개인정보보호기술에 관한 연구

박익수*, 양진희*, 서재현*, 오병균*
*목포대학교 정보보호학과
e-mail:{upark ispecter jhseo obk}@mokpo.ac.kr

A Study on Privacy Enhancing Technologies

Ik-Su Park* Jin-Hee Yang* Jea-Hyun Seo* Byeong-Kyun Oh*
*Dept of Information Security, Mokpo National University

요 약

일반적으로 사용자 ID는 인터넷의 여러 사이트에 분산, 중복 저장되어 있으며, 사용자 ID의 증가와 관리의 불편함, 개인정보 유출로 인한 프라이버시 문제가 발생하고 있다. 최근 개인정보보호를 위한 기술로 ID관리시스템 개발이 진행되고 있다. ID관리시스템은 웹 사이트에 한번 회원 등록 후, 하나의 ID로 한번의 로그인을 통해 모든 사이트의 서비스들을 이용할 수 있도록 해주는 역할이 가능하다. 본 논문에서는 ID관리시스템의 개념과 기술 동향에 관하여 살펴본다.

1. 서론

ID(Identity)는 인터넷 환경에서 사용자가 인터넷 사이트에 로그인하는 과정에서 사용하는 개인 식별자를 의미한다. ID정보란 개인을 식별하는 ID를 비롯해 신상정보와 같은 개인정보를 포괄한 개념이다. 인터넷 이용자가 회원 인증을 요구하는 웹 사이트에 접속하기 위해서는 반복되는 등록 절차를 수행한다. 사용자의 개인 정보를 포함하여 개인 신원 확인 정보 등이 가입된 사이트에 그대로 남아 있어 개인정보의 도용이나 프라이버시 침해 등의 심각한 문제를 야기 할 수 있다. 또한 회원가입 시 사용되는 ID는 개인이 보유하는 개수가 많아져서 기억하기 어렵게 되고, 여러 개의 웹 사이트를 방문하는 것이 일반적인 상황에서 매 사이트마다 로그인하는 것은 매우 불편한 일이다. 최근 한번의 등록 후, 하나의 ID와 PW로 한번의 로그인을 통해 모든 사이트의 서비스들을 이용할 수 있도록 해주는 ID관리시스템이 소개되었다[1].

ID관리는 ID관련 모든 정보를 단일 시스템 저장하는 중앙 집중형과 개인정보가 인터넷에 연결된 ID 관리시스템에 분산 저장되어 있고 서로 연동할 수 있는 사용자 중심의 ID관리가 있다[2]. 본 논문에서는 개인정보보호를 위한 ID관리기술에 관하여 소개한다.

2. ID 관리 시스템

최근 인터넷 이용의 증가에 따라 활용 분야는 전자상거래를 시작으로 하여 전자무역, 전자정부, 전자국방, 전자의료 등과 같이 공공과 민간영역을 구분하지 않고 급격히 확산되고 있다. 이러한 인터넷상에서 다양한 응용 서비스를 이용하기 위해서는 ID와 패스워드를 등록하고 주소, 전화 번호 등의 신상정보를 입력하는 절차를 통해 웹 사이트에 가입하게 된다. 이와 같은 ID를 안전하게 이용할 수 있도록 보호하고 관리하는 기술을 ID 관리 시스템이라 한다. ID관리시스템은 단일인증서비스(SSO), 개인정보 소유자가 설정한 프라이버시 정책에 의한 개인정보 공유, 분산 저장된 ID에 대한 일관성 있는 관리 기능을 수행한다.

ID관리란 사이버스페이스 상에서 개인 식별을 가능하게 함으로 각종 ID와 개인정보를 포함한다. 이러한 ID를 안전하게 이용할 수 있도록 보호하고 관

리하는 기술을 ID관리(Identity Management)라고 한다. ID관리는 ID의 생성에서 전파, 관리 및 소멸까지의 생명주기를 관리하는 프로세스와 ID관리를 위한 인증. 인가, 접근제어와 감사를 위한 기반구조를 포함한다.

2.1 SSO(Single Sing-On)

SSO는 한 번의 로그인을 통해 모든 서버에 접속할 수 있는 권한을 갖게 되는 개념으로 여러 웹 서비스를 이용하는데 하나의 서비스만 로그인을 하면 다른 서비스에는 로그인할 필요가 없이 바로 서비스 이용이 가능하도록 한다[3]. SSO 시스템은 SSO 대상 애플리케이션에서 사용되는 사용자 인증 방법을 별도의 SSO 에이전트가 대행해주는 인증 대행(Delegation)방식과 SSO 시스템과 신뢰관계를 토대로 사용자를 인증한 사실을 전달받아 SSO를 구현하는 인증정보 전달(Propagation)방식으로 구분된다.

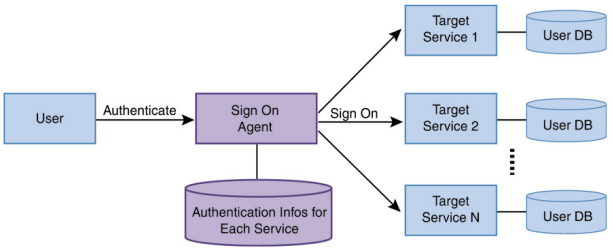

그림 1 Delegation model기본 개념

▪ Delegation model은 대상 애플리케이션의 인증 방식을 전혀 변경하지 않고, 사용자의 대상 애플리케이션 인증 정보를 에이전트가 관리해 사용자 대신 로그온 해주는 방식이다. 그림1은 SSO Delegation model이다.

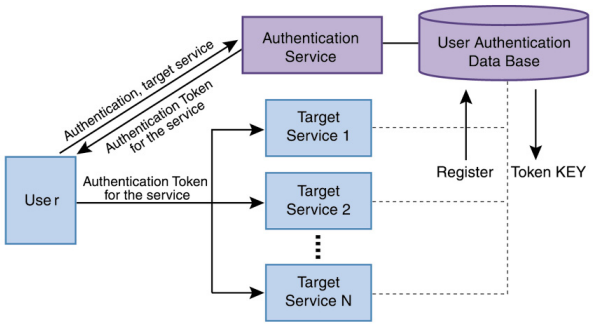

그림 2 Propagation mode

▪ Propagation model은 대상 애플리케이션에 사용자가 접근할 때 토큰을 자동으로 전달해 대상 애플리케이션이 사용자를 확인할 수 있도록 하는 방식이다. 웹 환경에서는 쿠키(cookie)라는 기술을 이용해 토큰을 자동으로 대상 애플리케이션에 전달할 수 있다.

현재 ID 관리 시스템에서 SSO 기술은 Microsoft의 passport 서비스와 Liberty Alliance의 Liberty가 있으며, 최대선[3]등은 개별 사이트에서의 Static한 관계 관리를 위하여 공인 IDO 구조를 제안하기 하였다.

2.2 ID Federation

ID Federation은 계정을 시스템, 네트워크, 도메인 간에 안전하고 신뢰기반으로 확장해서 사용할 수 있도록 해주는 비즈니스 및 기술적 행위들의 조합을 말하며, 사용자 편의성 증대 고객의 계정 관리에 대한 부담을 감소, 계정 정보들의 중복 제거, 비즈니스 민첩성 확보 및 확장 등의 장점이 있다. 관련 표준으로 SAML, Liberty ID-FF, Shibboleth Liberty ID-WSF 등이 있다[2].

2.3 Permission-Based Attribute Sharing

인터넷상의 온라인 상거래가 늘어나면서 민간 사업자에 의한 개인정보 수집, 악의적인 해킹 등으로 개인정보가 누출되어 스팸 메일, 스팸 문자 등의 피해가 발생하고 있다. 이에 대한 대책으로 ID 관리 솔루션이 제안되고 있다. PBAS는 SP의 개인정보 열람과 이에 대한 통제를 위해서 개인정보 통제 정책 수립과 이를 통한 개인정보 접근 제어 기술이 필요하다[3].

2.4. ID관리 환경

▪ 기업에 속한 ID 관리 환경

Company-controlled identity는 기업이 개인에게 ID를 부여한 뒤 개인이 어떤 ID를 관리하고 고유할 것인가를 결정한다. Liberty Alliance 표준에 기반 ID 관리 시스템이 대표적이다[3].

▪ 사용자가 생성한 ID 관리 환경

User-controlled identity는 ID 제공자(IdP), 개인정보, Id 사용 정책을 개인이 통제하는 시스템으로 기업에 속한 ID가 아니라 사용자 스스로 ID를 생성하고 관리하는 것이 특징이다. 대표적인 user-controlled identity로는 URL을 ID로 사용하는 OpenID 등이 있다[3]

3. ID 관리 환경에서 개인 정보보호 기술 동향

ID 관리 기술에서 요구되는 대표적인 보안기술은 인증(Authentication), 인가(Authorization), 프라이버시(Privacy)보호 기술 등이 요구 된다[4].

3.1 Passport

패스포트는 MS사가 개발한 단일 로그인 서비스이다. 패스포트는 중앙 집중적으로 관리되는 사용자 계정이다. 중앙 집중적 사용자 계정관리 때문에 사생활 보호 정책을 강화와 사용자가 동의하지 않은 정보 수집과 이용을 배제하고 사용자 중심의 관리 정책을 추가를 위해 분산되고 연방적인 모델을 연구 중에 있다.

3.2 OpenID

OpenID는 OpenID의 서버 이외에 응용 설치와 부가적인 디지털 ID 요청 없이 온라인상에서 기존의 웹 브라우저만을 이용해 개인에 대한 인증기능을 수행한다[4]. 그림3은 OpenID의 동작 절차를 보인다. 그러나 OpenID은 피싱 공격에 노출될 수 있다는 문제점이 있다[3].

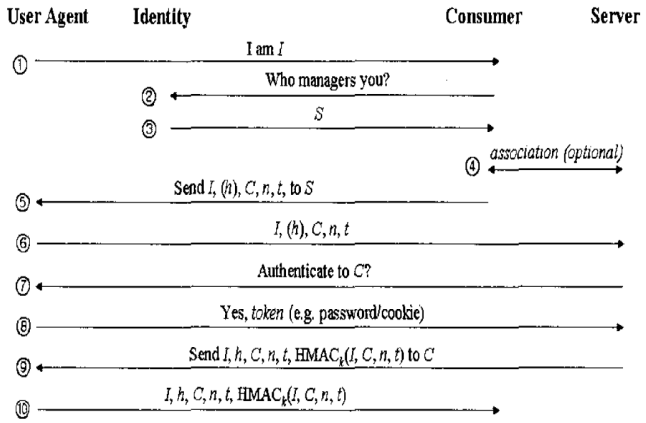

그림 3 OpenID[4]

3.3 Daum Sign 서비스

국내에서도 인터넷 ID관리 서비스가 시작되고 있다. 이중 포털 사이트인 Daum에서 제공하는 Daum Sign 서비스는 Daum의 기존 id를 이용해 로그인하면 가맹사이트에서 추가 로그인 없이 사용할 수 있는 SSO 서비스이다. 그러나 사용자의 개인정보를 가맹사이트에 제공할 때 사용자의 동의나 통제 기능을 추가해야 된다.

그림 4 Daum Sign

4.결론 및 향후 연구 과제

본 논문에서는 ID관리 개념과 기술동향을 살펴보았다. 현재 OpenID을 도입하여 개인 블러그 등 실환경에 도입이 시작된 단계이며, ID관리 환경에서 개인정보의 안전한 분산 저장관리를 위한 기술이 필요하다. 비밀분산 방식은 향후 유비쿼터스 사회에서의 개인정보보호를 위해 개인정보의 분산 저장관리를 가능하게 하는 기술로서 사용될 것이다.

참고문헌

[1] 최대선, 김태성, 진승헌, “공인 Web SSO 도입 방안에 대한 연구,” 한국정보과학회 2003 춘계학술대회 VOL, 30 NO.01, 2003. 04

[2] 조영섭, 진승헌, “Digital Identity 관리 기술 현황 및 전망,” 전자통신동향분석 제22권 제1호, 2007년 2월.

[3] 최대선, 진승헌, 정교일, “인터넷 ID 관리 서비스,” 전자통신동향분석.

[4] 문홍서, 최향창, 이형효, 노봉남, “SAML 기반 싱글 사인-온 환경에서의 프라이버시 보호 기법에 관한 연구,” 한국정보처리학회 추계학술대회 논문집 제11권 제2호, 2004. 11.

[5] 진승헌 “인터넷 서비스 환경이 고도화와 디지털 ID 관리 기술” www. dbguide.net

[6] 남기효 “개인정보보호 기술 동향: P3P” kidbs.itfine.or.kr

[7] 남택용, 장종수, 손승원 “개인정보보호를 위한 기술적 요구사항,” 정보통신연구진흥원 주간기술동향 통권1224호, 2005.11.