인트라넷에서 역할기반 접근제어 에이전트

고영한, 오수열, 서재현
목포대학교 컴퓨터공학과

The Role-based Access Control Agent on Intranet

Young-Han Go, Soo-Yul Oh, Jae-Hyun Seo
Dept. of Computer Engineering in Mokpo National University

요 약

본 논문에서는 인트라넷환경에서 허가된 사용자만이 개체에 접근할 수 있도록 하기 위하여 역할기반 접근제어 정책을 이용하였다. 이러한 방법은 사용자와 데이터 사이의 권한부여의 복잡성을 감소시킨다. 또한 역할을 지역역할 및 전역역할로 구성하고 접근제어 연산 및 역할의 갱신에 따른 절차를 구현하였다. 구현을 위하여 분산객체 컴퓨팅 환경의 객체요청중개자 CORBA/ORB를 이용하였다.

1. 서 론

일반적으로 인트라넷 시스템은 운영조직을 위해, 메일서버, 웹서버, 데이터베이스 서버, 게이트웨이 서버 등의 다양한 컴퓨터 시스템을 포함하며, 이러한 시스템은 여러 가지 서비스를 이용하는 접근연산을 제공하게 된다. 이러한 기업군내에서 보안 대책은 첫 번째의 관심사이며, 이용할 수 있는 자원에의 접근과 인증에 관련된 보안, 전송에 있어서 정보의 보호에 관련한 전송 보안등이 있다. 특히 자원에의 접근은 정당한 권한을 가진 사용자에게만 허용해야 한다. 따라서 인트라넷 시스템은 인터넷에서처럼 지속적으로 해결하고자 하는 보안 문제를 수반하게 되며, 특히 허가된 사용자만이 객체에 접근할 수 있도록 하는 적절한 접근제어 정책이 적용되어야 한다[8]

최근의 인트라넷 환경은 기술의 발전에 따라 분산객체 패러다임이 분산객체 컴퓨팅 환경으로 구축되고 있다. 표준 플랫폼으로 OMG에서 제안한 CORBA 사양을 따르고자 하는 추세에 있으며 이를 지원하는 상용 패키지도 개발되어 널리 보급되고 있다. 또한 보안서비스를 제공하고자 하는 안전한 객체요청중개자(Secure ORB)에 관한 연구 및 개발이 함께 진행되고 있다[4,6]

본 논문은 실세계에서 사람, 일, 데이터 사이의 관계가 역할(role)과 권한(authorization) 유무에 따라 접근제어가 이루어지는 것처럼 컴퓨팅 환경에서 사용자 또는 응용에 따라 데이터에의 직접 접근을 제공하지 않고 역할(일)과의 관계를 통하여 접근제어를 수행함으로써 권한의 관리에 따른 복잡성을 감소시키고, 일관성을 유지할수 있도록 한다. 또한, 객체에 대한 안전한 관리를 가능케 하는 분산객체 환경에서의 역할기반 접근제어를 위하여 사용자의 전역(global)과 지역(local)역할을 구성하고 접근 연산 및 역할의 갱신에 따른 절차를 보인다.

2. 역할기반 보안 에이전트

2.1. 역할기반 접근제어

기존 보안정책의 대표되는 것으로는 자율적 접근제어(DAC)와 강제적 접근제어(MAC)의 방법이 있다 그러나 자율적 및 강제적 접근 방법은 실세계를 제대로 반영하지 못하고 있다 즉, 일반적인 조직에서의 권한 부여는 일 및 직급에 따라 지정되는 경우가 많은데 앞서의 방법들은 이러한 방법에 유연성을 제공하지 못하고 있다[2,3].

따라서 새로운 보안 접근 방법이 필요하게 되었으며 자율적 접근제어 방법에서의 그룹과 강제적 접근제어 방법에서의 다단계(multi-level)등 실세계를 반영하는 개념을 제공하는 역할기반 접근제어 정책을 제안하였다 역할기반 접근제어 방법은 사용자 또는 응용 프로그램은 업무에 따라 데이터에의 접근 권한이 부여된 역할을 갖게되며 이것은 그룹 기반의 자율적 접근제어 방법을 제공한다 또한 각 역할은 임의의 조직 내에서 다단계의 계층을 이루고 있다. 즉, 역할기반 접근 방법은 데이터에 대한 접근권한을 사용자 각각에 부여하는 것이 아니라 수행하는 기능 즉, 역할에 부여한 것이다[7,8]

2.2. 역할간의 계층구조

역할계층(Role Hicrarchy)은 부모(parent) 및 후손(ancestor) 관계인 {(Ri+1, Ri), >}의 순서화된 쌍으로 표현할 수 있다. Ri+1은 부모, Ri는 후손, >는 포함관계를 표시한다 따라서 역할계층의 권한은 다음과 같이 정의할 수 있다

- 역할계층 : 만일 한 사용자가 임의의 역할에 속하고(권한속성을 부여받았고), 그 역할이 또 다른 역할을 포함한다면 그 사용자는 포함한 역할에 대한 권한속성을 갖는다.

인트라넷에서는 보안 연산의 유연한 수행을 허용하기 위하여 각 서버를 위한 지역 역할계층과 전체 인트라넷을 위한 전역 역할계층의 두 가지 유형으로 구성할 수 있으며, 전역 역할과 지역 역할을 다음과 같이 정의할 수 있다. 지역 및 전역의 중요한 차이점은 서버 내의 객체 또는 서버에 대한 권한속성인가 하는 것이다.

- 전역 역할 : 전체 인트라넷상에서 전역허가의 권한 속성을 표현하며, 역할이 어떤 서버에 어떤 권한을 갖는가를 나타낸다.
- 지역 역할 : 인트라넷의 각 서버 내에 객체에 대한 권한 속성을 표현하며, 역할이 어떤 권한들을 갖는가를 나타낸다.

각 역할은 개인의 권한속성과 부모로부터 상속(inherit) 받은 권한 속성으로 구성할 수 있다. 또한 상속은 부모로부터 모두 받는 경우와 일부분만을 받아 자신의 권한 속성과 함께 구성될 수 있으며, 다중상속도 가능하다. 역할 권한속성의 표현을 위해서 지역 및 전역 역할 권한을 {역할이름, 권한속성, 객체리스트}로 구성한다. 이러한 전역 및 지역 역할 권한 사이에는 객체지향의 상속개념이 적용되어 역할 계층 구조를 형성할 수 있다 전역 및 지역 역할 권한 테이블의 예를 <표 1>에 보였다.

<표 1> 역할 데이터베이스 표현의 예

지역역할	지역허가	객체리스트
웹관리자(r1)	[-,-,R,-,X]	Wo1, Wo2
웹출판자(r2)	[C,D,R,W,X]	Wo1, Wo2
웹편집자(r3)	[-,-,R,W,X]	Wo1

(a) 지역역할 테이블(웹서버)

전역역할	전역허가	객체리스트
총괄관리자(R1)	웹관리자,웹출판자	웹서버
부서관리자(R2)	웹관리자	웹서버
팀 장(R3)	웹출판자	웹서버
DB 관리자(R4)	DB관리자	DB서버

(b) 전역역할 테이블

C:Creat, D:Delete, R:Read, W:Write, X:eXcute

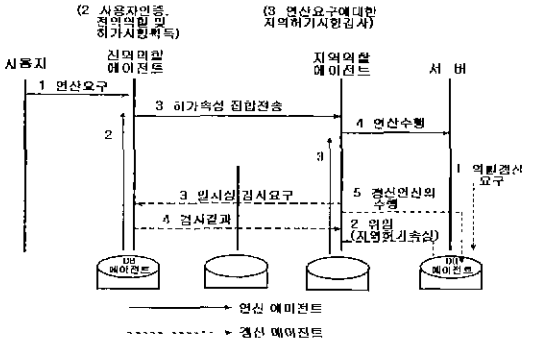
r : 지역역할, R : 전역역할, Wo Web object

지역허가(local permission)는 인트리넷의 각 서버 객체에서 이용할 수 있는 데이터 객체에 대한 권한속성 집합이며, 전역허가(global permission)는 전체 인트리넷 서버에 대한 권한속성의 집합이다 예를 들면, 지역역할은 웹 서버 내에서 특별한 작업을 수행하는 지역허가를 가질 수 있으며, 지역허가는 웹 서버 내에서 임의의 웹 페이지를 Read, Write, Modify, Create 할 수 있음을 의미한다. 또한 인트라넷에서의 전역역할은 총책임자, 부서 관리자, 팀장 그리고 일반 고용인으로 구성할 수 있으며, 전역역할 '팀장'은 임의 서버 객체에 접근하기 위하여 전역허가와 함께 지역역할을 위임(delegation) 받아야 한다. 전역 역할은 상호 상속될 수 있으며, 또한 각 인트라넷 서버에 대한 지역 역할들에 리스트를 포함한다 각 지역 역할은 지역 분산 객체에 대한 허가 권한을 포함하며, 하나의 서버는 여러 개의 분산객체를 포함할 수 있다.

3. 접근제어 에이전트

인트라넷이 분산환경인 점을 고려하며 보안기능 에이전트는 각 접근 요구에 대한 승인 및 거부 역할을 하는 참조모니터(reference monitor)로서 각 서버내의 지역 허기 및 전역 허가의 상태를 제어하고 역할에 부여된 권한속성 및 객체리스트 정보를 관리하는 기능을 하여야 한다. 또한 사용자의 연산요청에 대하여 전역 및 지역 에이전트와의 통신을 지원하는 연산 기능, 역할의 권한속성을 갱신하는 연산을 지원하는 기능이 필요하다.

이러한 기능을 같는 에이전트간의 접근연산 및 갱신 절차는 <그림 1>과 같다.



< 그림 1 > 접근제어 에이전트간의 통신

4. 접근제어 에이전트 구현

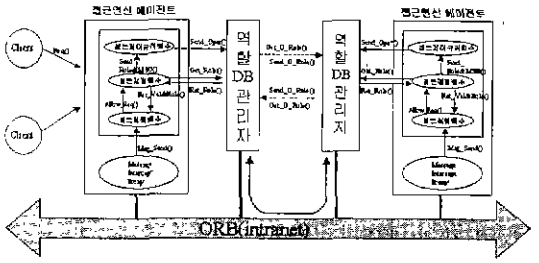
4.1. 역할기반 접근제어 에이전트 구현 모듈

본 논문에서 구축되는 접근 제어 에이전트의 모듈별 기능은 다음과 같다.

- 접근 연산 에이전트 : 사용자측과 목적지에 위치하여 메시지 처리와 역할 DB 에이전트와 통신하여 연산을 수행한다.
- 역할 DB 에이전트 : 사용자의 전역 및 지역에 대한 역할의 권한 속성을 검사하여 접근 연산 에이전트에 넘겨주고 갱신요청이 발생하면 해당연산을 수행한다

역할기반 접근제어 에이전트 구현 모듈은 <그림 2>와 같다

사용자의 요청에 의해 사용자측의 연산 에이전트가 전달되는 요청



< 그림 2 > 역할기반 접근제어 에이전트 구현 모듈

메시지를 ORB로부터 가로채는 메시지 인터셉터 대행자(MIP : Message Intercept Proxy)가 메시지의 내용을 접근제어 수행 함수(AEF : Access control Enforce Function)에 전달한다 그러면 AEF는 사용자가 요구가 정당한 지를 접근제어 결정 함수(ADF : Access control Decision Funtion)에 요구하고, ADF 는 역할 DB 관리자에게 사용자의 개체속성을 전달하여, 역할과 접근가능 여부를 AEF에 전달한다. 만일 타당하다면 AEF는 넘겨받은 전역역할과 기타 정보(메시지 포함)를 목적지로 ORB를 통하여 전달된다. 이때 AEF는 ADF에게 실행정보를 전달과 동시에 접근제어 규칙 함수(ACR : Access Control Rule)에게도 사용자의 역할과 요구 연산 메시지를 전달하게 된다, 그러면 ACR은 사용자의 메시지의 내용이 객체에 대한 연산요구에 대해서 어떤 일이 있을 것인지를 파악하여 요구시항에 맞게 역할 DB 관리자에게 제어 명령을 한다. 또한, 목적지의 에이전트는 전달된 메시지의 내용이 지역에 대해 어떤 역할을 가지는지 목적지의 역할 DB 에이전트에게 요구하여 사용자의 요구에 맞는 실행을 하고, 추후 감사를 위해 메시지 처리의 내용을 로깅해 둔다.

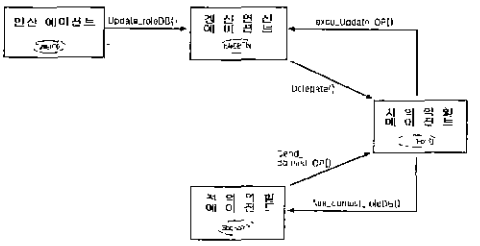
4.2. 갱신 연산 에이전트 구현 모듈

임의의 객체에 대한 역할 권한은 실세계처럼 수시로 변경될 수 있으므로 본 논문에서의 갱신연산 에이전트는 다음과 같은 기능을 하도록 구현되었다

- 역할갱신 에이전트 : 위임받은 갱신 연산의 수행 여부를 확인하기 위해 전역역할 에이전트와 통신하여 역할갱신 연산의 일치성 여부를 파악하여 결과를 지역 역할 에이전트에 통보한다.

접근제어에서의 AEF나 관리자의 요구에 의해 역할에 대한 속성의 변경을 갱신연산 에이전트에게 요청하게 되면 갱신 연산 에이전트는 서버의 권한을 지역역할 에이전트에게 위임하게 된다. 지역역할 에이전트는 역할 데이터베이스의 일치성을 위해 전역역할 에이전트에게 이 사실을 통보하게 되고 전역역할 에이전트는 일치성을 검사하여 일치성에 대한 사실을 지역역할 에이전트에게 응답하게 되면 지역역할 에이전트는 갱신을 갱신연산 에이전트에게 요구하며 최종적으로 역할 DB 에이전트가 역할에 대한 속성의 변경을 마무리하게 된다.

역할에 대한 갱신연산 에이전트 모듈의 구현은 <그림 2>와 같다.



< 그림 3 > 갱신 연산 에이전트

5. 결 론

인터넷에서 제공하는 상호 독립적인 전자우편, 원거리 로그인, 파일전송, 웹 등의 응용서비스를 이용하여 각 기업 및 기관에서는 인트라넷 시스템을 구축하고자 하는 연구 및 개발을 진행하고 있다. 본 논문에서는 분산객체 컴퓨팅 환경의 객체 요청중개자(ORB)를 이용하여 역할을 기반으로 한 접근제어 수행과 지역역할 및 전역역할의 구분을 통하여 권한 속성의 관리에 대한 복잡성을 감소시켰으며, 역할 갱신에 대해서 일관성을 고려한 접근제어 에이전트를 구현하였다

본 논문에서는 CORBA의 IDL및 JAVA를 이용하였으며, 유닉스용 Visibroker for Java와 JDK1.1.5를 서버로 사용하고 Windows 95를 운영체제로 사용하는 PC용 Visibroker for Java와 넷스케이프사의 브라우저를 설치하여 클라이언트로 사용하였다

향후, 역할 갱신시 역할 DB의 분산 중복 환경에서 위임 및 임무의 분리에 대한 고려가 필요하며, 감사 및 로깅에 대한 보완 구현이 필요하다.

참고문헌

[1] R W. Baldwin, "Naming and Grouping Privileges to Simply Security Mangement in Large Database", IEEE Computer Society Symposium on Research in Security and Privacy, May 1990 pp.116-132.
[2] David F. Ferraiolo, J. A. Cugini, and D. R. Kuhn, "Role-Based Access Control(RBAC) Features and Motivations", IEEE Conf. on Computer Security Application, 1995. pp 241-248.
[3] A. Giuri, etc, " A New Model for Role-based Access Control", IEEE Computer Security Applications, 1995 pp.249-255.
[4] IONA, "Programming guide orbix2 distributed object technology ", Release 2.0 Vol. 1, Nov 1995.
[5] V. Nicomette and Y. Des warte, " An Authorization Scheme for Distributed Object Systems", IEEE Symp. on Security and Privacy, 1997.
[6] Object Management Group, "CORBA Security", Document No. 95.12.1, Dec., 1995.
[7] R. S. Sandhu, E J. Coyne, and C E Youman, "Role-based Access Control Models", Feb 1996 pp. 38-.
[8] Z.Tari and S.Chan, "A Role-based Access Control for Intranet Security", IEEE Internet Computing, Sept/Oct. 1997. pp. 24-34.
[9] Visigenic, "VisiBroker for Java Reference Manual ", Ver 3.0, Sept 1997.
[10] Visigenic, "VisiBroker for Java Programmer's Guide", Ver3.0, Sept. 1997.