OpenID 기반의 MOTP를 이용한 사용자 인증 시스템의 설계

최도현*, 이재식*, 김현철*, 전문석*
*숭실대학교 컴퓨터학과
e-mail: cdhgod0@nate.com, {j30231, dmzpolice, mjun}@ssu.ac.kr

A Design of User Authentication System Using MOTP Based on OpenID

Do-Hyun Choi*, Jae-Sik Lee*, Hyun-chul Kim*, Mun-Seog Jeon*
*Dept of Computer Science, Soongsil University

요 약

인터넷 인구가 크게 증가함에 따라 인터넷 상의 ID와 개인정보 관리 문제가 크게 대두되고 있다. 이에 대한 해결책으로 통합 ID 관리 시스템이 고안되었으며 이 방법들 중 하나로 사용자 중심의 분산형 인증을 제공하는 OpenID가 있다. 현재 OpenID는 보안적인 기능을 담당하는 신뢰모델에 대한 표준화가 되어있지 않기 때문에 ID와 Password 이외에 사용자를 인증하는 다른 방법이 없는 문제점이 있다. 본 논문에서는 OpenID의 인증 및 신뢰성을 강화하기 위해 OTP 생성 매체인 Mobile One Time Password를 적용한 OpenID기반의 MOTP를 이용한 사용자 인증 시스템을 제안하고 설계한다.

1. 서론

최근 웹을 통한 개인정보 유출에 대한 피해발생률이 지속적으로 증가하고 있으며, 사용자가 웹 서비스를 사용하기 위해 생성한 ID와 Password에 대한 관리 부실이 대표적인 요인으로 지적되고 있다.

현재 사용자가 웹 서비스를 이용하기 위해서는 각각의 사이트나 도메인에 자신의 신용/비신용 정보를 제공한 후에 ID와 Password를 생성하여야한다. 그러나 사용하고자 하는 웹 사이트 및 도메인의 증가는 사용자의 ID관리를 어렵게 만든다. 이런 번거로움을 줄이기 위하여 사용자는 각 사이트마다 동일한 ID와 Password를 사용하는 경우가 비일비재하며 이러한 사용자의 행위는 하나의 ID와 Password가 노출되면 모든 개인 정보가 노출될 수 있다는 위험이 있다[4].

이런 아이디 도용에 따른 개인정보유출 문제에 대한 해결책으로 ID와 Password 인증 방법을 대체 할 인증 서비스가 필요하게 되었고 그 결과 통합 ID 관리 기술이 등장하였다.

통합 ID 관리는 사용자 ID의 생성, 이용, 관리, 폐기 등 개인정보 생명주기 전반에 대한 포괄적인 제도적, 관리적, 기술적 기능을 통해 개인정보를 보호하는 제공한다. 그러나 SSO(Single Sign On)로 대변되는 기존의 통합 ID 관리 기술은 서비스 업체 내 ID를 통합하는 서비스를 제공하였지만 특정 다수의 사이트의 통합 ID관리만으로는 여전히 수많은 웹 사이트의 ID관리를 해야 하는 사용자의 입장에서는 큰 해결책이 되지 못하는 한계가 존재한다[1].

본 논문에서는 기존의 통합 ID 관리 기법의 문제점을 해결하고 최근 대두 되고 있는 사용자 중심 ID 관리 기술의 안전성을 확보하기 위하여 사용자가 OpenID 서비스를 제공하는 사이트에 접속하여 로그인시 필요한 ID와 Password 이외에 MOTP(Mobile One Time Password)를 이용하여 OpenID 기반의 MOTP를 이용한 사용자 인증 시스템을 제안하고 설계한다.

본 논문에 구성은 다음과 같다. 2절에서는 관련연구로 OpenID의 동작 및 인증절차, OTP(One Time Password) 활용에 따른 OTP 생성매체의 종류에 대해 기술한다. 3절에서는 본 논문에서 제안하는 OpenID와 MOTP 인증 서비스를 적용한 시스템을 제안한다. 4절에서는 기존 기법과의 비교 분석을 수행하고 마지막으로 5절에서는 결론을 맺는다.

2. 관련연구

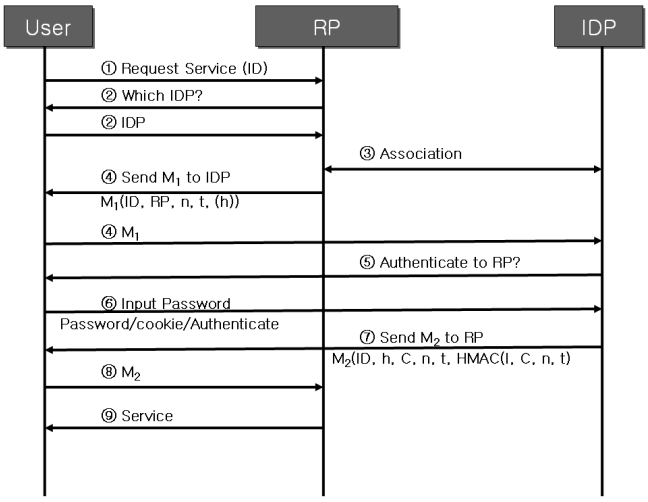
2.1 OpenID

OpenID는 사용자 중심 ID관리 시스템을 만족시켜주는 URI(Uniform Resource Identifier) 기반의 단일한 사용자 Identity를 제공하고, 사용자 중심의 분산형 인증체계를 제공하는 규격이다[2]. 기존 웹 환경의 ID, Password가 다수의 서비스 제공자에 의해 보관되었지만 OpenID는 다수의 ID를 관리할 필요 없이 직접 운영하는 서버나 OpenID 인증서버에 보관되어 OpenID를 지원하는

모든 사이트의 서비스를 OpenID 하나만으로 사용할 수 있다. OpenID는 현재 세계적으로 많은 서비스들이 상용화 되었고, 국내에서도 OpenID 제공 사이트가 운영되고 있으며, 이를 응용한 서비스도 다양하게 등장하고 있다[3]. 표<1>은 (그림1)와 (그림3)에 대한 약어표를 나타낸다.

<표 1> 약어표

이름	설명
User	사용자
RP	Relying Party : OpenID 서비스 지원 사이트
IDP	Identity Provider : OpenID 인증 제공 사이트
ID	사용자가 입력한 ID
M1	RP가 USER를 경유하여 IDP로 보내는 메시지
n	nonce
t	Time Stamp
h	서버로부터 생성된 세션 식별자
M2	IDP가 USER를 경유하여 RP로 보내는 메시지
HMAC	ID, H, n, t를 해시 기반 메시지 인증 코드를 이용하여 검증



(그림 1) OpenID의 인증절차

① 사용자는 서비스를 받고자 하는 RP에 자신의 식별자인 URI(OpenID)를 전송한다.
② RP는 사용자의 URI에서 가져온 웹페이지를 통해 서버 정보를 참조한다.
③ RP와 IDP로사용자의 인증을 위임하는데 안전한 통신을 위해 세션키를 생성하는 단계이다.
④ M_1(ID, RP, n, t, (h))이라는 정보를 가지고 사용자를 경유하여 IDP에 인증요청을 한다.
⑤ IDP에서 인증정보를 사용자에게 전송한다.
⑥ 사용자는 Password를 입력하고 Password/cookie/Authenticate 정보를 IDP에 전송한다.
⑦ IDP는 M_2(ID, h, C, n, t, HMAC(I, C, n, t)정보를 사용자에게 전송한다.
⑧ 사용자는 인증정보 RP를 허용할 지 선택하고, 인증정보를 RP에 전송한다.
⑨ 사용자는 RP의 서비스를 이용한다.

2.2 OTP

OTP는 사용할 때마다 다른 Password를 생성하여 사용자를 인증하는 일회용 Password를 의미한다. 대부분 OTP알고리즘이 일방향 함수를 이용하기 때문에 현재의 OTP값으로 다음 Password를 유추하기 어렵다. 기존의 Password 방식은 생성 후 변경하지 않으면 영구적으로 사용가능하지만 OTP는 일정시간 내에 반복적으로 Password를 생성하기 때문에 Password가 노출되더라도 큰 문제가 없다. OTP의 생성 매체의 종류에는 OTP 토큰, Mobile OTP, 카드형 OTP 등으로 나뉘고, 현재 많은 서비스분야에 제공되는 OTP의 활용은 다음과 같다[4].

2.2.1 OTP 토큰

OTP를 생성 가능한 연산기능 내장하고 있는 OTP생성 전용 하드웨어 매체로, 계산기, 열쇠고리, USB, 목걸이 등 그 형태가 다양하다. OTP전용기기는 추가 장비 필요 없이 사용가능하여 시스템에 적용하는데 용이하지만 사용자가 기기를 구매하여 휴대해야 하는 단점이 있다.

2.2.2 MOTP(Mobile OTP)

Mobile OTP는 생성알고리즘을 휴대폰 내에 모듈로 탑재되어, 별도의 OTP기기의 구매가 필요 없고 휴대할 필요가 없는 장점을 가지지만 텔레뱅킹 서비스나 Mobile 뱅킹 서비스는 이용이 불가능 하다.

2.2.3 카드형 OTP

OTP생성 모듈이 내장된 IC카드를 내장하고 있고, 디스플레이 창, OTP생성 버튼이 부착되어 있다. 휴대가 간편하고 다양한 전자 금융 서비스에서 이용 가능하지만 구입비용이 높다.

2.2.4 보이스 OTP

OTP생성 모듈, 배터리, 버튼, 스피커를 IC카드에 내장하여 사용자가 버튼을 누르면 특정 소리를 생성하여 이 소리를 OTP로 이용한다. 시각장애인, 노인에게 적용할 수 있는 방식이지만 시스템 환경이 복잡하고 마이크 및 부가 장치들이 필요하여 구입비용이 높다.

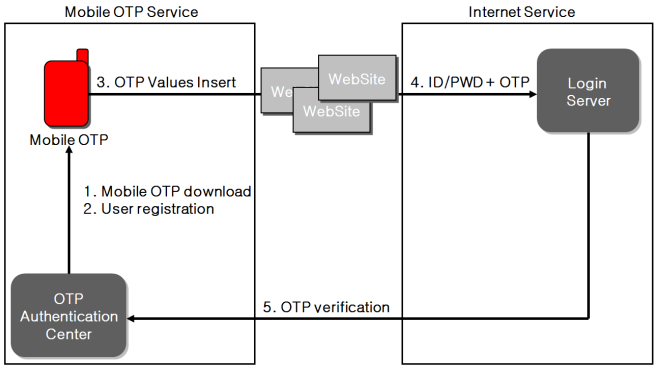
현재 사용되고 있는 OTP생성 매체들을 분류해 각 특징을 알아보았다. 본 논문에서는 기존 OpenID의 문제점을 해결하기 위해서 OpenID기반에 MOTP를 적용하는 시스템을 설계하였다.

3. 제안 시스템

OpenID는 사용자가 웹 서비스를 받기 위해 여러 사이트에 분산되어 있는 ID와 Password를 IDP라는 인증 제공 업체를 이용하여 통합하였고 기존의 SSO와 비슷한 개념이지만 한정된 범위가 아닌 모든 웹 서비스를 OpenID 하나만으로 이용할 수 있다.

이러한 OpenID의 문제점은 ID와 Password 유출 시 사용자의 IDP 서버내의 개인정보, 등록되어 있는 OpenID 사이트 리스트 정보 등 사용자가 등록한 모든 OpenID 사이트를 이용할 수 있게 되기 때문에 기존의 ID관리 방식과 같은 문제가 발생할 수 있다. 현재까지 OpenID는 사용자가 신뢰할 수 있는 신뢰모델이나 특별한 보안장치가 없다는 문제가 있다.

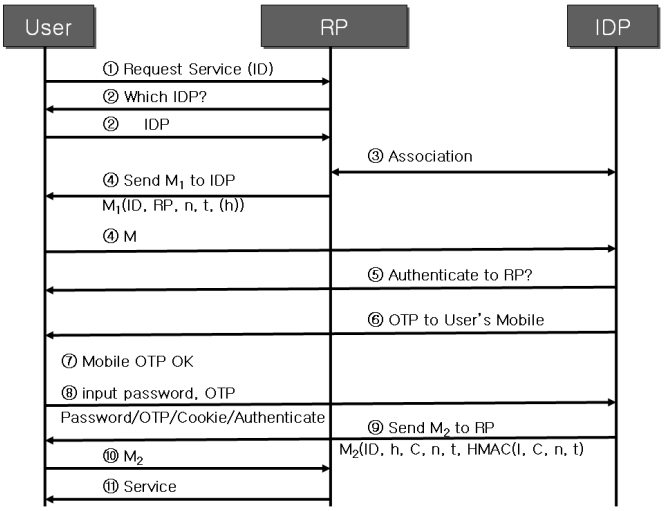
실제로 현재 OpenID를 지원하는 여러 서비스 제공 업체들이 IDP들 간에 호환성의 문제로 호환되는 다른 사이트를 이용하기 위해서는 새로운 OpenID를 생성해야 한다. 이것은 기존의 다수의 ID를 관리한 것과 같이 다수의 OpenID를 관리해야 하는 문제가 발생한다. 본 논문에서는 사용자의 신뢰도와 사용자의 인증성을 보완하기 위해 OpenID에 OTP생성 매체인 MOTP를 적용하였다. (그림 2)은 MOTP 서비스의 구조도를 나타낸 것이다.



(그림 2) MOTP의 서비스의 구조도

① 사용자는 Mobile OTP를 인증 센터로부터 다운로드 한다.
② 사용자 등록을 한다.
③ 사용자는 OTP 확인하고 OTP 인증번호를 입력한다.
④ 사용자의 ID, Password, OTP로 서비스를 시도한다.
⑤ OTP인증 센터에서 OTP가 인증되면 서비스를 이용한다.

MOTP는 휴대전화에 탑재 가능한 OTP 생성 S/W(Software)로 OTP S/W가 매번 다른 Password를 생성한다. (그림 3)은 OpenID 기반에 MOTP를 적용한 인증절차를 나타낸 것이다.



(그림 3) OpenID의 인증절차

① 사용자는 서비스를 받고자 하는 RP에 자신의 식별자인 URI(OpenID)를 전송한다.
② RP는 사용자의 URI에서 가져온 웹페이지를 통해 서버 정보를 참조한다.
③ RP와 IDP로사용자의 인증을 위임하는데 안전한 통신을 위해 세션키를 생성하는 단계이다.
④ M_1(ID, RP, n, t, (h))이라는 정보를 가지고 사용자를 경유하여 IDP에 인증요청을 한다.
⑤ IDP에서 인증정보를 사용자에게 전송한다.
⑥ IDP에서 OTP를 사용자의 Mobile로 전송한다.
⑦ 사용자는 OTP 인증번호를 확인한다.
⑧ 사용자는 Password를 입력하고 Password/OTP/Cookie/Authenticate 정보를 IDP에 전송한다.
⑨ 인증 후 IDP는 M_2(ID, h, C, n, t, HMAC(I, C, n, t)정보를 사용자에게 전송한다.
⑩ 사용자는 인증정보 RP를 허용할 지 선택하고, 인증정보를 RP에 전송한다.
⑪ 사용자는 RP의 서비스를 이용한다.

OpenID가 기본적으로 다수의 ID관리에 따른 개인정보의 유출문제를 보완할 수 있는 기술이지만 역으로 한번의 ID, Password 유출로 모든 정보를 유출할 수 있으며, ID 제공 업체라는 제 3자를 경유하여 사용자를 인증하기 때문에 IDP는 사용자가 신뢰할 수 있는 보안적인 기능을 제공해야 한다. 현재 OpenID는 IDP에 등록된 OpenID의 단일 Password를 이용하여 사용자 인증하기 때문에 보안적인 면에서는 아직 신뢰성이 부족하다. 본 논문에서 제시한 방법으로는 ID, Password, OTP 인증정보를 이용하여 사용자를 인증한다. 현재 MOTP는 대부분 OTP 기기와 OTP인증서버 간에 미리 공유된 비밀정보, 동기화 정보를 이용하여 OTP가 생성되는 방식을 이용한다. OTP인증 서버에서는 공격자가 OTP를 유추하기 짧은 시간 내에 변경된 OTP를 계속 전송하기 때문에 공격자는 OTP를 유추하기 어렵다.

4. 비교분석

현재 대부분 웹 서비스 환경은 사용자를 인증하기 위해 주민등록번호의 오류검증이나 실명확인 서비스를 통해 회원가입 및 사용자 본인확인을 하고 있다. 최근에는 개인정보 유출에 대한 문제를 해결하기 위한 방안으로 공인인증서를 활용한 전자서명, Mobile 인증, 신용카드정보 인증 방법 등 사용자의 인증을 강화하기 위해서 여러 가지 방법들이 적용되고 있다. <표 2>은 최근 웹 환경에서 사용자 인증 기술로 사용되고 있는 방법들을 비교분석 하였고 <표 3>은 기존의 OpenID와 본 논문에서 제시한 MOTP을 적용한 OpenID을 비교분석 한 것이다.

<표 2> 인증서, MOTP, 신용카드 비교분석

	편의성	비용	대중성
인증서	△	○	×
신용카드	×	○	△
MOTP	○	○	○

○: 높음 △: 보통 ×:낮음

현재 대표적으로 국내 웹 서비스에서 사용되는 보안 기술로 국내 금융권에서 많이 사용되고 있는 신원확인 수단인 공인인증서와 신용카드정보, 본 논문에서 제안한 OTP 생성 매체 중 Mobile을 이용한 OTP 방식인 MOTP을 비교분석 하였다.

편의성으로 현재 웹 서비스에서 결제를 사용하는 대부분의 사용자가 핸드폰을 사용하고 있는 사실을 고려하여 MOTP는 발급 및 수령 절차가 비교적 복잡한 인증서와 신용카드에 비해 간편하게 발급받을 수 있다.

비용으로는 인증서(범용 인증서 제외)와 카드는 발급 및 수령 후 사용자를 인증하는데 추가비용이 없지만 카드유지 비용이 들었고, MOTP는 모듈을 다운로드 할 때 통화료 이외에 드는 비용에 셋 모두 큰 차이가 없다.

대중성 관점에서 보면 08년 5월 기준으로 인증서는 약 1821만명[5], 신용카드의 수는 약 9348만장[6], 08년 말까지 국내 경제인구(2434만명)[7]으로 한 사람당 3.84장의 신용카드를 보유 하였고, 08년 6월말 기준으로 국내 휴대폰 이용자 수는 약 4285만명[8]으로 알려졌다. 이것은 편의성과 비용, 대중성을 종합해 볼 때 MOTP가 OpenID에 사용자 인증을 위한 기술로 적용하기에 적합하다고 볼 수 있다.

<표 3> OpenID와 MOTP을 적용한 OpenID의 비교분석

	OpenID	OpenID + MOTP
회원가입 정보	ID, Password, E-mail	ID, Password, Email, Phone Number
실명확인	×	○
스팸메일	○	×
신뢰성	×	○
편의성	○	×
비용	×	○

MOTP를 적용한 OpenID의 경우 회원가입 시 OTP를 확인하기 위한 Phone Number가 필요하였고, 핸드폰으로 본인 인증을 확인함으로써 실명확인이 가능하였다.

스팸메일의 경우 OpenID는 IDP를 통한 인증이 아닌 사용자가 직접 OpenID 서버를 만들 수 있어 OpenID를 무작위로 생성하여 스팸메일 같은 공격이 가능하다. OTP 인증 기관을 통해 핸드폰으로 사용자 인증을 하게 된다면 이런 문제를 보완할 수 있고, 사용자의 신뢰도를 높일 수 있는 계기가 될 것이다.

편의성으로 로그인 마다 사용자가 핸드폰을 이용하여 OTP를 확인해야 하는 불편함이 있지만 보안성을 위해서는 감안해야 하는 부분이다.

비용으로 MOTP는 사용자 입장에서는 OTP를 받아 확인만 하면 되기 때문에 초기에 모듈을 다운받은 비용이외에는 추가 비용이 들지 않았다.

5. 결론

본 논문에서는 기존의 OpenID에 MOTP라는 일회용 Password 기법을 적용하여 기존의 공인인증서, 보안카드, 네트워크 스니핑, 키로거 등 의미 있는 Password를 얻어내어 재사용하는 공격 방식의 단점을 보완 하였고, 대부분 사용자가 휴대하고 다니는 핸드폰이라는 Mobile 기기의 장점과 수명이 다하면 교체해야 하는 H/W 토큰 방식과는 달리 영구적인 사용이 가능한 S/W 토큰 방식으로 추가적인 비용의 부담감을 줄일 수 있었다.

OpenID는 여러 IDP와 RP로 인해 하나의 업체에 독점되지 않기 때문에 결국 사용자가 중심이 되어 앞으로 더 나은 서비스를 제공하게 될 것이며, 최근 해킹기법이 나날이 교묘해지고 공격방식도 다양하기 때문에 OpenID의 신뢰성 및 보안성을 위해서는 사용자의 OTP와 OpenID에 대한 인식, 서비스 제공자 는 여러 보안 솔루션 제공과 신뢰모델, 보안정책의 수립 및 이행 등이 이뤄져야 할 것이다.

참고문헌

[1] 조영섭, 진승헌, “사용자 중심 ID관리 기능을 제공하는 전자 ID 지갑 시스템”, 전자통신 동향분석 제 23권 제 4호, 2008.8

[2] 스프링노트, http://openid.springnote.com/pages/158154

[3] 위키디피아, http://ko.wikipedia.org/wiki/OpenID

[4] 서승현, 강우진, “OTP 기술현황 및 국내 금융권 OTP 도입사례”, 정보보호학회지 제 17권 제3호, 2007.6

[5] 한국정보보호진흥원, “식별번호를 이용한 본인확인 기술규격”, 2002

[6] 금융감독원, “08년 3분기 신용카드사 경영실적”,2008.12

[7] 통계청, “경제활동인구조사 > 성및농가·비농가별 경제활동인구”

[8] 방송통신 위원회, “유 무선 가입자 통계 현황(2008.12월)참조”, 2009.1