프라이버시 증진형 역할기반 접근통제를 위한 정책결정점 설계 및 구현

김지혜[O1] 이영록[O2] 이형효[O3] 노봉남*
[O1]전남대학교 정보보호협동과정, [O2]전남대학교 시스템보안연구센터.
[O3]원광대학교 정보전자상거래학부, *전남대학교 전자컴퓨터공학부
[O1]jihye@lsrc.ac.kr, [O2]dogu@jnu.ac.kr,
[O3]hlee@wonkwang.ac.kr, *bbong@jnu.ac.kr

Design and Implementation of The Policy Decision Point for Privacy Enhanced RBAC

Jihye Kim[O1] YoungLok Lee[O2] HyungHyo Lee[O3] BongNam Noh*
[O1] [O2] *Chonnam national University [O3]WonKwang University

1. 서 론

근래에는 정보시스템 및 개인정보의 보호와 관련된 IT보안 규정 및 정책에 대한 관심이 높아졌으며, 법적 요구사항 역시 강화되고 있다. 각 국마다 다양한 법규와 정책들이 있으며, 이러한 개인 정보 보호 규정들은 '개인정보'라는 데이터보다 그에 관한 '권리'를 보호한다는 것에 주안점을 두고 있다. 또한 위의 정책을 따라야 할 비즈니스 영역에서는 관련 업무 조직이 보유한 정보(지적재산, 고객정보 등)에 접근하는 모든 요소들을 관리하는 접근통제가 이루어져야 하고, 통제에 대한 기술적인 방법이 제공되어야 한다. 따라서 정보에 대한 접근이 개별적 주체가 아닌 조직단위로 또는 조직 내에서 직무(역할)에 따라 결정 되어야하며 이들에게 접근통제 정책을 정의 할 수 있어야 한다. [1].

본 논문에서는 정보에 접근하려는 요청에 적합한 정책을 찾고 이를 평가하여 시스템으로의 접근을 허가하거나 거부하는 P-RBACML PDP(Policy Decision Point)를 정보 시스템에 적용 할 수 있도록 설계 및 구현한다. 본 PDP는 SUNXACML[2]의 복잡한 구성과 역할기반 접근 통제정책을 완벽하게 표현할 수 없다는 단점을 보완하고, 정보보호 담당자가 IT보안 규정 및 정책을 프라이버시 관리 측면에서 관리하는데 도움을 줄 수 있다.

2. 본 론

P-RBACML 정책언어 모델은 다음과 같은 요구사항을 만족 하도록 설계되어 있다[3]. 첫째, 산술연산 및 논리연산을 사용한 제약이 가능하여 풍부하게 조건을 표현 가능하다. 둘째, 요청자의 요구와 정책 간에 쉬운 연결이 가능하다. 이를 위해 요청자의 요청문에 표현되어 있는 값들과 정책에 정의되어 있는 값들 간에 매칭을 통해 연결이 이루어지도록 하는 XACML의 매칭기법을 차용하였다. 셋째, RBAC의 철학을 반영한다. 먼저 RBAC처럼 충돌되는 퍼미션 배정이 존재하지 않는 다는 것을 가정한다. 역할 단위로 접근통제를 수행하고 그 후 그 역할에 배정된 퍼미션에 따라 접근제어를 한다. 넷째, 프라이버시 강화 요소를 포함한다. 개인정보 소유자가 자신의 정보를 제공 할 때 동의했던 수집목적과 이용목적이 일치하는지, 또는 언제 이용되었는지를 알 수 있도록 하는 의무사항 등을 시스템 상에 명시한다.

P-RBACML 접근제어 모듈을 적용한 시스템에서의 시나리오는 아래와 같다.

A라는 회사의 마케팅 부서에서 새 상품 출시를 기해 판촉 목적으로 기존의 자사 고객에게 새 상품에 관한 이메일을 보내려고 한다. 마케팅 부서의 '김 대리'는 이를 위해 고객들의 이메일 주소를 고객 정보 DB에서 알아내고 싶다. 회사는 아래와 같은 고객 이메일 정보 이용에 대한 정책을 가지고 있다.

> "마케팅 부서 직원은 판촉 목적으로 고객이 허가하였다면 고객의 이메일 주소를 읽을 수 있다."

따라서 '김 대리'는 회사의 ERP 시스템에 접속해서 고객 정보를 취득하기 위해 자신이 마케팅 부서원이고, 원하는 정보는 이메일 주소이며, 이메일 주소를 읽기 원하고, 목적은 판촉(promtion)임을 입력한

다. 그러면 캐노니컬한 표현으로 바뀌어 시스템에 요청된다. 회사의 정책은 P-RBACML을 사용해서 관리되고, PDP는 이 정책과 요청을 비교 및 판단해서 평가를 내린다. 그에 대한 결과로 응답이 PDP를 통해서 시스템에 전달되게 된다.

정책은 실제 구현된 시스템에 policy/Marketing.xml이라는 문서에 정의되어 있으며, 이 정책은 policyFileStore에 의해서 읽히고, 적재된다. 요청 입력인 request/Request.xml은 RP에 입력으로 들어오고 파싱되어 PDP에 입력되며, 요청에 대한 정책의 평가 결과를 response 작성기에서 작성하여 내보낸다. 시스템이 이 응답을 이해하기는 매우 쉽다. Decision 요소의 텍스트 컨텍스트 문자열만을 판독하면 되기 때문이다. 따라서 이 모듈을 사용하는 시스템은 응답 XML문서를 파싱해서 사용자에게 데이터에 접근을 허가함을 알려줄 수 있다.

P-RBACML을 구현한 PDP모듈은 아래와 같은 구성 요소를 가지고 동작한다.

- P_RBACML_PDP : 모든 구성 요소들을 가지고 있는 클래스이다.
- policy files : 정책파일들을 모아놓은 것으로 policy 폴더 아래의 모든 '.xml' 파일들이다.
- PolicyFileStore : jnu.ssrc.prbacml 패키지의 클래스로 policy 파일을 위한 파서이다. 이 클래스의 policies에 모든 정책파일들이 저장된다.
- request : 도메인에 한정된 입력 값들을 xml문서로 표현한 request폴더 아래의 Request.xml 파일이다.
- Request Parser(RP) : PDP에 입력으로 Requset.xml 파일이 들어오면 jnu.ssrc.prbacml.ctx 패키지의 RequestCtx 클래스에 의해서 request라는 변수에 모든 요소가 파싱되어 PDP가 이행할 수 있는 형태가 되도록 해준다.
- PDP : 실제로 정책과 요청간의 평가를 내리는 PDP클래스이다. PDP(policyFileStore, requset) 형태를 취한다. 요청에 대해 evaluate 메소드를 사용하여 평가를 내리는데 이때 result라는 변수의 값을 True나 False로 정한다.
- Match : 요청에 대한 정책과의 비교를 위해서 사용하는 boolean 타입의 메소드이다. PDP의 evaluate에서 가장 먼저 불리어지며, 실제로 매치의 과정은 jnu.ssrc.prbacml.parsing.type 패키지 내의 RoleMatch, PurposeMatch, PersonalDataMatch, ActionMatch라는 클래스를 통해 이루어진다. 클래스 모두 Match 메소드를 사용하고, 정책에 쓰여 진 순서에 따라 각 요청 요소들을 정책과 비교한다. 모든 과정이 True이면 해당 요청을 허가할 수 있다. Match 과정 중에 한 요소라도 반환 값이 False이면 다음정책으로 이동한다.
- Result : Match에 의한 비교과정이 끝난 결과를 가지고 허가나 불가의 결정을 내려주는 역할을 한다. 이것은 result라는 값이 true인 경우 결과가 'Permit'이고 false이면 'Deny'이다. 이때 해당 정책에 Condition이 있다면 값을 확인하여 결과에 영향을 주도록 한다.
- response작성기 : Result의 결과를 가지고 response.xml을 작성하는 역할을 한다. 이때 의무사항(Obligation)이 존재하는지를 확인 한 후 존재하면 이를 포함시켜서 xml형태로 내보낸다.

3. 결 론

최근 비즈니스분야의 IT보안 정책 및 규정 동향을 보면 프라이버시의 보장이 매우 중요하다는 것을 알 수 있다. 따라서 기업이 복잡한 정책들을 관리하고 개인정보를 투명하게 유지 및 이용할 수 있는 시스템이 필요하다. SUNXACML은 다양한 타입들과 이미 표준화된 XACML을 구현 했다는 장점이 있다. 하지만 그만큼 그 구성이 복잡하고 역할기반 접근 통제정책을 완벽하게 표현하기에는 한계가 있다. 반면 P-RBACML은 프라이버시를 강화한 역할기반 접근통제 정책을 명세 하는데 보다 적합하다. 그래서 P-RBACML로 작성된 정책을 평가하고 시스템으로의 접근을 허가, 또는 거부하는 P-RBACML PDP(Policy Decision Point)를 정보 시스템에 적용 할 수 있도록 설계 및 구현하였다. 이는 SUNXACML의 단점을 보완하고, 정보보호 담당자가 IT보안 규정 및 정책을 프라이버시 관리 측면에서 관리하는데 도움을 줄 수 있다. 지금은 PDP모듈만 구현 된 상태이다. 하지만 추후 도메인에 한정된 입력 데이터들을 정규 형으로 변환할 수 있는 핸들러와 관리자가 정책을 작성 할 수 있는 정책 작성기를 추가하여 정책 관리 시스템으로 확장 할 계획이다.

참 고 문 헌

[1] Reid Jason, et al., A novel use of RBAC to protect privacy in distributed health care information systems, Lecture notes in computer science, 2003.

[2] Sun, Sun's XACML Implementation Programmer's Guide for Version 1.2, http://sunxacml.sourceforge.net/guide.html, 2004

[3] 이영록, 박준형, 노봉남 외 3명,"프라이버시 강화형 역할기반 접근통제정책 표현", 한국정보처리학회 논문집 제14권 제3호, 2007 정보통신분야학회 합동학술대회, 2007