제26회 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호 (2006. 11)

사내 기밀문서 유출방지를 위한 데이터 접근제어 시스템

김규일*, 황현식*, 고혁진*, 이혜경**, 김웅모*
*성균관대학교 컴퓨터 공학과
**용인송담대학 컴퓨터게임 정보학과
{kisado, hjko, hhs486, umkim}@ece.skku.ac.kr
leehk@ysc.ac.kr

Access Control for Secrecy Document Protection in the Company

Kyu-Il Kim*, Hyun-Sik Hwang*, Hyuk-Jin Ko*, Ung-Mo Kim*, Hae-Kyung Lee**
*Dept of Computer Science, Sungkyukwan University
**Dept of Computer Game&Information, Songdam College

요 약

현재, 대기업이나 중소기업에서는 회사 내 정보보호 및 누출을 막기 위해 데이터 접근 기술을 적용 및 개발하고 있다. 하지만 기존 XML기반 RBAC 접근제어 기술은 회사환경에 적용하기에 무리가 있고 한계를 지니고 있기 때문에 사용자로부터 회사의 기밀정보를 보호하고, 시스템 디바이스에 대한 사용을 제어하기 위해서는 회사는 시스템의 보안 관리자에 의해 관리될 수 있는 보안메커니즘의 확립이 필요하다 .

따라서 본 연구에서는 회사 특성에 맞는 데이터 접근방법을 제시하고자 한다. 제안방법은 기존 XML 기반 RBAC 확장하여 사내 데이터 접근환경에서 사용자를 식별할 수 있는 인증 메커니즘과 사용자의 사용권한을 식별하는 인가 메커니즘을 설계 및 구현한다. 또한 각 부서에 성격에 맞는 메시지 프로토콜을 정의하고 제시함으로써 해당 부서에 요청하는 시스템에 따라 다른 정책을 제공할 수 있다.

1. 서론

사용자로부터 회사의 기밀정보를 보호하고, 시스템 디바이스에 대한 사용을 제어하기 위해서는 회사는 시스템의 보안 관리자에 의해 관리될 수 있는 보안메커니즘의 확립이 필요하다. 시스템의 보안 관리자는 이러한 보안 메커니즘[1][4]으로 사용자를 식별할 수 있는 인증 메커니즘과 사용자의 사용 권한을 식별하는 인가 메커니즘을 사용한다. 개인제어형 접근제어기술은 위의 두 보안메커니즘 중 인가 메커니즘에 해당한다. 통계에 의하면 지금껏 발생한 보안사고의 약 70% 가량이 내부 사용자의 소행에 의한 보안사고이다.

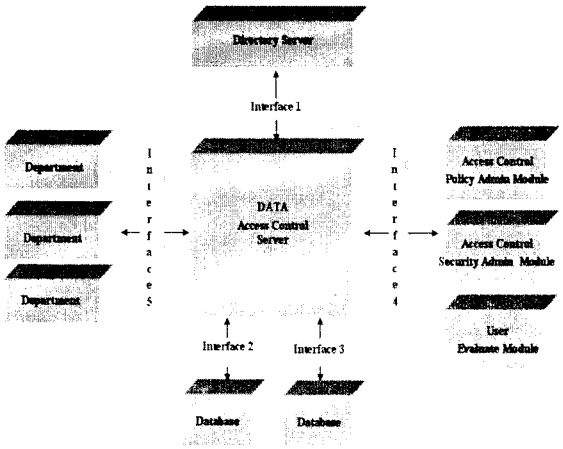
따라서 보안관리자는 회사의 기밀문서에 대해서는 외부 시스템 사용자들뿐만 아니라 내부 시스템 사용자의 접근에 대해서도 철저한 제어가 필요하다. 예를들어 회사의 중요한 기술문서를 내부시스템 사용자가 아무 제약 없이 접근하고, 그것을 유출할 수 있도록 보안정책이 기술되어 있다면 그것은 회사의 존폐와도 관련될 수 있는 큰 문제가 될 것이다.

본 연구에서는 사내 기밀문서 유출방지 시스템에 사용될 개인제어형 접근제어 기술로 기존 XML기반 RBAC[2][3][5]를 확장한다. 기존 접근방법은 회사 환경에 적용하기에는 무리와 한계를 지니고 있다. 회사 환경은 많은 부서와 수많은 다른 정책이 존재하기 때문에 새로운 접근제어 정책이 필요하다. 따라서 각 정책을 모듈별로 세분화하여 접근제어 정책관리 모듈, 사용자 접근권한 평가 모듈, 보안 관리자 모듈을 설계 및 구현하고 각 부서에 성격에 맞는 메시지 프로토콜을 정의하고 제시함으로써 해당 부서에 요청하는 시스템에 따라 다른 서비스를 제공할 수 있는 사내에 꼭 필요한 접근방법을 제시하고자 한다.

2. 사내 기밀방지 접근제어 시스템 모듈 제안

사내 기밀문서 유출방지에서 접근제어시스템은 시스템 보안관리자로부터 보안정책을 데이터베이스에 저장하고 관리하는 접근제어 정책관리모듈과 다른 내부 시스템으로부터의 개인의 접근권한에 관한 질의를 평가하고 응답하는 사용자 접근권한 평가 모듈로 구성된다.

(그림2)는 사내 기밀문서 유출방지 시스템에서 기밀문서와 시스템 디바이스에 대한 접근을 제어하는 접근제어 시스템 구성도이다.



(그림1) 사내 기밀문서 유출방지 접근제어 시스템

각 부서는 접근 요청이 제안 메세지 프로토콜에 의해 데이터 접근제어 서버에 접근하고 서버는 그 요청을 분석하여 각 해당 모듈 정책기반으로 기밀문서에 대한 개인의 접근을 제어한다.

2.1 접근제어 정책관리 모듈

접근제어 정책관리 모듈 중 XML형태의 접근제어 정책을 데이터베이스에 저장하기 위한 보안정책 저장모듈이다.

접근제어 정책관리 모듈은 보안 관리자가 기술한 XML 형태의 보안정책을 읽고 보안정책에 미리정의한 DTD로 유효성을 검사한다. 그리고 데이터베이스의 스키마에 따는 데이터 값을 뽑아내기 위하여 읽어들인 XML문서에서 컨텐츠 값을 뽑아낸다.

뽑아낸 컨텐츠 값을 데이터베이스의 스키마에 따르도록 데이터 값의 형을 변환시키고 데이터 값을 저장하기 위하여 DBMS와 상호작용하여 정책을 저장한다.

2.2 접근제어 정책관리 모듈

접근제어 정책관리 모듈 중 시스템의 보안관리자가 정책 관리를 목적으로 저장된 보안 정책에 대해서 질의를 수행하는데 사용되는 모듈이다.

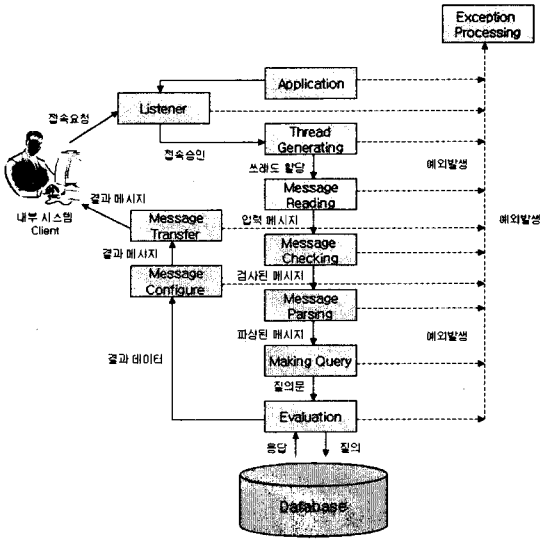
먼저 질의를 위한 데이터 값을 읽고 데이터 값을 데이터베이스에 질의하기 위한 쿼리 형태로 만든다.

쿼리는 데이터베이스의 DBMS와 상호작용하여 데이터베이스에 저장된 정책과 질의문을 비교하여 접근 여부를 판단한다.

3.2 사용자 접근권한 평가모듈

접근제어 시스템이 인트라넷을 통해 다른 내부 시스템으로부터의 개인의 접근권한에 관한 질의를 평가하고 응답하는 사용자 접근권한 평가 모듈이다.

(그림2)와 사용자 접근권한 평가 모듈이다.



(그림2) 인트라넷을 통한 사용자 접근권한 평가모듈

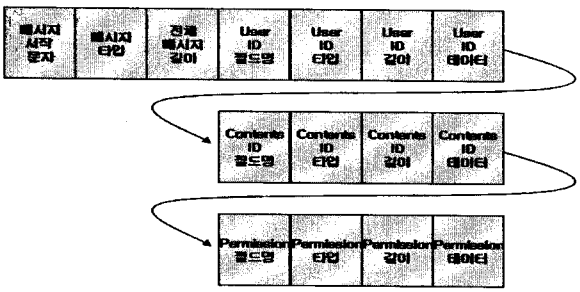
다른 내부 시스템으로부터 접근제어 서버로의 접속요청을 받을 준비를 하기위해 리스너 모듈을 호출한다. 리스너는 다른 내부 시스템이 접근제어 서버로 접속할 때까지 기다린 후, 만약 내부 시스템 클라이언트로부터 접속요청이 들어오면 Thead Generation Module를 호출한다. 쓰레드 모듈은 접속한 내부시스템 클라이언트에게 서비스를 제공하기 위해서 새로운 쓰레드를 할당한다.

내부 시스템 클라이언트와 쓰레드 간의 접속이 이루어지면서 내부 시스템 클라이언트로부터 질의 메

시지를 읽고 메세시자가 미리 정의된 프로토콜에 잘 따르고 있는지 유효성을 검사하고, 메시지가 유효하면 Message Parsing Module을 호출하고 그렇지 않으면 예외처리를 한다. 파싱 모듈은 유효성이 검증된 메시지에서 필요한 데이터 필드 값들을 추출해낸다. 평가 모듈에서 데이터베이스의 DBMS와 상호작용하여 DB에 저장된 정책과 질의문을 비교하여 접근 가능여부를 판단한다.

3. 부서와 접근제어 간의 메시지 프로토콜

회사 내 접근제어 서버는 제안한 프로토콜에 따라 메시지 형태로 질의/응답을 수행한다. 메시지 형태는 질의를 수행하는 내부 시스템에 따라 다르다. (그림3)은 사내 기밀문서 유출방지 시스템의 내부시스템이 침입감내 부서에서 접근제어 서버로의 질의하는 메시지 프로토콜이다.



(그림3) 침입 감내 시스템에서 접근제어 서버로의 메시지 프로토콜

메시지 시작문자는 메시지의 시작과 질의를 수행하는 내부 시스템이 누구인지를 알려주는 필드이다. 메시지 타입은 내부 시스템에 따라 서로 다른 형태의 타입을 갖기 때문에 메시지 타입만으로도 어떤 내부시스템으로부터의 메시지인지를 알 수 있다. 전체 메시지 길이는 실제 질의에서 사용될 이후의 필드들이 총 길이를 나타낸다. 따라서 이 필드의 값은 질의에 사용되는 데이터의 길이에 따라서 가변적이다. User ID 필드명, Userm ID 타입, User ID길이는 실제 User ID데이터를 위한 메타데이터이다. User ID 필드명은 접근제어 서버가 데이터베이스로부터 질의하기 위한 데이터베이스 스키마의 User ID필드에 해당한다.

(그림4)은 접근제어 서버에서 침입 감내 부서로 질의 결과를 응답하는 메시지 프로토콜이다. 그림과 같이 데이터 접근제어 서버에서 침입 감내 부서로의 메시지 프로토콜은 질의에 사용되는 메시지 프로토콜과 유사하다. 하지만 이 프로토콜에서 사용되는 요청 결과 데이터는 접근허가, 접근거부와 같이 고정된 길이 값을 갖기 때문에 메시지의 길이는 항상 고정되어 있다.

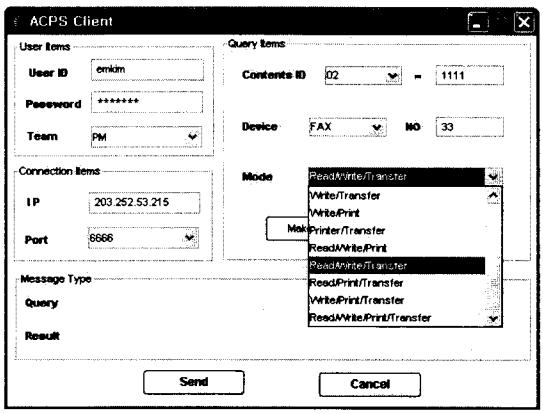
(그림4) 접근제어 서버에서 침입 감내 시스템으로의 메시지 프로토콜

4. 회사 내 접근제어 시스템 구현 및 동작

본 시스템은 앞의 모듈을 설계를 바탕으로 실제 구현과 동작과정을 제시한다.

접근제어 서버에서 서비스를 제공하기 위해 XML 형태의 보안정책을 파싱하고 파싱된 정책은 데이터베이스에 저장되어 접근제어 서비스를 수행하게 된다.

(그림5)은 접근제어 서버에 개인에 대한 접근권한을 질의하고 그 결과 값을 반환받기 위한 내부 시스템 클라이언트 초기화면이다. 내부 시스템 클라이언트는 크게 4가지의 필드로 구성되며 각각의 필드에 설명은 다음과 같다.



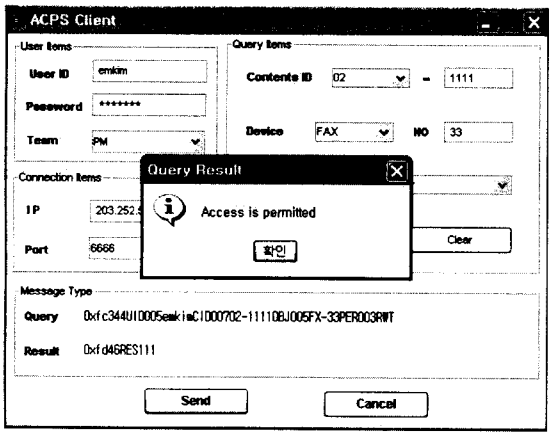
(그림5) 질의를 위한 데이터 값 입력

User Item필드는 질의할 개인의 아이디와 패스워드를 입력한다. 그리고 질의를 수행하는 내부시스템이 어디인지를 선택한다. Connection Item 필드는 접속할 접근제어 서버의 IP정보와 Port번호의 정보

를 나타내고 Query Item 필드는 실제로 질의를 수행할 기밀문서의 Contents ID값, 기밀문서를 처리할 디바이스 번호, 개인이 질의할 권한을 입력한다.

Message Type필드는 Query라는 TextField는 Query Items 필드로부터 입력된 값을 가지고 구성된 메시지를 나타내고, Result라는 TextFiled는 질의 메세지가 접근제어 서버에 전송된 이후 반환된 결과 메시지를 나타낸다.

(그림6)은 침입감내 부서의 입력 값에 대한 질의 결과를 나타낸다. 만약 허가 되었다면 그림과 같이 허가 메세지와 함께 Result TextFiled에 결과메세지가 반환된다. 내부 시스템 클라이언트는 반환된 결과 메시지의 파싱을 통해 결과 값을 알 수 있다.



(그림6) 침입감내 부서의 질의결과

5. 결론

본 연구는 사내 기밀문서 유출방지를 위한 데이터 접근제어 시스템을 제안하였다. 기존 XML기반 RBAC를 확장하였기 때문에 같은 권한을 갖는 사용자들을 역할이라는 형태이 그룹으로 묶음으로써 보안 관리자는 사용자 권한의 위임과 회수가 유용하다. 그리고 역할계층(Role Hierarchy)을 고려함으로써 명시적으로 권한을 명시하지 않아도 역할계층을 고려한 접근제어가 가능하다.

또한 XML 형태로 접근제어 정책을 정의함으로써 시스템의 관리자는 좀 더 구조화되고 획일된 형태로 보안정책을 구성할 수 있고, 새로운 정책의 삽입, 삭제 및 수정작업이 유용하다. 추후 인터넷을 통해 다른 시스템에 데이터를 전달할 수 있어서 보안정책을 다른 시스템으로 전달하는데도 용이하다.

가장 큰 제안 시스템의 장점은 회사환경에 적합하도록 정책을 세분화한 모듈 설계와 메세지 프로토콜을 제시함으로써 요청하는 각 부서에 따라 다른 정책을 제공할 수 있다.

끝으로 보안 관리자는 시스템을 관리하다가 보면 스스로 보안 정책에 대해서 질의를 수행하고, 그 결과에 대해 모니터링 해야 할 경우가 많다. 본 시스템 모듈은 데이터베이스에 저장된 보안정책을 보안관리자가 질의하고 결과에 대해서 모니터링 할 수 있는 기능을 제공하기 때문에 보안관리자에게 질의 및 모니터링 기능을 제공함으로써 효과적인 시스템 관리를 수행할 수 있다.

참고문헌

[1] Elisa Bertino, Ravi Sandhu "Database security-Concepts, Approaches, and Challenges" IEEE Transaction Vol.2, No1 (2005) 2-19

[2] R.S.Sandhu, E.J. Cynek, H.L.Fensteink, C.E.Youmank, "Role-Base Access Control Model" IEEE Computer, Vol 29, No.2 February(1996)

[3] Ahn, G.J, And Sandhu, R. "Role-based authorization constraints specification." ACM Transactions on Information and System Security Vol.3 issue4(2000)

[4] Apu Kapadia, Geetanjali Sampenmane, Roy H. Campbell "KNOW Why Your Access Was Denied: Regulating Feedback for Usable Security" ACM CCS'04 October 25-29, (2004)

[5] James B.D.Joshi, Elisa Bertino"Access Control Language for Multidomain Environments" IEEE Computer Society. (2004)