인증기관을 이용한 OpenID 피싱 방지 기법에 관한 연구

김성수*, 김재우*, 김현철*, 전문석*
*숭실대학교 컴퓨터학과
e-mail : {indielazy, saypeace, dmzpolice, mjun}@ssu.ac.kr

A Study on Phishing Prevention Mechanism of OpenID using Certificate Authority

Sung-Soo Kim*, Jae-Woo Kim*, Hyun-Chul Kim*, Moon-Seog Jun*
*Dept of Computer Science, Soong-Sil University

요 약

OpenID는 서비스와 ID 관리를 사이트 독자적으로 수행하는 Silo 모델의 계정 및 정보 관리 문제를 해결한다. 그러나 악의적인 공격자로 인한 OpenID Provider에 대한 피싱 공격 위험이 발견됨에 따라 개인 정보 유출에 대한 큰 위협이 되고 있다. 본 논문에서는 기존 OpenID 구조에 인증기관을 추가하여 사용자 인증 이전에 IDP에 대한 유효성 검증을 먼저 수행함으로써 IDP 피싱으로 인한 개인 정보 유출 문제를 사전에 방지 할 수 있는 인증기관을 이용한 OpenID 피싱 방지 기법을 제안한다. 또한, 기존의 OpenID 피싱 방지 기법과의 비교 실험을 통하여 편리성, IDP 신뢰성, 피싱 공격의 대한 안전성 항목에서 우수함을 확인 할 수 있었다.

1. 서론

초고속 네트워크와 웹 기술의 발전은 기존의 오프라인 상에서의 처리를 온라인으로 옮겨오는 계기가 되었다. 이러한 온라인 환경에서 서비스 제공자로부터 제공되는 서비스를 이용하기 위해서는 각 사이트에서 요구하는 사용자 자신의 신상, 비 신상 정보를 제공한 후 ID와 Password를 발급받아야 한다. 하지만 각각의 사이트에 대한 모든 ID와 Password를 사용자가 기억할 수 없다는 문제와 사용자 정보가 여러 사이트에 산재한다는 문제가 존재한다[1].

이런 문제점들을 해결하기 위하여 각 사이트마다 사용자 ID를 등록하지 않아도 서비스를 이용할 수 있는 OpenID가 등장하였다. OpenID는 분산 시스템 기반의 사용자 중심의 인증체계를 제공하는 공개 표준 기술이다[2][3].

OpenID는 여러 웹 사이트에서 하나의 아이디 즉 본인의 URL(OpenID)을 통해 사용자 인증을 처리함으로써 Silo 방식의 문제를 해결한다. 그러나 사용자 인증 단계에서 악의적인 공격자에 의한 IDP 피싱 위험이 존재한다[4]. 위와 같은 IDP 피싱의 문제를 해결하기 위해 여러 방안들이 제시되고 있지만 편이성과 사용자 이동성 및 IDP 신뢰성에서의 문제가 여전히 존재한다.

본 논문에서는 기존에 제시 되었던 IDP 피싱 방지 기법에 대한 문제점을 보안하고 IDP 피싱으로 인한 개인정보 유출 위협을 사전에 방지할 수 있는 인증기관을 이용한 OpenID 피싱 방지 기법을 제안하고 설계한다.

본 논문에서 제안 하는 메커니즘은 기존 OpenID 구조상에 문제로 인해 발생할 수 있는 IDP 피싱을 방지하기 위하여 기존 OpenID 시스템의 인증기관을 추가적으로 설치한다. 인증기관은 IDP에 대한 정보를 사전에 소유하고 있으며 해당 정보를 통해 IDP 인증을 처리한다. 사용자는 인증기관으로부터 검증 되어진 IDP에게만 자신의 ID와 Password를 제공하고 OpenID를 이용함으로서 악의적인 공격자가 생성한 IDP 피싱으로부터의 위협을 제거할 수 있다.

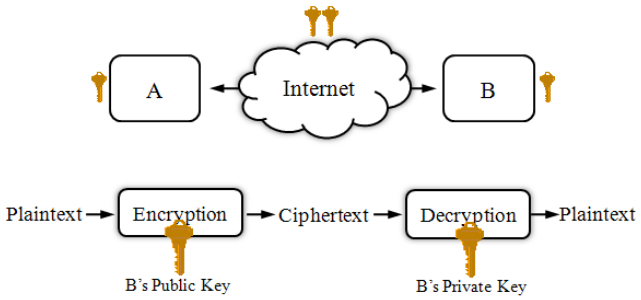
본 논문의 구성은 다음과 같다. 제 2절은 관련연구로 OpenID를 이용하기 위한 사용자 인증 절차에 대해서 살펴보고, 사용자 인증 단계에서의 피싱 공격 절차와 기존에 제시 되었던 IDP 피싱 방지 기법에 대해 기술한다. 제 3절에서는 본 논문에서 제안하는 피싱 방지 기법에 대해 제안하고 설계한다. 제 4절에서는 본 논문에서 제안한 메커니즘과 기존에 제안된 방법과의 비교분석 및 평과를 수행한다. 제 5절에서는 결론을 맺고자 한다.

2. 관련연구 및 문제점

2.1. 공개키 암호 알고리즘

공개키 암호 알고리즘(Public-Key Crypto Algorithm)은 비대칭 암호 알고리즘(Asymmetric Crypto Algorithm)이라고도 한다. 이 암호 알고리즘은 암호화와 복호화에 사용

되는 공개키와 개인키의 쌍이 존재한다. 두 개의 키 중 어느 하나의 키로 암호화를 하면 다른 하나의 키로만 복호화가 가능한 알고리즘이다. 이 공개키 암호 알고리즘의 공개키와 개인키는 수학적 함수 기반으로 서로 연관 관계를 가지고 있으며, 키 쌍의 하나는 누구든지 사용 가능 하도록 공개되어 있으며, 다른 하나의 키는 외부에 공개 되지 않는 비밀(Secret) 속성을 가진 키이다. 이때 외부에 공개되는 키를 공개키(Public-Key)라고 하고, 외부에 공개 되지 않는 키를 개인키(Private-Key)라고 한다. 송신자는 외부에 공개 되어있는 수신자의 공개키로 자신의 메시지를 암호화하여 수신자에게 전송하고, 암호문을 받은 수신자는 자신의 개인키로 송신자의 암호문을 복호화 하여 메시지를 얻는다. 공개키 암호 알고리즘의 처리 과정은 다음 (그림 1)과 같다.



(그림 1) 공개키 암호 알고리즘 과정

암호화 방법은 송신자가 수신자 B의 공개키로 원본 메시지(Plaintext)를 암호화 하고, 수신자 B에게 전송한다. 수신자는 수신된 암호문(Ciphertext)을 자신의 개인키로 메시지를 복호화 하여, 원본 메시지를 얻게 된다.

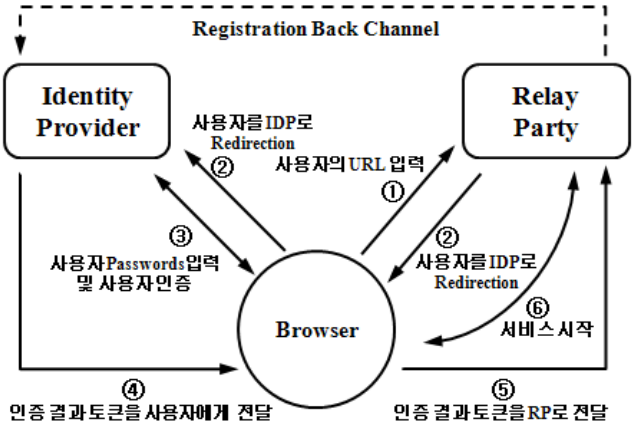
공개키와 비밀키의 키 쌍은 수학적 함수 기반의 키 간의 연관 관계를 가지고 있으므로 외부에 공개된 공개키로 암호화하고, 해당 공개키의 다른 키인 개인키만이 그 암호문을 복호화 할 수 있게 된다. 이는 송신자와 수신자의 비밀메시지의 교환이 가능하여 인증 방법에 사용된다[5].

2.2. OpenID

OpenID는 ID 제공 사이트(Identity Provider)와 OpenID의 정보를 이용하여 실제 사용자에게 서비스를 제공하는 RP(Relay Party), 그리고 OpenID 서비스를 이용하는 사용자로 구성된다.

OpenID를 이용하기 위해서는 (그림 2)에서 보여지는 것과 같이 총 6단계의 절차로 이루어진다. 다음은 (그림 2)에 따른 OpenID 동작 절차이다.

① 사용자는 원하는 서비스 웹 사이트에 자신의 URL (OpenID)를 입력한다.
② RP는 사용자를 OpenID 제공자인 IDP에게 Redirection 시킨다.
③ 사용자는 자신의 Password를 입력하고, 사용자 자신을 인증한다.
④ IDP는 사용자를 확인하고, 인증 결과 토큰을 사용자에게 전달한다.
⑤ 사용자는 서비스 웹 사이트인 RP로 해당 토큰을 전달한다.
⑥ RP는 사용자에게 서비스를 제공한다.



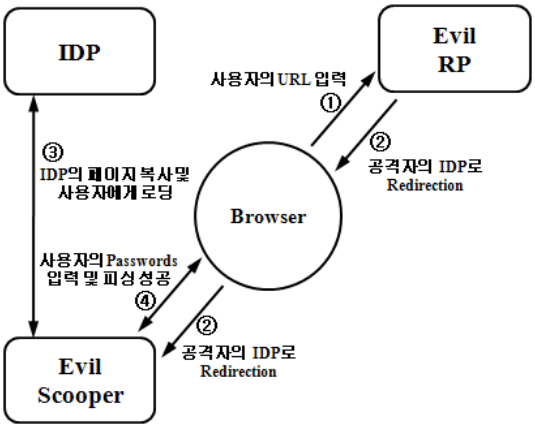
(그림 2) OpenID의 동작 과정

2.3. OpenID 피싱

OpenID의 간단한 사용자 인증 동작 과정으로 인해 보안성과 신뢰성에 관한 문제점이 제기되는 가운데 피싱 공격의 여러 위험이 제시되고 있다

OpenID의 가장 큰 특징은 하나의 URL(OpenID)로 여러 웹 사이트의 사용자 인증이 가능하다는 점이다. 그러나 피싱 공격에 노출 되면, OpenID로 사용자 인증이 가능한 모든 웹 사이트까지 사용자의 URL을 도용하여 서비스를 받는 문제점이 있다. 이러한 문제점을 해결하기 위해 OpenID와 CardSpcae의 결합 방법[6], 시각적 효과를 이용 방법[7], 웹 브라우저 즐겨찾기 방법[8]이 있다.

OpenID에서의 피싱 공격은 (그림 3)과 같이 4단계의 절차를 가진다.



(그림 3) OpenID의 피싱 공격 과정

다음은 (그림 3)에 근거한 OpenID 피싱 공격 절차이다.

① 사용자는 서비스 웹 사이트에 자신의 OpenID를 입력한다.
② 공격자 RP는 사용자를 정당한 IDP에게 Redirection이 아닌 공격자의 IDP(Evil Scooper)로 Redirection을 시킨다.
③ 사용자를 피싱 하기 위하여 Evil Scooper는 정당한 IDP의 페이지를 복사하여 사용자에게 로딩 한다.
④ 사용자는 로딩된 페이지가 정당한 IDP의 페이지로 인식하고, 자신의 Password를 입력 한다.

위와 같은 피싱 공격으로 인해 사용자의 OpenID와 Password가 노출되고 피싱 공격에 성공한다. 이러한 피싱 공격 성공의 근본적인 이유는 사용자가 IDP와 RP가 정당한 IDP와 RP인지를 확인 할 수 없다는 점과 Redirection 단계에서 정당한 IDP로 Redirection되었는지를 확인할 수 있는 방법이 없다는 것에서 비롯된다. 따라서 IDP를 정당한 IDP인지 확인하는 절차가 필요하다.

3. OpenID 피싱 방지 메커니즘

기존 OpenID 시스템에서는 낮은 신뢰도와 가벼운 사용자 인증으로 인해 피싱 공격에 취약하다. 본 논문에서 제안하는 피싱 방지 기법은 OpenID의 사용자 편의성을 유지하고 사용자 인증에 대한 신뢰도를 높이며, 피싱 공격에 취약한 기존 시스템을 사용자가 안심하고 자신의 Password를 입력하여 원하는 웹 사이트의 서비스를 이용하는 기법을 제안한다.

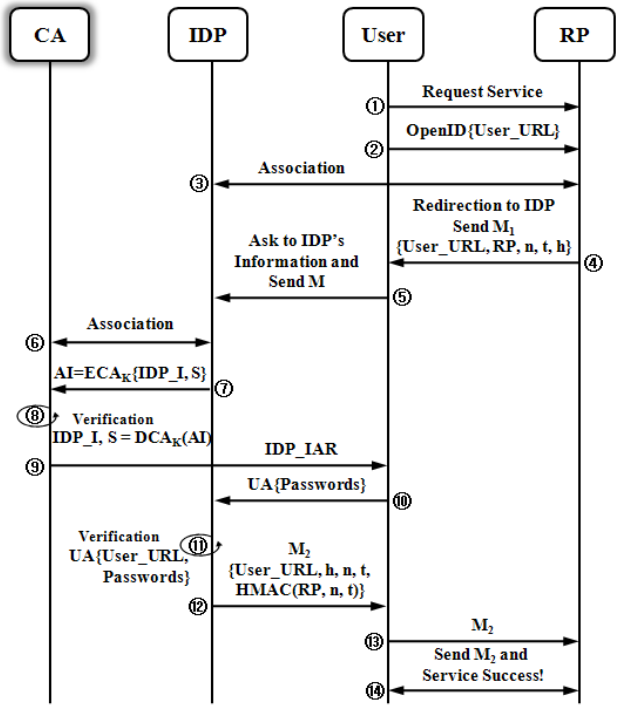
3.1. 피싱 방지 메커니즘의 요구사항

본 논문에서 제안하는 OpenID 피싱 방지 메커니즘은 사용자가 CA를 신뢰하고, CA는 IDP의 관한 정보를 DB에 모두 저장하고 있어야 하며, 사용자가 IDP의 정보를 요구할 때, IDP는 자신의 정보를 CA에게 입증하고, 그 입증 결과를 사용자에게 전송해야 한다.

3.2. 피싱 방지 메커니즘의 설계

본 논문에서 제안하는 OpenID 피싱 방지 메커니즘의 과정은 (그림 4)와 같다.

- User_URL : 사용자 OpenID
- RP : RP의 식별 정보
- n : Nonce
- AI : Authentication IDP
- h : IDP의 세션 식별 정보
- S : CA의 세션 정보
- IDP_I : IDP의 정보
- t : Timestamp
- ECA_K : CA의 공개키 암호화
- DCA_K : CA의 개인키 복호화
- IDP_IAR : IDP Information Authentication Response



(그림 4) OpenID 피싱 방지 메커니즘

① 사용자는 원하는 서비스 웹 사이트에 접속한다.
② 사용자는 자신의 URL을 입력한다.
③ RP와 IDP는 협의를 진행한다.
④ RP는 사용자를 IDP로 Redirection하면서 RP, URL, n, t, h 값인 M1을 전송한다.
⑤ 사용자는 IDP가 정상적인 IDP임을 확인하기 위하여 IDP에게 정보를 요청한다.
⑥ IDP와 CA는 협의를 진행한다.
⑦ IDP는 CA의 공개키로 자신의 정보(IDP_I)와 ⑥단계에서의 세션 정보(S)를 암호화한 값을 전송한다.
⑧ CA는 AI값을 자신의 개인키로 복호화하여 IDP의 정보와 ⑥단계에서의 세션 정보(S)를 확인하여 IDP가 정상적인 IDP라는 것을 확인한다.
⑨ CA는 정상적인 IDP의 입증 값인 IDP_IAR을 사용자에게 전송한다.
⑩ 정상적인 IDP를 확인한 사용자는 자신의 Password를 IDP에 입력한다.
⑪ IDP는 ④단계에서 받은 M1과 사용자의 Password를 이용하여 사용자 인증을 한다.
⑫ IDP는 사용자 인증에 대한 결과를 사용자에게 M2를 전송한다.
⑬ 사용자는 자신의 인증 결과 M2를 RP에게 전송한다.
⑭ 사용자는 RP의 서비스를 이용한다.

4. 비교분석 및 평가

기존 OpenID에서 피싱 방지를 위해 제시된 OpenID와 Cardspace의 결합 방법(P1), 시각적 효과를 이용한 방법

(P2), 웹 브라우저 즐겨찾기 방법(P3)이 있으며 본 논문에서 제안한 메커니즘(P4)과의 사용자 편의성, 사용자 이동성, 인증 신뢰성, IDP 신뢰성, 피싱 공격의 안전성 항목에 대하여 비교 분석을 수행하였다. 비교 분석 결과는 <표 1>과 같다.

<표 1> OpenID 피싱 방지의 비교

비교항목	P1	P2	P3	P4
사용자 편이성	△	◎	◎	◎
사용자 이동성	△	×	×	◎
인증 신뢰성	◎	△	△	◎
IDP 신뢰성	◎	△	△	◎
피싱 공격의 안전성	◎	×	×	◎

◎ : 해당함, △ : 일부 해당함, × : 해당사항 없음

사용자 편이성 측면에서 P1은 자신을 인증하기 위해서 OpenID 뿐만 아니라 Cardspace까지 본인 인증이 필요하고, P2는 사용자 인증에서 시각적인 이미지를 이용함으로써 추후 인증에는 유용하다. P3은 웹 브라우저의 즐겨찾기에 추가하여 편이성 측면에는 우수하다. P4 제안 메커니즘은 기존의 OpenID의 사용자 인증 절차와 유사하다. 그러나 P1과 P2, P3는 사용자 이동성 측면에서는 P1은 보통의 성능을 제공하나, P2와 P3은 이동성을 지원해 주지 못 한다. 즉, P1은 개인 PC에 저장 되어있는 Cardspace를 사용자 이동시 이동식 메모리에 저장해야 하지만 이동식 메모리의 분실의 위험성을 가지고 있고, P2는 Cookie를 이용한 이미지로 Cookie 삭제와 동시에 이미지도 삭제된다. P3 또한 개인 PC에 저장 되어있기 때문에 사용자 이동성에 문제가 되지만 제안 메커니즘 P4는 사용자 이동성 문제점에 국한되지 않는다.

인증 신뢰성 측면에서 P1은 OpenID와 Cardspace를 결합하여 Password를 안전하게 관리하고 있고, P2와 P3은 개인 PC가 아닌 타 PC에서의 사용자 인증 신뢰성은 피싱 공격의 위험성을 가지고 있다. 제안 메커니즘 P4는 인증기관에 IDP를 입증한 후, 사용자를 인증하므로 피싱 공격에 안전하다. IDP의 신뢰성 측면에서 P1은 Cardspace를 제출하기 때문에 IDP를 신뢰할 수 있다. P2와 P3은 사용자 인증 신뢰성 부분과 같이 타 PC에서 사용자 인증을 할 경우 IDP를 신뢰할 수가 없으므로 피싱의 공격에 노출되어있다. 본 논문에서 제안하는 메커니즘 P4는 IDP가 CA로부터 IDP 자신을 입증 받기 때문에 IDP를 신뢰한다.

피싱 공격 취약성 측면에서 P1은 Password를 관리 하는 Cardspace를 사용하기 때문에 피싱 공격에 안전하다. P2와 P3은 Cookie 삭제 또는 타 PC에서 인증 할 경우 Redirection 과정에서 피싱 공격에 취약하다. 제안 메커니즘 P4는 Redirection 과정에서 IDP를 신뢰하기 위해 인증기관을 통해 IDP를 입증하므로 피싱 공격을 예방할 수 있다.

5. 결론

본 논문에서는 공개키 기반의 인증기관을 사용하여 사용자가 정상적인 IDP임을 확인하고 자신의 Password를 안전하게 입력함으로써 IDP 피싱 공격에 안전한 인증기관을 이용한 OpenID 피싱 방지 기법을 제안하고 설계 하였다. 제안하는 메커니즘은 기존 OpenID 시스템에서 사용자가 피싱 공격에 노출될 수 있는 구조적 문제를 해결하기 위하여 인증기관을 추가하였다. 또한 기존 기법과의 비교 분석을 통해 사용자 편이성과 이동성, 인증 및 IDP 신뢰성, 피싱 공격의 대한 안전성 측면에서 정성적 평가를 통해 우수함을 확인 할 수 있었다. 향후 본 논문에서 제안하는 메커니즘을 실제 환경에 적용할 수 있도록 지속적인 연구를 수행하고자 한다.

참고문헌

[1] 최대선, 진승헌, 정교일 “인터넷 ID 관리 서비스” 한국전자통신연구원, 디지털ID보안연구팀, 2006.
[2] David Recordon VeriSign Inc, Drummond Reed, “OpenID 2.0:A Platform for User-Centric Identity Management", 2006.
[3] http://itmedia.kaist.ac.kr/tag/OpenID
[4] http://marcoslot.net/apps/openid/
[5] E. Rescorla, "Diffie-Hellman Key Agreement Method" IETF, RFC 2631, 1999.
[6] http://ayo79.egloos.com/3373092
[7] https://www.myopenid.com/set_cookie_image
[8] http://usablesecurity.com/2007/01/20/phishing-and-openid/