사용자 중심 ID 관리 기법을 이용한 OpenID 시스템의 설계

정의경, 윤철용, 김현철, 전문석
숭실대학교 컴퓨터학과
e-mail:{sooho1004, yfemir, dmzpolice, mjun}@ssu.ac.kr

A Design of OpenID System Using ID Management Method User-Centric

Eui-Kyeong Jeong, Cheol-Yong Yun, Hyun-Chul Kim, Moon-Seog Jun
Computer Communication Lab, Graduate School of SoongSil University

요 약

인터넷의 확산과 웹 2.0 서비스의 등장은 기존 서비스 제공자 중심의 ID 관리를 사용자 중심의 ID 관리 형태로 변화시키는 계기가 되었다. 그러나 기존 사용자 중심 ID 관리 기법은 사용자 인증 및 정보 관리에 대한 문제가 존재한다. 본 논문에서는 서비스 제공자가 필요로 하는 정보만을 사용자가 선별적으로 선택하여 제공함으로서 기존 ID 관리 기법의 문제를 해결할 수 있는 사용자 중심의 ID 관리 기법을 이용한 OpenID 시스템을 제안한다. 또한, 실험 및 비교분석을 통하여 보안성 및 효율성 측면에서 우수함을 확인 할 수 있었다.

1. 서론

인터넷의 확산과 웹 2.0의 도래는 사용자에게 여러 형태의 웹 서비스를 제공하는 계기가 되었다. 이러한 웹 서비스를 이용하기 위해서 사용자는 각각의 서비스 제공자에게 자신의 정보를 제공한 후 아이디와 패스워드를 부여받아 서비스를 이용하여야한다[1].

위와 같은 환경하에서 웹 서비스를 이용하기 위해서는 사용자는 매번 로그인을 해야 하는 불편함과 여러 사이트에 산재되어 있는 자신의 정보에 대한 분실과 유출의 대한 위험을 감수해야 한다. 또한, 서비스 제공자 입장에서도 관리부실 또는 해킹 등에 의한 개인 정보 유출 문제가 발생할 수 있다. 이러한 Silo ID관리 모델의 문제를 해결하기 위한 방안으로 하나의 아이디로 모든 서비스를 이용할 수 있는 SSO(Single-Sign-On) 방식의 ID 관리 모델이 제기되었다[2]. 그러나 이 방법 또한 사용자 정보의 대한 관리 주체가 사용자가 아닌 서비스 제공자라는 점에서 관리의 문제가 존재한다.

OpenID 시스템은 오픈 소스 기반에 사용자 중심 ID 관리 분산 시스템으로 서비스 제공 사이트에 사용자의 아이디와 패스워드를 입력할 필요 없이 ID로 사용되는 URL을 입력하여 OpenID 시스템의 서버를 통해 사용자를 인증함으로써 기존 SSO 방법의 문제를 해결한다[3]. 그러나 OpenID시스템은 사용자의 아이디와 패스워드만을 관리하기 때문에 서비스 제공자가 필요로 하는 사용자 정보를 효과적으로 제공 할 수 없으며 정보 전송에 있어서 사용자를 인증하는 방법이 취약하다.

본 논문에서는 기존 OpenID 시스템에 인증 시스템을 추가하여 사용자 인증을 강화하며 서비스 제공자가 원하는 특정 정보를 사용자가 선별적으로 선택하고 암호화하여 전송함으로서 효율성과 안정성을 보장할 수 있는 사용자 중심의 ID 관리 기법을 이용한 OpenID 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 제 2절에서는 관련연구로 기존의 OpenID 시스템의 구성, 회원가입, 동작에 대하여 기술한다. 제 3절에서는 본 논문에서 제안하는 시스템에 대하여 기술한다. 제 4절에서 본 논문에서 제안하는 OpenID 시스템과 기존 시스템과의 비교 분석 결과를 제시하고 마지막으로 5절에서 결론과 향후 연구 방향에 대하여 제시하였다.

2. 관련연구

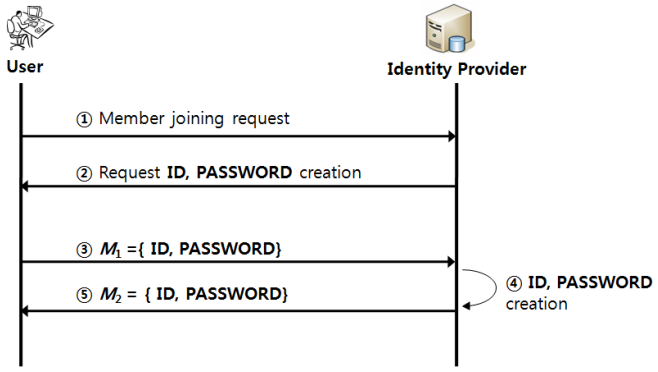
2.1 OpenID

OpenID는 하나의 아이디로 여러 서비스 제공자 사이트에 접속하여 서비스를 제공 받을 수 있는 사용자 중심의 ID 관리 시스템으로 오픈 소스 기반에 분산 시스템이다. 이러한 OpenID 시스템은 아이디 발급 및 인증을 제공하는 IDP(Identity Provider)와 실제적인 서비스를 제공하는 RP(Relying Party) 그리고 제공되는 서비스를 이용하는 사용자로 구성된다.

OpenID는 공개된 S/W를 사용하여 누구나 IDP를 구축할 수 있으며 사용자는 서비스 제공 사이트에 가입한 IDP의 OpenID URL을 입력하여 인증을 받을 수가 있다[4].

2.1.1 OpenID 회원가입

OpenID 회원가입은 (그림 1)과 같은 순서를 가진다. (그림 1)에서와 같이 사용자는 자신이 신뢰하는 IDP를 선택하여 회원가입을 한 후 서비스를 이용하면 된다. 회원가입 시 IDP는 사용자가 사용할 아이디, 패스워드, e-mail 등을 저장하고 사용자에게 URL형태의 OpenID를 부여한다.



(그림 1) OpenID 회원가입 절차

① User는 IDP에게 회원가입을 요청한다.

② IDP는 User에게 앞으로 사용할 ID, PASSWORD의 입력을 요청한다.

③ User는 IDP에게 사용할 ID와 PASSWORD를 담고 있는 메시지 M_1을 전송한다.

$$M_1 = \{ID, PASSWORD\}$$

④ IDP는 사용자의 ID와 PASSWORD를 생성한다.

⑤ IDP는 생성한 사용자 ID와 PASSWORD 메시지 M_2를 사용자에게 전송한다.

$$M_2 = \{ID, PASSWORD\}$$

2.1.2 OpenID 동작 과정

(그림 2)의 OpenID 수행 과정에서와 같이 사용자는 서비스 제공자에게 서비스 제공을 요청한 후 IDP를 통해 인증이 완료된 후에 서비스를 이용할 수 있다. 이 과정에서 서비스 제공자는 사용자의 ID 즉 URL 주소만을 획득하며 자신이 필요로 하는 어떠한 정보도 획득 할 수 없다. 다음은 (그림 2)의 각 절차를 보여주고 있다[5].

① User는 서비스 제공자에게 자신의 ID를 전송하고 Service를 요청한다.

② RP는 User에게 어떠한 IDP에 가입되어 있는지를 확인한다.

③ User는 자신이 가입되어 있는 IDP 식별자를 RP에게 전송한다.

④ RP는 사용자가 전송해 준 IDP 식별자를 통해 해당 IDP와 연결 설정을 수립한다.

⑤ RP는 User를 통해 IDP에게 인증 요청 메시지 *ARM*을 전송한다. *ARM*은 User ID값 ID, 서비스 제공자 식별자 RP, IDP와 RP의 연결 설정 식별자 n, 타임 스탬프 t, IDP와 RP의 세션 식별자 s를 포함한다.

$$ARM = \{ID, RP, n, t, s\}$$

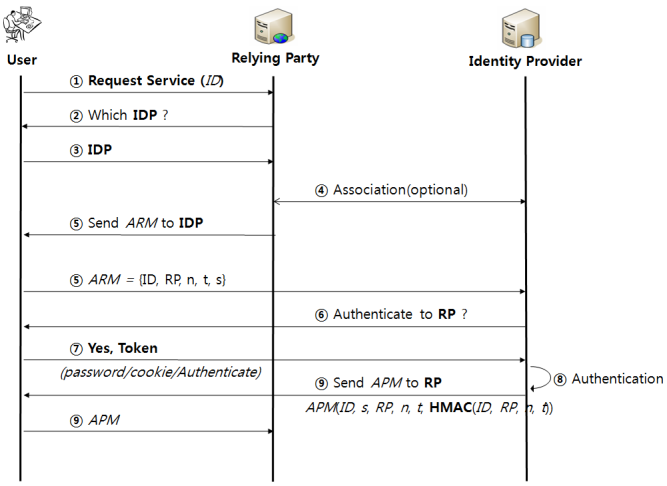
⑥ IDP는 User에게 RP를 인증할 것인지 요청한다.

⑦ User는 인증을 승인하고 인증 정보를 닮을 Token을 생성한다. 해당 토큰에는 사용자의 *password*, 해당 사이트의 주소를 가지고 있는 *cookie*, 인증 값 *Authenticate*를 포함한다.

⑧ IDP는 User를 인증한다.

⑨ IDP는 User를 통해 RP에게 인증 허가 메시지 *APM*을 전송한다.

$$APM = \{ID, s, RP, n, t, HMAC(ID, RP, n, t)\}$$



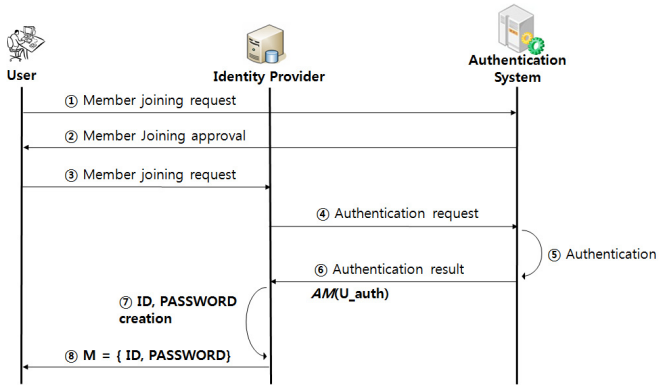
(그림 2) OpenID 동작 절차

3. 제안하는 시스템

3.1 제안하는 시스템의 OpenID 회원가입

기존의 OpenID 시스템에서 IDP는 사용자의 아이디, 패스워드, e-mail등의 정보만을 저장하였다. 그러나 사용자입장에서 RP의 서비스를 이용하기 위해서는 RP에서 별도로 요구하는 회원가입 절차나 정보를 제공해야 되며, 이 과정에서 사용자는 자신이 원하지 않는 신상, 비 신상 정보를 서비스 제공자에게 제공해야 한다.

본 논문에서는 기존 OpenID 시스템과 달리 회원 가입 단계에 인증 과정을 추가적으로 수행한다. 즉 기존에 OpenID 시스템은 인증 과정 없이 누구나 가입 할 수 있었던 반면에 본 논문에서 제안하는 시스템은 (그림 3)과 같이 인증된 사용자에게만 ID를 부여하고자 한다.



(그림 3) 제안한 OpenID 회원가입 절차

① User는 인증 시스템(AS)에 회원 가입을 요청한다.

② AS는 회원 가입을 수행하고 User에게 그 결과를 통보한다.

③ User는 IDP에게 ID 및 PASSWORD 발급을 요청한다.

④ IDP는 해당 User에 대한 유효성 검증을 AS에 요청한다.

⑤ AS는 해당 요청에 대한 검증을 수행한다.

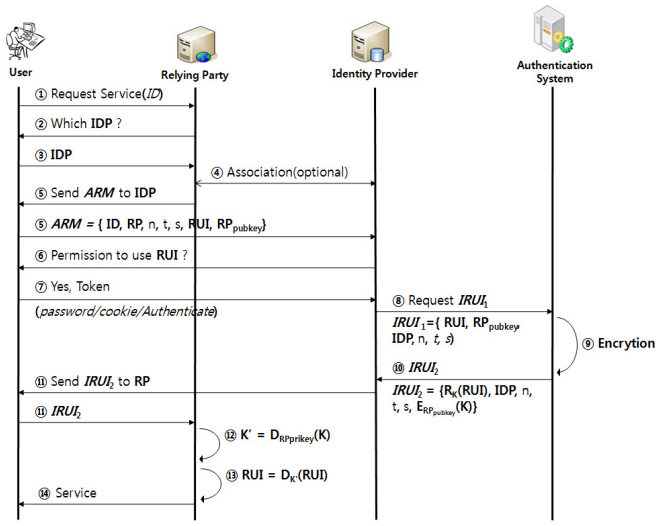
⑥ AS은 IDP에게 인증 결과 값 *AM*을 전송한다.

⑦ IDP는 인증 결과를 확인한 후 User에 대한 ID와 PASSWORD를 생성한다.

⑧ IDP는 생성한 사용자의 ID와 PASSWORD를 User에게 전송한다.

3.2 제안하는 시스템의 OpenID 동작 과정

(그림 4)는 본 논문에서 제안하는 시스템의 동작과정을 보여주고 있다.



(그림 4) 제안한 OpenID 동작 절차

① User는 RP에게 자신의 ID를 전송하고 Service를 요청한다.

② RP는 User에게 어떠한 IDP에 가입되어 있는지를 확인한다.

③ User는 자신이 가입되어 있는 IDP 식별자를 RP에게 전송한다.

④ RP는 사용자가 전송해 준 IDP 식별자를 통해 해당 IDP와 연결 설정을 수립한다.

⑤ RP는 User를 통해 IDP에게 인증 요청 메시지 *ARM*을 전송한다. *ARM*은 User ID값 ID, 서비스 제공자 식별자 RP, IDP와 RP의 연결 설정 식별자 n, 타임 스탬프 t, IDP와 RP의 세션 식별자 s, RP가 필요로 하는 사용자 정보 RUI, RP의 공개키 RP_{Pubkey}를 포함한다.

$$ARM = \{ID, RP, n, t, s, RUI, RP_{pubkey}\}$$

⑥ IDP는 User에게 RP가 필요로 하는 User의 정보를 허가할 것인지 요청한다.

⑦ User는 인증을 승인하고 인증 정보를 닮을 Token을 생성한다. 해당 토큰에는 사용자의 *password*, 해당 사이트의 주소를 가지고 있는 *cookie*, 인증 값 *Authenticate*를 포함한다.

⑧ IDP는 AS에게 RP가 필요로 하는 User의 정보값 $IRUI_1$을 전송한다.

$$IRUI_1 = \{RUI, RP_{pubkey}, IDP, n, t, s\}$$

⑨ AS는 RP가 필요로 하는 User의 정보를 대칭키 K를 이용하여 암호화하고 사용자 정보 암호화에 사용된 대칭키 K를 RP의 공개키 RP_{Pubkey}를 이용하여 암호화한다.

⑩ AS는 IDP에게 암호화한 결과값 $IRUI_2$을 전송한다.

$$IRUI_2 = \{E_K(RUI), IDP, n, t, s, E_{RP_{pubkey}}(K)\}$$

⑪ IDP는 RP에세 $IRUI_2$을 전송한다.

⑫ RP는 RP의 개인키로 복호화하여 AS의 대칭키를 획득한다.

$$K' = D_{RP_{prikey}}(K)$$

⑬ RP는 획득한 대칭키 K'를 이용하여 사용자 정보값 RUI를 복호화하여 사용자 정보를 획득한다.

$$RUI = D_{K'}(RUI)$$

⑭ RP는 사용자에게 Service를 제공한다.

4. 비교분석

4.1 보안성 측면

기존의 OpenID는 사용자가 본인인지를 확인하는 인증 부분에서 IDP가 저장하는 정보는 아이디, 패스워드정보와 e-mail 정보만을 원하기 때문에 서비스를 이용하려는 사용자가 실제 사용자인지를 확인하는 인증이 부족하였다. 본 논문에서는 기존 OpenID 시스템에 인증 모듈을 추가하여 인증된 사용자에 한해서만 아이디와 패스워드를 제공한다. 또한, 서비스 제공자가 필요로 하는 정보에 대하여 사용자가 선별적으로 선택하여 제공함으로써 무분별한 사용자 정보에 대한 사용을 예방할 수 있다.

<표 1>은 본 논문과 기존 OpenID와의 보안성 측면에서 비교 분석 결과를 보여주고 있다. 비교 분석에서 확인할 수 있듯이 인증 시스템으로 사용자 실명확인과 인증 절차를 강화하고 사용자 정보를 인증 시스템이 소유하여 사용자정보노출의 위험도를 줄여줌으로서 제안하는 시스템의 우수함을 확인 할 수 있다.

<표 1> 보안성 비교 분석 결과

평가대상 / 평가요소	OpenID	제안하는 시스템
사용자 확인 인증	e-mail 인증	실명인증
사용자 인증 절차	IDP가 인증	AS가 인증
사용자 정보 전송	RP에 직접 전송	AS가 사용자를 통해 전송

4.2 효율성 측면

기존의 OpenID를 사용하여 서비스 제공자로부터 사용자가 서비스를 제공받기 위해서는 서비스 제공자가 필요로 하는 정보를 매번 입력해야 하는 번거로움이 있다. 그러나 본 논문에서 제안하는 시스템은 회원 가입 단계에서 인증 시스템이 확보하고 있는 사용자 정보를 가지고 인증 시스템이 필요시점마다 서비스 제공자에게 제공함으로써 기존의 번거로움을 해결할 수 있다.

<표 2>는 본 논문과 기존 OpenID와의 효율성 측면에서 비교 분석 결과를 보여주고 있다. 비교 분석에서 확인할 수 있듯이 사용자 정보 소유 주체, 사용자 정보 제공에서 제안하는 시스템의 우수함을 확인 할 수 있다.

<표 2> 효율성 비교 분석 결과

평가대상 / 평가요소	OpenID	제안하는 시스템
사용자 정보 소유 주체	없음	AS
서비스 이용 시 사용자 정보 제공	사용자가 직접 입력	사용자가 정보제공 승인여부 선택

5. 결론

본 논문에서는 기존의 OpenID 시스템과 달리 인증 시스템을 통해 검증된 사용자에게만 아이디와 패스워드를 부여함으로서 허가받지 않은 사용자의 ID 생성을 제한한다. 또한 서비스 이용 시 사용자가 원하는 정보만을 선별적으로 제공함으로서 사용자 정보의 무분별한 남용을 사전에 예방할 수 있다.

향후에는 인증시스템, IDP, RP 간 사용자 정보 전송에 있어서 사용되는 대칭키와 공개키 알고리즘을 설계 및 구현하여 사용자 정보의 보안성을 높이는 방향을 제시하고자 한다. 또한 사용자 정보에 따른 등급을 부여하여 등급별로 정보를 묶어 효율적으로 정보를 보내는 연구를 진행하고자 한다.

참고문헌

[1] 조영섭, 진승헌 "Digital Identity 관리 기술 현황 및 전망" 전자통신동향분석 제22권 제1호 2007. 2

[2] 조영섭, 진승헌 "사용자 중심 ID 관리 기능을 제공하는 전자 ID 지갑 시스템" 전자통신동향분석 제23권 제4호 2008. 8

[3] 한양대학교 산학협력단 "전자 ID 지갑 상호연동성 확보방안연구" KISA-WP-2008-0024 2008. 12

[4] http://www.OepnID.net

[5] 유재형 "다중 도메인간 SSO 실현을 위한 통합 Identity 관리 기술 분석" KNOM Review, Vol. 10, NO.1, 2007. 8

[6] 조영섭, 진승헌 "인터넷 ID 관리 시스템 개요 및 비교" 전자통신동향분석 제22권 제3호 2007. 6