특 집

권한관리를 위한 기반기술

김 봉 환, 원 유 재, 손 중 만
(주)아이에이시큐리티

요 약

기업간 파트너쉽이 e-비즈니스 네트워크로 발전하면서 사용자에 대한 안전하고 효과적인 인증은 물론 인증된 사용자의 특정 서비스에 대한 접근권한의 관리요구가 크게 대두되고 있다. PKI 기반 기술로 사용자 인증, 데이터 기밀성 및 무결성 서비스는 가능하지만 사용자 및 자원에 대한 권한 관리는 별도의 기반기술이 요구된다. 웹 사이트들을 파트너 쉽으로 연결해주는 크로스 도메인간의 단일인증, 보호 대상 자원에 대한 접근제어, 파트너간의 상호연동성 및 이기종 연동 등의 요구사항을 만족시키기 위한 권한관리 기반기술이 필요하다. 본고에서는 PMI 표준, 접근제어, RBAC, SAML 및 XACML 기술에 대한 소개와 권한관리 시스템 구축 모델에 대하여 설명한다.

I. 서 론

최근 모든 어플리케이션으로부터 독립적으로 적용되면서 다양한 어플리케이션의 사용자 보안관리를 통합적으로 수행해 조직의 사용자 보안관리를 반영구적으로 수행할 수 있는 권한 관리 인프라 구축의 필요성이 대두되고 있으며 이를 권한관리 기반구조(Privilege Management Infrastructure, 이하 PMI) 개념을 통해 달성하고자 하는 시도가 실질적으로 진행되어 오고 있다. 즉, 사용자 보안 관리를 특정 어플리케이션에 종속적으로 제공되어온 보안 기능이 아닌 새로운 어플리케이션 개념의 PMI 도입, 새로운 사용자의 추가/삭제/변경 등에 유기적으로 대처할 수 있는 보안 관리의 기반구조로의 인식이 증가하고 있다.

이와 관련된 연구가 몇몇 표준화 단체에서 진행되고 있다[7,8,9]. 그 중에서도 IETF의 RFC 3281을 기반으로 하는 권한관리 기반구조를 현실적인 대안으로 여겨지고 있다. RFC 3281에서는 사용자(속성인증서 소유주)의 속성정보를 속성인증서(Attribute Certificate, 이하 AC)의 형태로 발급하고 운용하는 모델을 제시하고 특히 속성정보 중에서 그룹, 역할, 클리어런스 등을 정의하고 있다[9].

현재 기업 비즈니스 조직은 역동적인 구조로 변하고 있기 때문에 사용자와 자원에 대한 관리를 더욱 복잡하게 만든다. 효과적인 사용자 인증과 인증된 사용자에게 적절한 자원을 제공하기 위하여 역동적인 조직구조를 효과적으로 표현하고 구현할 수 있는 접근제어 기법이 요구되고 있다. 역할기반 접근제어(Role Based Access Control, 이하 RBAC)은 사용자와 서비스에 대한 접근권한 간의 관계성을 역할이라는 개념을 도입하여 사용자와 역할, 역할과 접근권한이라는 2단계 구조의 접근제어 기법이다. 권한관리 기반구조의 속성 인증서에 사용자 및 정보자원에 대한 그룹 및 역할을 적용하는 방법론으로 이용될 수 있다.

본 고에서는 보안 정책 기반의 권한관리를 위한 기반 기술에 대하여 간단하게 소개한다. 정책

기반의 권한관리를 위해서는 인프라로서의 권한 관리 구조가 기반을 이루어져야 하며 사용자 및 정보자원의 특성에 따라 접근권한 관리를 할 수 있어야 하며 이러한 접근권한 관리 정보를 안전하고 표준적인 방법으로 유통시킬 수 있는 기술이 필요하다. 관한관리 인프라로서 AC 기반 PMI 기술을 설명하고, 사용자 및 정보자원의 특성의 정의 및 표현을 위해서 RBAC 및 XACML 기술을 설명하며 안전하고 표준적인 인증/인가 정보의 유통을 위하여 SAML 및 XACML 기술을 설명한다. 또한 AC 기반의 PMI 기술과 RBAC 및 XACML/SAML을 융합한 통합인증 권한관리 시스템 구축 모델을 제시한다.

본 논문은 다음과 같이 구성되어 있다. II 장에서는 PMI 표준에서 언급하는 AC 기반의 권한관리 인프라, 접근제어 일반 기술, RBAC 개요 및 적용 기술, SAML 및 XACML 기술에 대하여 설명하고 III장에서 결론을 맺는다.

II. 권한관리 기반기술

1. PMI 표준

1) PMI 개념

PMI는 그 용어에서 내포하고 있는 것처럼, IT 환경에서의 사용자들에 대한 서비스 수행 권한을 관리하는 기반구조라고 할 수 있다. 즉, 인트라넷, 엑스트라넷 기반의 조직 업무 및 비즈니스 수행 환경에서 정의된 사용자 보안 정책 기반의 권한관리 기반구조를 달성하는 제반 보안 관리 시스템으로 설명할 수 있다. 따라서 PMI에서는 정보서비스 환경에서 이용 가능한 권한, 지위, 임무 등과 같은 사용자들의 속성을 정의하여 사용자들에 대한 권한 정보(예, 〈사용자, 권한〉)를 표준화된 형태로 관리할 수 있는 체계를 정의하고 있으며 또한 이러한 권한 정보의 생성, 변경, 이용, 폐기 등과 같은 Life Cycle을 관리할 수 있는 체계를 정의하고 있다.

현재, 인터넷과 같은 개방된 네트워크 환경에서 사용자 인증을 위해 PKI(Public Key Infrastructure) 기술이 보편적으로 사용되고 있다. 일반적으로 PKI는 비 대면의 특성을 지닌 정보화 환경에서 특정 사용자의 신원을 공식적으로 확인해 주는 사용자 인증 관리 체계라 할 수 있고, PMI는 정보화 환경에서 특정 사용자가 어떠한 정보서비스 수행의 권한을 보유하고 있는지를 관리하는 체계라는 측면에서 PKI는 여권, PMI는 비자의 개념으로 비유되어 설명할 수 있다.

최근, 이러한 PMI 개념을 달성하는 다양한 시스템 구현 모델이 제시되고 있으나, 일반적으로 IETF의 PKIX 워킹 그룹에서 제안하고 있는 AC 관리 체계가 PMI 개념의 기술적 실체로 제시되고 있는 상태이다. 즉, 사용자 인증은 PKI 기반의 공개키 인증서를 통해, 사용자 권한관리는 PMI 기반의 AC를 통해 달성하고자 하는 노력이 PMI의 가장 보편적 현상으로 볼 수 있다.

2) PMI 관련 기술 동향

본 절에서는 앞 절에서 언급한 바와 같이 PMI의 보편적인 개념으로 인식되고 있는 IETF PKIX 워킹 그룹의 AC 관리 체계를 중심으로 기술적 동향을 살펴본다.

PMI 기술은 다음과 같은 3가지 방향의 표준화 작업을 통해 진행되어 오고 있다.

- IETF PKIX 워킹 그룹의 X.509 3rd Edition 정의
- ITU-T SG8의 X.509 Version 4에서 AC와 AC 관리 체계 기술
- IETF PKIX 워킹 그룹의 IETF3281 : An Internet Attribute Certificate Profile for Authorization 정의

IETF의 PKIX 워킹 그룹에서는 PKI 개념의 표준화를 구체화하면서, 정보화 환경에서 표준화된 방식의 권한 관리의 중요성을 인식하고 이를 PKI 체계 내에서 수용하고자 하는 노력으로 X.509 3rd Edition에서 PKI 인증서의 확장 필드에 권한 정보를 추가하고자 하는 시도로 PMI

〈표 1〉 AC 표준 필드 및 내용

version	Attribute Certificate의 버전 : Default V2
Serial Number	발급된 Attribute Certificate의 일련번호
Signature Algorithm ID	AA가 발급한 Attribute Certificate의 서명에 사용한 서명 알고리즘
Issuer Name	AA의 이름
Holder	Attribute Certificate 소유자 이름
Validity	Attribute Certificate의 유효기간
Attributes	Attribute Certificate 소유자에게 할당된 속성(권한)정보 리스트
Issuer Unique Identifier	Attribute Certificate 발급자 식별을 위한 추가 D 정보
Extensions	Attribute Certificate 정보의 확장 필드
Signature	AA의 서명값

개념 도입을 시작했으나, 일반적으로 공개키 인증서의 1년 이상의 긴 유효기간 특성과 권한정보의 1일 이내의 짧은 유효기간 특성의 차이와 PKI 인증 관리 체계의 주체인 CA(Certificate Authority)가 사용자의 권한 속성 관리 역할 수행의 부적절성 등의 문제점으로 실제적으로 구현되기 어렵다.

이후로 ITU-T의 X509 version 4 AC 및 AC 관리 체계 정의 시도와 IETF PKIX 워킹 그룹의 AC 프로파일 및 관리 체계의 정의 시도가 이루어졌으며 상기의 두 개념은 기본적으로 거의 일치하지만, ITU-T의 X.509 인증서 기반 PKI 개념이 인터넷 환경에 직접 적용하기에 복잡한 요소를 포함하고 있어 현재 IETF의 RFC 3281을 기반으로 한 PMI 개념 구현이 주류를 이루고 있는 실정이다.

IETF3281에서는 X.509 인증서 기반의 PKI의 주요 엔터티 및 인증서 구조체, 인증서 발급 관리의 기본 개념을 이용해 다음과 같은 주요 요소에 대한 표준화를 중점적으로 정립하고 있다.

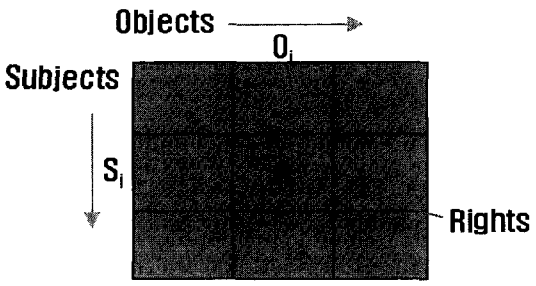
1. 사용자와 사용자의 권한정보 매핑 관리를 위한 AC 구조체 정의
2. AC의 생성/발급, 폐지, 갱신, 검증 등 유통 관리 메커니즘의 정의
3. PMI 상에서의 주요 Entity의 정의

AC의 표준 필드 구조 및 내용은 〈표 1〉과 같다.

2. 접근제어 기술

접근(Access)이란 컴퓨터 내 자원의 사용, 변경, 조회 등 어떤 행위를 할 수 있는 능력을 말하며 접근제어는 접근을 허용하거나 제한할 수 있는 수단이라 말할 수 있다. 전통적으로 접근제어(Access Control)는 보안영역 중에서 상대적으로 가장 상위의 어플리케이션에 대한 관리적 보안을 의미한다. 여기서 접근제어가 관리적인 보안의 개념을 띄는 것은 IT 환경의 다수 사용자와 다수의 어플리케이션을 제공하고 있다는 특성과 접근 권한이 있는 사용자들에게만 특정 데이터 또는 자원들이 제공되는 것을 보장하기 위한 자원관리의 특성을 가지고 있기 때문이다.

접근제어의 모형은 접근 메트릭스 모델에 의해 설명될 수 있다. 〈그림 1〉은 접근메트릭스 모델을 나타낸다. 그림에서 서브젝트는 일반적으로 사용자에 해당하는 개념이며 오브젝트는 리소스의 개념이며 권한은 접근하여 수행할 수 있는



〈그림 1〉 접근 메트릭스 구조

행위를 나타낸다. 이 모델을 기반으로 에이클(Access Control List, ACL), 케이퍼빌리티(Capability) 및 릴레이션(Access Control Triple)의 형태로 구현될 수 있다.

에이클은 각 오브젝트에 〈Si, Ri〉 쌍의 리스트를 유지하는 형태로 구현되며 케이퍼빌리티는 서브젝트에 〈Oi, Ri〉 쌍의 리스트를 유지하는 형태로 구현되며 릴레이션은 〈Si, Oi, Ri〉의 트리플 튜플로 유지되는 관계 DB의 기본적인 레코드 형식이다.

또한 응용 수준에서 실제로 보안정책을 적용하는 접근제어 기법으로는 강제적 접근제어(Mandatory Access Control, MAC)과 임의적 접근제어(Discretionary Access Control, DAC) 크게 구분할 수 있다.

강제적 접근제어는 각 정보에 결합된 보안 등급과 사용자에게 부여된 인가등급을 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 사용자에게만 접근 권한을 부여하는 보안정책으로서, 군사적 환경과 같이 정보의 기밀성이 매우 중요시되는 환경에서 사용되고 있지만 보안 등급과 같이 확연하게 구분되는 기준의 설정이 모호한 경우에는 적용에 한계가 있다.

임의적 접근제어는 사용자 본위로 접근권한을 정의하는 방법으로 사용자의 식별(identification)과 권한인가에 기초한 접근제어 방식이다. 만일 사용자가 특정 모드로 객체에 접근할 수 있다는 것을 기술하는 권한을 소유하였다면 접근은 허락되고, 그렇지 않다면 거절된다. 임의적 접근제어의 임의적 유연성은 다양한 시스템과 응용에 적당하여 상업 및 기업 환경에서 다양하게 구현되어 사용되고 있지만 접근권한의 명백한 표현과 관리성에 대한 개선의 여지가 있다.

3. RBAC

RBAC은 새롭고도 오래된 기술이다[6]. RBAC의 근원은 UNIX 시스템이나 다른 OS의 사용자 그룹과 데이터베이스의 특권 그룹 및 직무 분리 개념을 포함한다. 근대 RBAC의 개념은 하나의 접근 통제에 역할, 역할의 계층구조, 역할의 활성화, 사용자-역할 멤버십 및 역할 집합 활성화에 대한 모든 개념을 의미한다. 이러한 구조는 이전에 발표되었던 다양한 형식들을 일반화시킨 것이다. 현재의 RBAC 모델을 위한 구조는 Sandhu에 의해 정의되었고[1] 이후의 지속적인 연구들이 진행되고 있다[2,3,4,5].

본 논문에서는 RBAC이 접근제어 기법의 하나이기는 하지만 권한관리 기술 측면에서 별도의 기술 항목으로 설명할 것이다.

1) RBAC 구성 요소

RBAC의 구성요소는 크게 핵심(Core) RBAC, 계층(Hierarchical) RBAC, 제약(Constraint) RBAC이다[6]. 핵심 RBAC은 RBAC 시스템을 완전하게 구성하기 위한 기본 구성요소로서 사용자-역할 할당 관계, 퍼미션-역할 할당 관계가 기본으로 필요하다. 또한, 사용자 세션의 일부로서 역할 활성화(role activation)라는 개념이 필요하다. 핵심 RBAC은 모든 RBAC 시스템에 기본적으로 필요하다.

RBAC 참조모델에서 정의하는 엔터티는 다음과 같다.

- 사용자 : 인간으로 국한하며, 기계, 네트워크 또는 에이전트 등으로 확장 가능
- 역할 : 어떤 사용자에게 부여된 직권과 책임에 관련된 어떤 조직의 작업함수
- 오브젝트 : 정보를 저장하거나 정보를 수신하는 엔터티
- 오페레이션 : 사용자가 수행하는 이미지
- 퍼미션 : 오브젝트와 오퍼레이션의 쌍

(1) 핵심 RBAC

핵심 RBAC은 RBAC의 필수적인 부분을 구성하는 요소이다. RBAC의 기본 개념은 사용자가 역할에 할당되고, 퍼미션이 역할에 할당되고, 사용자는 역할의 구성원으로서 퍼미션을 획득하는 것이다. Core RBAC은 사용자-역할, 퍼미션-역할 할당의 다대다(many to many)관계에 대한 요구사항을 포함하여 사용자는 여러 역할에

할당되고 하나의 역할은 많은 사용자를 포함할 수 있다. 퍼미션에 대해서도 마찬가지이다.

(2) 계층 RBAC

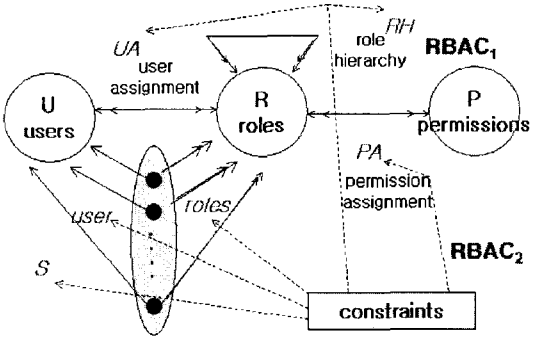
계층 RBAC은 역할 계층의 지원을 위해 필요한 구성요소이다. 역할의 계층은 역할의 선후 관계를 수학적 부분 순서(Partial Order)로 정의하는 것이다. 이로서 상위 역할은 하위 역할에 할당된 퍼미션을 획득하며 하위 역할은 상위 역할에 할당된 사용자를 멤버로 획득한다. 계층 RBAC은 일반 계층 RBAC(General hierarchical RBAC)과 한계 계층 RBAC(Limited hierarchical RBAC)으로 구분된다.

(3) 제약 RBAC

직무 분리(Separation of Duty) 관계는 정책 설정 시 역할에 대한 사용자의 충돌을 방지하기 위한 것이다. SSD 관계는 역할기반 시스템에서 역할의 특성상 한 사용자가 동시에 서로 상충되는 역할에 할당되어 관련된 퍼미션을 획득하는 시점에서 발생한다. 이러한 충돌을 막는 방법은 사용자가 역할에 할당될 때 제약 조건(정적 직무분리)을 부과하는 것이다. DSD 관계는 정적 직무분리와 같이 사용자에 대한 퍼미션을 제약하는 것이다. 그러나 정적 직무분리와는 달리 사용자 세션 동안에 활성화된 역할들 중에서 퍼미션이 충돌을 제한하는 것이다. 즉, 정적 직무분리는 세션과 무관하게 충돌을 원천적으로 피하는 방법(전체 퍼미션 공간의 제약)이라면 동적 직무분리는 실제 실행 시점에서 퍼미션의 충돌을 피하는 방법(사용자의 접근 가능성의 제약)이다.

2) RBAC 모델

RBAC은 그 적용되는 범위 및 방식에 따라 RBAC 0, RBAC 1, RBAC 2 및 RBAC 3로 모델링된다. RBAC 0는 핵심 RBAC 만을 포함하고, RBAC 2은 RBAC 0에 역할계층이 추가되며, RBAC 2는 RBAC 0에 제한 RBAC이 추가된다. 마지막으로 RBAC 3는 RBAC 0에 역할 계층 및 제한 RBAC을 포함하는 포괄적인



〈그림 2〉 RBAC 기본 모델

RBAC이다. 기본 모델은 RBAC 0이지만 현실적인 적용을 위해서는 RBAC 3의 구현이 필요하다.

4. SAML(Security Assertion Markup Language)

기업간 파트너쉽의 성장이 e-비즈니스 네트워크로 발전하면서 인터넷을 통한 상거래에서의 웹서비스 플랫폼이 출현하게 되었다. 이때 해결되어야 하는 문제점으로 대두된 것이 웹사이트들을 파트너로 연결해주는 크로스 도메인간의 단일인증(Single Sign-On), 보호 대상 자원에 대한 접근제어, 파트너간의 상호연동성과 이기종 환경의 지원에 대한 것이다. 이는 조직간 분산처리 추세와 더블어 퍼미션 관리를 위한 데이터가 서로 공유되고 있으며 웹기반의 어플리케이션들이 더욱더 독립적이면서도 상호연관성이 증대되고 있기 때문이다.

SAML은 위에서 서술한 환경에서 인증 및 인가 정보를 안전하게 교환하기 위한 XML 기반의 보안 규격으로 XML 문서의 형태로 인터넷을 통하여 보안정보를 공유하기 위한 오픈 프레임워크인 것이다. SAML은 XML Encryption, XML Signature, XKMS, XACML과 같은 XML 기반 보안 표준의 일부이다.

1) 표준화 동향

2000년 12월 OASIS SSTC(Security Service Technical Committee)가 결성되었으며

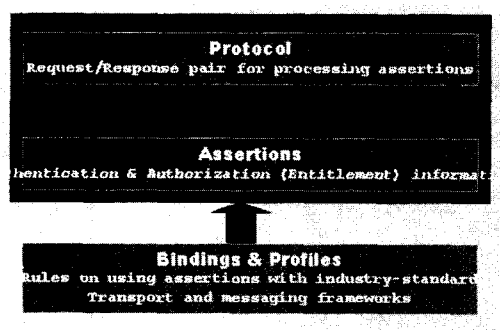
2001년 1월 S2ML(Security Service ML), AuthXML로 활동이 시작되었으며 2002년 1월에 '베타' 버전의 규격을 완성하였다. 이 규격에서는 "Core" 어서션(Assertion) 및 프로토콜 규격, 바인딩/프로파일 규격, Conformance 규격, 보안 및 프라이버시 고려사항 규격 등이 정의되었다. 2002년 5월에는 SAML 1.0 규격이 완성되었다. Committee 규격은 2002년 11월에 제정되어 이를 기반한 SAML 툴킷(JSAML, JSR 155)들이 출현하기에 이르렀다.

2) SAML 구조

SAML의 구조는 〈그림 3〉에서 보는 바와 같이 어서션(SAML Assertions), 프로토콜(SAML Protocol) 및 바인딩과 프로파일(SAML Bindings and Propiles)로 구성된다.[10]

SAML 어서션은 정보자원을 접근하는 주체인 서브젝트(subject)에 대하여 특정 도메인에서 식별가능한 엔터티(entity)임을 선언하는 것으로 어서션은 인가기관(authority)에 의해 발급된다. 물론 발급시 전자서명을 통하여 발급주체를 명시한다.

어서션은 인증 어서션(Authentication assertion), 속성 어서션(Attribute Assertion), 및 권한인가 어서션(Authorization Decision Assertion)으로 구분된다. 인증 어서션은 서브젝트, 인증 수단 및 시간에 대하여 기술하며, 속성 어서션은 서브젝트, 각 속성에 대한 속성 값에 대하여 기술하며, 권한인가 어서션은 서브젝트, 액션, 자원, 증거 등으로 기술한다.



〈그림 3〉 SAML 구조

SAML 프로토콜은 Request-Response 구조로서 SAML 요청자와 SAML 응답자 간의 상호 동작을 기술한다. 일반적으로 SAML 요청자는 클라이언트이며 SAML 응답자는 보안 서비스이다. SAML 요청자는 인증 어서션, 속성 어서션 및 권한관리 어서션을 위한 질의를 포함할 수 있다.

5. XACML(eXtensible Access Control Markup Language)

대기업의 보안 정책은 관리해야 하는 많은 요소들을 포함하고 있다. 정책 요소들은 기업의 정보 시스템 부서, 관리자 등 다양한 방법으로 관리되는 상황이며 또한 익스트라 넷, 메일, WAN 등에서 임의로 구현된 보안정책에 의해 제어되고 있다.

현재는 가능한 한 정확하게 보안정책을 구현하기 위해서 독립적으로 보안정책을 관리하고 있다. 그 결과 전체적인 보안 정책을 변경 적용하기는 비용이 많이 들며 신뢰성에도 문제가 있다. 또한 기업 전체를 대상으로 하는 조합적인 보안 정책을 실현하기는 본질적으로 불가능하다.

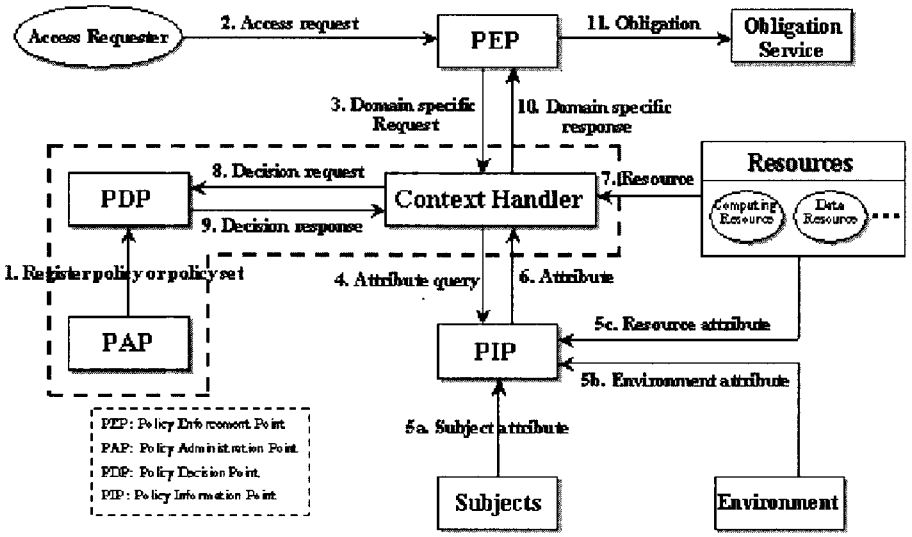
이러한 이유로 보안 정책을 표현하기 위한 일반적인 언어가 필요하게 되었다. 만약 이러한 일반화된 정책 언어로 구현되었다면, 기업 전반의 정보 시스템에 대하여 보안 정책을 적절한 요소에 적용할 수 있다. XML은 문법적으로나 의미적으로 쉽기 때문에 보안 정책 언어로서 선택된 것이며 XML을 기반으로 하는 보안정책 표현 언어가 XACML이다.

1) 표준화 동향

XACML은 OASIS XACML TC에서 작업을 진행하여 OASIS 표준 XACML 1.0 규격을 2003년 2월에 제정하였다.

2) XACML 구조

XACML의 데이터 흐름 구조는 〈그림 4〉와 같다. 접근 요청자는 SAML 등으로 표현된 인

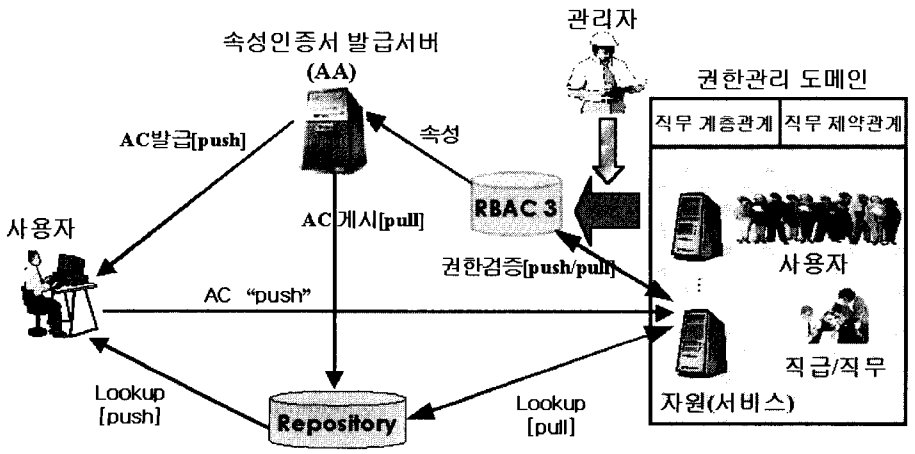


〈그림 4〉 XACML 데이터 흐름 구조

증/인가 정보를 가지고 보안정책 시행모듈(PEP)에 요청하며, 보안정책 시행모듈은 XACML로 표현되는 도메인의 컨텍스트 핸들러에 요청을 한다. 요청-응답 프로토콜에 의하여 컨텟스트 핸들러는 요청자의 권한 및 요청자가 접근하기 원하는 자원에 대한 속성을 참조하고 보안정책 결정 모듈에게 요청하여 접근 요청자의 접근 권한을 관리할 수 있도록 한다. 이때, 자원에 대한 속성과 서브젝트에 대한 속성은 RBAC 등의 접근제어 기법을 통하여 부여될 수 있다.

6. 권한관리 시스템 구축 모델

본고에서는 IETF3281 표준화 문서에서 제시하는 AC와 RBAC 개념이 융합된 다중 어플리케이션 도메인에서의 통합 권한관리에 대한 모델을 아래 〈그림 5〉에 제시한다. 이 모델은 사용자와 정보자원에 대한 체계적이고 종합적인 보안정책을 설정할 수 있는 중앙 집중적 보안정책을 기반으로 한다. 보안 정책은 조직구조의 지급 및 직무를 적절히 표현(기본 역할 관계, 역할 계층 및 제약 관계 등) 하고 관리할 수 있어야 되며 이를



〈그림 5〉 권한관리 시스템 구축 모델

위해서 역할 개념의 권한을 할당하고 관리할 수 있는 RBAC 3 모델을 적용하고 있다. 또한 사용자 및 정보자원에 대한 권한정보의 안전한 유통을 위하여 AC기반의 PMI 권한관리 기법을 적용하고 있다.

관리자가 조직 내의 사용자와 정보자원을 단일의 뷰를 통하여 관리할 수 있기 위해서는 각 어플리케이션의 특성과 사용자 특성을 파악하여야 한다. 이 과정에서 사용자 특성과 정보자원의 특성을 관리자에게 보여주기 위해서 기존의 인사 DB와의 연동 및 추가 사용자의 관리 도구를 제공하여야 하며 정보자원과의 연동을 위하여 다양한 에이전트를 제공해야 한다. 관리자는 지관적인 인터페이스를 통하여 전사적 또는 협력 비즈니스 영역의 모든 정보자원을 관리할 수 있어야 한다.

사용자는 한번의 간단한 로그인 절차를 통하여 권한관리 도메인 내의 모든 자원에 추가적인 인증절차 없이 접근하여 서비스를 이용할 수 있어야 한다.

Ⅲ. 결 론

본 고에서는 복잡한 사내 정보 시스템 환경에서 보안 정책 기반의 권한관리를 위한 기반 기술에 대하여 간단하게 소개 하였다. 정책기반의 권한관리를 위해서는 인프라로서의 권한관리 구조가 기반을 이루어져야 하며 사용자 및 정보자원의 특성에 따라 접근권한 관리를 할 수 있어야 하며 이러한 접근권한 관리 정보를 안전하고 표준적인 방법으로 유통시킬 수 있는 기술이 필요한다. 이러한 관점에서 본고에서는 관한관리 인프라로서 AC 기반 PMI 기술을 설명하였고, 사용자 및 정보자원의 특성의 정의 및 표현을 위해서 RBAC 및 XACML 기술을 설명하였으며 안전하고 표준적인 인증/인가 정보의 유통을 위하여 SAML 및 XACML 기술을 설명하였다. 또한 AC 기반의 PMI 기술과 RBAC 및 XACML/SAML을 융합한 통합인증 권한관리 시스템 구축 모델을 제시하였다.

전술한 바와 같이 각종 응용 시스템의 내부 정보 자원과 사용자에 대한 접근 인증 및 권한관리가 개별적인 응용 시스템별로 적용되고 있고, 개별적인 응용 시스템 및 운영체계 자체가 보유하고 있는 권한관리 기법만으로는 조직의 직제 및 직능을 적용하기에 한계가 있기 때문에 조직 내의 모든 사용자와 정보자원에 대하여 통합인증 권한관리 시스템을 도입하고 구축하는 필요성이 점점 커지고 있다.

권한관리 기술을 적용시킨 진정한 의미의 통합인증 권한관리 시스템이 권한관리 인프라로 구축되면 정보시스템과 사용자의 보안관리 비용이 절감되며 정보 시스템에 대한 보안성을 향상시키며 정보자원의 이용 및 관리에 편리성이 향상될 수 있을 것이다.

참 고 문 헌

〔1〕 R Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. *IEEE Computer*, 29(2), February 1996.

〔2〕 Ravi Sandhu, Venkata Bhamidipati and Qamar Munawer. "The ARBAC97 Model for Role-Based Administration of Roles." *ACM Transactions on Information and System Security*, Volume 2, Number 1, February 1999, pages 105-135.

〔3〕 Ravi Sandhu, "Role Activation Hierarchies." *Proc. Third ACM Workshop on Role-Based Access Control*, Fairfax, Virginia, October 22-23, 1998, pages 33-40.

〔4〕 S. Osborn, R. Sandhu and Q. Munawer. Configuring Role-Based Access Control to Enforce Mandatory and

Discretionary Access Control Policies. *ACM Transactions on Information and System Security*, 3(2), 2000.

〔5〕 Gail Ahn and Ravi Sandhu. "Role-Based Authorization Constraints Specification." *ACM Transactions on Information and System Security*, Volume 3, Number 4, November 2000.

〔6〕 David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli, "A Proposed Standard for Role-Based Access Control", NIST, 2000

〔7〕 RFC 2459, "Internet X. 509 Public Key Infrastructure Certificate and CRL Profile", IETF PKIX Working Group, January 1999.

〔8〕 ITU-T RECOMMENDATION X.509| ISO/IEC 9594-8, "INFORMATION TECHNOLOGY. OPEN SYSTEMS INTERCONNECTION. THE DIRECTORY : PUBLIC KEY AND ATTRIBUTE CERTIFICATE FRAMEWORKS", 2001.

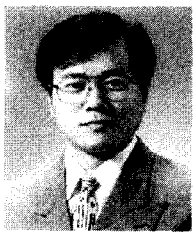
〔9〕 RFC 3281, "An Internet Attribute Certificate Profile for Authorization", IETF PKIX Working Group, 2002.

〔10〕 http://www.oasis-open.org/committee/

저 자 소 개

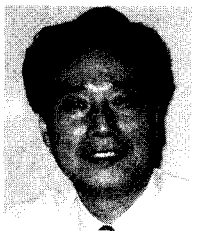
김 봉 환

1992년 2월 충남대학교 전산학과 졸업, 1994년 2월 충남대학교 전산학과 대학원 졸업, 1994년 3월~2000년 1월 : 국방과학연구소 연구원, 2000년 2월~2000년 4월 : 국가보안기술연구소 선임연구원, 2000년 5월~2001년 4월 : 전자통신연구원 선임연구원 2001년 5월~현재 : (주)아이에이시큐리티 팀장, 〈주관심 분야 : 컴퓨터 및 모바일 시큐리티, 공개키기반구조, 권한관리기반구조, 모바일 Anti-Virus〉



원 유 재

1985년 2월 충남대학교 계산통계학과 졸업, 1987년 2월 충남대학교 전산학과 대학원 졸업, 1998년 2월 충남대학교 전산학과 대학원 박사, 1987년 3월~2001년 1월 : 전자통신연구원 책임연구원, 무선인터넷 정보보호 연구팀장, 2001년 2월~현재 : (주)아이에이시큐리티 연구소장, 〈주관심 분야 : 컴퓨터 및 모바일 시큐리티, 공개키기반구조, m-커머스〉



손 중 만

1975년 2월 부경대 졸업, 1982년 2월 동아대 대학원 졸업, 2002년 8월 동아대 대학원 박사과정 수료, 1982년 2월~2002년 1월 : 한국아이비엠(주), 2002년 2월~2003년 3월 : (주)SSIT, 2003년 4월~현재 : (주)아이에이시큐리티 대표이사, 〈주관심 분야 : Wireless Internet Security, Mobile Computing, PKI/PMI〉