블록체인을 활용한 OpenID의 Relying Party 피싱 방지 연구

김건민, 이은성, 장현지, 이서준, 김경백*
전남대학교, *전남대학교 인공지능융합학과
204869@jnu.ac.kr, 200750@jnu.ac.kr, gka1225@jnu.ac.kr, tjwns1300@jnu.ac.kr,
*kyungbaekkim@jnu.ac.kr

A Study on Preventing OpenID Relying Party Phishing Using Blockchain

Geon Min Kim, Eun Seong Lee, Hyeon Ji Jang, Seo Jun Lee, *Kyung Baek Kim
Chonnam National Univ., *Dept. of Artificial Intelligence, Chonnam National Univ.

요 약

본 논문은 OpenID 시스템에서 발생할 수 있는 Relying Party(RP) 피싱 공격을 분석하고, 이를 방지하기 위한 기존 대응 방안들의 한계를 검토한다. OpenID는 사용자가 여러 웹사이트에서 하나의 디지털 ID로 로그인할 수 있도록 해주는 편리한 인증 시스템이지만, 이러한 편의성 뒤에는 보안 취약점이 존재한다. 특히, 악성 RP가 사용자의 인증 정보를 가로채는 RP 피싱 공격은 심각한 보안 위협으로 간주된다. 이에 대한 해결책으로 블록체인 기술을 활용한 RP 신뢰도 검증 시스템을 제안한다. 블록체인의 투명성과 변조 불가능한 특성을 활용하여, 중앙 기관 없이도 RP의 신뢰도를 검증하고 피싱 위험을 줄일 수 있다. 또한, RP의 신뢰성을 실시간으로 기록하고 관리하여, 신뢰도가 낮은 RP를 선별하는 방식으로 보안을 강화한다.

1. 서 론

급증하는 온라인 서비스에 사용자 각 개인은 많은 계정과 비밀번호를 등록하게 되었고, 이를 효과적으로 관리하기 위해 OpenID[1]가 등장하였다. OpenID는 URI 기반의 사용자 중심의 개방형 사용자 인증 프로토콜로, Google, Facebook, Microsoft 등의 웹 기반 서비스에서 널리 채택되고 있는 인증 메커니즘이다. 이 프로토콜은 사용자가 여러 웹사이트에서 단일 디지털 ID를 사용할 수 있게 해주어 사용자의 편의성을 크게 향상시켰다. 그러나 이러한 편의성의 이면에는 몇 가지 잠재적인 보안 위협이 존재하며, Relying Party(RP) 피싱[2]은 가장 위험한 공격 유형 중 하나로 꼽힌다.

본 논문에서는 OpenID 시스템에서 RP 피싱 공격을 분석하고, 기존의 대응 방안들의 한계를 검토한다. 이를 바탕으로 블록체인 기술을 활용한 새로운 RP 신뢰도 검증 시스템을 제안하고, 예상되는 효과를 논의한다.

2. OpenID and RP 피싱

2.1. OpenID

OpenID는 모든 사용자 ID를 URL에 부여하는 디지털 신원 시스템으로, 사용자가 여러 웹사이트에서 단일 Identity로 로그인할 수 있게 해준다. OpenID 사용자는 OpenID 지원 웹사이트에 로그인하기 위해 새로운 계정을 생성하고 관리할 필요 없이, OpenID를 제공하는 하나의 신뢰할 수 있는 제공자 (OpenID Provider, OP)에서 인증을 받을 수 있다. OP는 관련 ID의 소유권을 RP에 확인할 수 있다. 사용자는 OP에 가입하여 인증 절차를 관리하며, RP는 사용자의 신원을 검증하기 위해 OP에 의존하게 된다.

2.1.1. OpenID 주요 개체

OpenID의 주요 개체는 다음과 같다.

① Resource Owner(사용자)
자신의 ID를 이용해 여러 서비스에 로그인하는 주체로, Identity라고도 한다.

② Relying Party(RP)
사용자의 인증 정보를 받는 서비스 제공자이다.

③ OP(OpenID Provider)
사용자 신원을 인정하는 기관으로, RP에게 사용자(Identity)에 대한 정보를 제공하기 때문에 IDP(Identity Provider)라고도 한다.

2.1.2. OpenID의 작동 방식

OpenID의 작동 방식은 다음과 같다.

① 사용자가 RP에 URL 형식의 OpenID를 입력한다.

② RP는 OpenID의 URL을 확인하고, 이를 OP와 연결한다.

③ RP는 사용자를 통해 OP에 사용자 인증을 요청한다. 즉, RP는 사용자를 OP로 리디렉션한다.

④ OP는 사용자 인증을 위해 사용자에게 OpenID의 비밀번호를 입력하도록 요청하고, 사용자는 OP에 비밀번호를 입력한다.

⑤ OP는 사용자가 입력한 비밀번호와 OpenID를 확인하고, OpenID 사용자를 인증한다. 인증이 완료되면 OP는 인증 토큰을 통해 RP에 인증을 알린다.

⑥ RP는 사용자의 인증을 확인하고 서비스의 제공 여부를 결정한다. 사용자는 OpenID를 통해 RP가 제공하는 서비스를 이용할 수 있게 된다.

2.2. RP 피싱

OpenID에서 인증 과정 중 사용자는 OP로 리다이렉트되어 본인의 신원을 확인하게 된다. 이 때 악성 RP가 이 과정을 가로채어 사용자가 접속한 OP 페이지를 위조할 수 있다. 악성 RP는 사용자를 속이기 위해 OP에서 제공하는 것과 동일한 내용을 가진 피싱 페이지를 표시하게 된다. 사용자는 OP가 제공하는 로그인 페이지와 동일한 내용을 보고 있기 때문에 위조된 페이지임을 인식하지 못하고, 그 곳에 자신의 자격 증명(아이디와 비밀번호 등)을 입력할 위험이 있다. 사용자는 자신의 비밀번호로 인증할 수 있지만, OP를 인증할 수는 없다. 사용자 자신이 OP를 신뢰할 수 있는지 직접적으로 검증할 방법이 없어 OpenID는 이러한 피싱 공격에 취약하다.

2.2.2 RP 피싱에 대한 기존 대응 방안 및 한계

기존에 제시되었던 RP 피싱 방지 방법[3]들은 다음과 같다.

① myOpenID의 Personal Icon

OP는 사용자의 PC에 대한 쿠키를 가지고 있기 때문에, RP에 의해 리디렉션된 OP는 사용자가 처음 입력한 사진이나 텍스트를 표시한다. 하지만 이 방법은 사용자의 PC에 저장된 쿠키를 활용하므로, 다른 PC나 브라우저에서 로그인할 때는 보호 기능이 동작하지 않는다는 한계를 갖는다.

② VeriSign과 IE7의 확장 검증 인증서

이 인증서는 VeriSign과 IE7이 공동 개발 한 것으로, OP가 VeriSign에 의해 검증된 경우, 웹 브라우저의 주소 창이 녹색으로 변한다. 이 기능은 특정 브라우저(IE7)에서만 동작하므로, 다른 브라우저나 최신 버전의 브라우저에서는 이 기능을 사용할 수 없다. 또한, 사용자가 이 기능의 존재를 인지하지 못하거나 녹색 주소 창을 무시할 경우 보안 효과가 제한된다.

③ Vidoop의 새로운 비밀번호 솔루션

사용자가 Vidoop으로 로그인할 때 비밀번호 대신 그림을 선택한다. 활성화 코드는 이메일로 발급되며, 그림이 비밀번호로 입력된다. 사용자가 비밀번호 대신 그림을 선택하는 방식은 직관적일 수 있지만, 이메일을 통해 활성화 코드를 받는 방식은 이메일 해킹의 위험에 노출될 수 있다.

④ Jabber의 메신저 또는 SMS 인증

RP가 올바른 OP로 리디렉션되면, OP는 메신저 또는 SMS로 사용자에게 이를 알린다. 이 기능을 사용하려면 사용자가 메신저에 로그인하거나 SMS를 받을 수 있는 기기가 필요하다. 하지만 이 방법은 메신저나 SMS 인증은 사용자가 메시지를 실시간으로 확인할 수 있어야 하므로, 메시지 전달이 지연될 수 있고, SMS 자체가 피싱이나 스미싱(sms phishing)에 취약할 수 있으며, 인증 과정이 번거로울 수 있다.

3. 블록체인을 활용한 새로운 RP 신뢰도 검증 시스템

3.1. 블록체인의 역할

본 시스템에서 블록체인은 RP의 신뢰도를 기록하고 검증하는 핵심 역할을 한다. 블록체인의 특성상 중앙화된 인증 기간 없이도 RP의 신뢰도를 객관적으로 평가하고 기록할 수 있고, 블록체인의 불변성에 의해 한 번 기록된 RP의 신뢰도는 임의로 조작하거나 삭제할 수 없다.

블록체인은 다음과 같은 두 가지 중요한 기능을 수행한다.

① RP 인증 정보 저장

OpenID 시스템에서 처음 등록되는 RP의 공개 키 및 인증서 등과 같은 중요한 정보를 블록체인에 기록한다.

② 실시간 신뢰도 기록

사용자가 OpenID로 인증 절차를 수행할 때마다 해당 RP의 행동에 따른 신뢰도를 기록하여 실시간으로 블록체인에 저장하며, 이후 다른 사용자들도 이를 참고할 수 있도록 한다.

3.2. RP 신뢰도 검증 흐름

1) RP 등록 및 검증

새로운 RP가 OpenID 생태계에 참여하려면 블록체인에 등록이 필요하다. 등록 과정에서는 RP의 공개 키, 도메인 정보, 그리고 신뢰도 평가 알고리즘에서 사용할 초기 신뢰도 점수 등이 블록체인에 저장된다. 이 때 RP의 인증 정보를 다수의 노드가 검증하고, 해당 RP가 정상적인 서비스 제공자인지 확인하는 절차를 거친다.

2) RP의 신뢰도 기록

① 신뢰도 평가 메커니즘

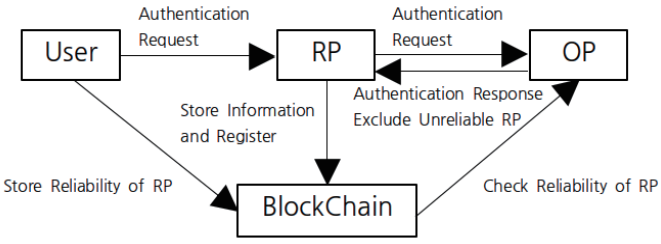
사용자가 특정 RP와 상호작용할 때마다 해당 RP의 활동에 대한 신뢰도를 블록체인에 기록한다. 이 신뢰도는 사용자와 RP간의 거래 내역, 서비스 제공의 적합성, 보안 이슈 발생 여부 등을 바탕으로 평가된다. 예를 들어, 사용자가 정상적인 인증 절차를 거치지 못하거나, 서비스의 일관성이 떨어지면 신뢰도 점수가 하락할 수 있다.

② 평판 기반 필터링

누적된 신뢰도 데이터를 바탕으로 일정 기준 이하의 RP는 제외시키거나, 사용자에게 경고 메시지를 제공한다.

3) OpenID 이용

사용자가 특정 웹사이트에서 OpenID를 사용하려 할 때, 시스템은 즉시 해당 RP의 신뢰도를 조회하여 사용자가 인증을 수행할 지 여부를 결정한다. 만약 신뢰도가 낮거나 최근 불량 활동이 기록된 RP라면, 사용자에게 경고 메시지를 제공하거나 인증 절차를 차단한다. 또한, 사용자는 블록체인에 기록된 해당 RP의 신뢰 기록을 실시간으로 확인할 수 있어 이를 통해 신뢰할 수 없는 RP와의 상호작용을 미연에 방지할 수 있다.



(그림 1) 블록체인 기반 RP 신뢰도 검증 시스템 작동 흐름

4. 결론

RP 피싱은 사용자의 인증 정보를 악성 RP가 가로채는 심각한 보안 위협으로, 기존 대응책들은 특정 환경에 제한되거나 사용자의 주의에 의존하는 문제를 가지고 있다. 이에 대한 해결책으로 블록체인을 활용한 새로운 RP 신뢰도 검증 시스템을 제안하였다. 블록체인을 통해 중앙 기관 없이도 RP의 신뢰도를 투명하게 검증하고, 신뢰도가 낮은 RP를 선별하여 피싱 위험을 줄일 수 있으며 블록체인의 불변성 덕분에 시스템의 신뢰성을 높일 수 있다. 향후 연구에서는 제안된 시스템의 실제 구현 및 성능 검증이 필요하며, 블록체인 기술을 활용한 보안 강화의 가능성을 탐구하는 본 논문의 접근은 OpenID의 안전성 향상에 중요한 기여를 할 수 있을 것이다.

ACKNOWLEDGMENT

본 연구는 한국인터넷진흥원(KISA)-정보보안 특성화대학 지원사업의 지원을 받아 수행된 연구임. 본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 첨단분야 혁신융합대학사업의 연구결과입니다.

참 고 문 헌

[1] K. Dodanduwa and I. Kaluthanthri, "Role of Trust in OAuth 2.0 and OpenID Connect," 2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS), Colombo, Sri Lanka, 2018, pp. 1-4

[2] J. -H. You and M. -S. Jun, "A Mechanism to Prevent RP Phishing in OpenID System," 2010 IEEE/ACIS 9th International Conference on Computer and Information Science, Yamagata, Japan, 2010, pp. 876-880

[3] H. Lee, I. Jeun, K. Chun and J. Song, "A New Anti-phishing Method in OpenID," 2008 Second International Conference on Emerging Security Information, Systems and Technologies, Cap Esterel, France, 2008, pp. 243-247