특집

RBAC을 이용한 PMI 기반 권한관리

김봉환[1] 김기수[1] 원유재[2]

목 차

1. 서 론

컴퓨터와 인터넷의 급속한 보급으로 다양한 기능 및 형태의 어플리케이션이 등장함에 따라 인터넷을 기반으로 하는 e비즈니스 환경이 출현하게 되었다. 이는 기존에 존재하는 수많은 어플리케이션과 새롭게 적용되는 어플리케이션이 사내 인트라넷, B2B 엑스트라넷 및 e-Commerce 서비스에 적용되는 것이다. 즉, 다양한 사용자는 언제 어디서나 어플리케이션(정보, 서비스)에 접근할 수 있는 비즈니스 환경이다. 이러한 IT 기반의 정보서비스는 기존의 사람과 사람 또는 회사와 회사가 직접 대면하여 처리하던 비즈니스의 전통적 절차를 바꾸어 놓았으며 이는 비즈니스의 신속성, 정확성, 경제성 측면에서 획기적인 일이다. 이에 따라 모든 업무 및 비즈니스의 수행 절차가 IT 기반의 어플리케이션으로 지속적으로 증가되고 있는 추세다. 그러나 최근까지 대부분의 IT 기반 어플리케이션의 사용자 인증 및 권한 관리 측면의 보안 서비스는 각각의 어플리케이션에서 독립적으로 제한적인 기능만을 처리하는 형태였다. 이러한 상태가 지속되어 사용자의 수와 어플리케이션의 수가 늘어나고 다양해진다면 IT 기반의 정보화를 통해 추구하려던 신속성, 정확성, 경제성 및 보안성의 효과를 극대화하는 데에는 한계가 있을 것이다. 최근 모든 어플리케이션에 독립적으로 적용되어 다양한 어플리케이션의 사용자 보안 관리를 통합적으로 수행해 조직의 사용자 보안 관리를 영구적으로 수행할 수 있는 권한 관리 인프라 구축의 필요성이 대두되고 있으며 이를 권한관리 기반구조(Privilege Management Infrastruc- ture, 이하 PMI) 개념을 통해 달성하고자 하는 노력의 시도가 실질적으로 진행되어 오고 있다. 즉, 사용자 보안 관리를 특정 어플리케이션에 종속적으로 제공되어야 할 보안 기능이 아닌 새로운 어플리케이션의 도입, 사용자의 보안 등급에 따른 정책 설정 및 집행, 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 대안

1) (주)아이에이시큐리티 팀장
2) (주)아이에이시큐리티 기술이사

으로 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]. 비즈니스의 안전한 구축과 안전하고 효과적인 관리에서 크게 대두되고 있는 사용자 인증과 인증된 사용자의 특정 서비스에 대한 접근권한의 관리 문제다. 사용자 인증은 공개키 기반구조(Public Key Infrastructure, 이하 PKI)를 기반으로 하는 보안 서비스이며 자원에 대한 접근권한 관리는 권한관리 기반구조(Privilege Management Infrastructure, 이하 PMI) 기반의 보안 서비스다. PKI를 기반으로 하는 보안 기술은 데이터 기밀성 및 사용자 인증 서비스를 제공하고 있지만 사용자 및 자원에 대한 접근제어 서비스는 제공하지 못하고 있다. 서두에서 언급한바와 같이 비즈니스 조직은 상당히 역동적인 구조를 가지고 있기 때문에 사용자와 자원에 대한 관리를 복잡하게 만든다. 효과적인 사용자 인증과 인증된 사용자에 적절한 자원의 제공을 위하여 역동적인 조직 구조를 효과적으로 표현하고 구현할 수 있는 접근제어 기법이 요구되고 있다. RBAC(Role Based Access Control)은 사용자와 서비스에 대한 접근권한 간의 관계성을 역할이라는 추상화된 개념을 도입하여 사용자와 역할, 역할과 접근권한이라는 2 단계 구조의 접근제어 기법이다. 이 개념은 오래 전부터 언급되었지만, 최근에 권한관리 이슈와 맞물려 새롭게 각광받고 있다. 상기 개념은 본 고에서 제시하는 권한관리 기반구조의 속성 인증서에 사용자 및 정보자원에 대한 그룹 및 역할을 적용하는 방법론으로 이용될 것이다. 상기의 언급한 비즈니스 환경의 변화에 따르는 제반 요구사항은 사용자 인증정보의 중앙 집중적 제어 및 서비스 자원에 대한 접근권한 관리를 통하여 기업 조직의 모든 정보 자원에 대한 TCO를 감소시키고 ROI를 증대시키는 것을 기본 목표로 한다. 본 논문에서는 최근 표준화 단계를 거치고 있는 PMI 기술에 대하여 설명을 하고 PMI에서 적요되는 접근제어 기법에 대하여 전반적으로 고찰하고 이 중에서 RBAC에 대한 기본 개념 및 기술 현황을 설명한다. 또한 RBAC 및 PMI에 대한 전반적인 특성을 바탕으로 RBAC을 이용한 PMI 기반 권한관리 구축 모델을 제시하고 그 구현 사례를 설명한다. 본 논문은 다음과 같이 구성되어 있다. 2장에서는 다양한 어플리케이션 환경에서 발생하는 정보보호의 요구사항을 기술한다. 3장에서는 PMI의 표준화 현황과 전망과 접근제어 일반 현황 및 RBAC과 PMI의 관계를 설명한다. 4장에서는 RBAC을 이용한 PMI기반 권한관리 구축 모델을 소개하고 실제 구현 사례를 소개한다. 5장에서는 결론을 맺는다.

2. 어플리케이션 환경과 정보보호 요구사항

다양한 장치를 사용하는 다양한 사용자에 의해 접근되는 다양한 어플리케이션은 조직으로 하여금 관리의 요구를 증대시키고 있다. 이는 기업조직의 합병, 사업착수, 인력 변동, 전략적 제휴 및 규모의 확대 등 그 변화의 정도가 매우 역동적인 것과 무관하지 않다. 이 같은 조직 환경에서의 비즈니스 절차와 조직 구조를 지원하고 반영하기 위해서 다양한 사용자의 인증 및 다양한 기업 서비스 자원에 대한 관리의 비용 문제는 화두가 되기 충분하다. 사용자의 인증의 문제와 조직 내 정보자원에 대한 관리의 문제는 근본적으로 조직 내부의 비즈니스 절차와 정보자원이 새로운 사용자 환경에 공개되면서 시작되는 복잡한 도전이다. 관리 비용 절감, 비즈니스 환경의 구축 및 관리, 안전하면서도 지속적인 서비스의 제공이 그 도전의 중심에 있다. 도전에 대한 요구사항은 현실적으로 비즈니스 환경의 구축과 관리의 이슈를 내포하고 있다.

2.1 어플리케이션 환경

최근의 어플리케이션 환경의 흐름을 분석하면 크게 어플리케이션의 다양성과 어플리케이션의 통합성으로 말할 수 있다. 우선 사용자 측면에서 보면 수많은 사용자들이 인터넷을 통하여 다양한 서비스를 이용하고 있고 사내 망에서도 다양한 어플리케이션 서비스를 이용한다. 이는 다양한 서비스에 자신을 등록하는 과정을 통하여 가능하다. 이 결과로 사용자들은 일반적으로 ID와 패스워드를 부여받게 된다. 이러한 정보는 어플리케이션의 수가 증가함에 따라 점점 많아지게 된다. 이러한 정보의 관리는 사용자에게 부담으로 작용하며 동시에 보안성 저해요인으로 작용한다. 어플리케이션의 통합은 기업 비즈니스의 형태가 기업 단독이 아니고 기업대 기업 간의 연계를 통해 구매, 판매, 생산 등의 비즈니스 절차의 통합을 의미한다. 기업조직 및 비즈니스 영역이 확대되면서 비즈니스 통합을 가능케 해주는 어플리케이션의 통합은 관리비용의 최소화 및 비즈니스 기회의 극대화를 그 목표로 한다.

2.2 정보보호 요구사항

어플리케이션 환경의 변화는 정보보호에 대한 요구사항을 동반한다. 정보보호에 대한 대책이 없이 어플리케이션이 다양화되고 통합된다면 IT 인프라 자체의 존재의미가 위협받을 수 있을 것이다. 어플리케이션이 다양화됨에 따라 대두되는 정보보호 요구사항으로는 다양한 어플리케이션과 함께 증가하는 다양한 사용자에 대한 ID와 신상정보에 대한 관리와 안전한 배포다. 또한 사용자의 편리성을 증가시킬 수 있는 단일 인증 체계가 요구되며 사용자의 프라이버시를 보호할 수 있는 신상정보에 대한 접근제어가 필요하다. 또한 서비스의 이용에 관련된 과금에 대한 요구사항도 중요시되고 있다.어플리케이션의 통합되면서 대두되는 정보보호 요구사항으로는 통합환경에서의 단일 인증 체계와 통합환경에서의 권한관리 기법, 통합 감사 관리 및 단위 도메인간 인증 및 권한정보의 통합 연동 체계다. 특히, 통합 환경에서 그룹 및 역할 기반의 권한관리 요구사항은 관리비용 이슈와 맞물려 크게 이슈화되고 있다.

3. PMI와 접근제어

3.1 PMI(Privilege Management Infrast - ructure)기술

3.1.1 PMI의 기본 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 있는 지를 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 상태다. 즉, 사용자 인증은 PKI 기반의 공개키 인증서를 통해, 사용자 권한관리는 PMI 기반의 AC를 통해 달성하고자 하는 노력이 PMI의 가장 보편적 현상으로 볼 수 있다.

3.1.2 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 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 RFC3281을 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

X.509 인증서 기반의 PKI와 AC 인증서 기반의 PMI 주요 핵심 구성 요소에 대한 비교는 〈표 1〉과 같다.

〈표 1〉 PKI 와 PMI 비교

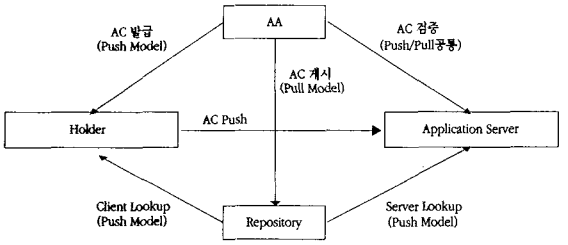
개 념	PKI Entity	PMI Entity
인증서	Public Key Certificate	Attribute Certificate
인증서 발급자	Certificat Authority(CA)	Attribute Authority(AA)
인증서 사용자	Subject	Holder
인증서 용도	Subject name과 Subject 공개키의 Binding	Holder name과 Holder의 권한 Attribute의 Binding
인증서 취소 관리방식	CRL(Certificate Revocation List)	ARL(Attribute Revocation List)

AC의 표준 필드 구조 및 내용은 〈표 2〉와 같다.

〈표 2〉 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 ID 정보
Extensions	Attribute Certificate 정보의 확장 필드
Signature	AA의 서명값

RFC3281에 언급하고 있는 PMI 속성 인증서 발급 관리 기본 체계는 (그림 1)과 같다.



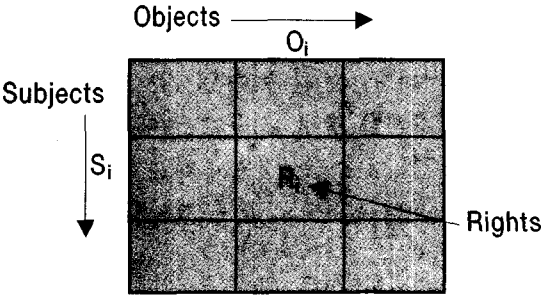
(그림 1) 속성 인증서 발급 관리 기본 체계

3.2 접근제어와 RBAC 기술

3.2.1 접근제어

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 접근권한이 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 2)는 접근메트릭스 모델을 나타낸다. 그림에서 서브젝트는 일반적으로 사용자에 해당하는 개념이며 오브젝트는 리소스의 개념이며 권한은 접근하여 수행할 수 있는 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 서



(그림 2) 접근 메트릭스 구조

브젝트에 〈Oi, Ri〉 쌍의 리스트를 유지하는 형태로 구현되며 릴레이션은 〈Si, Oi, Ri〉의 트리플 튜플로 유지되는 관계DB 의 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. 역할기반 접근제어(Role-based Access Control, 이하 RBAC)는 임의적

접근제어와 강제적 접근제어와 달리 사용자와 접근권한간의 1:1 매핑구조를 탈피하여 역할이라는 추상화된 개념을 도입하여 사용자-역할, 역할-접근권한의 2단계 구조를 가지는 접근제어 기법이다. RBAC의 기본적인 개념은 임의의 사용자가 기업이나 조직의 정보 자원을 접근할 수 없도록 하는 것이다. 대신에 접근권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원(Least of Privilege)만을 접근할 수 있도록 한다. 이러한 아이디어는 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다. 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경이 없이도 역할의 변경을 쉽게 할 수 있다. 이 외에도 행위기반의 접근제어 등을 비롯하여 다양한 방법으로 접근제어를 달성할 수 있지만 기업조직 특성의 보안정책 반영과 사용자와 정보자원에 대한 권한관리의 유연성을 제공하는 RBAC이 권한관리 기반구조를 구축하는 대안으로 떠오르고 있다. 다음절에서는 RBAC에 대하여 자세한 설명을 한다.

3.2.2 RBAC

RBAC은 새롭고도 오래된 기술이다[6]. 역할의 개념은 적어도 25년 동안 소프트웨어 어플리케이션에서 사용되어 왔다. 그러나 RBAC의 개념이 정립되어 전통 MAC와 DAC 개념처럼 충분하게 발달한 메커니즘으로 나왔던 것은 불과 10년 이내이다. 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].

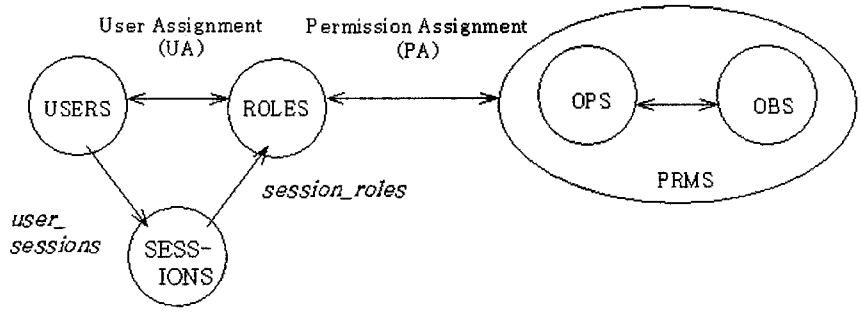
3.2.2.1 RBAC 구성 요소

RBAC의 구성요소는 크게 핵심(Core) RBAC, 계층(Hierarchical) RBAC, 제약(Constraint) RBAC이다[6]. 본 논문에서는 제한 RBAC을 정적직무분리(Static Separation of Duty, 이하 SSD)와 동적 직무분리(Dynamic Separation of Duty Relations, 이하 DSD)로 나누어 설명한다. 본 논문에서는 제약 RBAC을 SSD와 DSD로 나누어 4가지 구성요소로 설명한다. 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-역



(그림 3) 핵심 RBAC의 원소집합과 관계들

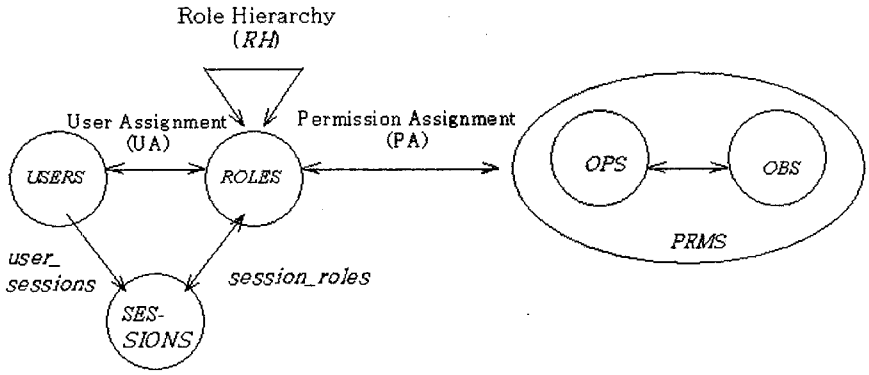
할, 퍼미션-역할 할당의 다대다(many to many)관계에 대한 요구사항을 포함하여 사용자는 여러 역할에 할당되고 하나의 역할은 많은 사용자를 포함할 수 있다. 퍼미션에 대해서도 마찬가지다.

② 계층 RBAC

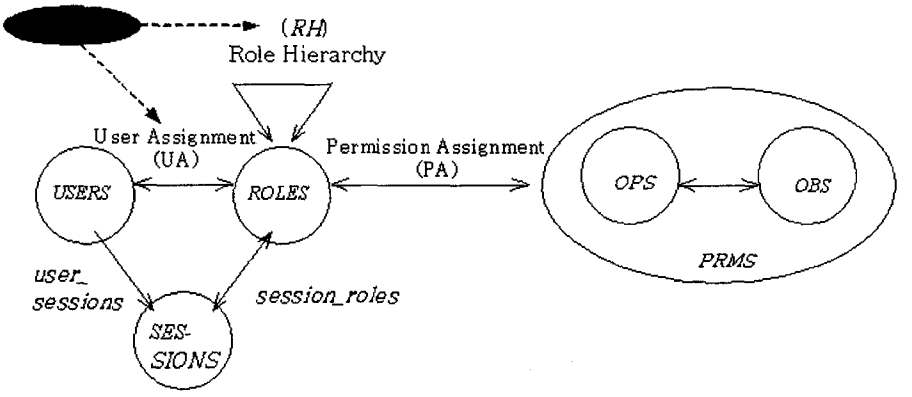
계층 RBAC은 역할 계층의 지원을 위해 필요한 구성요소다. 역할의 계층은 역할의 선후 관계를 수학적 부분 순서(Partial Order)로 정의하는 것이다. 이로서 상위 역할은 하위 역할에 할당된 퍼미션을 획득하며 하위 역할은 상위 역할에 할당된 사용자를 멤버로 획득한다. 계층 RBAC은 일반 계층 RBAC(General hierarchical RBAC)과 한계 계층 RBAC (Limited hierarchical RBAC)으로 구분된다.

③ 제약 RBAC

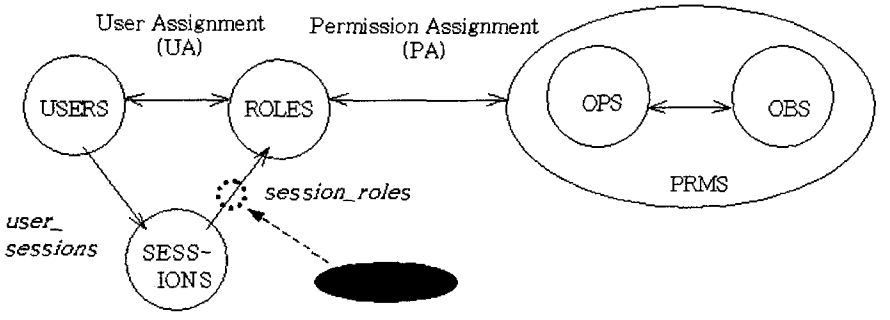
직무 분리(Separation of Duty) 관계는 정책 설정 시 역할에 대한 사용자의 충돌을 방지하기 위한 것이다. SSD 관계는 역할기반 시스템에서 역할의 특성상 한 사용자가 동시에 서로 상충되는 역할에 할당되어 관련된 퍼미션을 획득하는 시점에서 발생한다. 이러한 충돌을 막는 방법은 사용자가 역할에 할당될 때 제약 조건(정적 직무 분리)을 부과하는 것이다. DSD 관계는 정적 직무분리와 같이 사용자에 대한 퍼미션을 제약하는 것이다. 그러나 정적 직무분리와는 달리 사용자 세션 동안에 활성화된 역할들 중에서 퍼미션이 충돌을 제한하는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



(그림 4) 계층 RBAC의 원소집합과 관계들



(그림 5) 계층 RBAC에서의 SSD 관계



(그림 6) 세션상의 DSD 관계

간의 제약)이라면 동적 직무분리는 실제 실행 시점에서 퍼미션의 충돌을 피하는 방법(사용자의 접근 가능성의 제약)이다.

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

3.2.2.3 RBAC 함수

RBAC에서 정의한 각 구성 요소의 요구조건에 부합될 수 있는 함수는 3가지로 분류할 수 있다.

- 관리함수 : 각 RBAC 모델의 구성요소 집합을 생성하고 유지하는 함수
- 지원함수 : 사용자가 IT 시스템과 상호 작용하는 동안 RBAC 모델 구성을 지원하는 함수
- 확인함수 :관리 함수에 의해 만들어진 결과를 확인하는 함수

〈표 3〉 RBAC 함수

구 분	RBAC 모델	함 수 명	설 명
관리함수	핵심 RBAC	AddUser	사용자 추가
		DeleteUser	사용자 삭제
		AddRole	역할 추가
		DeleteRole	역할 삭제
		AssignUser	UA 관계에서 역할에 사용자 할당
		DeassignUser	UA 관계에서 역할에 할당된 사용자 삭제
		GrantPermssion	PA 관계에서 역할에 퍼미션 할당
		RevokePermission	PA 관계에서 역할에 할당된 퍼미션 삭제
	계층 RBAC	AddInheritance	역할 간의 상속관계 설정
		DeleteInheritance	설정되어 있는 역할간의 상속관계를 제거
		AddAscendant	상위 역할 추가
		AddDescendant	하위 역할 추가
	SSD RBAC	CreateSSDSet	SSD 관계 생성
		DeleteSSDSet	SSD 관계 삭제
		AddSSDRoleMember	SSD 역할 집합에 해당 역할 추가
		DeleteSSDRoleMember	SSD 역할 집합에서 해당 역할 삭제
		SetSSDCardinality	일반 사용자 권한의 제한적 응용을 위한 SSD 역할로부터의 역할들의 subset의 cardinality를 지정
지원함수	핵심 RBAC	CreateSession	사용자 세션 생성
		AddActiveRoles	현재 세션에 활성화된 역할 추가
		DropActiveRoles	현재 세션에서 활성화된 역할 삭제
		CheckAccess	세션 서브젝트가 해당하는 오브젝트에 요구한 오퍼레이션을 수행할 수 있는지 확인
	계층 RBAC	핵심RBAC과 동일하지만, CreateSession 과 AddActiveRoles 함수는 역할 계층 요소에 의해 재정의	
		핵심 RBAC과 동일	
검사함수	핵심 RBAC	AssignedUsers	특정 역할에 할당된 사용자 확인
		AssignedRoles	특정 사용자에 할당된 역할 확인
	계층 RBAC	AuthorizedUser	특정 역할에 대하여 계층 관계에 의해 상속된 사용자 확인
		AuthorizedRoles	특정 사용자에 대하여 계층 관계에 직접 상속된 역할 확인
	SSD RBAC	SSDRoleSets	SSD 관계에 있는 집합 확인
		SSDRoleSetROLES	SSD 역할 집합과 연계된 역할 집합 확인
		SSDRoleSetCardinality	SSD 역할 집합내에 subset의 cardinality를 반환

4. RBAC을 이용한 PMI 기반 권한관리

4.1 권한관리 체계 구축

2장과 3장에서는 어플리케이션 환경과 정보보호 요구사항 및 접근제어 및 권한관리를 위한 PMI 기술의 배경과 기본적인 개념 및 관련 핵심 기술 요소들에 대한 표준화 동향을 살펴보았다. 이러한 환경 및 기술적인 동향을 기반으로 권한관리 기술은 정보화 환경의 급속한 발전과 함께 보다 더 복잡 다양해지는 어플리케이션 상에서 다양한 사용자의 다양한 정보자원에 대한 통합적인 권한 관리를 위한 핵심 기술로 대두되고 있으며

국내외에서 통합 권한관리 분야의 시장이 급속도로 성장하고 있는 추세이다. 최근까지, 인트라넷/엑스트라넷 및 E-비즈니스 서비스 상에서의 사용자들에 대한 권한 관리 체계의 구축은 크게 다음과 같은 3가지 방향으로 진행되어 오고 있으며 각각의 특성은 다음과 같다.

4.1.1 특정 어플리케이션 소프트웨어에 종속적인 권한관리 적용

현재 대부분의 IT 환경에서 적용되고 있는 방식으로 특정 어플리케이션 소프트웨어 내에서 사용자와 정보자원만을 대상으로 한 접근 권한 관리 기능을 구현하여 적용하는 방식이다. 다양한 어플리케이션 및 비즈니스 서비스가 존재하는 환경에서 각각의 어플리케이션 및 서비스마다 별도의 권한 관리 기능을 개발해 적용하고 있으며 ACL, DAC, MAC 등의 전통적인 접근제어 메커니즘을 이용하고 있다. 사용자 인증 및 권한관리 개념의 보안관리 기반 구조 구축 측면과는 거리가 먼 방식이라고 할 수 있다.

4.1.2 각 어플리케이션에 적용된 개별 접근제어 메커니즘의 단순 통합을 통한 권한관리 체계 운용

각 어플리케이션별로 적용되어 있는 기존의 접근제어 메커니즘의 단순 확장을 통하여 통합 관리하는 방식이다. 각 어플리케이션 벤더에 종속적인 통합관리 기능을 구현하기 때문에 다양한 어플리케이션 시스템 환경에서 공통적으로 적용될 수 있는 표준화된 권한관리 기반구조 구축에 한계가 있다. 권한 정보의 관리가 복잡하고, 관리자의 실수에 의한 권한 할당의 오류 및 관리자 고의에 의한 권한 오남용 문제 발생할 수 있다.

4.1.3 AC와 RBAC 개념이 융합된 다중 어플리케이션 도메인에서의 통합 권한 관리 체계의 개발

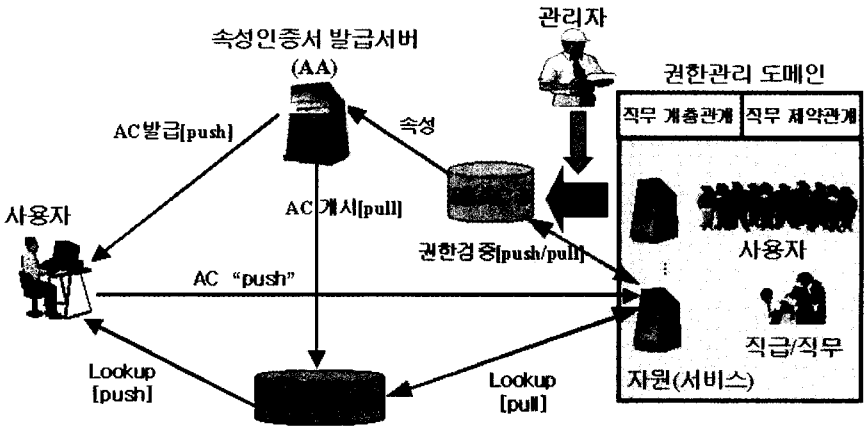
역할 개념을 기반으로 사용자의 권한 속성 정보(예, Role, Group, Clearance 등)를 AC에 포함시켜 관리하는 방식으로 조직 및 비즈니스 서비스 상에서의 보안 정책에 따라 사용자별로 할당된 권한 정보가 AC에 포함되어 있어 사용자 및 관리자가 언제라도 쉽게 할당된 권한 정보의 확인이 용이하다. 사용자의 권한 정보를 표준화된 AC 형태의 매개체를 이용하여 유통시키고 관리함으로써 다중 어플리케이션 환경으로 확장 시 권한정보 적용범위의 확장이 용이하다. AC의 발급 시 권한인증서발급서버(Attribute Authority)의 전자서명이 적용되어 권한정보의 위남용을 방지하고 권한 할당 사실에 대한 부인봉쇄 기능을 확보할 수 있다. 상기의 3가지 권한 관리 체계 구축 방향에서 최근의 통합 어플리케이션 환경 구축 측면에서 볼 때 AC와 RBAC 개념을 기반으로 한 구축 방향이 권한 관리 체계의 인프라 구축이라는 측면에서 가장 적절한 것으로 여겨지고 있어 국내외에서 다양한 솔루션의 개발이 추진되고 있다.

4.2 RBAC을 이용한 PMI 기반 권한관리 구축 모델

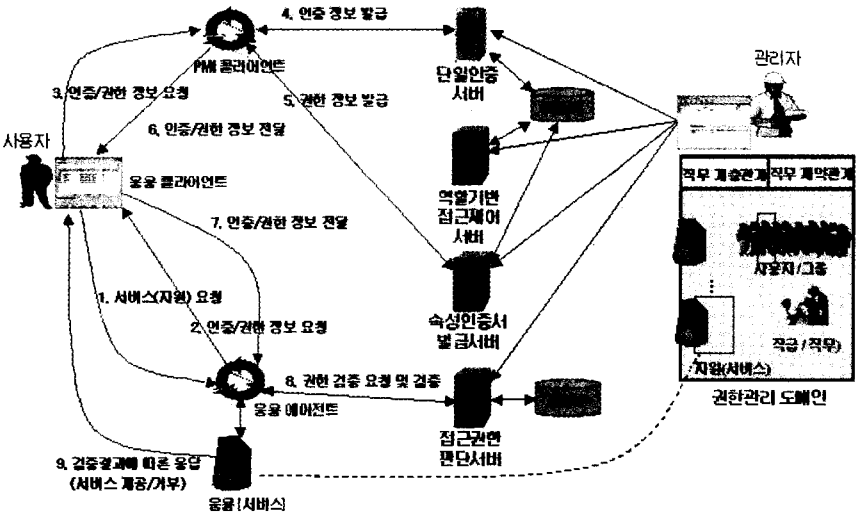
AC와 RBAC 개념이 융합된 다중 어플리케이션 도메인에서의 통합 권한관리에 대한 모델을 아래(그림 7)에 제시한다. 이 모델은 사용자와 정보자원에 대한 체계적이고 종합적인 보안정책을 설정할 수 있는 중앙 집중적 보안정책을 기반으로 한다. 보안 정책은 조직구조의 지급 및 직무를 적절히 표현(기본 역할 관계, 역할 계층 및 제약 관계 등)하고 관리할 수 있어야 되며 이를 위해서 역할 개념의 권한을 할당하고 관리할 수 있는 RBAC 3 모델을 적용하고 있다. 또한 사용자 및 정보자원에 대한 권한정보의 안전한 유통을 위하여 AC기반의 PMI 권한 관리 기법을 적용하고 있다.

4.3 구현 사례

본 절에서는 (주)아이에이시큐리티에서 개발한 통합인증 권한관리 제품인 EasyAccess를 예를



(그림 7) RBAC을 이용한 PMI 기반 권한관리 구축 모델



(그림 8) EasyAccess에 적용된 RBAC을 이용한 PMI 기반 권한관리

들어 본 논문에서 제시한 RBAC을 이용한 PMI 기반 권한관리 구축 모델이 어떻게 구현되고 있는지를 설명한다.관리자가 조직내의 사용자와 정보자원을 단일의 뷰를 통하여 관리할 수 있기 위해서는 각 어플리케이션의 특성과 사용자 특성을 파악하여야 한다. 이를 위해 EasyAccess는 직관적이고 유려한 관리자 인터페이스를 지원하고 있다. 이 과정에서 사용자 특성과 정보자원의 특성을 관리자에게 보여주기 위해서 기존의 인사 DB와의 연동 및 추가 사용자의 관리 도구를 제공하고 있으며 정보자원과의 연동을 위하여 다양한 에이전트를 제공한다. 관리자는 EasyAccess가 제공하는 인터페이스 상에서 간단한 조작을 통하여 전사적 또는 협력 비즈니스 영역의 모든 정보자원을 관리할 수 있다. 사용자는 한번의 간단한 로그인 절차를 통하여 권한관리 도메인 내의 모든 자

원에 추가적인 인증절차 없이 접근하여 서비스를 이용할 수 있다. 물론 인증 과정에서 사용자에게 할당된 권한이 허용되는 범위 안에서 가능하다.

5. 결 론

최근의 IT 환경과 발전 동향을 분석해 볼 때 다양한 형태의 어플리케이션 서비스들이 존재하고 지속적으로 새로운 어플리케이션이 개발되어 적용될 것이다. 이 어플리케이션들은 서로 통합 운용되어야 하는 요구사항을 만족해야한다. 인터넷 기반의 e-비즈니스 환경에 의하여 다양한 사용자들이 다양한 장치를 통하여 다양한 어플리케이션에 접근할 수 있게 되었고 이는 안전한 비즈니스와 효율적인 관리 및 안정적이고 지속적인 서비스 제공의 문제를 야기시키고 있다. 이는 기반구조로서의 권한관리 필요성에 대한 인식이 확산되고 있다는 의미다. 본 고에서는 권한관리 기반 구조의 여러 접근 방식 중에서 조직구조와 권한의 표현 및 적용에 유연한 RBAC 접근제어를 이용한 권한관리 기반구조를 설명하고 그 모델과 적용사례를 제시하였다. 향후, 관리 도메인간 인증 및 권한 정보의 통합 및 연동을 위한 기술의 표준화가 진척이 되어 분산 환경의 서비스 통합 기반이 정착된다면 지금까지 관리비용 때문에 안전하지 않은 서비스를 경험했던 사용자와 관리자에게 보다 안전하고 편리한 환경을 제공할 수 있을 것이다.

참고문헌

[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 Work - shop 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 ATTRI-

BUTE CERTIFICATE FRAMEWORKS", 2001.
[9] RFC 3281, "An Internet Attribute Certificate Profile for Authorization", IETF PKIX Working Group, 2002

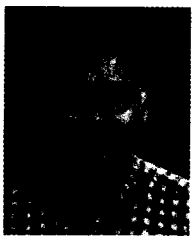
저자약력

김 봉 환

1992년 충남대학교 전산학과 (이학사)
1994년 충남대학교 전산학전공 (이학석사)
1994년-2000년 국방과학연구소 연구원
2002년-2001년 전자통신연구원 선임연구원
2001년-현재 (주)아이에이시큐리티 팀장
관심분야 : 컴퓨터 및 모바일 시큐리티, 공개키기반구조, 모바일 Anti-Virus
이 메 일 : bhkim@iasecurity.com

원 유 재

1985년 충남대학교 계산통계학과 (이학사)
1987년 충남대학교 전산학전공 (이학석사)
1998년 충남대학교 전산학 (이학박사)
1987년-2001년 전자통신연구원 책임연구원, 무선인터넷 정보보호 연구팀장
2001년-현재 (주)아이에이시큐리티 기술이사
관심분야 : 컴퓨터 및 모바일 시큐리티, 공개키기반구조, m-커머스
이 메 일 : yjwon@iasecurity.com



김 기 수

1994년 충남대학교 전산학과 (이학사)
1996년 충남대학교 전산학전공 (이학석사)
1996년-2000 한국전산원 연구원
2000년-2001년 전자통신연구원 연구원
2001년-현재 (주)아이에이시큐리티 팀장
관심분야 : 컴퓨터 및 모바일 시큐리티, 공개키기반구조, m-커머스
이 메 일 : kisukim@iasecurity.com