OpenID에서 I-PIN을 이용한 사용자 인증 구현 및 설계

유재회*, 박찬길*, 전문석*
*숭실대학교 컴퓨터학과
e-mail:hwe100@ssu.ac.kr

Design and Implement of User Authentication using I-PIN in OpenID Service

Jae-Hwe You*, Chan-Kil Park*, Moon-Seog Jun*
*Dept of Computer Science, Soong Sil University

요 약

인터넷 서비스를 사용하기 위해서 사용자들은 이름과 주민등록번호로 실명 인증을 받은 후에 ID를 부여 받았으나, 최근 보안상 문제로 주민등록번호 대체 수단인 I-PIN 서비스를 사용하고 있다.
그리고 하나의 ID로 통합하여 인터넷 서비스를 받을 수 있는 OpenID 서비스가 국내에서도 시행중이지만 사용자 인증이 없어 악성 댓글과 스팸 등으로 악용될 수 있으며 피싱에 대한 문제점을 지적하고 있다. 본 논문에서는 OpenID에서 회원가입을 할 때 I-PIN을 사용하여 사용자 인증을 하는 기법을 제안하고 악의적인 IDP와 RP의 피싱 문제점을 보안하였다. 기존의 OpenID와 I-PIN을 적용한 OpenID를 비교분석을 통하여 보안적인 측면이 강화된 것을 확인할 수 있으며 피싱에 안전하도록 설계하였다.

1. 서론

네트워크 기술의 급격한 적전과 확산은 기존의 오프라인 시스템들을 온라인 시스템으로 전환시키는 결과를 가져왔다. 이러한 인터넷 서비스를 이용하기 위해서 사용자들은 서비스를 제공하는 각각의 사이트에 자신의 개인정보를 등록하고 ID와 Password를 부여 받아야 한다. 이러한 방법은 수많은 사이트에 개인정보를 누출하고 있는 보안 문제 뿐 아니라, 사용자들은 단 한번 접속하는 사이트일지라도 서비스를 이용하기 위해서 개인정보를 등록하고 ID와 Password를 부여받아야 하는 번거로움이 생겨났다. 또한 각 사이트의 ID와 Password를 관리하기 위해서는 대부분의 사용자들은 ID와 Password를 동일하게 하거나 메모장 같은 곳에 적어 관리하고 있다. 이러한 문제점을 해결하기 위해서 여러 사이트를 매번 가입하지 않고 하나의 ID로 사용하는 OpenID가 시행되고 있다. 하지만 OpenID는 ID와 Password만을 가지고 최소한의 인증을 하기 때문에 신뢰성과 보안에 관한 많은 문제점을 가지고 있다. 본 논문에서는 OpenID서비스에서 I-PIN을 연동한 사용자 인증 기법을 제안한다.

2. 관련연구

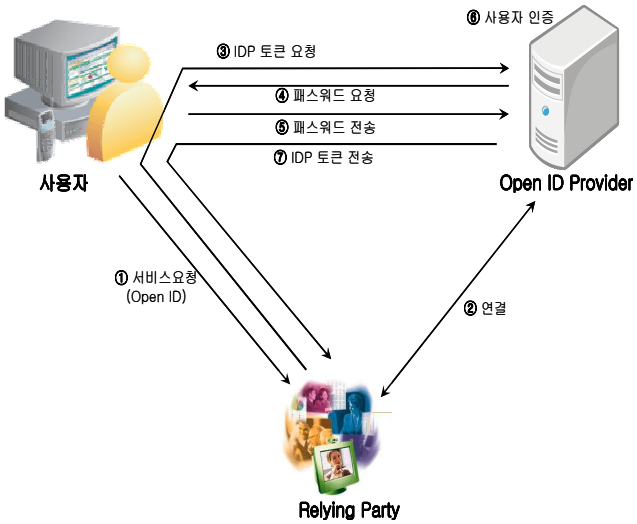
2.1 OpenID

OpenID는 사용자 중심의 새로운 ID 시스템으로 웹사이트처럼 URL 행태의 ID로 자신을 식별하게 해주는 분산형 공개 표준 기술이다[1]. OpenID 시스템은 누구든지 추가로 소요되는 비용 없이 이용할 수 있으며, 인터넷 이용자들은 자신의 온라인 ID를 관리하기 위하여 하나의 사이트에 의존할 필요가 없다. 즉, 각 사이트에서 제공하는 서비스를 이용하기 위하여 사이트마다 생년월일, 이름, 주소등과 같은 개인정보를 입력하고 ID와 Password를 부여받을 필요 없이 OpenID 협력 사이트에서 OpenID를 가지고 로그인하여 서비스를 제공받을 수 있다.

OpenID를 이용하면 이용자는 각 사이트마다 자신이 사용하던 ID와 Password를 따로 관리 하거나, 분실할 위험성이 없다. 또한 서비스를 제공하는 업체의 입장에서는 ID와 Password의 관리를 위한 비용들을 줄일 수 있으며, 사용자 인증 서비스와 SSO(Single Sign-on) 등의 아웃소싱 효과를 누릴 수도 있다[2].

2.1.1 OpenID 동작절차

OpenID는 사용자와 OpenID를 제공하는 사이트(IDP : Identity Provider), OpenID 정보를 사용하는 사이트(RP : Relying Party)로 구성되어 있으며, 동작과정은 [그림 1] 과 같다[1].



[그림 1] OpenID 동작 절차

① 사용자는 RP에게 URL형태의 OpenID를 입력 한다.
② RP는 OpenID의 URL을 확인하여 OpenID제공자인 IDP와 연결을 한다.
③ RP는 사용자를 통하여 IDP에게 사용자 인증을 요청한다.
④ IDP는 사용자 인증을 위하여 OpenID에 해당하는 Password를 요청한다.
⑤ 사용자는 IDP에게 Password를 입력한다.
⑥ IDP는 사용자가 입력받은 Password와 OpenID를 확인하여 OpenID 사용자임을 인증한다.
⑦ 인증이 완료되면 IDP는 사용자를 통하여 인증되었다는 것을 토큰 형태로 RP에게 전달한다. 인증 동작 절차가 완료되면 사용자는 OpenID를 가지고 RP에서 제공하는 서비스를 이용할 수 있다.

2.2 I-PIN

인터넷 서비스 사용자들이 증가함으로써 최근 몇 년간 개인정보가 유출 되는 사건이 빈번하게 생기고 있으며 사용자 주민등록번호가 유출 되면서 악의적인 목적으로 사용되고 있다. 2006년 정보통신부에서 개인정보보호를 목적으로 주민등록번호를 대신하여 사용자를 인증하는 인터넷 개인 식별번호인 I-PIN(Internet Personal Identification Number)을 제공하였다[4][5].

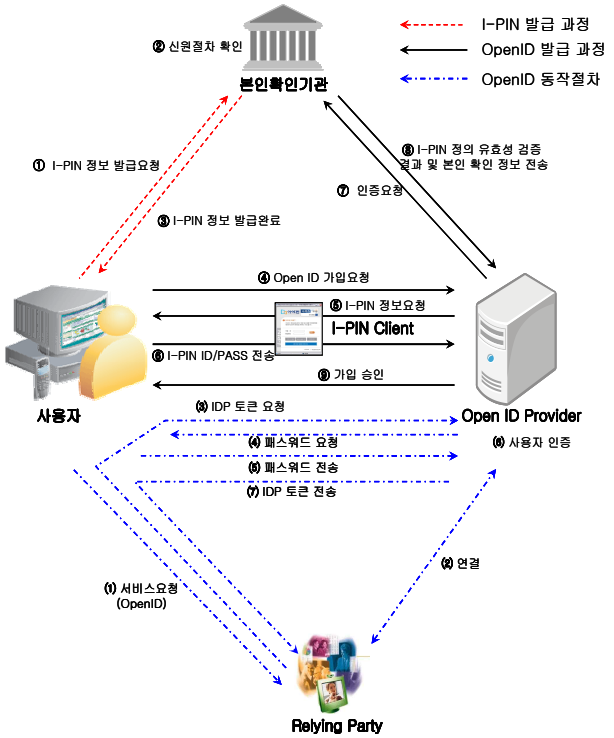
I-PIN은 온라인상에서 본인 확인을 하기 위한 하나의 수단으로, 5개 업체인 한국정보인증, 한국전자인증, 한국 신용정보, 한국 신용평가정보, 서울 신용평가정보에서 발급하고 있으며, 제3의 기관에서 개인정보를 인증하게 된다. I-PIN은 5개의 기관 중에서 한곳에서만 발급받아 사용할 수 있다. 개인정보가 외부로 노출되면 주민등록번호는 변경이 불가능하지만, I-PIN은 수시로 변경 가능하며, 인터넷 서비스 업체가 주민등록번호를 보관하지 않으므로 사용자의 정보를 안전하게 관리할 수 있게 된다[5].

2.2.1 I-PIN 가입 과정

I-PIN을 사용하여 인터넷 서비스 가입 시 주민등록번호를 입력하지 않아도 ID와 Password만으로 본인 확인을 받을 수 있다. 그러기 위해서 사용자는 I-PIN 발급기관에 접속하여 성명과 주민등록번호를 등록한 후 전송하면 본인확인기관에서는 이를 일치하는지 확인하고 추가로 공인인증서, 신용카드, 휴대폰, 대면 중 한 가지 방법으로 인증을 받는다. 신원절차 확인이 끝나면 본인확인기관에서는 사용자에게 13자리 난수 번호인 I-PIN를 발급하게 된다. 그 후, 사용자는 웹사이트에서 회원가입을 할 때 주민등록번호 대신 발급된 I-PIN의 ID와 Password를 가지고 인증을 받아 가입할 수 있고, 인터넷 서비스 업체는 입력받은 I-PIN ID와 Password를 가지고 본인확인기관에서 사용자 인증을 할 수 있다.

3. I-PIN과 OpenID 연동방향 제안

국내 OpenID 서비스를 받기 위해서 사용자는 OpenID를 제공하는 3개의 업체 중 1개를 선택하여 회원가입을 해야 한다. IDP에서 본인확인기관에 I-PIN 정보를 받음으로 사용자는 OpenID를 생성하게 되면 OpenID의 문제점인 본인 인증을 해결 할 수 있다, [그림 2]처럼 OpenID와 I-PIN을 연동 시켜 OpenID를 생성한다.



[그림 2] I-PIN을 이용한 OpenID 사용자 인증 절차

① 사용자는 본인의 성명과 주민등록번호를 가지고 본인확인기관에 I-PIN 정보를 발급 요청하게 된다.

② 본인확인기관에서 사용자의 성명과 주민등록번호와 일치한지 확인을 하고 추가로 공인인증서, 신용카드 정보, 휴대폰, 대면 중 하나의 방법으로 확인을 한다.

③ 사용자의 확인이 완료되면 본인확인기관은 사용자에게 I-PIN 정보를 발급 한다.

④ 사용자는 3개의 OpenID 업체(myid.net, idtail.com, openid.daum.net) 중 하나의 업체를 선택하여 사용자가 원하는 ID와 Password, 본인의 E-mail 주소를 입력하여 OpenID 가입요청을 한다.

⑤ OpenID Provider는 사용자 인증을 하기 위해서 사용자에게 I-PIN Client 창을 Open하여 I-PIN 정보 요청을 하게 된다.

⑥ 사용자는 Open된 I-PIN Client 창에 자신이 생성한 I-PIN ID와 Password를 입력하여 ID Provider에게 전송한다.

⑦ 사용자로부터 I-PIN 정보를 전달 받은 OpenID Provider는 본인확인기관에 사용자의 I-PIN 정보가 맞는지 확인을 요청한다.

⑧ 본인확인기관은 사용자의 I-PIN 정보의 유효성 검증을 하게 되고 결과 및 본인 확인 정보를 OpenID Provider에게 전송하여 사용자 인증을 해준다.

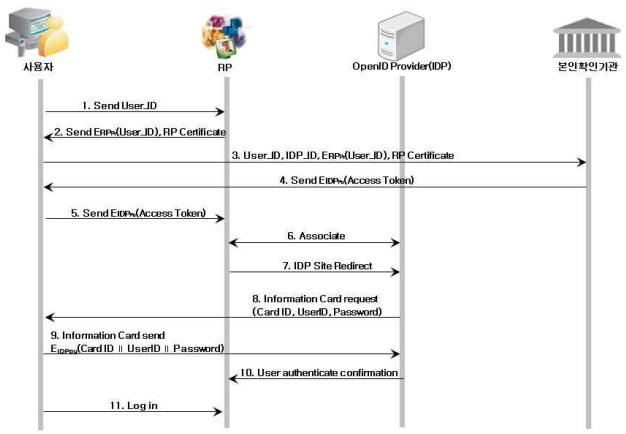
⑨ 사용자의 본인확인 인증이 끝나면 OpenID Provider는 [그림 2] 절차 ④에서 사용자가 제공한 OpenID의 URL(ID)와 Password를 가지고 가입을 승인을 전송함으로써 가입 완료를 한다.

그 후, 사용자는 [그림 2]의 절차 (1)~(7)은 (그림 1)과 같은 방법으로 RP(Relying Party)에 접속하여 서비스를 사용할 수 있다. 이는 기존 OpenID 동작절차와 동일하다.

I-PIN으로 인증을 받는 것은 OpenID를 발급받을 때 한번만 하면 되며, 그 후, OpenID로 로그인 하는 것만으로도 I-PIN으로 인증 받은 사용자라는 강점이 생긴다.

3.1 RP 인증 및 피싱방지

본 논문에서 제안하는 RP 인증과 피싱 방지를 통하여 사용자의 OpenID가 노출되지 않으며 IDP로 Redirect 될 때의 문제점을 보안할 수있다. 다음 [그림 3]은 RP 인증 및 피싱 방지를 위한 그림이며 절차는 다음과 같다.



[그림 3] RP 인증 방법

1. 사용자는 서비스 받고자 하는 인터넷 서비스(RP)에 접속하여 ID를 입력한다.
2. RP는 사용자의 ID를 RP의 공개키로 암호화하고 RP의 인증값을 사용자에게 보낸다.
3. 사용자는 본인확인기관에 사용자 ID, IDP_ID, RP로부터 받은 서명값과 인증값을 보낸다.
4. 본인확인기관은 Access Token을 사용자에게 보낸다.
5. 사용자는 RP인증을 위해 본인확인기관으로부터

받은 Access Token값을 RP에게 전달한다.

6. RP인증이 확인되면 RP와 IDP는 Associate를 한다.

4. 결론

현재 많은 나라에서 OpenID를 사용하고 있으며 최소한의 인증만을 제공하는 OpenID는 신뢰성과 보안에 많은 문제점을 가지고 있다. 본 논문에서는 기존 OpenID 시스템에 대해서 알아보고 많은 문제점 중 사용자 인증 부분과 피싱에 관련된 문제점을 알아보았다.

사용자 인증 없이 생성 가능한 OpenID는 개인당 무수히 많은 ID를 만들 수 있으며, 익명이 가능하기 때문에 악성 댓글과 스팸 등 악의적인 곳에 이용 가능하였다. 이러한 문제점을 해결하고자 주민번호 대체수단인 I-PIN을 도입하여 사용자 인증부분을 강화하고 PKI 방식을 도입하여 피싱에 안전한 OpenID 시스템을 제안하였다.

OpenID 서비스에서 사용자인증을 강화시키기 위해 회원가입 시 I-PIN을 적용함으로써 주민등록번호 노출 가능성이 없어졌으며 악의적인 RP가 가짜 IDP 인증화면을 보여주어 사용자의 ID와 Password를 가로 채가는 피싱에 대해 안전하다는 이점을 얻을 수 있다.

또한 기존 OpenID 서비스는 실명 및 성인인증이 안되어 있으며 무제한으로 ID 생성이 가능하였으나 사용자 인증을 강화시켜 이러한 문제점을 해결하였다.

본 논문에서 제안한 기법에서는 비대칭키 암호화 알고리즘을 사용하여 대칭키에 비하여 속도가 떨어지기는 하지만 키 관리에 대해 안전하다는 장점이 존재하며 비대칭키 암호화 알고리즘의 암·복호화 속도를 향상시킬 수 있는 방법에 대한 연구가 필요할 것이다.

참고문헌

[1] 오현경, 문필주, 전승현 "사용자 중심 ID 관리시스템이 지닌 취약점 분석" 한국인터넷정보학회 2007.06

[2] 윤재석, 민경식, 김정희 "인터넷 디지털 ID 추진 현황 및 전망" 정보통신연구진흥원

[3] http://ayo79.egloos.com/

[4] "주민번호 대체수단 서비스 개선 방안 연구", 한국정보보호진흥원,2007.

[5] "개인정보보호와 I-PIN", 한국정보보호진흥원, 2007.

[6] 최윤성, 이윤호, 김승주, 원동호, "주민등록번호 대체수단에 대한 구현 취약점 분석", 정보보호 학회 논문지 제17권 제2호, pp. 145 ~ 185, 2007. 4,

[7] 배준현, 김상욱 "개방형 모바일 서비스를 위한 OpenID를 이용한 사용자 인증 메커니즘의 설계", 한국컴퓨터종합 논문집 2007.