DBpia

인터넷 Identity 관리 시스템 환경에서 XACML을 이용한 프라이버시 컨트롤러

정회원 노 종 혁*, 진 승 헌*

Privacy Controller using XACML for Internet Identity Management System

Jong-Hyuk Roh*, Seunghun Jin* *Regular Members*

요 약

인터넷 환경에서 유통되는 사용자 정보는 실소유자가 원하는 데로 제어되어야만 한다. 이를 위해서는 사용자가 요구하는 정보 유통 방식을 표현할 수 있는 프라이버시 정책이 필요하고, 사용자가 편리하게 정책을 설정할 수 있는 인터페이스가 요구된다. 또한 정보 유통이 발생할 때 사용자의 정책에 위배되는지 판단할 수 있는 시스템이 필요하다. 본 논문에서는 인터넷 Identity 관리 시스템 환경에서 운영되는 프라이버시 컨트롤러 시스템 모델을 제안하고 시스템의 인터페이스 및 정책 설정 과정을 제안한다. 정책 구현을 위한 언어로는 OASIS의 XACML을 수정하여 적용하였고, 사용자 정책 외에 도메인 정책, 기본 정보 제공 정책, 정책 충돌 해결 정책을 제안한다.

Key Words : Privacy, Identity Management System, XACML

ABSTRACT

In the Internet, an identity service must to obtain permission from a user to allow them to share data with requesting service. For that, the privacy policy, which reflects legal regulations and preferences made by the user, is needed. Also, the management interface that aids the user to make the privacy policy and the PDP system that makes admission control and policy decisions in response to a request from an entity wanting to access the personal information are needed. In this paper, the privacy controller system model handled under the internet Identity management system environment is proposed. The system has the easy interface of policy generation and the efficient policy decision process. The system applies and modifies to the XACML of OASIS group. We propose that the privacy policy is divided into the three policies, which are the user policy, the domain policy and the basic offering policy. To resolve the collision between the policies, we also propose the collision resolution policy.

Ⅰ. 서 론

인터넷에서 많은 사이트들은 사용자에게 서비스를 제공하면서 사용자의 사이트 가입을 요구한다. 사용자가 자신의 정보를 알려주고 싶지 않더라도 서비스를 제공 받기 위해서는 정보를 제공할 수 밖에 없다. 이에 대한 부작용으로 사용자는 사이트 가입 시, 타인의 정보 또는 거짓 정보를 입력하기도

* 한국전자통신연구원 정보보호연구단 (jhroh@etri.re.kr)
논문번호 : KICS2005-04-154, 접수일자 : 2006년 10월 10일, 최종논문접수일자 : 2007년 4월 25일

www.dbpia.co.kr

한다. 한편, 사용자가 많은 사이트에 가입하다 보면, 사용자 자신이 어느 사이트에 가입을 했는지 어떤 정보를 등록하였는지 기억하기가 어렵다. 그러므로 인터넷에 존재하는 사용자 정보는 오래되어 쓸모없거나 잘못된 정보인 경우가 적지 않다.

최근의 인터넷 검색 엔진들은 강력한 능력을 갖게 되어 어지간한 보안은 쉽게 뚫어 인터넷의 수많은 정보를 수집하고 있다. 이로 인해 사용자들은 검색 사이트에서 손쉽게 타인의 개인 정보를 얻을 수 있다. 이러한 상황임에도 불구하고 인터넷의 영세 사이트들은 고객의 정보 관리 또는 웹서버 보안에 투자를 하지 않고 있다. 심지어 고객의 정보를 판매하는 일도 발생하고 있다. 이런 문제들을 해결하기 위해 많은 연구가 이루어지고 있으며, 그 중에 대표적인 기술로 인터넷 Identity 관리 시스템이 있다[7].

인터넷 Identity 관리 시스템은 사용자가 안전하고 편안한 환경에서 인터넷을 사용할 수 있게 해준다. 한번의 로그인으로 많은 사이트들을 사용할 수 있게 해주는 SSO(Single Sign On) 서비스를 제공하고 사용자의 정보를 안전하게 관리하고 유통시킬 수 있는 기능을 제공한다. 인터넷 Identity 관리 시스템에서는 사용자의 개인 정보를 관리하는 사이트(Identity Provider. IdP)가 있다. 사용자가 다른 사이트(Service Provider. SP)에서 서비스를 이용할 때, SP에서 사용자 정보가 필요하게 되면 SP는 IdP에게 사용자의 정보를 요청한다. IdP는 사용자 규칙에 따라 정보 제공 여부를 판단하고 이에 따라 행동한다. 또는 사용자에게 직접 동의를 얻는 경우도 있다. 이처럼 인터넷 Identity 관리 시스템에서는 신뢰할 수 있는 사이트 IdP가 사용자의 정보를 관리하도록 하여 사용자는 안심하고 자신의 정보 관리를 IdP에 위탁할 수 있고, 서비스를 제공하는 다른 사이트 SP는 사용자 개인 정보가 필요할 시에만 IdP에 정보를 요청하도록 하여 불필요하게 여러 곳에 개인 정보가 분산되지 않게 한다.

사용자 정보의 유통은 사용자의 의지 또는 사용자와 사이트 간의 협약에 의해서만 이루어져야 한다. 이를 위해서는 사용자가 자신의 정보 유통에 대해 원하는 방식 또는 규칙을 표현할 수 있는 언어와 사용자 인터페이스 환경이 필요하고, 정보 유통이 발생할 때 사용자가 표현한 규칙에 위배되는지 판단할 수 있는 시스템이 필요하다.

본 논문에서는 인터넷 Identity 관리 시스템 환경하에서 운영되는 프라이버시 컨트롤러 시스템을 설계하고 개발한 결과에 대하여 기술한다. 프라이버시 컨트롤러는 일반 사용자들이 프라이버시 정책을 손쉽게 설정할 수 있는 인터페이스를 지원한다. 그리고, 프라이버시에 관심 없는 사용자를 위하여 또는 사용자의 잘못된 정책으로 문제 발생을 사전에 없앨 수 있는 도메인 정책을 운영할 수 있는 환경을 지원한다. 프라이버시 컨트롤러는 OASIS에서 제정한 인가정책 기술 표준인 XACML (eXtensible Access Control Markup Language)을 활용하여 정책을 생성하고 이에 프라이버시 개념인 개인 정보 사용 목적을 추가하였다. 그리고, 정보 유통에 대한 질의를 수신하면 프라이버시 정책에 따라 이를 판단하고 그 결과를 리턴한다.

본 논문의 구성은 다음과 같다. 2장에서는 논문과 관련된 프라이버시, Identity 관리 시스템, XACML을 소개하고 3장에서는 프라이버시 컨트롤러 인가, 프라이버시 컨트롤러 모델 및 프라이버시 정책 정의에 대해 기술한다. 4장에서는 프라이버시 컨트롤러에서 메시지 생성, 프라이버시 정책 생성을 위한 인터페이스를 설명한 후, 5장에서 결론을 맺는다.

Ⅱ. 프라이버시 및 Identity 관리 시스템

본 장에서는 프라이버시의 개념과 논문의 배경이 되는 Identity 관리 시스템을 설명한다. 그리고 프라이버시 컨트롤러의 정책 표현에 기본이 되는 XACML을 간단히 소개한다.

2.1 프라이버시

프라이버시에 대한 논의는 19세기부터 “혼자 있을 권리”, “사생활에 대하여 타인으로부터 간섭 받지 않을 권리”, “사생활의 비밀이 공개 당하지 않을 권리”라는 개념에서 시작되었다[11]. 정보화 사회가 진행되면서 프라이버시 개념은 “자기 정보 통제권”이라는 적극적인 개념으로 바뀌었다. 이에 따라 1980년 OECD는 프라이버시 보호와 개인정보 유통에 관한 가이드라인을 만들어 각국들로 하여금 이를 준수하도록 권고하고 있다. 1998년 EU에서도 “EU 개인정보보호지침 제25조 및 제26조의 적용에 따른 제3국에 대한 개인정보 이전”이라는 실무작업 보고서를 발표하였다[13].

이렇게 프라이버시에 대한 사회적 관심 증가되고 각 나라마다 관련 법규들이 제정되고 있으며 이와 관련된 연구는 지속적으로 진행되고 있다. 하지만, 인터넷 환경에서 사용자들의 개인정보를 보호할 수 있는 실질적인 도구 및 시스템은 아직 우리 주변에

www.dbpia.co.kr

서 보기 쉽지 않다. 사용자는 자신의 정보가 얼마나 어떻게 노출되었는지 알 수 있는 권리가 있음에도 불구하고 정보를 관리하고 있는 사이트의 도덕적 양심에만 의존하고 있는 실정이다.

2.2 Identity 관리 시스템

Identity 관리 시스템은 사용자, 서비스, 정보통신기기 등 네트워크에 연결되는 개체의 Identity 속성, 신원 증명서(Credential), 정보 이용 자격(Entitlement) 등을 포함한 네트워크 Identity의 생명주기를 전체적으로 관리해주는 플랫폼 기반 구조이다. Identity 관리를 통하여 조직의 내부 통신망이나 외부 통신망으로부터 접속해오는 사용자 또는 단말기를 인증하고 해당하는 권한을 확인하며 정보 자원에 대한 적절한 접근 권한을 인가해주는 과정을 처리할 수 있게 된다. 즉, 기존의 AAA (Authentication, Authorization, Audit/Account) 기술, P3P 기술, 패스워드 재설정 기술, 패스워드 동기화 기술, 계정관리 셀프 서비스, 관리 권한 위임, SSO, 메타 디렉터리, LDAP (Lightweight Directory Access Protocol) 등 여러 기술을 망라하여 구현된 복잡한 시스템이 바로 Identity 관리 시스템이다[2,3,12].

인터넷 Identity 관리 시스템에 대한 연구는 수년 전부터 많은 연구 단체 및 기업들에 이루어지고 있다. 이와 관련된 표준은 Liberty Alliance의 ID-FF (IDentity Federation Framework), ID-WSF(IDentity Web Service Framework), ID-SIS(IDentity Service Interface Specifications), OASIS 그룹의 SAML 및 XACML, 그리고, 마이크로소프트, IBM의 WS-Security, WS-Federation, WS-Trust, WS-Policy 등이 있다[4,5,6,8].

2.3 XACML

본 논문에서는 인터넷 Identity 관리 시스템 환경에서 사용자 개인정보 유통을 제어하기 위한 프라이버시 컨트롤러를 제안한다. 프라이버시 컨트롤러의 주된 서비스는 정보 유통에 대한 프라이버시 정책을 설정하는 기능과 정보 유통 질의에 대한 결정을 내리는 기능이다. 본 논문에서는 프라이버시 정책을 표현하기 위해 XACML 표준을 활용하였다.

XACML은 XML 정보보호기술 중의 하나로써 자원 혹은 접근 요청 개체에 권한(authorization)을 부여하고 이를 통해 자원에 대한 접근제어(access control)를 하는 XML 기반의 언어이다. 또한, 다양한 접근제어 제품들에게 일관되게 적용될 수 있는 권한부여 정책들을 위한 통합 언어를 제공함으로써 광범위한 관리 및 권한부여 시스템 간에 상호운영성을 제공한다. OASIS 그룹에서 표준화가 진행되고 있으며, 2003년 1.0, 2005년 2.0이 표준으로 채택되었고 현재는 3.0에 대한 표준화가 진행되고 있다.

XACML은 정책언어 모델을 제안하고 XML로 구성된 요청, 응답, 그리고 정책 문법을 정의한다[9]. XACML은 다양한 환경에서 적용될 수 있도록 확장성을 충분히 고려하여 작성되었다. 프라이버시 컨트롤러에서는 XACML의 모든 기능을 사용하기 보다는 인터넷 Identity 관리 시스템 환경에 필요한 기능을 선별하고 XACML에서 지원하지 않는 부분은 표준을 벗어나지 않도록 확장 필드 등을 이용하여 기능을 추가하였다.

Ⅲ. 프라이버시 컨트롤러

본 장에서는 인터넷 Identity 관리 시스템에서 프라이버시 인가 서비스를 제공하기 위한 프라이버시 컨트롤러를 소개한다. 프라이버시 컨트롤러의 기본 요소인 프라이버시 인가 모델, 프라이버시 컨트롤러 모델, 프라이버시 정책 분류, 정책 판단 등에 대하여 설명한다.

3.1 프라이버시 인가

프라이버시 인가는 개인 정보에 대한 접근을 특정 규칙에 따라 제어하는 것이다. 특정 주체의 특정 자원에 대한 특정 행위를 제어한다는 점은 기존의 접근 제어(access control)와 유사하다고 할 수 있다. 하지만, 프라이버시 인가는 특정 자원이 개인 정보라는 점과 접근 허가 판단을 개인 정보의 소유자가 직접 제어한다는 점에서 다른 기술이라고 할 수 있다[1,10,12].

본 논문에서 제안하는 프라이버시 인가 모델은 XACML 모델을 보강한 것으로써, 그림 1과 같다. 인가 모델은 질의, 응답, 정책으로 구성된다. 질의는 개인 정보를 사용하려고 하는 주체(Subject), 사용 대상인 개인 정보 자원(Resource), 정보 사용 행위(Action), 그리고 사용하려는 목적(Purpose)로 구성된다. 여기서, 주체, 자원, 행위로 구성된 집합을 타겟(Target)이라 한다. 응답은 결정(Decision)과 의무사항(Obligation)으로 구성된다. 결정은 질의에 대한 응답으로 개인 정보 접근을 허가하는지 거부하는지

www.dbpia.co.kr

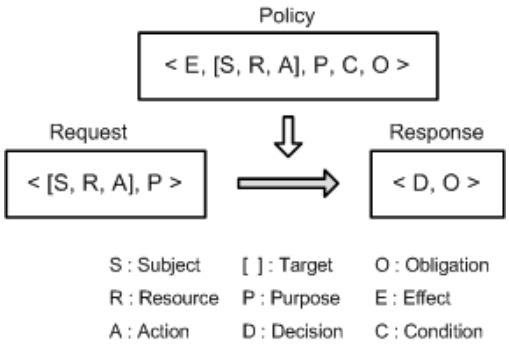


그림 1. 프라이버시 인가 모델

에 대한 결과를 포함한다. 의무 사항은 정보를 사용함에 있어 반드시 지켜야 할 사항을 의미한다.

프라이버시 정책은 효과(Effect), 타겟, 목적, 조건(Condition), 의무 사항으로 구성되어 있다. 효과는 해당 정책이 허가 정책 또는 금지 정책을 표현하는 필드이다. 조건은 주체, 자원, 행위 및 환경 변수 또는 속성함수에 대한 불리안 함수이다. 조건의 계산 결과가 "참"일 경우, 해당 정책이 질의를 판단할 근거가 된다. 즉, 프라이버시 컨트롤러가 정보 사용 요청을 수신하면 요청의 타겟으로 관련 정책을 검색한 후, 목적과 조건이 부합되는 정책을 선별하여 질의에 대한 결정을 내린다.

3.2 프라이버시 컨트롤러 모델

본 논문에서 제안하는 프라이버시 컨트롤러는 인터넷 Identity 관리 시스템에서 운영된다. 인터넷 Identity 관리 시스템에서는 개인 정보의 공유를 위해 ID-WSF 기술을 이용한다. 그림 2는 프라이버시 컨트롤러와 인터넷 Identity 관리 시스템의 관계를 보여준다[12].

그림 2의 왼쪽은 Identity 관리 시스템의 정보 공유 부분이고 오른쪽은 프라이버시 컨트롤러 부분이다. 데이터 요청자(Data Requester)는 사용자에게 서비스를 제공하기 위하여 또는 다른 목적을 위하여 사용자의 개인 정보를 필요로 하는 개체이다. 데이터 요청자는 특정 사용자 정보를 보관하는 데이터 제공자(Data Provider)의 위치 정보를 얻기 위해 디스커버리 서비스(Discovery Service)를 이용한다. 데이터 요청자는 데이터 제공자에게 개인 정보를 요청한다. 데이터 제공자는 정보 유통에 대한 정보 소유자(Principal)의 판단을 얻기 위해 프라이버시 컨트롤러에게 질의한다. 프라이버시 컨트롤러는 사전에 생성한 정보 소유자의 프라이버시 정책을 이

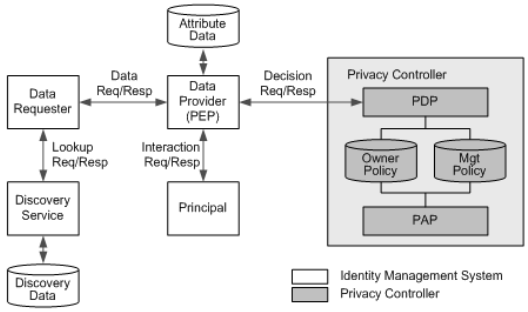


그림 2. 프라이버시 컨트롤러 모델

용하여 질의를 분석하고 관련 프라이버시 정책을 검색하여 판단을 내린 후, 데이터 제공자에게 결과 메시지를 전송한다. 결과는 허가, 거부, 질의로 나뉜다. 결과가 허가이면, 데이터 제공자는 데이터 요청자에게 개인 정보와 정보 사용에 대한 의무 사항을 전달하고, 결과가 금지이면 정보 제공이 거부되었다는 메시지를 전달한다. 결과가 질의이면 정보 소유자의 동의를 구하기 위해 데이터 제공자는 정보 소유자에게 정보 제공에 대해 질의한다. 프라이버시 컨트롤러의 PAP(Policy Administration Point)는 프라이버시 정책을 생성하고 관리하는 개체이다. 프라이버시 컨트롤러는 프라이버시 정책을 소유자 정책(Owner Policy)과 관리 정책(Management Policy)으로 구분하여 관리한다.

3.3 프라이버시 제어 주체 및 방법

본 절에서는 이러한 프라이버시 정책에 대한 분류, 정책 판단, 정책 생성에 대하여 살펴본다.

3.3.1 프라이버시 정책 분류

개인 정보의 모든 권한은 소유자에게 있으므로 정보의 유통은 소유자의 의지에 따라야 한다. 프라이버시 컨트롤러는 사용자가 프라이버시 정책을 용이하게 만들 수 있는 인터페이스를 제공한다. 그러나, 일반적으로 많은 사용자들은 아무리 편한 인터페이스를 제공하여도 프라이버시 정책 생성 작업을 어려워할 수 있다. 이러한 사용자들을 위해서 또는 사용자의 잘못된 정책 설정으로 인한 피해를 방지하기 위해 프라이버시 컨트롤러 관리자가 정책을 생성할 수 있다[12].

본 논문에서는 프라이버시 정책을 사용자 정책, 도메인 정책, 기본 정보 제공 정책으로 구분한다. 사용자 정책은 정보의 실소유자가 직접 설정하는 정책으로, 사용자들에게 편의성을 제공하기 위해 여

www.dbpia.co.kr

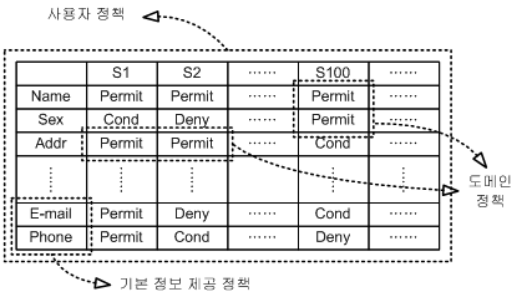


그림 3. 주체-자원 행렬

러 단계의 정책 설정 방법으로 구성되어 있다. 도메인 정책은 사용자 정보의 안전을 위해 관리자가 생성하는 정책이다. 편의성에 사용자 정책은 편의성에 우선을 두고, 도메인 정책은 정책의 정밀성에 우선을 둔다.

인터넷의 어떤 사이트들은 사용자 가입 절차 시, 전자 우편 주소와 같은 특정 정보에 대해서 자사의 목적에 맞게 이 정보를 사용할 수 있도록, 사용자에게 사용 허가를 요구하는 경우가 있다. 이는 자사의 광고, 판촉, 판매와 같이 사이트 운영에 필요한 정보를 확보하기 위함이다. 이러한 데이터 공유를 처리하기 위해 기본 정보 제공 정책이 있다.

그림 3은 사용자 정책, 도메인 정책, 기본 정보 제공 정책의 영역을 개념적으로 표현하고 있다. 주체 자원 행렬(Subject-Resource Matrix, S-R Matrix)은 정보 사용의 주체와 자원으로 이루어진 논리적인 다차원 행렬이다. 행렬의 셀은 하나의 자원 항목에 대해 특정 주체의 접근에 대한 결정을 의미한다. 정책을 표현하는 다른 항목인 행위 또는 조건 등을 표현하기 위해 하나의 셀은 여러 개의 값을 가질 수 있다.

사용자 정책은 각각의 개인 정보 필드와 해당 주체에 대한 결정을 표현할 수 있다. 예를 들어, 사용자는 전자우편 필드에 대하여 주체 S1에게는 허가하고 S2에게는 금지한다. 사용자는 주체-자원 행렬의 모든 셀에 대하여 정책을 생성하여야 한다. 프라이버시 컨트롤러는 사용자가 이러한 정책을 간편하게 생성할 수 있는 인터페이스를 제공한다.

도메인 정책은 자유로운 정책 생성이 가능하다. 특정 사용자 정보뿐만 아니라 모든 사용자 정보에 대한 접근도 제어할 수 있으며, 특정 주체 또는 특정 자원에 대한 정책을 생성할 수 있다. 그림 4에서는 두 개의 도메인 정책이 표현되어 있다. 한 정책은 주소 필드에 대해서 주체 S1, S2에 대해 허가한

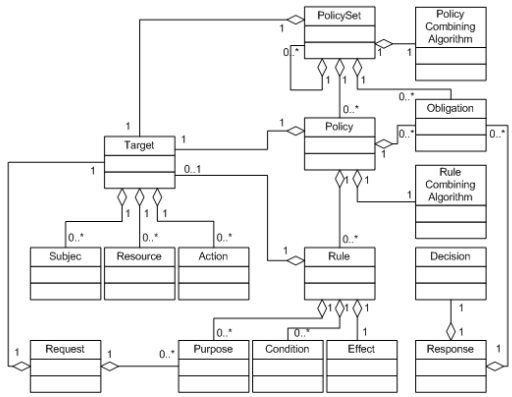


그림 4. 정책 재료 및 정책 모델

다는 것이고, 다른 정책은 주체 S100에 대해 사용자의 이름과 성별 항목을 공유하는 것에 대해 허가한다는 것이다.

기본 정보 제공 정책은 특정 정보 필드에 대해 접근을 허가하는 정책이다. 그러므로 기본 정보 제공 정책은 간단하게 개인 정보 필드 리스트로만 구성된다. 그림 4에서는 기본 정보 제공 정책이 전자우편과 전화 번호에 대해 모든 주체가 접근할 수 있도록 되어 있다.

3.3.2 프라이버시 정책 판단

프라이버시 컨트롤러는 요청에 대한 판단을 내리기 위해 사용자 정책, 도메인 정책, 기본 정보 제공 정책을 이용한다. 그런데, 임의의 요청에 대해서 세 종류의 정책은 각각 다른 결과를 보여줄 수 있다. 예를 들어, 그림 4에서 주체 S2가 전자우편에 대한 접근을 요청하는 경우, 사용자는 요청에 대해 거부 결정을 내리고, 도메인 정책은 이에 해당하는 정책이 없고, 기본 정보 제공 정책은 전자 우편에 대해 허가하라는 결정을 내릴 수 있다. 이와 같이 다른 결정을 내리는 경우를 처리하기 위해 프라이버시 컨트롤러에는 정책 충돌 해결 정책이 있다.

정책 충돌 해결 정책은 두 가지 방식 중 하나를 선택하게 되어 있다. 첫 번째는 세 정책에 대하여 우선 순위를 설정하고 우선 순위가 높은 정책에서 결정을 따르는 방법이다. 두 번째는 금지 우선 또는 허가 우선 방식을 선택하는 것이다. 예를 들어 금지 우선인 경우에 하나의 정책이라도 금지로 판단되면 응답 메시지는 금지로 결정하는 방식이다.

질의에 대한 결정은 허용(Permit), 금지(Deny), 불능(NotApplicable), 불확정(Indeterminate) 중에 선

www.dbpia.co.kr

택된다. 불능은 요청 메시지와 관련된 정책이 없는 경우를 표현하고 불확정은 프라이버시 컨트롤로 또는 네트워크 오류이거나, 요청 메시지 또는 정책 내에서 문법적 오류가 있는 경우를 의미한다.

3.3.3 프라이버시 정책 생성

앞서 설명하였듯이 프라이버시 정책은 효과, 주체, 자원, 행위, 목적, 조건, 의무 사항으로 구성된다. 이 항목들은 모두 XACML로 표현된다. 사용자 또는 관리자가 정책을 생성하기 위해 XACML을 배우고 사용하는 것은 불가능하므로, 프라이버시 컨트롤러는 XACM에 대한 지식 없이 정책을 생성할 수 있도록 편리하고 직관적인 인터페이스를 제공한다.

프라이버시 컨트롤러는 정책 생성을 보다 용이하게 처리하기 위해 정책 생성 과정을 두 단계로 구분한다. 첫 번째 단계는 프라이버시 정책을 구성하는 요소인 정책 재료(Ingredient)를 생성하는 단계이다. 두 번째 단계는 생성된 정책 재료를 기반으로 프라이버시 규칙(Rule)을 생성하고, 이 규칙을 이용하여 프라이버시 정책 및 정책 집합(PolicySet)을 생성하는 단계이다.

정책 재료는 프라이버시 컨트롤러 관리자가 생성한다. 프라이버시 도메인에서 예상되는 정책의 정책 재료들을 미리 생성하여 두고, 간단히 정책 재료를 선택하는 것만으로 프라이버시 정책을 생성할 수 있게 한다. 정책 재료는 주체, 자원, 행위, 목적, 조건, 의무 사항으로 자세한 설명은 4장에서 다룬다.

프라이버시 정책은 규칙, 정책, 정책 집합으로 구분된다. 규칙은 정책을 이루는 기초적인 요소이며, 결정을 내릴 수 있는 효과 필드(참/거짓 표현식)을 포함한다. 정책은 하나 이상의 규칙을 포함하며 질의에 대한 결과를 내리는 PDP에서 사용되는 기본 요소이며, 권한 부여 판정의 기본 형태이다. 정책 집합은 하나 이상의 정책으로 구성되고, 정책과 마찬가지로 결과 판정의 기본 요소이다.

자세히 설명하면, 규칙은 주체, 자원, 행위, 목적, 조건, 효과 필드로 구성된다. 여기서 효과 필드는 규칙 내의 정보에 의한 판단이 허가인지 금지인지를 명시하는 필드이다. 정책은 타겟, 규칙, 규칙 결합 알고리즘(Rule Combining Algorithm), 의무 사항으로 구성된다. 정책에 해당하는 질의가 허가인지 금지인지를 판단할 수 있는 근거는 정책이 포함하는 규칙의 효과 필드와 규칙 결합 알고리즘으로 판단할 수 있다. 규칙 결합 알고리즘은 금지 우선(Deny-overrides), 허가 우선(Permit-overrides), 최초 적용(First-applicable), 유일 적용(Only one applicable) 등으로 XACML의 알고리즘을 따른다. 정책 집합은 타겟, 정책, 정책 결합 알고리즘(Policy Combining Algorithm), 의무 사항으로 구성된다. 정책 결합 알고리즘은 규칙 결합 알고리즘과 대상만 틀릴 뿐 알고리즘은 동일하다[9]. 그림 4는 프라이버시 정책 재료, 정책, 요청 메시지, 응답 메시지를 표현한 모델이다.

Ⅳ. 프라이버시 컨트롤러 구현

본 장에서는 3장에서 기술한 프라이버시 인가, 프라이버시 컨트롤러 모델 및 정책 개념 등을 구현한 프라이버시 컨트롤러를 설명한다.

4.1 요청 메시지 및 응답 메시지

프라이버시 컨트롤러의 요청 메시지와 XACML의 요청메시지 간에 차이점은 두 가지가 있다. XACML에서는 요청 메시지에 자원 항목을 하나만 표현할 수 있게 되어있다. 그러므로 한 주체가 여러 개의 자원에 대한 공유를 질의할 경우 자원에 대한 개수만큼 요청 메시지를 생성하여야 했다. 본 시스템에서는 요청 메시지에 <Resource> 항목에 복수개의 자원을 지정할 수 있게 하였다.

XACML에는 목적이란 개념이 포함되어 있지 않으므로, 본 시스템에서는 목적 필드를 <Action> 항목의 하위 요소에 추가할 수 있도록 하였다.

그림 5는 요청 메시지를 보여준다. <Subject>의 subject-id 필드에는 정보 사용의 주체가 표현되고, <Resource>의 owner-id 필드에 자원 소유자를 그리고 resource-id 필드에는 자원을 명시한다. <Action>

```
<?xml version="1.0" encoding="euc-kr" ?>
- <Request xmlns="urn:oasis:names:tc:xacml:1.0:context"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  - <Subject>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>www.airline.com</AttributeValue>
      </Attribute>
    </Subject>
  - <Resource>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:owner-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>pc:sso:id:rsc:0001</AttributeValue>
      </Attribute>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>eid:email</AttributeValue>
      </Attribute>
    </Resource>
  - <Action>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>read</AttributeValue>
      </Attribute>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:purpose"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>entertainment</AttributeValue>
      </Attribute>
    </Action>
  </Request>
```

그림 5. 요청 메시지

www.dbpia.co.kr

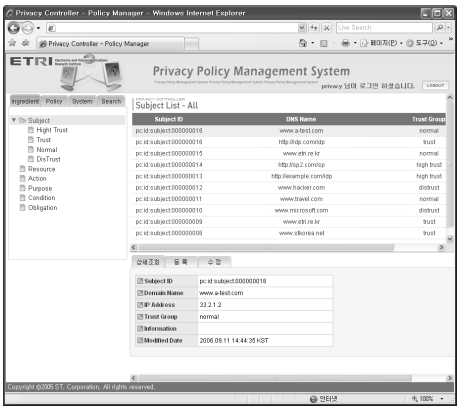


그림 6. 정책 재료 생성 - 주체

의 action-id 필드는 행위를 표현하고 purpose 필드는 목적을 표현된다.

프라이버시 컨트롤러의 응답 메시지는 XACML을 그대로 수용하였다. 프라이버시 컨트롤러는 XACML과는 다소 다른 요청메시지 형태를 따르지만, XACML 표준을 그대로 수용하고 있으므로 XACML 요청 메시지가 수신되어도 이를 처리할 수 있다.

4.2 프라이버시 정책 생성

프라이버시 정책은 정책 재료로 구성되고, 정책 종류는 도메인 정책, 기본 정보 제공 정책, 사용자 정책으로 구분된다. 그리고 정책 판단 시 정책 간의 충돌을 해결하기 위한 정책 충돌 해결 정책이 있다.

4.2.1 정책 재료 생성

프라이버시 컨트롤러에서 프라이버시 정책 생성은 정책 재료의 선택 작업으로 이루어진다. 프라이버시 컨트롤러 관리자는 프라이버시 정책을 생성할 수 있도록 미리 정책 재료를 생성해 두어야 한다. 그림 6은 프라이버시 컨트롤러 관리자의 정책 재료 관리 페이지이다. 좌측에서 해당 정책 재료를 선택하면 우측 상단 창에 해당 재료의 목록을 보여주고 지정된 목록의 내용이 우측 하단 창에 나타난다.

주체는 그림 6과 같이 주체의 식별자(Subject ID), 도메인 네임, IP 주소, 신뢰 그룹(Trust Group), 설명, 수정 일시로 이루어져있다.

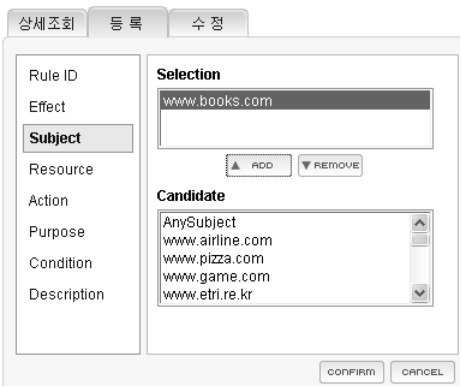
프라이버시 컨트롤러는 뒤에서 설명할 사용자 정책의 용이성을 얻기 위해, 주체를 신뢰 그룹이라는 등급으로 나누어 관리한다. 신뢰 그룹은 절대신뢰그룹, 신뢰그룹, 일반그룹, 비가입그룹 네 단계로 구성되어 있다. 표 1은 신뢰 그룹 단계를 설명하고 있다.

표 1. 신뢰 그룹 단계

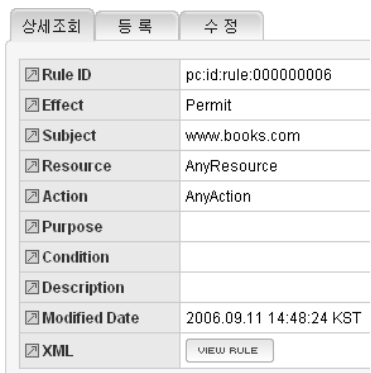
신뢰 그룹	설명
절대신뢰 그룹	금융권 또는 국가에서 운영하는 단체
신뢰 그룹	유명한 검색 사이트, 대형 쇼핑몰 등 사용자들에게 잘 알려진 사이트
일반 그룹	일반 사이트
비가입 그룹	인터넷 ID 관리 시스템의 신뢰 도메인 영역 밖의 사이트

4.2.2 도메인 정책

도메인 정책은 일반적으로 프라이버시 컨트롤러 관리자가 생성한다. 정책 재료를 이용하여 규칙을 생성하고 규칙을 기반으로 하여 정책을 생성한다. 그림 7은 규칙 상세조회 화면과 규칙을 생성할 때 규칙의 주체 항목을 설정하는 화면을 보여준다. 창의 하단에 보이는 Candidate는 정책 재료 생성 과



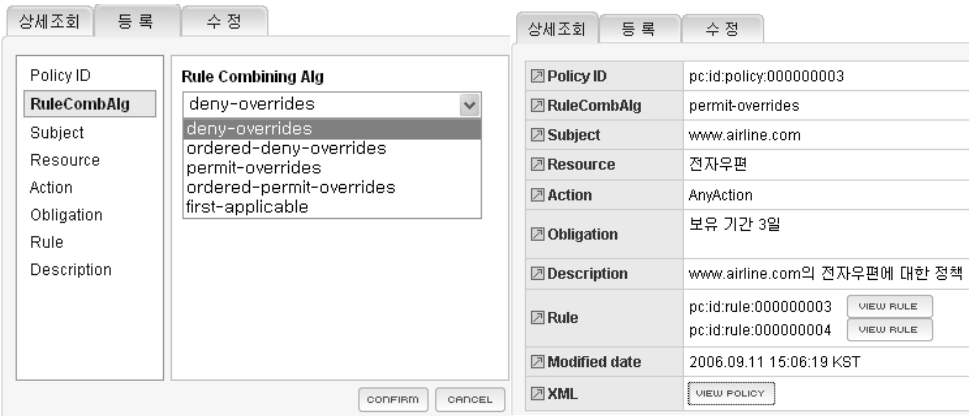
(a) 규칙 생성



(b) 규칙 상세 조회

그림 7. 규칙 생성 및 상세 조회

www.dbpia.co.kr



(a) 도메인 정책 생성 (b) 도메인 정책 상세 조회

그림 8. 도메인 정책 생성 및 상세 조회

정에서 이미 만들어진 주체 항목들이다. 원하는 항목을 선택하는 add 버튼을 눌러서 주체 항목을 규칙에 포함시킨다. 자원, 행위, 목적, 조건 항목 또한 그림 7과 같이 생성된 재료를 선택하는 방식으로 구성되어 있다.

그림 8은 도메인 정책의 상세조회 화면과 정책을 생성할 때 규칙 결합 알고리즘을 설정하는 화면을 보여준다. 정책 또한 규칙을 생성하는 방식처럼, 미리 생성된 정책 재료 또는 규칙을 선택하여 정책을 설정할 수 있다. 그림 8의 상세 조회 화면에서 Rule과 XML 부분을 보면 라는 VIEW RULE, VIEW POLICY 버튼이 있다. 이 버튼을 누르게 되면 해당 규칙 또는 정책의 XACML 표현을 볼 수 있다. 프라이버시 컨트롤러는 정책을 XACML 형태로 관리하고 정책 판단 시에도 XACML 포맷을 그대로 사용한다.

4.2.3 기본 정보 제공 정책

기본 정보 제공 정책은 사용자가 사이트 가입 시에 승낙한 정보 유통 항목을 표현한다. 정책 관리 방법은 그림 9에서 보여주는 것처럼 자원 항목을 선택하는 것으로 이루어진다.

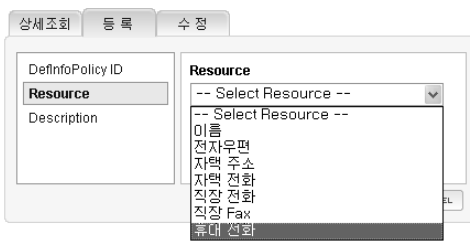


그림 9. 기본 정보 제공 정책 관리

4.2.4 사용자 정책

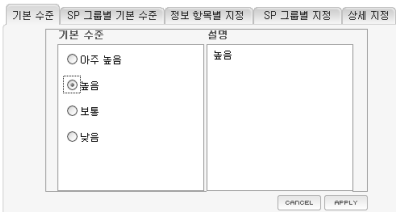
사용자 정책 관리에서 가장 중요한 점은 사용자가 얼마나 정책을 편하게 설정할 수 있는가 이다. 본 논문에서 제안하는 프라이버시 컨트롤러에서는 “기본 수준”, “SP 그룹별 기본 수준”, “정보 항목별 지정”, “SP 그룹별 지정”, “상세 지정”, 이렇게 다섯 가지 방법을 지원한다. 그림 10은 각 방법을 보여준다.

“기본 수준”은 사용자가 “아주 높음”, “높음”, “보통”, “낮음” 등 네 가지 레벨만을 단순히 선택하게 하는 방법이다. 네 가지 레벨은 프라이버시 컨트롤러가 미리 생성해 놓은 정책이다. 생성한 정책이 각 주체 및 자원 항목에 대해 어떤 방식으로 되어 있는지 확인하려면 “상세 지정” 방법을 이용하면 된다. 예를 들어, “아주 높음” 레벨은 대부분의 자원 항목에 대해 “금지”되어 있는 정책이고, 상대적으로 “낮음” 레벨은 대부분의 자원 항목에 대해 “허용”되어 있는 정책이다.

“SP 그룹별 기본 수준”은 주체의 신뢰 그룹에 대한 “기본 수준” 레벨을 지정하는 방법이다. “정보 항목별 지정”은 각 자원 필드에 대해 “허용”, “금지”, “질의” 등을 선택하게 하는 방법이다. “SP 그룹별 지정”은 각 자원 필드에 대해 신뢰 그룹에 대한 정책을 생성하는 방법이다.

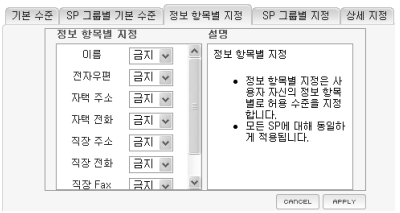
상기 네 가지 방법으로 생성된 정책이 각각의 주체와 자원 필드에 대해서 어떻게 정책이 설정되었는지 확인하려면 “상세 지정” 부분을 선택하면 된다. “상세 지정”은 그림 13처럼 주체-자원 행렬과 같은 모습을 보인다. 각 셀에 대해 일일이 정책을 설정할 수 있다.

www.dbpia.co.kr



(a) 기본 수준

(b) SP 그룹별 기본 수준



(c) 정보 항목별 지정

(d) SP 그룹별 지정

(e) 상세 지정

그림 10. 사용자 정책 설정

4.2.5 정책 충돌 해결 정책

정책 충돌 해결 정책은 질의에 대해 도메인 정책, 사용자 정책, 기본 정보 제공 정책이 서로 다른 결과를 내는 경우를 이를 처리하기 위한 정책이다. 정책 충돌 해결 정책은 아래 그림과 같이 정책간에 우선 순위를 두는 방식과 금지 우선, 허가 우선과 같은 오버라이드 방식을 선택하여 처리한다. 그림 11은 정책 충돌 해결 정책의 인터페이스를 보여준다.

우선 순위 방식을 사용할 시, 가장 높은 우선 순위를 갖는 정책으로 판단하여 그 결과를 얻게 되면 다른 정책에 대해서는 판단을 하지 않는다. 관련 정책이 존재하지 않아 결과를 얻지 못하면 다음 순위의 정책으로 판단을 수행한다.

오버라이드 방식에서는 결정을 판단하기 위해 임의의 정책 순서에 따라 판단을 시도한다. 예를 들어 허가 우선인 경우, 첫 번째 정책으로 판단한 결과가 "허가"가 나오는 경우에는 그 외의 정책에 대해서는 판단을 하지 않는다. 그 이유는 다른 정책에서 "금지"가 나오더라도 최종 판단은 "허가"이기 때문이다.

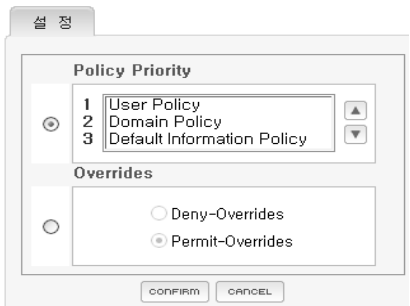


그림 11. 정책 충돌 해결 정책

V. 결 론

본 논문은 인터넷 Identity 관리 시스템 환경에서 개인 정보 유통을 제어하기 위한 프라이버시 컨트롤러를 제안한다. 프라이버시 컨트롤러는 정보 유통에 대한 프라이버시 정책을 설정하고 정보 유통 질의에 대한 판단을 내린다. 프라이버시 정책을 편리하게 생성할 수 있도록 정책 재료 생성 단계와 정책 생성 단계로 구분하였다. 그리고, 프라이버시 정

www.dbpia.co.kr

책을 사용자 정책, 도메인 정책, 기본 정보 제공 정책으로 구분하여 다양한 입장에서 프라이버시 정책 개념을 반영할 수 있다. 여러 정책의 충돌 문제를 해결하기 위해 정책 충돌 해결 방법을 제시하였다. 한편, 사용자가 편리하게 정책을 생성할 수 있도록 여러 단계의 인터페이스를 제공하였다.

향후 연구 과제로는 인터넷 Identity 관리 시스템이 다중 도메인 환경에 적용될 시, 도메인을 넘어 정보 유통이 발생할 경우, 서로 상이한 프라이버시 정책을 소유하는 도메인 간의 충돌 문제를 해결할 수 있는 연구가 필요하다.

참 고 문 헌

〔1〕 G.Karjoth, M.Schunter, and M.Waidner, "Platform for Enterprise Privacy Practices: Privacy-enbaled Management of Customer Data," *LNCS 2482*, 2002.

〔2〕 L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C 2002.

〔3〕 Liberty Alliance Project, *Privacy and Security Best Practices*, Nov. 2003.

〔4〕 Liberty Alliance Project, *Liberty ID-FF Architecture Overview*, Nov. 2003.

〔5〕 Liberty Alliance Project, *Liberty ID-WSF Web Services Framework Overview*, 2003.

〔6〕 Liberty Alliance Project, *Liberty ID-SIS Personal Profile Service Specification*, 2003.

〔7〕 M. Backes, B. Pfitzmann, and M.Schunter, "A toolkit for managing enterprise privacy policies," *ESORICS 2003, LNCS 2808,* 2003.

〔8〕 OASIS, *Assertion and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, 2005.

〔9〕 OASIS, *eXtensible Access Control Markup Language(XACML) Version 2.0*, Committee draft 04, 2004.

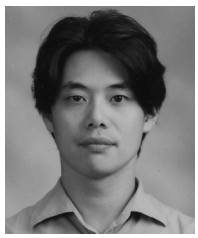
〔10〕 P. Ashley, "Authorization For A Large Heterogeneous Multi-Domain System," *Australian Unix and Open Systems Group National Conference*, 1997.

〔11〕 Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review,* 1980.

〔12〕 노종혁, 진승헌, 이균하, "인터넷 Identity 관리 시스템을 위한 프라이버시 인가," *한국통신학회논문지*, 제30권, 10B호, 2005.

〔13〕 류종현, "사이버공간에서의 프라이버시 침해에 관한 사례연구," *코리아크립토*, 2002.

노 종 혁(Jong-Hyuk Roh) 정회원



1996년 2월 인하대학교 전자계산공학과

1998년 2월 인하대학교 전자계산공학과 석사

2006년 8월 인하대학교 컴퓨터정보공학과 박사

2000년 12월~현재 한국전자통신연구원 정보보호연구단 디지털ID보안연구팀 선임연구원

<관심분야> 정보보호(프라이버시, PKI), 컴퓨터네트워크, 네트워크 보안

진 승 헌(Seunghun Jin) 정회원

1993년 2월 숭실대학교 전자계산공학과

1995년 2월 숭실대학교 전자계산공학과 석사

2004년 2월 충남대학교 컴퓨터과학과 박사

1994년 12월~1996년 4월 대우통신 종합연구소

1996년 5월~1999년 5월 삼성전자 통신연구소

1999년 6월~현재 한국전자통신연구원 정보보호연구단 디지털ID보안연구팀장/선임연구원

<관심분야> 컴퓨터/네트워크 보안, 정보보호(PKI), Digital Identity Management

www.dbpia.co.kr