제22회 한국정보처리학회 추계학술발표대회 논문집 제11권 제2호 (2004. 11)

스마트카드 시스템을 위한 RBAC기반의 보안정책모델

이정림, 권기현
경기대학교 전자계산학과
{jrim, khkwon}@kyonggi.ac.kr

RBAC-Based Security Policy Model for SmartCard System

Jungrim Lee, Gihwon Kwon
Department of Computer Science, Kyonggi University

요 약

공통평가기준(CC, Common Criteria)의 고등급 평가를 받으려면 정형화된 보안정책 모델이 필요하다. 보안정책 중 하나인 접근제어 정책은 시스템의 자원과 데이터의 접근을 중재하여 오직 허가된 접근만 가능하도록 한다. 오늘날 임의적 접근제어(DAC, Discretionary Access Control)와 강제적 접근제어(MAC, Mandatory Access Control)의 대안으로 주목받는 역할기반 접근제어(RBAC, Role-Based Access Control)는 기업이나 정부의 다양한 조직체계를 반영하는 데 적합한 접근제어 정책이다. 다양한 기능과 보안성이 강조되는 스마트카드 시스템의 접근제어정책으로 RBAC을 적용하고 그에 관한 그래프형태의 정형화된 SPM을 보인다.

1. 서론

오늘날 시스템의 복잡성이 커짐에 따라 보안에 대한 관심이 날로 증가하고 있다. 고 보안성 정보보호 시스템의 중요 관심사중의 하나는 보안 기능성을 확인하는 보안평가이다. 정보보호시스템의 보안 평가에는 ISO 표준(ISO/IEC 15408:1999)인 공통평가기준(CC, Common Criteria)이 널리 사용되고 있다. 공통평가기준은 시스템의 보안 기능과 보증 수단에 대한 공통의 요구사항들을 제시함으로써, 독립적으로 수행한 보안성 평가 결과들 간에 상호 비교를 가능하게 한다.

공통평가기준의 평가보증등급은 EAL1 ~ EAL7까지 총 7단계가 있다. 각각의 평가보증등급을 받기 위해서는 각각의 단계가 요구하는 보증요구사항을 제출해야한다. 이중 고 신뢰성을 요하는 높은 보증등급을 받기 위해 가장 중요시되는 것이 보안정책 모델(SPM, Security Policy Model)*이다. 보안정책 모델은 기본적으로 시스템이 구현하고자 하는 기능의 기준이 되며, 보안정책 모델의 신뢰도에 따라 정보보호시스템의 신뢰도가 결정된다. EAL5이상의 고등급에서는 정형 SPM을 요구하고 있다 [1].

우리는 여러 보안정책 중 접근제어에 관심이 있다. 역할기반 접근제어(RBAC, Role-Based Access Control)에 기반한 스케쥴링 시스템에 역할의 식별, 인증을 위해 고보안성을 지닌 스마트카드를 이용한다. 그리고 역할기반 접근제어 정책에 대한 SPM은 균일하고 명확한 그래프 형태의 정형 모델을 사용한다.

2장에서는 배경연구를 설명하고 3장에서는 스케쥴링 시스템의 설계를 보인다. 4장에서는 시스템의 역할기반 접근제어 정책의 그래프형태의 정형화된 SPM을 보이고 5장에서 결론을 맺는다.

2. 배경연구

2.1 접근제어 정책

* 본 연구는 2004년 한국정보보호진흥원 정보보호시스템 보안정책모델 평가방법론 연구 지원에 의하여 수행되었음.

사용자가 네트워크를 통하여 시스템에 접근할 때, 허용된 시스템에서 접근요청을 하는지, 통신 대상이 되는 목적지 시스템에 대한 접근권한이 있는지를 검사하여 허용여부를 결정한다. 따라서 네트워크의 특정자원에 대해서 접근권한이 있는지를 검사한 후 접근여부를 결정하므로써 불법 침입자에 의한 불법적인 자원 접근 및 파괴를 방지할 수 있다.

접근제어는 접근제어 규칙(Access Control Rule)에 의해서 이루어지며 또한 접근제어 규칙은 보안정책에 의해 결정된다. 일반적으로 전통적인 접근제어 정책은 임의적 접근제어(DAC, Discretionary Access Control)와 강제적 접근제어(MAC, Mandatory Access Control)가 적용된다.

임의적 접근제어는 객체에 접근을 하고자 하는 주체의 접근권한에 따라 접근제어를 하는 방법으로 임의적으로 주체가 다른 주체에게 접근을 허가하기 때문에 트로이목마의 공격에 대한 취약점을 가진다. 강제적 접근제어는 주체의 레이블과 주체가 접근하고자 하는 객체의 보안레이블을 비교하여 보안정책에 합당한 접근제어 규칙에 의하여 접근제어를 하는 방법으로 사용자 임의로 접근 제한을 변경치 못하므로 트로이 목마에 의한 피해를 제한시킬 수 있다. 하지만 주체와 객체단위의 정책 적용이 어려운 단점이 있다. 따라서 기존의 접근제어 정책들로는 시스템의 보안요구사항을 모두 만족시킬 수 없기 때문에 역할기반 접근제어라는 조직에서의 역할과 권한이 관련된 접근제어 정책이 등장했다. 이것은 의무분리의 원리, 권한의 남용을 방지하기 위한 최소 권한의 원리, 기업의 조직과 의미적 일치를 갖는 역할계층 등, 현대사회의 기업 조직에 적합한 여러 가지 장점을 가지고 있어서 기존의 강제적 접근제어(MAC)나 임의적 접근제어(DAC)에 대한 대안으로 주목 받고 있다 [2, 3].

2.2 스마트 카드

스마트카드는 I/C칩을 내장한 소형 컴퓨터의 능력을 가진 신용카드 크기의 보안장치이다. 다중 애플릿을 탑재할 수 있어 가치이전의 수단 외에도 전화카드, 이동통신 보안수단, 신분증, 교통카드 등 그 활용분야가 아주 다양하다. 결국 보안성, 편의성, 경제성 및 다기능성 등을 획기적으로 개선시킨 새로운 개념의 카드이다.

기존의 자기띠(M/S, Magnetic Stripe)를 두른 카드가 발급당시 기록한 접근정보만을 저장하고 있다가 접근이 허락되는 접속장비(Interface Device)에 의하여 정보가 읽혀지는 수동적인 시스템으로 시중에서 손쉽게 구입할 수 있는 간단한 장비로도 복제가 가능하여 보안성이 취약한 반면, 스마트카드는 자체적으로 보안솔루션을 탑재하여 저장된 정보의 복제를 막고 나아가 스스로 외부의 공격에 대응하여 저장된 정보를 보호하며 내장된 어플리케이션의 중요도에 따라 보안정도를 구분하여 설정함으로써 외부의 접근정도를 스스로 선택하는 등 칩에 저장된 정보를 스스로, 그리고 적극적으로 보호·관리 한다 [4].

3. 스케쥴링 시스템 설계

먼저 UML을 이용하여 스케쥴링 시스템에 대한 요구사항 분석을 통한 기능모델을 만든다. 이런 기능모델들을 통해 역할기반 접근제어 정책에서의 Role과 Permission을 얻어낼 수 있다 [5].

3.1 유즈케이스

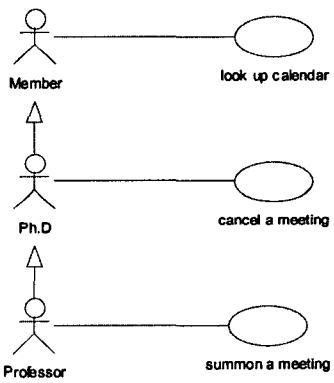


그림1. 액터들이 상속관계를 갖는 유즈케이스

- 시나리오

어느 대학 내 연구실에는 Professor와 Ph.D등의 Member들이 연구 활동을 한다.

1. Professor는 Calendar에서 일정을 확인한다.
2. Professor는 Member들에게 회의를 요청한다.
3. 회의를 요청 받은 모든 Member들은 자신의 Calendar의 일정을 확인한다.
4. 모든 Member가 회의 요청에 동의한다.
5. Calendar에 회의 일정을 기록한다.

4a. 한 명의 Member라도 회의 요청에 동의하지 않는다.

4a1. 그 회의는 취소된다.

5a. Ph.D는 Professor대신 예약된 회의일정을 취소한다.

5a1. 회의가 취소되면 Calendar 에서 회의일정을 지운다.

유즈케이스의 액터들은 역할기반 접근제어정책에서의 역할과 대응된다. 따라서 이 조직에서의 역할은 Role = { Professor, Ph.D, Member }가 된다.

3.2 시퀀스 다이어그램

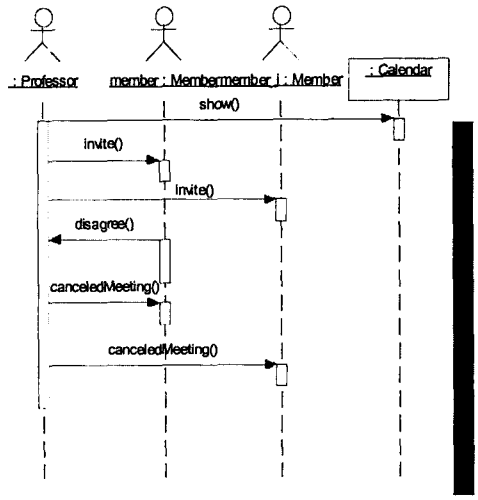


그림2. 회의요청이 취소되는 시퀀스 다이어그램

그림2 이외에 여러 시퀀스 다이어그램에서 나타나는 operation들을 통해 그에 대응하는 Permission을 얻어낸다.

Permission = { show, invite, agree, disagree,
cancelMeeting, addMeeting }

3.3 스마트카드의 상태 다이어그램

스마트카드 내에 User_ID와 PIN(개인식별번호)를 가지고 Member들의 역할을 식별하고 인증한다. 그림3은 스마트카드 애플릿의 식별 및 인증을 위한 상태 다이어그램을 나타낸다.

인증 3회 이상 실패 시 카드는 블록 되어지고 스케쥴링 시스템으로의 접근이 차단된다. 성공 시에는 정책 규칙에 따라 사용자 역할과 그에 따른 권한정보가 담겨있는 DB에 접근해서 시스템에 사용자 권한 정보를 넘겨주게 된다.(기본적으로 카드 인증 시 출퇴근시간을 체크하는 프로세스를 가지고 있다.)

다음에서 그래프를 이용하여 RBAC기반 스케쥴링 시스템을 위한 정형적인 SPM을 설명한다.

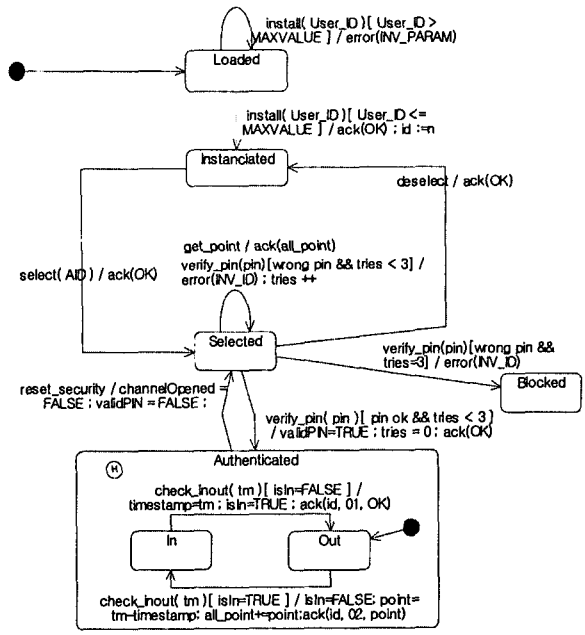


그림3. 스마트카드 애플릿의 상태 다이어그램

4. 그래프 변환을 통한 정형 SPM

시스템의 부정확한 행위를 예측하기위해 정책의 정확한 명세가 필요하다. 그래프변환은 접근제어정책의 명세를 위해 균일하고 정확한 프레임워크를 제공한다. 상태는 그래프에 의해 표현되고 상태전이는 그래프변환에 의해 표현된다. 정책은 아래 3가지 컴포넌트로 정형화 된다 [6, 7].

1) 타입 그래프 : 시스템 개체들을 node와 edge로 구성하고 node 내에 타입을 기술한다. u, r, p, s는 각각 User, Role, Permission, Session을 의미하는 타입이다. r타입의 node에 형성된 loop는 Role의 계층성을 의미한다. Role에 User와 Permission이 할당되고 Session을 통해 시스템에 접근하는 RBAC 기반의 타입그래프이다.

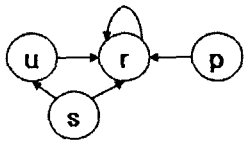


그림4. RBAC기반의 타입 그래프

2) 정책 규칙 : 앞 절의 기능모델을 통해 얻어낸

Role과 Permission을 이용하여 시스템의 행위를 제어하기 위한 정책 규칙을 그래프변환으로 표현한다.

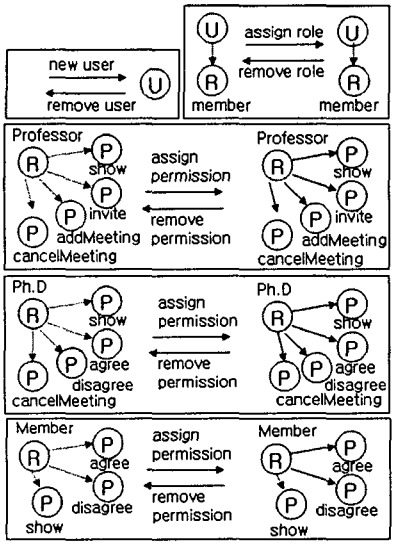


그림5. 정책 규칙

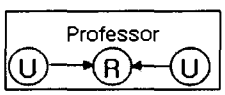
그림5의 정책 규칙은 role에 permission을 할당하는 부분으로 일부만 표현했다. 이것은 타입 그래프의 인스턴스 그래프이다. 그래프 변환 $r : L \rightarrow R$ 은 왼쪽편(L)에서 오른쪽 편(R)으로 상태가 전이된다. 왼쪽편의 점선으로 된 화살표는 상태 전이가 일어나기 전 만족해야 하는 제약 조건(NAC, Negative Application Condition)을 말한다. 위 규칙에서는 Role이나 Permission을 할당받기 전에 이미 할당되어져있으면 안 된다는 NAC을 가진다.

3) 제약 사항

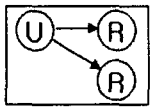
위 스케줄링 시스템에서 완전하진 않지만 아래와 같은 제약사항(Negative Constraint)을 가질 수 있다.

제약사항 그래프가 정책 규칙 그래프에 존재하지 않는다면 정책규칙은 제약사항을 만족한다고 할 수 있다.

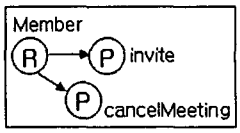
1. 오직 한명의 사용자만 Professor 역할을 할당받는다.



2. 사용자는 한 가지 역할만 할당받는다.



3. Member는 회의 요청과 일정을 취소 할 수 없다.



5. 결론

공통평가기준에서는 정보보호 시스템의 고등급 평가를 위해 정형화된 보안 정책 모델을 요구하고 있다. 우리는 정형화된 보안 정책 모델을 위해 그래프 변환을 통해 역할기반 접근제어의 정책 규칙과 제약사항들을 표현하여 RBAC 기반의 간단한 스케줄링 시스템을 구현하였다. 역할에 대한 식별 및 인증에는 스마트카드를 이용하였다. 따라서 각 카드에 부여된 역할에 따라 인증을 거쳐 시스템에 접근할 수 있다.

향후 연구로 그래프 변환 이외에 정형적인 보안 정책 모델에 대한 접근법과 검증에 대한 연구를 제안하고자 한다.

참고문헌

[1] 한국정보보호진흥원, 정보보호시스템 공통평가기준, 2002.

[2] D. Ferraiolo and R. Kuhn, "Role-Based Access Control," Proceedings of 15th National Computer Security Conference, 1992.

[3] R. Focardi and R. Gorrieri, "Access Control: Policies, Models, and Mechanisms," FOSAD 2000, LNCS 2171, pp.137-196, 2001.

[4] 금융감독원, "금융감독정보 제2003-13호," pp43-63, 2003.

[5] M. Koch and F. Parisi-Presicce, "Formal Access Control Analysis in the Software Development Process," in Proc. of Formal Methods in Security Engineering: From Specifications to Code (FMSE'03), 2003.

[6] M. Koch, L. V. Mancini, and F. Parisi-Presicce, "Graph Transformations for the Specification of Access Control Policies," Electronic Notes Theoretical Computer Science 51, 2001.

[7] M. Koch, L. V. Mancini, and F. Parisi-Presicce, "A graph-based formalism for RBAC," ACM, Trans. Inf. Syst. Secur, 5(3), pp.332-365, 2002.