웹 환경에서 정책 기반 개인정보보호 기술

Policy Based Privacy Technology in Web Environment

노종혁 (J.H. Roh) 디지털ID보안연구팀 선임연구원
진승헌 (S.H. Jin) 디지털ID보안연구팀 팀장

목 차

본 논문에서는 웹 환경에서 개인정보를 안전하게 관리할 수 있는 기술을 소개한다. 프라이버시와 관련된 기술을 분류하고, 웹 환경에서 적용될 수 있는 정책 기반 프라이버시 기술인 P3P, EPAL, XACML을 설명한다. 또한 이 기술을 활용한 마이크로소프트 인터넷 익스플로러의 P3P 기능, AT&T의 웹 브라우저용 P3P 사용자 에이전트 privacy bird, 그리고 identity 관리 시스템 환경에서 XACML을 이용한 ETRI IDMS의 privacy controller에 대하여 자세히 기술한다. 그리고 상기 기술의 장단점을 비교하여 향후 해결해야 할 점을 고찰한다.

I. 서론

현재 인터넷은 우리의 삶 구석구석과 연결되어 있다. 국민 대부분이 인터넷을 사용해 보았을 정도로 널리 보편화되어 있으며, 인터넷이 없는 세상은 상상하기 힘들 정도이다. 인터넷 사용자들은 쇼핑, 금융, 뉴스, 게임 등 수많은 사이트들을 수시로 방문하여 정보를 얻고 사이트가 제공하는 서비스를 이용한다.

인터넷에서 서비스를 제공하는 사이트들은 사용자들에게 서비스를 제공하기 앞서, 사용자의 가입을 요구한다. 요구되는 정보에는 이름, 주소, 전화번호, 주민등록번호 등의 중요한 사용자 정보들이 포함된다. 사용자들은 자신의 정보를 제공하기 싫더라도 서비스를 이용하기 위해서는 자신의 정보를 제공해야만 한다. 사이트들은 이러한 고객의 정보를 안전하게 관리한다는 개인정보규약을 제시하고 있지만, 사실 이 규약이 제대로 시행되고 있는지는 전혀 알 수 없는 상황이다.

개인정보 유출에 대한 사건은 심심치 않게 발생하고 있다. 그러나 사건 발생 순간에만 프라이버시와 관련 기술이 중요한 것처럼 다루어지고, 얼마 지나지 않아 사용자를 귀찮게 하는 버거운 기술로 인식이 되고 있다. 이는 아직 프라이버시 문제를 확실하게 해결할 수 있는 기술과 이와 함께 사용자 편의성을 제공하는 기술이 부재하기 때문이다.

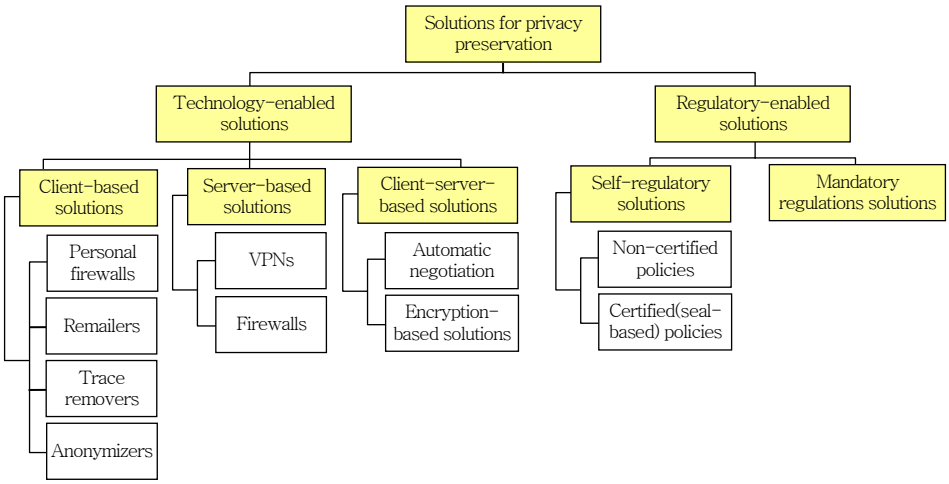
이러한 웹 환경에서 개인정보 사용에 대한 유출 및 오남용을 방지하기 위해 국제 웹 표준화 기구인 W3C는 P3P를 프라이버시 보호 표준기술 플랫폼으로 제안하였다. 현재 P3P는 마이크로소프트의 인터넷 익스플로러에 탑재되어 많이 사용되고 있다. 그러나, P3P가 제정된 지 현재 5년이 되어가고 있지만 인터넷 사용자들에게 잘 알려져 있지 않고, 그 기능 또한 미약한 편이다.

본 논문에서는 개인정보보호 기술에 대한 분류를 살펴보고 현재 웹 환경에서 프라이버시 보호를 위한 정책 기반 기술에 대하여 설명하고 비교한다.

II. 개인정보보호 기술 분류 및 표준

개인정보보호 기술은 다양한 형태로 연구가 진행되고 있다. 2003년에 IEEE Security&Privacy에서 발표된 Abdelmounaam의 논문에서는 개인정보보호 기술을 (그림 1)과 같이 분류하고 있다. 크게 기술 기반 솔루션과 정책 관련 솔루션으로 구분하고 있다[1].

기술 기반 솔루션은 사용자의 정보를 보관하고 있는 개인 컴퓨터를 보호하는 클라이언트 기반 기술, 사용자의 정보를 관리하고 사용자에게 서비스를 제공하는 서버 및 사이트와 관련된 서버 기반 기술,



(그림 1) 프라이버시 기술 분류

그리고 클라이언트와 서버간에 유통되는 개인정보와 관련된 클라이언트/서버 기반 기술로 구분된다. 정책 관련 솔루션은 사용자 정보를 관리하는 서버가 자체적으로 규정을 정립하고 제어하는 자율 규제 솔루션과 국가 차원에서 개인정보보호의 문제점을 알리고 예방 및 방지와 관련된 법률을 제정하고 적용하는 의무 규제 솔루션이 있다.

클라이언트 기반 기술에는 개인 방화벽, 리메일러, 경로 제거 기술, 익명성 기술이 있다. 개인 방화벽 기술은 개인 사용자 시스템에서 백그라운드로 실행되는 소프트웨어 방화벽과 관련된 기술이다. 리메일러는 메일 전송의 익명성을 제공하는 서비스 기술로 개인 이메일 송신자로부터 받은 메일에서 송신자의 정보를 숨긴 후 수신자에게 전달하고, 수신자의 답장을 대신 송신자에게 보내주는 기술이다. 경로 제거 기술은 인터넷 사용자의 웹 사용 정보가 노출되지 않도록 컴퓨터에 기록된 관련 정보를 제거하는 기술이다. 익명성 기술은 웹 사용자가 자신의 IP 주소 등의 정보를 숨길 수 있는 기술로서, 프록시 기반 기술, 라우팅 기반 기술, mix 망 기반 기술, P2P 기반 기술이 있다.

서버 기반 기술은 VPN과 방화벽 기술로 분류된다. 이 기술들은 개인정보보호 기술이라기 보다는 정보보호 분야의 일반적인 기술이므로 본 고에서는 설명을 생략한다.

클라이언트/서버 기반 기술은 자동 협상 기술과 암호화 기반 기술로 구분된다. 자동 협상 기술은 클라이언트와 서버가 각각 프라이버시 정책을 세우고 협상을 통해 사용자의 개인정보를 유통하고 관리하는 기술이다. 가장 대표적인 기술로는 W3C의 P3P가 있다. 암호화 기반 기술은 PGP 기술이 대표적이다. 서버와 클라이언트간의 개인정보 교환에 있어 대칭키, 비대칭키 등을 이용하여 기밀성, 무결성, 인증, 부인 방지 서비스를 제공한다.

본 논문에서는 프라이버시 정책 기반에 개인정보 공유 및 노출을 제어하는 기술로써, 상기 분류에 따르면 자동 협상 기술에 속한다. 정책 기반 개인정보보호 기술을 설명하기에 앞서 관련된 표준 및 기술을 설명한다.

1. P3P

P3P는 W3C에서 개발한 프라이버시 보호 관련 표준 기술로써 웹 사이트에서 이루어지는 데이터 처리 및 사용자의 개인정보와 관련된 표준이다. 사용자가 웹 브라우저를 이용하여 특정 웹 사이트에 접근하면, 해당 웹 사이트에서 이루어지는 사용자 개인정보 처리 방식에 관한 정책을 웹 브라우저에 제공하고, 사용자가 미리 설정해 놓은 프라이버시 정책에 따라 그 수준을 비교한 후, 그 결과에 따라 처리하는 기술이다[2].

P3P는 1997년부터 W3C 주도로 AOL, HP, 마이크로소프트 등 업계와 시민단체가 참여하여 진행하였으며, 2001년 개발이 완료된 후 시험 운용 끝에 2002년 4월에 국제표준으로 승인되었다. 마이크로소프트는 인터넷 익스플로러 6.0에 P3P 기능을 일부 채택하였고, AT&T는 P3P와 관련된 제품을 무료로 제공하고 있다.

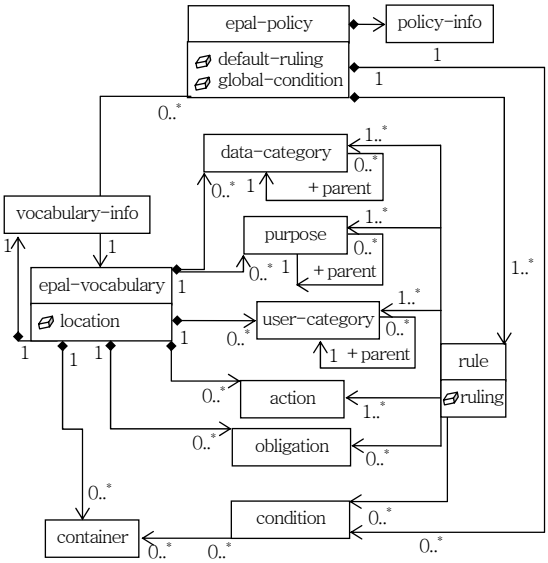
P3P와 더불어 W3C는 사용자가 자신의 정책을 표현하고 P3P 에이전트들 간에 P3P 정책을 교환할 수 있도록 APPEL을 제안하였다. APPEL은 웹 사이트가 제시하는 P3P 정책에 대해 사용자가 이를 요청, 제한, 차단할 수 있는 방법을 표현할 수 있는 언어를 제공한다[3].

P3P가 발표된 지 이미 5년이 지났다. 그리고, 많은 사용자들이 매일 웹 브라우저를 사용하고 있지만 아직 P3P에 대한 존재를 인식하고 있는 사용자는 IT 관련 특히 정보보호 관련 종사자 외에는 거의 없는 실정이다.

2. EPAL

EPAL은 IBM과 ZKS가 공동으로 개발한 기술로 기업 내 고객 정보와 같은 프라이버시 정보에 대한 정책을 수립하고 이를 교환하고 판단하기 위한 기술이다. 프라이버시 정책을 생성하기 위해 EPAL은 어휘(vocabularies)라는 개념을 사용한다. 이는 기업간에 다양한 정책을 수립할 수 있도록 EPAL의 확장성을 염두에 둔 방법으로 사용자 카테고리, 데이터

카테고리, 목적, 행위, 조건, 의무 등의 계층 리스트를 정의하고 이 어휘를 이용하여 프라이버시 정책을



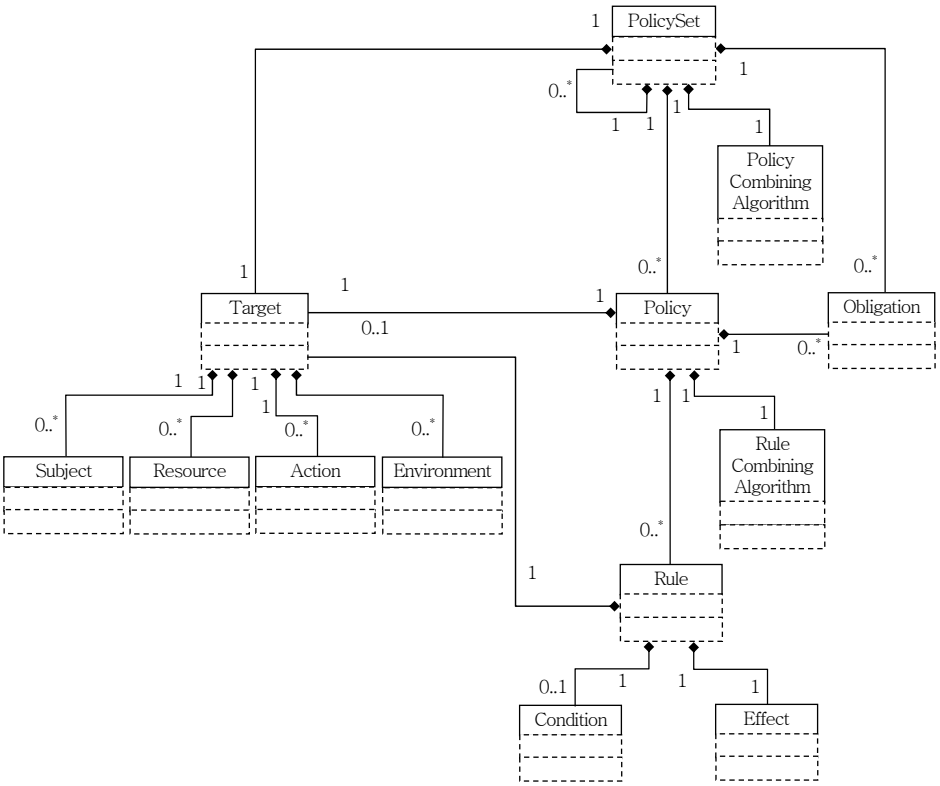
(그림 2) EPAL 정책의 UML

생성하도록 되어 있다[4].

사용자 카테고리는 데이터를 사용하는 주체에 대한 계층 구조이고, 데이터 카테고리는 수집된 데이터를 프라이버시 관점에서 정의한 것이다. 목적은 데이터가 사용되는 의도를 의미하고, 행위는 데이터가 어떤 방식으로 사용되는지를 표현한다. 조건은 정책 판단에 요구되는 제약, 요구 사항 등으로 이에 합당한 경우만 정보에 접근이 가능하다. 의무는 정보 접근에 따르는 지켜야 할 항목을 표현한다. 이러한 어휘를 조합하여 EPAL 정책을 생성한다. EPAL에는 정보 사용을 요청하는 요청 메시지 포맷을 정의하고 있다. 요청 메시지에는 사용자 카테고리, 행위, 데이터 카테고리, 목적이 포함된다. (그림 2)는 EPAL 정책을 UML로 표현한 것이다.

3. XACML

XACML은 XML 정보보호기술 중의 하나로써 자



(그림 3) XACML 정책

원들 혹은 접근 요청 개체들에 권한부여를 통해 자원들에 대한 접근 제어를 하는 XML 기반의 언어이다. 또한, 다양한 접근제어 제품들에게 일관되게 적용될 수 있는 권한부여 정책들을 위한 통합 언어를 제공함으로써 광범위한 관리 및 권한부여 제품들에게 상호 운영성을 제공한다. OASIS 그룹에서 표준화가 진행되고 있으며, 2003년 1.0, 2005년 2.0이 표준으로 채택되었고 현재는 3.0에 대한 표준화가 진행되고 있다[5].

XACML은 정책언어 모델을 제안하고 XML로 구성된 요청, 응답, 그리고 정책 문법을 정의한다. XACML은 다양한 환경에서 적용될 수 있도록 다양한 기능 요구사항을 만족하며 확장성을 충분히 고려하여 작성되었다.

XACML은 EPAL과 비슷하게 주체, 자원, 행위, 조건, 의무 사항 등으로 규칙을 구성할 수 있다. 규칙이 모여서 프라이버시 정책을 구성하고 프라이버시 정책이 모여서 정책 집합을 구성한다. 주체, 자원, 행위로 구성된 타깃이라는 개념을 제공하여 요청 메시지와 관련된 정책을 빠르게 접근할 수 있게 하였다. (그림 3)은 XACML 정책의 구조를 보여준다.

P3P, EPAL, XACML은 프라이버시 정책을 생성할 수 있도록 해주는 표준이라는 점에서 비슷하지만, P3P는 웹 환경에서 개인정보를 보호하기 위한 것으로 다른 표준에 비해 다소 간단한 편이다. 이에 비해 EPAL과 XACML은 기업 내 데이터 접근 및 사용자 정보를 보호하기 위한 기술로 보다 다양하고 복잡한 프라이버시 정책을 생성하고 관리할 수 있다.

Ⅲ. 정책 기반 개인정보보호 기술

본 장에서는 상기 기술을 이용하여 프라이버시 서비스를 제공하는 시스템들을 소개한다. 우선 가장 많이 사용되는 프로그램 중 하나인 마이크로소프트의 인터넷 익스플로러에서 P3P를 적용하고 있는 방법을 설명하고, AT&T의 privacy bird를 살펴본다. 그리고, ETRI에서 개발한 ID 관리 시스템인 IDMS의 privacy controller를 소개한다.

1. 인터넷 익스플로러에서 P3P

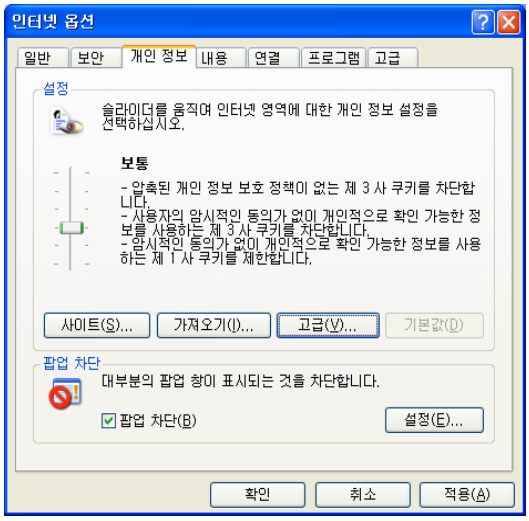
마이크로소프트의 웹브라우저인 인터넷 익스플로러는 P3P를 탑재하여 사용자가 스스로 쿠키를 선별적으로 수용할 수 있게 하는 기술과 컴퓨터가 읽을 수 있는 프라이버시 정책 파일의 자동 비교 기능을 적용하여 인터넷 사용자가 자신의 개인정보를 보호할 수 있도록 되어 있다. 자신의 개인정보 유출과 정보에 대한 공유 등 프라이버시에 대한 사용자들의 우려가 높아지는 웹 환경에서 인터넷 익스플로러의 기능에 쿠키 통제 기술을 추가한 것이다[6].

인터넷 익스플로러의 개인정보 기능을 설명하기에 앞서, 쿠키에 대하여 간단하게 언급하겠다. 웹의 가장 기본적인 프로토콜인 HTTP는 stateless 특성으로 인해 지속적인 세션을 보장하지 못한다. 전자상거래 및 금융 지불 사이트 등에서는 지속적인 세션이 반드시 필요하며, 이를 해결하기 위해 쿠키가 개발되었다. 쿠키는 HTTP 세션 관리에 사용되는 텍스트 파일로써, 사용자의 정보를 보관할 수 있고 사이트에 대한 사용자 통계 자료를 만들기 위해서도 사용된다. 일반적으로 간단한 문서편집기로 읽을 수 있으며, 특정 웹사이트에 대한 사용자 로그인 정보인 패스워드 및 개인정보들이 기록될 수 있다. 쿠키의 보안상 문제는 텍스트 파일인 쿠키 안의 중요 정보들이 노출되거나, 웹브라우저와 사이트 간에 쿠키를 주고 받을 때 중간에서 쿠키를 가로채어 악용할 수 있다는 것이다. 쿠키는 영구 쿠키와 임시 쿠기가 있다. 영구 쿠키는 만료일자가 지정되어 웹 브라우저가 닫혀도 컴퓨터에 남아 있는 쿠키이고, 임시 쿠키는 브라우저가 닫히면 자동으로 삭제되는 쿠키이다.

(그림 4)와 같이 인터넷 익스플로러는 쿠키에 대한 통제를 6단계로 구분하여 설정할 수 있다. <표 1>은 개인정보 설정 단계를 설명하고 있다. 설정은 모두 쿠키와 관련되었으며, 제 1사의 쿠키(익스플로러 7에서는 '자사의 쿠키'라고 표현함)는 사용자가

보고 있는 사이트의 쿠키를 의미한다. 제 3사의 쿠키(익스플로러 7에서는 '타사의 쿠키'라고 표현)는 현재 보고 있는 사이트가 아닌 다른 사이트에서 보내온 쿠키이다. 이것은 img 태그나 frame 태그 등을 통해 다른 사이트의 콘텐츠를 링크한 경우 해당 콘텐츠에서 쿠키를 보내면 제 3사의 쿠키가 된다.

설정 표현 중에 개인적으로 확인 가능한 정보(익스플로러 7에서는 '사용자에게 연락하는 데 사용할 수 있는 정보'라고 표현함)는 성명, 비밀번호, 주민번호, 신용카드번호 등을 의미한다. 그리고, 압축된



(그림 4) 인터넷 익스플로러의 개인정보 옵션

개인정보보호정책이란 P3P 정책을 시스템에서 용이하게 인식하기 위해 개인정보 태그를 세네 글자로 줄여서 표현한 것을 말한다.

명백한 동의, 암시적인 동의는 태그의 속성 옵션인 opt-in과 opt-out을 의미한다. Opt-in은 사용자의 동의를 구하겠다는 것이고 opt-out은 사용자의 동의를 구하지 않겠다는 태그이다. 한편 불만족 쿠키(unsatisfactory cookie)라는 개념이 있는데, 이는 속성 옵션 opt-in, opt-out, always가 붙지 않은 개인적으로 확인 가능한 정보를 의미한다. 불만족 쿠키의 태그는 <표 2>와 같다.

익스플로러에서 제공하는 기본 설정 외에 고급 설정이 있다. 고급 설정은 현재 사이트의 쿠키와 링크된 사이트의 쿠키에 대하여 허용, 차단, 사용자 선택을 지정할 수 있게 되어 있다.

외부에서 제작한 프라이버시 정책을 가져오는 방법 또한 존재한다. 프라이버시 정책 표현 방법으로는 <MSIEPrivacy>라는 마이크로소프트의 자체적인 정책 포맷을 사용한다. <MSIEPrivacy>는 <p3p CookiePolicy> 안에 제 1사 쿠키를 표현하는 <firstParty>와 제 3사 쿠키를 표현하는 <thirdParty>가 있다. 이 내부에는 if 문을 사용하여 특정 압축 토큰이 있으면 거부하거나 허용하는 방식으로 구성되어 있다.

〈표 1〉 인터넷 익스플로러 6 개인정보 설정

설정	내용
모든 쿠키 차단	- 모든 웹 사이트의 쿠키를 차단합니다. - 컴퓨터의 기존 쿠키를 웹 사이트에서 읽을 수 없습니다.
높음	- 압축된 개인정보보호정책이 없는 쿠키를 차단합니다. - 사용자의 명백한 동의가 없이 개인적으로 확인 가능한 정보를 사용하는 쿠키를 차단합니다.
보통 높음	- 압축된 개인정보보호정책이 없는 제 3사의 쿠키를 차단합니다. - 사용자의 명백한 동의가 없이 개인적으로 확인 가능한 정보를 사용하는 제 3사 쿠키를 차단합니다. - 암시적인 동의가 없이 개인적으로 확인 가능한 정보를 사용하는 제 1사 쿠키를 차단합니다.
보통	- 압축된 개인정보보호정책이 없는 제 3사 쿠키를 차단합니다. - 사용자의 암시적인 동의가 없이 개인적으로 확인 가능한 정보를 사용하는 제 3사 쿠키를 차단합니다. - 암시적인 동의가 없이 개인적으로 확인 가능한 정보를 사용하는 제 1사 쿠키를 제한합니다.
낮음	- 압축된 개인정보보호정책이 없는 제 3사 쿠키를 제한합니다. - 사용자의 암시적인 동의가 없이 개인적으로 확인 가능한 정보를 사용하는 제 3사 쿠키를 제한합니다.
모든 쿠키 허용	- 모든 쿠키는 이 컴퓨터에 저장됩니다. - 이 컴퓨터의 기존 쿠키는 그 쿠키를 만든 웹 사이트에서 읽을 수 있습니다.

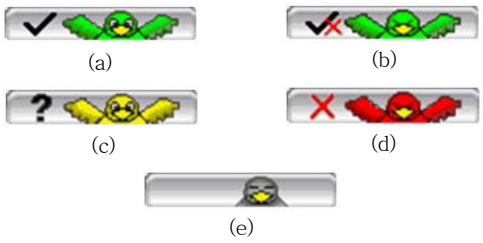
〈표 2〉 개인적으로 확인 가능한 정보 태그

Category	압축 토큰	설명
<physical/>	PHY	Contact or location information
<online/>	ONL	Contact or location information on the Internet(for example, e-mail address)
<government/>	GOV	Identification issued by the government(for example, social security number)
<financial/>	FIN	Information about an individual's finances
Purpose	**압축 토큰**	**설명**
<individual-analysis/>	IVA	Analysis that can be related to individual users
<individual-decision/>	IVD	Taking actions based on user history
<contact/>	CON	For contact by means other than telephone
<telemarketing/>	TEL	For contact by telephone
<other-purposes/>	OTP	Any other purpose not captured by other P3P purposes
Recipient	**압축 토큰**	**설명**
<same/>	SAM	Legal entities that use the data for their own purposes under equable practices
<other-recipient/>	OTR	Entities that are accountable to the provider but might use data in unknown ways
<unrelated/>	UNR	Entities that use data in ways unknown to the provider
<public/>	PUB	Public forums

2. Privacy Bird

Privacy bird는 AT&T가 무료로 제공하고 있는 웹 브라우저용 P3P 사용자 에이전트이다. Privacy bird는 새 모양의 아이콘이 웹 브라우저의 타이틀 바에 부착되어 사용자가 웹 사이트에 방문하면 해당 사이트의 P3P 정책을 로딩하고 사용자의 프라이버시 정책을 비교하여 그 결과를 화면으로 보여주는 프로그램이다[7],[8].

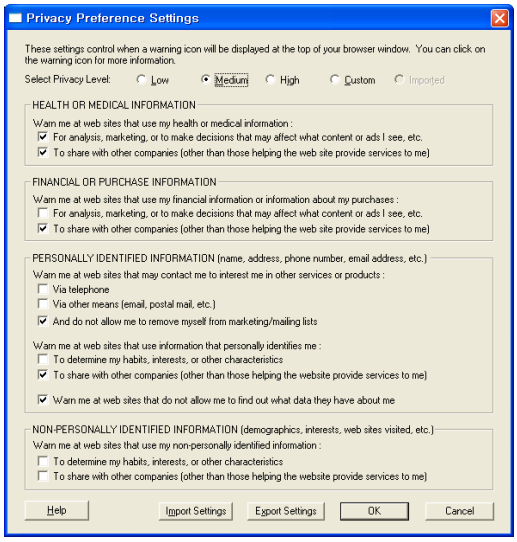
(그림 5)는 privacy bird 아이콘의 모습을 보여준다. 녹색 새와 체크 표시가 있는 (a)는 사이트의 정책과 사용자의 정책이 정확하게 매치되었음을 표현하고, 녹색 새, 체크 표시, 빨강색 X가 표시되어 있는 (b)는 정책은 상호간에 매치되었으나 P3P 정책에 없거나 정책에 매치되지 않는 콘텐츠가 있는 경우이다. 물음표와 노란색 새가 있는 (c)는 해당 사이트가 P3P 정책이 없음을 의미하고, 빨강색 새와 X가 있는 (d)는 정책이 상호간에 매치되지 않았음을 표현한다. 회색 새인 (e)는 privacy bird 프로그램이 정지되었음을 표현한다.



(그림 5) Privacy Bird 아이콘

Privacy bird는 policy summary라고 하는 기능이 있다. 이는 해당 사이트의 P3P 정책을 사용자가 읽기 편하도록 재구성하여 보여주는 기능이다. 그리고 해당 사이트의 프라이버시 정책 페이지 링크, 웹 페이지에 포함된 콘텐츠 목록을 보여주는 기능을 제공한다.

(그림 6)은 privacy bird에서 사용자 정책을 생성할 수 있는 윈도다. 정책 생성에 편의성을 제공하기 위하여 low, medium, high로 구성되어 있고, 고급 사용자는 해당 체크 박스를 직접 선택할 수 있다. 정책 생성은 개인 정보의 종류에 따라 의료 정보 부분, 재정 또는 구입 정보 부분, 개인 식별 정보 부분, 관심분야, 웹 방문과 같은 비개인 식별 정보 부분으로 구분되어 있다.



(그림 6) Privacy Bird 프라이버시 정책 생성 윈도

한편 익스플로러와 마찬가지로 생성된 정책을 임포트할 수 있는 기능도 있다. Privacy bird는 W3C의 표준인 APPEL을 사용하여 익스플로러 보다 호환성이 우수하다.

3. ETRI IDMS의 Privacy Controller

ETRI IDMS(e-IDMS)란 ETRI에서 개발한 identity 관리 시스템을 말한다. 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 기술, P3P 기술, 패스워드 재설정 기술, 패스워드 동기화 기술, 계정관리 셀프 서비스, 관리 권한 위임, SSO, 메타 디렉터리, LDAP 등 여러 기술을 망라하여 구현된 복잡한 시스템이다[9].

● 용 어 해 설 ●

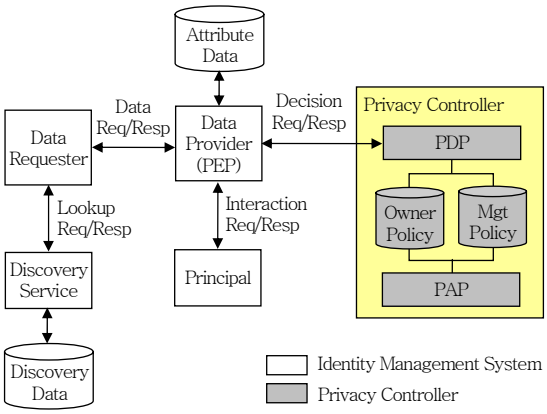
Identity: 일반적으로 identity라고 하면 계정정보, 즉 로그인 정보 또는 크리덴셜을 주로 생각하지만, identity 관리 시스템에서 identity는 해당 개체를 유익하게 식별할 수 있는 정보 및 해당 개체에 영향을 주고 받는 모든 정보로써 각종 개인정보(identifier, 주민번호, 신용카드번호, 신용도, 이메일 주소 등)를 포괄하는 개념이다.

인터넷 identity 관리 시스템에 대한 연구는 수 년 전부터 많은 연구단체 및 기업들에 의해 이루어지고 있다. 이와 관련된 표준은 Liberty Alliance의 ID-FF, ID-WSF, ID-SIS, 그리고, OASIS 그룹의 SAML, XACML, 마이크로소프트, IBM의 WS-Security, WS-Federation, WS-Trust, WS-Policy 등이 있다[5],[10]-[14].

ETRI IDMS는 SSO, ID 연계, 데이터 공유 등은 Liberty Alliance의 표준을 따르고 있으며, 개인정보보호 부분은 XACML을 이용한다. 앞에서 설명한 P3P 관련 기술은 웹 브라우저와 사이트 간의 쿠키 설정을 다루고 있지만, ETRI IDMS의 프라이버시는 사용자의 개인정보를 보관하고 있는 IDP와 사용자에게 서비스를 제공하고자 하는 SP 간에 사용자 개인정보 공유를 제어하는 것을 목표로 한다.

가. Privacy Controller의 데이터 공유와 프라이버시 제어

(그림 7)의 왼쪽은 identity 관리 시스템의 정보 공유 부분이고 오른쪽은 privacy controller 부분이다. Data requester(IDMS의 SP)는 사용자에게 서비스를 제공하기 위하여 또는 그 외의 목적으로 인하여 사용자의 개인 정보를 필요로 하는 개체이다. Data requester는 특정 사용자 정보를 보관하는 Data provider(IDMS의 IDP)의 위치 정보를 얻기 위해 discovery service를 이용한다. Data requester는 위치 정보를 이용하여 data provider에게 개인 정보를 요청한다. Data provider는 정보 요청에 대한 판단을 내리기 위해 privacy controller에게 질의한다. Privacy controller의 PDP는 질의를 분석하고 관련 프라이버시 정책을 검색하여 판단을 내린 후, data provider에게 결과 메시지를 전송



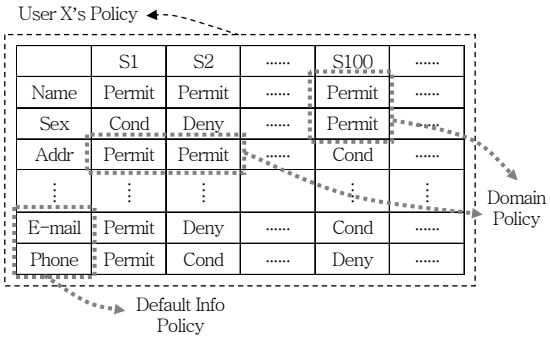
(그림 7) IDMS의 데이터 공유와 프라이버시 제어

한다. 결과는 허가, 거부, 질의로 나뉜다. 결과가 허가이면, data provider는 data requester에게 개인 정보와 정보 사용에 대한 의무 사항(obligation)을 함께 전달하고, 결과가 금지이면 정보 제공이 거부되었다는 메시지를 전달한다. 결과가 질의이면 정보 소유자의 동의를 구하기 위해 data provider는 principal(정보 실소유자)에게 정보 제공에 대해 질의한다. Privacy controller의 PAP는 프라이버시 정책을 생성하고 관리하는 개체이다. Privacy controller는 프라이버시 정책을 소유자 정책(owner policy)과 관리 정책(management policy)으로 구분하여 관리한다[15].

나. Privacy Controller의 프라이버시 정책 표현

직관적으로 개인 정보의 모든 권한은 소유자에게 있으므로 정보의 유통은 소유자의 의지에 따라야 한다. 그러나 실제로 인터넷을 사용하며 스스로 자신의 정보를 관리하기란 결코 용이하지 않다. Privacy controller는 일반 사용자들이 쉽게 사용할 수 있는 인터페이스를 제공한다. 그러나 자신의 정보를 직접 관리하지 않거나 어려워하는 사용자들을 위한 다른 관리 방법이 필요하다. 이를 위해 본 논문에서는 관리 정책을 사용한다[15].

Privacy controller에서 개인 정보를 제어하는 정책은 소유자 정책(user policy), 관리 정책(프라이버시 도메인 정책, domain policy), 기본 정보 제공



(그림 8) Subject-Resource Matrix

정책(default info policy)으로 구분된다. 소유자 정책은 정보의 실소유자가 직접 설정하는 정책으로, 사용자들의 수준에 따라 정책을 설정할 수 있도록 여러 단계로 구성되어 있다. 관리 정책은 사용자 정보의 안전을 위해 관리자가 프라이버시 정책을 생성한다. 편의성에 우선을 두는 사용자 정책 인터페이스와는 달리 정책을 세밀하게 생성할 수 있다.

인터넷의 어떤 사이트들은 사용자 가입절차 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 방식을 처리하기 위해 privacy controller에는 기본 정보 제공 정책이 있다.

(그림 8)은 사용자 정책, 도메인 정책, 기본 정보 제공 정책의 영역을 표현하고 있다. S-R matrix는 정보 사용의 주체와 자원으로 이루어진 논리적인 이차원 배열이다. 배열의 셀은 하나의 자원 항목에 대해 특정 주체의 접근에 대한 결정이다. 행위 또는 조건 등으로 인해 하나의 셀은 여러 개의 결과를 가질 수 있다.

사용자 정책은 임의의 개인 정보 필드에 대해 임의의 주체에 대한 개별적인 결정을 가질 수 있다. 예를 들어, 사용자 x의 우편 번호에 대하여 주체 S1에게는 허가하고 S2에게는 금지한다. 사용자는 자신의 모든 정보 필드에 관해서 모든 주체의 접근을 제어해야 한다. 다시 말해, 한 사용자의 S-R matrix의

모든 셀에 대한 정책을 표현하여야 한다. Privacy controller는 사용자가 모든 셀에 대한 정책을 간편하게 또는 정밀하게 생성할 수 있는 인터페이스를 제공한다.

도메인 정책은 특정 사용자 정보에 대한 접근보다는 전체 사용자 정보에 대한 접근을 제어한다. 그리고 모든 주체 및 모든 자원에 대해 정책을 생성할 수 있고 생성하지 않을 수도 있다. (그림 8)에서는 도메인 정책을 S-R matrix의 일부분에 대해서만 정의하고 있다. 주소 필드에 대해서 주체 S1, S2에 대해 허가한다. 이름과 성별 필드에 대해 주체 S100에게 허가한다.

기본 정보 제공 정책은 특정 정보 필드에 대해 접근을 허가하는 정책이다. 그러므로 기본 정보 제공 정책은 정보 필드 리스트로 구성되어 있다. (그림 8)의 기본 정보 제공 정책에 따르면 전자 우편과 전화번호에 대해 모든 주체가 접근할 수 있다.

다. Privacy Controller의 정책 판단

Privacy controller는 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 8)에서 주체 S2가 전자 우편에 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. 이런 경우를 처리하기 위해 privacy controller에는 정책 충돌 해결 정책이 있다[15].

정책 충돌 해결 정책은 두 가지 방식 중 하나를 선택하게 되어 있다. 첫번째 방식은 정책의 우선 순위를 두어 처리하는 방법이다. 우선 순위가 높은 정책에서 결정이 나면 그 외의 정책에 대해서는 판단하지 않는다. 두번째 방식은 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 선택된다. 불능은 요청 메시지와 관련된 정책이 없는 경우를 표현하고 불확정은 privacy controller 또는 네트워크 오류이거나, 요청 메시지 또는 정책 내에서 문법적 오류가 있는 경우를 의미한다.

라. Privacy Controller의 인터페이스

Privacy controller에서 도메인 정책, 기본 정보 제공 정책, 정책 충돌 해결 정책은 관리자가 설정하는 정책이므로, 다양한 정책 생성을 구성할 수 있도록 인터페이스가 구성되어 있다. 이에 반해 사용자 정책은 일반 웹 사용자가 편리하게 정책을 생성할 수 있도록 되어 있다. 이를 위해 “기본 수준”, “SP 그룹별 기본 수준”, “정보 항목별 지정”, “SP 그룹별 지정”, “상세 지정”, 이렇게 다섯 가지 방법을 지원한다.

“기본 수준”은 사용자가 “아주 높음”, “높음”, “보통”, “낮음” 등 네 가지 레벨만을 단순히 선택하게 하는 방법이다. 네 가지 레벨은 privacy controller가 미리 생성해 놓은 정책이다. 사용자가 정책을 생성하는 창 옆에 각 레벨에 대해 자세한 설명이 되어 있으며, 생성된 정책은 “상세 지정” 부분에서 확인할 수 있다. 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. (그림 9)는 “SP 그룹별 기본 수준”을 보여준다. SP 그룹은 정보를 사용하려는 SP를 네 단계로 구분한 것이다. 절대 신뢰 그룹은 일반적으로 국가 기관을 의미하고, 신뢰 그룹은 은행, 카드회사 또는 포털과 같은 회사를 말한다. 일반 그룹은 쇼핑몰 등을 의미하며, 비가입 그룹은 privacy controller에 등록되지 않은 사이트를 의미한다.

“정보 항목별 지정”은 각 자원 필드에 대해 “허용”, “금지”, “질의” 등을 선택하게 하는 방법이다.

(그림 9) SP 그룹별 기본 수준

(그림 10) SP 그룹별 지정

"SP 그룹별 지정"은 각 자원 필드에 대해 신뢰 그룹에 대한 정책을 생성하는 방법이다. (그림 10)은 "SP 그룹별 지정"을 보여준다.

상기 네 가지 방법으로 생성된 정책이 각각의 주체와 자원 필드에 대해서 어떻게 정책이 설정되었는지 확인하려면 "상세 지정" 부분을 선택하면 된다. "상세 지정"은 S-R matrix와 같은 모습으로 구성되어 있다[14].

4. 비교

본 절에서는 앞에서 설명한 기술을 비교 설명한다. <표 3>은 각 기술의 특징을 간단하게 보여준다.

익스플로러에서 제공하는 개인정보 정책은 단순하게 되어 있다. 제공되는 기본 설정 방법 또는 고급 설정으로는 고급 사용자가 원하는 프라이버시 정책을 생성하기에는 다소 문제를 안고 있다. 하지만, 쿠키가 무엇인지 알지 못하는 사용자가 대부분인 웹 환경에서 정책 설정의 단순함은 최고의 선택일 수도 있다. 현재, 대부분의 인터넷 사용자들이 알게 모르게 가장 많이 사용하고 있는 시스템이다. 한편, 개인정보 기능을 이용하여 쿠키 설정을 다르게 지정하면 웹사이트가 제공하는 서비스를 이용하지 못하는 경우가 있다. 이로 인해 대부분의 사용자는 설정을 '보통'으로 지정하고 사용한다.

Privacy bird는 익스플로러 보다 다양한 정책 생성이 가능하다. 익스플로러는 사용자가 잘 알지 못하는 불만족 쿠키라는 이미 정해진 항목에 대해서만 단계를 지정할 수 있지만, privacy bird는 데이터의 종류를 네 가지로 구분하고 이에 따라 쿠키 사용 여부를 지정할 수 있다. 그리고, 사용자가 생성한 정책과 사이트의 P3P 정책을 비교하여 그 결과를 시각적으로 보여주는 기능이 있다. 또한, 해당 사이트의 P3P 정책을 사용자가 읽기 편하도록 정리해서 보여주는 policy summary 기능이 있다.

ETRI IDMS의 privacy controller는 identity 관리 시스템 환경에서 개인정보보호 기술이다. 상기 두 방법과는 다르게 IDMS 환경이 구축되어야만 사용할 수 있다는 제약을 안고 있다. 그러나, 사용자가 자신의 정보를 제어하기에 보다 능동적이고 상대적으로 많은 편의성을 제공하고 있다. 그리고, 프라이

〈표 3〉 정책 기반 개인정보보호 기술 비교

기술	인터넷 익스플로러	Privacy Bird	Privacy Controller
목적	- 웹 브라우저 쿠키 제어	- 웹 브라우저 쿠키 제어 - 사이트 P3P 정책 알림	- Identity 관리 시스템에서 정보 유통 제어
사용 표준	- P3P - Microsoft 자체 정책	- P3P - APPEL	- XACML
환경	- 웹 환경	- 웹 환경	- 웹 환경의 Identity 관리 시스템
사용자 인터페이스	- 단순함 - 기본 6단계로 지정 - 쿠키마다 직접 사용자 선택	- 단순함 - 기본 3단계로 지정 - 데이터 종류별 정책 생성	- 다양함 - 5가지의 정책 생성 방법 - 정보 유통시 직접 사용자 제어 가능

버시에 관심이 없는 사용자들을 위하여 도메인 정책을 제공하고 있다.

Ⅳ. 결론

본 논문에서는 프라이버시 기술 분류를 살펴보았고, 정책 기반 프라이버시 기술인 P3P, EPAL, XACML을 설명하였다. 또한 이를 활용한 마이크로소프트 인터넷 익스플로러의 P3P 기능과 AT&T의 privacy bird, 그리고 XACML을 이용한 ETRI IDMS의 privacy controller에 대하여 자세히 기술하였다.

인터넷 사용자가 자신의 개인정보를 보호하기 위한 제품들은 여러 가지 존재하고 있다. 그리고 이러한 기술들을 이용하여 개인 정보 수집을 최소화하거나 어느 정도 프라이버시에 대한 위협을 줄일 수 있다. 이러한 면에서 P3P, EPAL, XACML 등의 기술은 개인정보를 보호하는 데 중요한 위치를 차지할 수 있을 것이다.

약 어 정 리

AAA Authentication, Authorization, Audit/Account
APPEL A P3P Preference Exchange Language
EPAL Enterprise Privacy Authorization Language
ID-FF IDentity Federation Framework
ID-SIS IDentity Service Interface Specifications
ID-WSF IDentity Web Service Framework
IDP IDentity Provider
LDAP Lightweight Directory Access Protocol
P3P Platform for Privacy Preferences
PAP Policy Administration Point
PDP Policy Decision Point
PGP Pretty Good Privacy
S-R Matrix Subject-Resource Matrix
SP Service Provider
W3C World Wide Web Consortium
XACML eXtensible Authorization Control Markup Language

● 용 어 해 설 ●

프라이버시: 프라이버시라는 용어는 주관적이고 가변적이며 포괄적인 성격을 가지고 있다. 1890년 Warren은 논문에서 "혼자 있을 권리(right to be let alone)"라는 개념을 주장하였으나, 정보 사회가 진행되며 프라이버시 개념은 보다 적극적인 개념인 "자기 정보 통제권(self-control on personal)"으로 바뀌었다.

참 고 문 헌

[1] A. Rezgui, A. Bouguettaya, and M.Y. Eltoweissy, "Privacy on the Web: Facts, Challenges, and Solutions," *IEEE Security & Privacy*, Vol.1, 2003.

[2] W3C, "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification," 2006.

[3] W3C, "A P3P Preference Exchange Language 1.0 (APPEL1.0)," 2002.

[4] W3C, "The Enterprise Privacy Authorization Language(EPAL 1.2)," 2002.

[5] OASIS, eXtensible Access Control Markup Language (XACML) Version 2.0, Committee Draft 04, 2004.

[6] MSDN, "Privacy in Internet Explorer 6."

[7] L.F. Cranor, P. Guduru, and M. Arjula, "User Interfaces for Privacy Agents," *ACM Transactions on Coumputer-Human Interaction*, Vol.13, 2006.

[8] L.F. Cranor, M. Arjula, and P. Guduru, "Use of P3P User Agent by Early Adopters," *Proc. 2002 ACM Workshop on Privacy*, 2002.

[9] 김승현, 진승헌, 정교일, "인터넷 ID 관리 서비스 기술 동향," 주간기술동향, 2004.

[10] Liberty Alliance Project, Privacy and Security Best Practices, Nov. 2003.

[11] Liberty Alliance Project, Liberty ID-FF Architecture Overview, Nov. 2003.

[12] Liberty Alliance Project, Liberty ID-WSF Web Services Framework Overview, 2003.

[13] Liberty Alliance Project, Liberty ID-SIS Personal Profile Service Specification, 2003.

[14] OASIS, Assertion and Protocols for the OASIS Security Assertion Markup Language(SAML) V2.0, 2005.

[15] 노종혁, 진승헌, 이균하, "인터넷 Identity 관리 시스템을 위한 프라이버시 인가," 한국통신학회논문지, 제 30권, 2005.