유비쿼터스 컴퓨팅 환경에서의 XML접근제어 모델 설계

정성우° 박중선 이남용
숭실대학교 컴퓨터학과
{swjeong°, whybear}@ssu.ac.kr
nylee@computing.ssu.ac.kr

Design for XML-based Access Control Model in the Ubiquitous Computing Environment

SungWoo Jeong° Joongsun Park NamYong Lee
Department of Computing Graduate School, SoongSil University

요 약

유비쿼터스 컴퓨팅 환경에서는 정보에 대한 접근이 시간과 공간의 제약 없이 이루어지므로 기존의 접근제어기법을 그대로 적용하는 것은 보안상의 취약점이 노출되어 중요한 정보자원의 유출의 위험을 가진다. 따라서 유비쿼터스 컴퓨팅 환경의 특성을 고려한 보안사항을 만족시키기 위해서는 단순한 신원확인 뿐만 아니라 사용자 속성 정보를 이용한 인증이 필요하다. 그리고 XML자원에 대한 상세한 접근제어 및 유비쿼터스 컴퓨팅의 다양한 환경정보와 복잡한 접근제어정책을 효율적으로 관리할 수 있는 접근제어모델이 필요하다. 이를 위하여 본 연구에서는 PMI의 속성인증서와 표준XML접근제어 기술인 XACML을 적용한 접근제어 모델을 제시한다.

1. 서 론

유비쿼터스 컴퓨팅은 언제, 어디서나 사용자가 접속하여 원하는 정보와 서비스를 제공 받을 수 있도록 다중 디바이스와 현실 세계를 연결하는 기술이다. 이러한 유비쿼터스 컴퓨팅 환경에서는 다수의 사용자가 다수의 정보객체, 센서, 시스템과 커뮤니케이션을 하기 위해 접근하기 때문에 정보 유출의 위험이 증가하게 되어 정보보안에 대한 경각심을 갖고 다양한 인증 방식 및 유연한 접근제어 기법과 함께 이를 지원할 수 있는 보안기술을 도입해야 한다. 이를 위하여 본 논문에서는 유비쿼터스 컴퓨팅의 인증 및 접근제어시의 보안문제점 해결을 위해서 조직의 임무, 지위, 역할 등 다양한 속성정보에 대한 인증을 제공하는 X.509 속성인증서와 XML문서 및 자원에 대한 상세한 접근과 복잡한 접근제어정책을 관리할 수 있는 XACML을 적용한 XML기반 접근제어 모델을 제시한다.

2. 관련연구

2.1 PMI(Privilege Management Infrastructure)

PMI는 PKI(Public Key Infrastructure)인증서에 사용자에 대한 속성 정보를 삽입하여 권한 관리가 가능하도록 하는 속성 인증서 기술이며 속성 인증서 발급, 저장, 유통을 제어하는 기반구조이다. PKI는 단순한 사용자의 신원확인만을 제공하는 여권이라면 PMI는 사용자의 속성정보를 통해 다양한 접근제어를 가능하게 하는 비자와 같은 역할을 수행한다.[7]

2.2 XACML(eXtensible Access Control Markup Language)

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 및 응답 언어를 포함하고 있다.[6]

<표 1> 환경에 따른 접근제어의 특성 비교

비교항목	전통적인 정보시스템 환경에서의 접근제어	유비쿼터스 컴퓨팅 환경에서의 접근제어
주체	인간 사용자, 프로세스	인간 사용자, 프로세스, 지능형 장치
객체	파일, 데이터베이스, 프로그램	지능형 장치(지능형 장치의 특정 기능)
접근의 형태	read, write, execute	read, write, execute, turn on/off, push, touch
세션	생성, 유지 종료의 안정성	세션 개념의 적용이 어려움
권한의 유효성	정적으로 유지됨	컨텍스트에 따라 동적으로 변화함

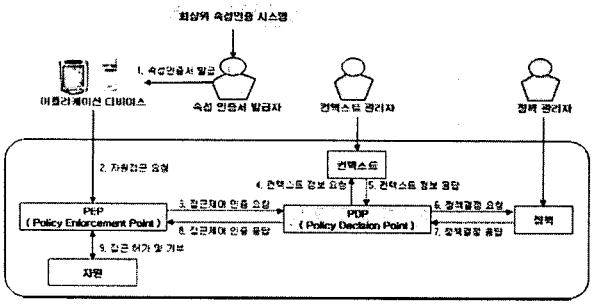
2.3 xoRBAC

xoRBAC는 상황 정보를 접근제어 결정에 이용하기 위하여 역할 기반 접근제어의 제약사항을 사용하는 모델이다. 상황 제약사항은 미리 정의된 조건이 있어 상황 정보 속성의 실제 값과 비교하는 역할 기반 접근제어 제약사항이다. 권한결정은 여러 개의 상황 제약과 관련되고 모든 상황 제약이 참 값을 가질 때 접근이 허용된다.

2.4 유비쿼터스 컴퓨팅 환경과 접근제어 기법

유비쿼터스 컴퓨팅 환경은 사용자가 컴퓨터나 네트워크를 장소에 상관없이 자유롭게 네트워크에 접속할 수 있기 때문에 기존의 정보시스템과 달리 다음과 같은 접근제어시에 다른 특징을 보인다. 이러한 특징을 바탕으로 유비쿼터스 컴퓨팅 환경의 인증 및 접근제어 시 주요 보안문제점을 분석하고 각각의 문제점이 해결될 수 있는 방법을 제시할 수 있다. <표 1>은 전통적인 정보시스템에서의 접근제어와 유비쿼터스 컴퓨팅 환경에서의 접근제어를 비교하여 유비쿼터스 환경에서의 접근제어가 갖는 특징을 정리한것이다.[10]

3. 유비쿼터스 컴퓨팅 환경의 특성을 고려한 PMI기반의 XML접근제어모델



[그림 1] 유비쿼터스 컴퓨팅 환경에서의 XML기반 접근제어모델

[그림 1]은 유비쿼터스 컴퓨팅 환경에서의 XML기반 접근제어모델을 나타내며 XACML을 사용한 속성인증서 정보를 이용하여 상세 접근제어를 하는 과정을 나타낸다. 과정에 대한 상세 설명은 다음과 같다.

1. 속성인증서 발급 : 공개키인증서와 같은 신원확인과 함께 사용자의 역할, 직급등과 같은 다양한 속성을 통한 인증을 제공하는 속성인증서를 발급받는다.
2. 자원접근 요청 : 유비쿼터스 환경에서는 컴퓨터뿐만 아니라 PDA, 휴대전화등 다양한 어플리케이션 디바이스가 존재하며 이를 통하여 접근제어 시스템에 원하는 정보 및 자원에 접근을 요청하게 된다.
3. 접근제어 인증 요청 : 속성인증서에 의하여 인증된 사용자의 자원 접근 요청을 PEP가 PDP에 전달한다.
4. 컨텍스트 정보 요청 : PDP는 다양한 유비쿼터스 환경에 관한 정보를 얻기 위하여 컨텍스트 관리자가 설정한 컨텍스트 정보를 요청한다.
5. 컨텍스트 정보 응답 : 컨텍스트는 해당 자원 요청 환경을 고려하여 요청 정보에 대한 응답을 한다.
6. 정책결정 요청 : 자원에 대해 정책 관리자가 설정한 다양한 정책에 대한 접근요청을 한다.
7. 정책결정 응답 : PDP는 정책을 받아 속성인증서에 의한 사용자 정보와 다양한 컨텍스트 및 복잡한 정책을 고려하여 정책결정에 대한 응답을 한다.
8. 접근제어 인증 응답 : PEP는 PDP의 정책결정응답을 받아 사용자 및 XML 엘리먼트 별로 자원에 관한 접근 허가 및 거부 권한을 할당한다.
9. 접근 허가 및 거부 : 사용자는 8번에서 할당된 권한에 의해 자원에 대해 접근할 수 있게 된다.

본 논문에서 제안한 XML접근제어모델은 다음과 같은 특성을 갖는다.

첫째, 기존 공개키인증서에 추가로 속성인증서를 병행하여 사용함으로서 다양한 속성에 대한 인증이 가능하다. 둘째, 유비쿼터스 컴퓨팅 환경에서 사용자의 컨텍

스트를 고려하여 정보자원 및 서비스에 유연하고 효율적인 접근제어가 가능하다. 셋째, XML기반 접근제어기술인 XACML을 사용함으로써 다양한 장치에서 XML 정보자원에 대한 엘리먼트별 상세한 접근제어가 가능하다.

4. 결론 및 향후연구

유비쿼터스 환경에서는 어플리케이션과 서비스가 항상 고정되어 있는 것이 아니라 동적으로 결합되고 분리되므로 사용자가 실행한 어플리케이션이 신뢰할 수 있는지에 대한 검증 및 어플리케이션이 이용하려고 하는 서비스에 대한 동적인 접근권한관리가 요구된다. 그리고 사용자마다 다른 역할 및 접근권한을 부여하여 유비쿼터스 환경에서 사용자의 다양한 상황정보를 고려한 유연하고 효율적인 접근제어가 필요하다.

이에 본 논문에서는 PMI의 속성인증서와 신원확인 뿐만 아니라 역할 및 직급에 따른 다양한 속성정보를 통한 인증이 가능하도록 하였다. 그리고 XML접근제어기술인 XACML과 컨텍스트를 결합하여 다양한 사용자의 상황 및 복잡한 정책을 지원하는 동적인 접근권한 관리를 제안하였다.

향후 연구로는 유비쿼터스 컴퓨팅 환경은 매우 다양하고 시스템 구축의 종류가 서로 다르기 때문에 이를 지원하기 위해서 중앙의 인증 및 접근제어 시스템 뿐만 아니라 개별 소규모 접근제어 시스템에 대한 접근제어 모델이 연구되어야 한다. 그리고 앞서 제시한 접근제어 모델을 기반으로 OASIS의 XACML과 W3C의 XML 서명, XML 암호화, XKMS(XML Key Management Specification)와 연동을 위한 프로파일의 개발 및 테스트에 관한 연구가 진행되어야 한다.

5. 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] 심완보, 박석 "애드호크러시 조직의 특성을 고려한 역할기반모델". 한국정보보호학회, 정보보호학회지, 2002. 8

[10] 오세종, 박제호, "유비쿼터스 컴퓨팅 환경에서의 접근제어 모델을 위한 요구사항 분석", 정보처리학회지, 2004. 12