서드파티 취약점 영향에 따른 전자지갑에 보호 메커니즘에 관한 연구

황도영[1], 유동영[2],
[1]홍익대학교 스마트시티형 도시재생융합전공
[2]홍익대학교 소프트웨어융합학과
hdy@g.hongik.ac.kr, ydy@hongik.ac.kr

A Study on the Protection Mechanism of Electronic Wallet according to the Influence of Third Party Vulnerability

Do-Yeong Hwang[1], Dong-Young Yoo[2]
[1]Smart City & Urban Regeneration Converge, Hongik University
[2]Department of Software Convergence, Hongik University

요 약

최근 블록체인 기술이 발달함에 따라 사이버 범죄자의 공격 대상이 되고 있다. 특히, 암호화폐가 등장하게 되면서 화폐를 관리하는 전자지갑의 보안이 중요해지고 있다. 전자지갑은 내부에 저장된 개인 키를 통해 네트워크에 트랜잭션을 요청하게 되고 사용자 인증을 위해 중앙 기관에 검증을 요청한다. 이때, 전자지갑은 서드파티 취약점에 영향을 받아 공격 대상이 될 수 있다. 따라서, 본 연구에서는 블록체인 환경에서 서드파티 의한 위협으로부터 전자지갑을 보호하는 메커니즘 연구를 진행했다.

1. 서론

기존의 대다수 IoT는 중앙집중 방식의 관리가 이루어졌다. 중앙서버를 통해 연결된 노드를 관리하고 제어하기 때문에 IoT 기반의 가전기기, CCTV, 자동차 등 다양한 사례가 증가함에 따라 IoT에 보안성을 강화하고자 블록체인 기술을 적용하는 시도가 증가하는 추세다[1]. 블록체인 환경에서는 연결된 노드를 식별하기 위해 전자지갑에 저장된 private key를 통해 노드를 식별하고 블록체인 네트워크의 public key에 저장된 주소인지 확인하고 네트워크에 연결한다. 이때, 전자지갑의 취약점을 노리고 공격하여 개인 키를 탈취하여 지갑에 대한 권한을 상승시키고 암호화폐 거래를 막거나 자산을 탈취하는 경우가 종종 발생하고 있다.

2. 관련 연구

IoT는 사물과 인터넷을 하나로 연결하는 기술이다. 또한 IoT는 의료, 주택, 도시, 금융 등 여러 분야로 확대되어 급속한 성장을 이루고 있다. 하지만 IoT 기술에 대한 수요가 증가함에 따라 IoT에 존재하는 취약한 부분을 공격하여 사용자 개인정보를 탈취하거나 내부 데이터를 위변조하여 IoT 기기와 연결된 중앙서버를 마비시킨다. 공격 유형으로 악성코드 주입, 사회공학 기법, 피싱, DoS 등 하드웨어 및 소프트웨어를 공격하거나 스푸핑, MITM 공격 등 인터넷과 연결된 IoT 기기의 네트워크를 공격하여 중앙서버에 저장된 정보를 탈취할 수 있다. IoT 기기를 보안 위협으로부터 보호하기 위해 블록체인 기술을 적용한 IoT 시스템이 증가하고 있다[2].

스마트홈 환경에서 IoT 장치로 수집되는 정보에 민감한 정보인 사생활 영상이 담긴 IP Camera의 정보를 탈취하여 영상을 불법 촬영하고 유포하는 사건이 발생하게 되면서 데이터를 안전하게 보호할 필요성이 증가하였다. 이에 악의적 사용자가 특정 IoT에 접근하는 것을 차단하기 위해 사용자와 장치 간의 그룹 ID를 생성하여 이 ID를 통해 그룹을 구성한다. 사용자는 인증 서버를 통해 사용자 정보 등록 및 IoT 등록 요청을 하게 되면 서버는 요청에 따른 그룹 ID를 생성하게 되고 이를 블록체인에 저장한다. 사용자는 서버를 통해 IoT 장치를 인증하고 데이터를 전송할 수 있다. 이는 그룹 ID를 통해 사용자와 IoT 장치를 관리하여 악의적 사용자가 해당 IoT에 장치에 대한 정보를 탈취하더라도 장치에 대한 접근은 차단할 수 있다[3].

또한 금융, 자동차, 항만 물류 분야에서도 사용된

다. 금융 분야에서는 주로 화폐에 많이 응용되고 전자 화폐 네트워크에서 일어나는 거래를 기록하여 관리하는 분산 데이터베이스의 형태로 사용된다. 자동차 분야에서는 차량 간(V2V) 및 차량과 네트워크 간(V2X)에 적용되고 항만 물류 분야는 거래 원장을 분산하여 저장하고 데이터 위변조가 어려운 블록체인 특징에 적합하다. 제품의 생산부터 최종 소비까지 공급 이력이 투명하게 공개되어 소비자들에게 제품에 대한 신뢰도를 높여준다[4].

블록체인은 중앙 제어 장치 없이 데이터를 저장 및 전송하고 네트워크 내에서 거래된 정보를 블록체인 내 연결된 네트워크에 분산하여 저장하고 관리하는 기술이다. 블록체인은 퍼블릭 블록체인과 프라이빗 블록체인으로 분류된다. 퍼블릭 블록체인은 각 참여자가 합의를 만드는 과정에 참여할 수 있고 프라이빗 블록체인은 허가된 참여자만 합의를 만드는 과정에 참여할 수 있다[5].

블록체인 기술이 발달함에 따라 사이버 범죄자의 공격 대상이 되고 있다. 특히 이메일이나 웹사이트 또는 둘 다 사용하여 사용자 자격 증명을 도용하는 피싱 공격 시도가 점차 증가하고 있다. 이는 시스템의 취약점을 노리면서 사용자의 부주의함도 함께 노린다. 피싱 공격은 사용자가 특정 작업(악성 파일 다운로드, 인증되지 않은 링크 이동 등)을 수행한 후 활성화된다. 여러 피싱 공격 중 가짜 지갑 앱을 앱 스토어에 배치하는 공격이 있다. 사용자는 정상 앱이라 생각하고 설치하고 악성 앱을 실행하게 된다. 이때 악성 앱은 공격자의 공개 주소를 네트워크 주소로 표시하고 생성된 사용자의 개인 키는 공격자가 가지게 된다. 사용자는 자신의 암호화폐를 입금하기 위해 주소로 자금을 보내면 개인 키가 없기에 사용자는 자금을 출금할 수 없는 상황을 맞이하게 된다[6].

전자지갑은 블록체인을 거래하는 데 사용되는 소프트웨어 패키지이다. 전자지갑은 하나 이상의 고유한 암호화폐 공용 주소를 저장한다. 공용 주소는 대소문자 및 숫자와 문자를 조합한 16진수 문자열로 이루어진다. 암호화폐를 받기 위해서는 공개적으로 공유되어야 하고 블록체인에 직접 연결하게 된다. 이렇게 연결된 지갑은 사용자가 트랜잭션을 읽고 블록체인에 제출할 수 있게 한다[7].

전자지갑은 항상 네트워크에 연결되어있는 스마트폰 앱이나 PC로 접속 가능한 핫월렛과 USB나 개인 키를 인쇄한 종이 등 인터넷에 연결되지 않은 오프라인의 형태인 콜드 월렛으로 분류된다. 웹 브라우저를 통해 지갑에 접근하는 온라인 지갑은 전자지갑에 대한 모든 권한이 제3자 또는 중앙 기관에 있어서 중앙 기관이 공격받게 되면 자신이 가지고 있던 전자지갑에 대한 권한을 잃어버릴 수 있다. 인터넷이 연결된 모든 장소에서 접근이 가능한 모바일 지갑은 다른 유형의 지갑보다 사용하기 쉽지만, 모바일 장치에는 사용자의 취약한 PIN 잠금 설정과 기기의 OS의 최신 버전 미설치로 인한 취약점이 존재하고 모바일 지갑 앱에는 모바일 스마트 장치를 통한 전자지갑과 연결하는 서드파티의 S/W 및 페어링 장치의 취약점이 있다[8]. 데스크탑 전자지갑의 개인 키는 사용자의 컴퓨터에 저장되어 쉽게 사용되지만, 시스템 문제로 모든 데이터가 손실될 수 있기에 정기적인 백업이 필요하다. 하드웨어 지갑은 USB에 전자지갑 소프트웨어가 포함된 형태이다. 다른 유형의 지갑보다 안전하게 보관되지만 한번 잃어버리게 되면 복구가 어렵다는 단점이 있다. 종이 지갑은 컴퓨터에 연결하지 않고 공개 키와 개인 키를 종이에 인쇄하여 사용하게 된다. QR 코드를 사용하여 모든 거래에 사용한다. 다만, 거래를 완료하기 위해 많은 시간이 걸리며 하드웨어 지갑과 같이 분실 또는 도난에 대한 문제가 있다[9].

또한, 전자지갑은 개인 키 관리 미흡, 해킹에 취약한 핫월렛 저장소 사용, 개인 키가 저장된 온라인 서버 해킹 등 전자지갑의 보안 체계가 허술한 점을 대상으로 한 해킹 사례가 증가하고 있다. 그중에 사용자의 관리 미흡으로 인한 개인 키 도용 문제는 공격자가 지갑에 대한 접근 권한을 상승시켜 거래 승인과 자산 이동을 불가능하게 막는다[10].

3. 연구 내용

블록체인 환경에서 사용되는 전자지갑 내 개인 키는 네트워크에 접근하기 위한 중요한 요소이다. 블록체인 네트워크 내 참여한 사용자의 개인 키 정보가 저장되어 있어야 트랜잭션을 요청할 수 있다. 사용자는 참여한 네트워크에서 트랜잭션 승인을 요청하기 위해 전자지갑 내 저장된 개인 키를 통한 전자서명 과정을 거친다. 전자서명을 통해 사용자 인증을 하게 된다. 이때, 중앙 기관이나 제3자를 통해 사용자 인증을 받는 경우, 서드파티 취약점에 영향을 받을 수 있다. 중앙 기관에서 사용자 인증 요청에 대한 검증을 거칠 때 사용되는 S/W에서 문제가 발생한다. 이는 최신 버전의 S/W를 사용하지 않거나

오픈소스 코드를 그대로 인용하여 취약한 부분이 존재한다. 취약한 부분을 공격자가 노리고 침투하고 악성 앱을 설치한다. 전자지갑 사용자가 사용자 인증을 요청하면 검증에 사용되는 S/W가 사용되면서 전자지갑에 대한 정보가 노출되게 된다. 공격자는 수집한 정보를 통해 전자지갑의 권한을 상승시켜 사용자의 접근을 막아 더 이상 사용하지 못하게 한다.

따라서 취약점에 대한 보안 조치로 첫째, 사용자 인증 후 접속 시간을 제한한다. 사용자가 블록체인 네트워크에 참여한 후 일정 시간이 지나면 자동으로 인증이 해제되도록 한다. 둘째, 일정 주기마다 사용자를 인증한다. 네트워크 내 일정한 시간과 주기를 설정하여 참여하고 있는 사용자에 대한 무결성을 검증한다. 셋째, 중앙 기관의 주기적인 S/W 업데이트를 통해 최신 공격 유형에 대해 사전에 방어하고 공격자가 침투하지 못하도록 한다. 넷째, 서드파티에서 제공하는 S/W를 별도로 관리하는 모듈을 사용하여 전자지갑의 보안을 강화한다.

4. 기대효과 및 향후 과제

본 논문은 블록체인 환경에서 발생하는 전자지갑에 대한 취약점을 분석하고 대응 방안을 제안하였다. 대응 방안으로 제시한 생체 인증방식 외에도 사용자 신원을 증명하는 DID 인증, 다중 인증방식을 적용한 전자지갑 연구가 지속해서 이루어지고 있다. 추후 연구에서는 현재 지속해서 이루어지고 있는 사용자 인증방식을 활용하여 전자지갑을 보호하고 제안한 방법을 테스트하여 검증하여 안전하게 정보를 교류할 수 있도록 블록체인 환경을 구성하는 연구를 진행할 것이다.

이 논문은 홍익대학교의 '지역특화형 스마트시티 전문대학원 구축 사업'의 지원을 받아 수행된 결과입니다.

참고문헌

[1] 민연아. "사물인터넷 (IoT) 환경의 보안성강화를 위한 블록체인 적용가능성 연구." (2020).

[2] Ahmad, Irfan, et al. "Survey on IoT: security threats and applications." Journal of Robotics and Control (JRC) 2.1 (2021): 42-46.

[3] 박지호, 맹주현, and 조인휘. "스마트 홈 환경에서 IoT 장치의 보안 강화를 위한 Hyperledger Fabric 기반 Architecture." 한국정보처리학회 학술대회논문집 28.1 (2021): 93-95.

[4] Choi, Jongseok, et al. "블록체인 기반 탈중앙화 사물인터넷 플랫폼 연구." Review of KIISC 27.6 (2017): 5-14.

[5] Guegan, Dominique. "Public blockchain versus private blockhain." (2017).

[6] Andryukhin, A. A. "Phishing attacks and preventions in blockchain based projects." 2019 International Conference on Engineering Technologies and Computer Science (EnT). IEEE, 2019.

[7] Suratkar, Saurabh, Mahesh Shirole, and Sunil Bhirud. "Cryptocurrency wallet: A review." 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP). IEEE, 2020.

[8] Bosamia, Mansi, and Dharmendra Patel. "Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures." Int. J. Comput. Sci. Eng 7.1 (2019): 810-817.

[9] Jokić, Stevo, et al. "Comparative analysis of cryptocurrency wallets vs traditional wallets." Ekonomika 65.3 (2019): 65-75.

[10] Yeom, Gwyduk. "Blockchain-Based Mobile Cryptocurrency Wallet." Journal of The Korea Society of Computer and Information 24.8 (2019): 59-66.

[11] 조병철, and 박종만. "다중 생체인식 기반의 인증기술과 과제." 한국통신학회논문지 40.1 (2015): 132-141.