 부처는 필요한 자료는 XML형태로 된 문서를 홈페이지를 통해 정보를 보냈지만, 부분적인 각 페이지에 보안에 관련된 사항이 부분적으로 있어, 필요한 정보 중 보안사항이 첨가된 부분은 삭제하고 정보를 보내어 이 교수는 자신이 원하는 정보 중 일부는 볼 수 없게 되었다. 이 교수는 결국 계속적으로 정보 요청을 하게 되었고, 각 부서는 이를 원활히 해결하기 위해 노력하였지만, 프로젝트를 진행하는데 많은 시간이 지연되는 불편을 겪고 있다.

[시나리오 3] 내부 보안문제 해결

정보통신부 김 차장은 프로젝트를 진행하기 위한 정보통신부의 책임자로, 내부적으로는 정보통신부의 내부보안 유출을, 외부적으로는 EA구축을 위한 협조의 책임을 가지고 있다. 그는 정보통신부에서 사용하는 현 전자정부에서 사용하고 있는 공개키인증시스템(PKI)과 EAM(Enterprise Access Management)시스템과 연동하여 내부적 보안과, 외부적 보안을 모두 해결하려 하였으나, 각 인원에 관한 속성인증서 발급 문제와 XML문서에 관한 접근제어에 관한 문제가 발생하여, 새로운 보안 기술의 도입을 시도하였다.

2.2 시나리오에서 도출된 보안 문제점 및 해결방안

[문제점 1] “시나리오 1”, “시나리오 2”에서는 공공기관의 XML문서에 대한 접근권한관리 시에 현재의 접근제어기법으로는 단순한 허가, 거부는 가능하지만 XML문서에 대한 상세한 접근제어를 지원하지 못한다는 문제가 발생한다.

[문제점 1의 해결방안] 기존의 공공기관의 접근제어 기법인 강제적 혹은 임의적 접근제어 기법을 통해 공공기관의 XML문서에 대한 접근제어를 할 경우 XML문서에 대한 허가,거부 같은 단순한 접근권한 관리는 가능하지만, XML문서내의 엘리먼트 별 상세한 접근제어는 불가능하다. XML문서의 상세한 접근제어를 위하여 XML접근제어기술 표준인 XACML을 적용하여 XML문서에 대한 동적인 권한관리를 수행한다. 이는 각각의 사용자별, 역할별 인증 정보를 바탕으로 접근제어 정책에 따라 접근권한을 평가한 후에 권한에 따른 XML문서의 상세한 접근 허가 여부를 판단하여 문제를 해결한다.

[문제점 2] “시나리오 1”, “시나리오 2”, “시나리오3”에서의 EA구축을 위한 공공기관간의 웹서비스를 연동할 경우 현재의 인증 보안 시스템은 동일한 서비스에 대하여 한번의 인증이 아니라 여러 번의 사용자 인증을 거쳐야 하므로 보안시스템의 유연성이 부족하다.

[문제점 2의 해결방안] EA 프레임워크에서는 업무와 정보시스템의 연계를 위하여 다수의 기관 및 부처간의 웹 서비스 연동에 대한 요구가 예상된다. 현재의 인증보안시스템은 사용자가 동일한 서비스를 사용하더라도 여러 기관의 인증을 각각 받아야 한다. 따라서 동일한 서비스 사용 시에는 한 번의 인증으로 정의된 보안 정책에 따라 정해진 시간 동안 유효한 인증을 받으며 웹 서비스 호출을 위한 인증까지 받을 수 있도록 웹 서비스 기반의 SSO를 구축해야 한다. 이를 위해 SAML과 같은 SSO관련 표준을 적용하고, 보안 정책을 표준화된 방식으로 정의하고 공유하여 위와 같은 문제점을 해결한다.

[문제점 3] “시나리오 3”에서의 행정기관에서 사용하고 있는 공개키인증서를 이용한 인증방식은 단순한 신원확인은 가능하지만 공공기관내의 직무, 지위, 역할 같은 다양한 속성정보가 필요한 인증 시에 적용하기에는 비효율적이다.

[문제점 3의 해결방안] EA도입과 함께 지식정부를 위한 정부조직의 변화에 따라 기존의 관료제적인 정부조직과 신축적인 정부조직을 위한 다양한 인증의 지원이 필요하게 되었다. 현재 사용되고 있는 국내 행정기관의 인증기반인 GPKI는 단순한 신원확인은

지원하지만 행정기관내의 임무, 지위, 역할 등과 같은 다양한 속성정보에 대한 인증기능의 제공에는 한계가 있다. 따라서 이를 해결하기 위해 기존의 공개키인증서는 그대로 활용하여 신원확인을 하며 사용자의 속성정보에 대한 인증을 제공하기 위한 속성인증서를 제공하여, 공개키인증서와 병행하여 사용할 수 있도록 하여, 문제를 해결하도록 하였다.

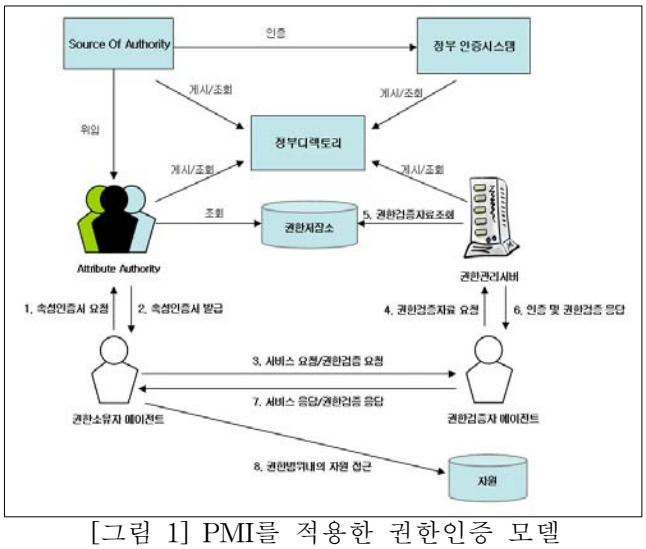
III. 공공기관의 특성을 고려한 PMI기반의 XML접근제어모델

3.1 PMI기반의 XML접근제어모델

논문에서 제안하는 모델은 우선 예상되는 공공기관 보안모델을 시나리오로 작성한 후, 이에 발생되는 보안요구사항의 도출 후 이를 해결 할 수 있는 보안모델을 제시하였다. 기존의 정부 조직에서 수행하는 행정전자서명인증체계(GPKI)를 정부기반의 조직이라고 가정하고, 도출된 보안요구사항을 해결할 수 있는 보안 기술로 속성인증서 기반인 PMI와 XML접근제어 기술인 XACML을 연동한 보안모델을 제시하였다. 모델은 크게 PMI모델과 XACML 모델 두 개로 구성되어 있으며, 각 모델은 서로 유기적으로 연동하여 정보를 주고받는 구조를 띄고 있다. 우선 PMI모델을 통해 인증을 받고 인증 받은 사용자는 인증정보를 XACML모델로 보내 최종적인 접근제어정책에 따라 자원에 대한 접근권한을 갖게 된다.

3.1.1 PMI 모델

공공기관의 권한관리를 위한 PMI모델은 [그림 1]와 같으며, 기존의 행정전자서명인증체계와 연동하기 위해 PMI의 핵심 구성요소인 권한소유자 에이전트(Privilege Holder), 권한검증자 에이전트(Privilege Verifier), 권한관리서버(Privilege Manager), Source of Authority, Attribute Authority를 포함한다. 그리고 전자서명인증서를 발급하는 정부인증시스템과인증서와 인증서폐지목록을 게시하는 정부 디렉토리로 구성한다. PMI모델에서 사용자가 정보시스템에 접근하기 위한 권한인증 처리흐름은 다음과 같다.

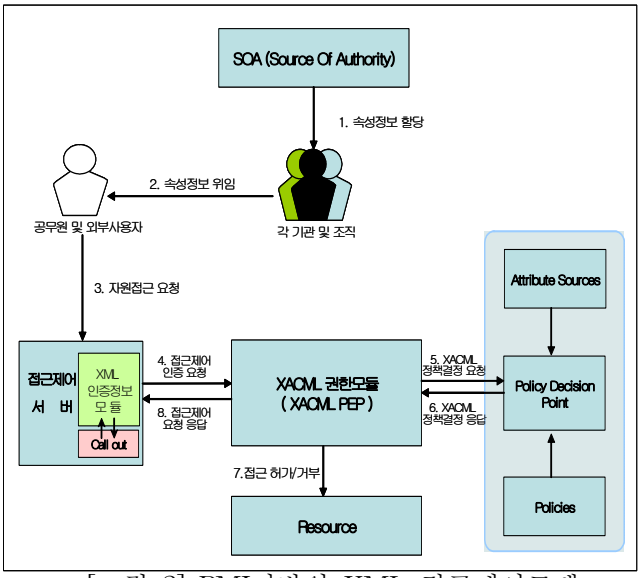


[그림 1] PMI를 적용한 권한인증 모델

1. 권한소유자 에이전트는 속성인증서 요청형식을 작성하여 AA에게 속성인증서의 발급을 요청한다.
2. AA는 각 사용자에 대한 권한정책을 참조하여 속성인증서를 권한소유자 에이전트에게 발급한다.
3. 권한소유자 에이전트는 신원인증을 위한 전자서명인증서와 속성정보를 통한 권한관리를 위한 속성인증서를 사용하여 권한검증자 에이전트에게 자원에 대한 접근서비스의 요청 및 권한에 대한 검증을 요청한다.
4. 권한검증자 에이전트는 사용자의 접근서비스를 검증하기 위해 사용자에 대한 신원인증과 권한검증을 위한 자료를 권한관리서버에게 요청한다.
5. 권한관리서버는 사용자에 대한 인증 및 권한검증을 위해 권한저장소에 접근하여 자료를 수집하며, 경우에 따라서는 정부디렉토리까지 접근하여 필요한 자료를 수집한다. 그리고 권한관리서버는 자신이 갖고 있는 SOA의 속성인증서와 권한검증자 에이전트가 전달한 최상 위 인증기관 속성인증시스템의 속성인증서를 비교하여 검증한다.
6. 권한검증자 에이전트는 권한관리서버로부터 인증 및 권한검증을 위한 정보를 수신하여 권한소유자 에이전트가 요청한 권한에 대한 검증을 완료한다.
7. 권한검증자 에이전트는 접근서비스의 응답 및 권한에 대한 검증결과를 권한검증자 에이전트에게 전달한다.
8. 권한소유자 에이전트는 권한검증결과를 받은 후에 권한정책에서 주어진 권한소유자의 권한범위내의 자원을 접근한다.

3.1.2 PMI기반의 XML 접근제어모델

[그림 2]는 XACML을 권한 인증 접근제어 시스템의 아키텍처를 나타내고 있다. 본 논문에서는 XACML이라는 보안기술을 사용하여 속성정보를 받아 접근제어 할 수 있게 한다.



[그림 2] PMI기반의 XML 접근제어모델

[그림 2]는 PMI모델로부터 속성인증을 받은 사용자가 자원 사용을 요청하여 자원사용의 권한을 획득하는 시스템 아키텍처를 묘사한 그림이다. 접근 순서를 살펴보면 다음과 같다. 우선 PMI모델로부터 인증을 받은 상용자가 접근제어 서버에 자원 접근을 요청하게 되면, 접근제어 서버는 사용자의 인증 정보를 요청하게 되고 사용자는 인증 정보를 서버로 보내게 된다. 서버는 인정정보를 사용하기 위해 내부 모듈인 XML 인증정보 생성모듈을 호출하게 되고, 인증정보 생성모듈은 X.509에 있는 문서를 XML형태로 인코딩하여 XACML 권한모듈이 읽을 수 있는 형태로 문서를 변환하게 된다. 변환된 정보

는 오류가 없을 경우 서버로 리턴 된 후 바로 XACML 권한모듈로 정보를 보내는 과정을 거치게 된다. XACML권한모듈은 사용자에게 자원 접근에 관한 정책을 결정하기 위해 PDP로 정보를 보내 사용자 별 정책을 결정하게 한다. PDP로부터 정책에 관한 결정을 응답 받은 XACML권한모듈은 자원에 관한 접근 허가/거부를 정책에 따라 사용자/엘리먼트별로 구분하여 권한을 할당하게 되며, 사용자는 자원에 대한 권한을 할당 받아 사용할 수 있다.

IV. 결론 및 향후연구

현재 공공기관의 인증을 위한 행정전자서명인증체계는 신원 확인을 위하여 PKI기반의 사용자 인증을 사용하고 있는데, 이는 다양한 속성정보를 이용한 인증 시 나타나는 한계점과, 접근권한, 및 역할정보 등을 효율적으로 관리할 수 없는 단점이 있다. 또한 각 부처별로 독립적으로 접근제어시스템이 구축되고 운영됨에 따라 공공기관을 위한 통합권한관리체계 구축 시 상호연동성과 호환성에 문제가 발생 할 수 있다. 본 논문에서는 이러한 문제점의 해결을 위해 공공기관의 특성을 고려한 XML기반의 접근제어에 관한 보안모델을 제시하였다. 제시는 다음과 같은 시나리오작성, 보안요구사항 도출, 인증 및 접근기술 적용의 적용의 세 가지 단계를 통하여 공공기관의 특성을 고려한 접근제어 모델을 제시하였다. 제안한 모델은 공공기관에서 발생할 수 있는 시나리오를 통해 발생할 수 있는 상황에 맞게 설계하였으며, 그 특징을 다음과 같이 다섯 가지 특징으로 정리할 수 있다. 첫째, 공공기관에서 EA프로젝트시 일어날 수 있는 문제점을 중점으로 시나리오를 작성하였다. 둘째, EA를 위한 공공기관의 특성 및 상황을 고려한 주요 보안요구사항을 도출하였다. 셋째,도출된 보안요구사항을 해결하기 위하여 최신 국제 표준 인증기술 및 접근제어기술을 적용하여 접근제어 모델을 제시하였다. 넷째, 제시한 접근제어모델은 현재 공공기관에서 사용하고 있는 행정전자서명인증체계와 연동 및 개선을 위하여 PMI역할모델을 적용한 속성인증서를 병행하여 사용함으로써 다양한 사용자의 속성정보에 대한 인증이 가능하도록 하였다. 다섯째, OASIS의 표준 XML보안기술인 SAML과 XACML을 연동하여 싱글사인온과 복잡한 권한관리정책관리가 가능할 뿐 아니라, XML접근제어의 표준적용 및 상세한 접근제어를 통하여 안전하고 효율적인 XML 접근제어 또한 가능도록 하였다.

결론적으로 우리가 제안한 공공기관의 특성을 고려한 PMI 기반의 XML 접근제어 모델은 기존의 공공기관에서 사용하는 인증체계를 기반으로 필요한 보안기술을 통합하였기 때문에 각 기관에서 사용하는 보안기술과 함께 연동하여 보다 향상된 보안 시스템의 구축과 연동이 가능하게 될 것이다.

향후 연구로는 제시한 모델을 기반으로 공공기관의 접근제어시스템의 구축을 위하여 OASIS의 XACML과 W3C의 XML 서명, XML 암호화, XKMS(XML Key Management Specification)와 연동을 위한 프로파일의 개발 및 테스트에 관한 연구를 진행할 것이다. 또한 XACML의 표준화 진행에 따른 NIST의 역할기반 접근제어의 단계별 적용에 대한 연구도 병행할 것이다.

참고문헌

[1] R Sandhu, E.J.Coyne, H.L.Feinstein, and C.E. Youman, “Role Based Access Control Model”, IEEE Computer, February 1996.

[2] J.Park, G.Ahn, and R.Sandhu, “RBAC on the Web using LDAP”, In Proceedings of the 15th IFIP WG 11.3 Working Conference on Database and Application Security, July 2001.

[3] J.Park, R.Sandhu, and G.Ahn., “Role-based Access Control on the Web”, ACM Transactions on Information and System Security, February 2001.

[4] L.Zhang, G.Ahn, and B.Chu, “A Rule-Based Framework for Role-Based Delegation”, In Proceedings of ACM Symposium on Access Control Models and Technologies, May 2001.

[5] ITU-T, “ITU-T Recommendation X.509. Information Technology: Open Systems Interconnection -The Directory: Public-Key And Attribute Certificate Frameworks”, ITU-T, 2000.

[6] Markus Lorch, “First Experiences Using XACML for Access Control in Distributed Systems”. ACM Workshop on XML Security, 2003

[7] 김봉환, 김기수, 원유재 “RBAC을 이용한 PMI기반 권한관리, 한국정보처리학회”, 정보처리학회지, 2003. 10

[8] 진승헌, 최대선 ″속성인증기술과 PMI″, 한국정보보호학회, 정보보호학회지, 2000. 12

[9] 추경균, “정부의 행정전자서명인증체계(GPKI) 활성화 및 발전방안”, 정보보호학회 논문지, 2004. 4

[10] 심완보, 박석 “애드호크러시 조직의 특성을 고려한 역할기반모델”. 한국정보보호학회, 정보보호학회지, 2002. 8