2025년도 한국통신학회 하계종합학술발표회

에어갭 트랜잭션 기반 하드웨어 지갑의 트랜잭션과 펌웨어 분석

오윤석, 신용호, 최형기*
성균관대학교

ysoh1205@g.skku.edu, base@g.skku.edu, meosery@skku.edu

Analysis of Transactions and Firmware in Air-gapped Transaction Based Hardware Wallets

Yoon-Seok Oh, Yong-Ho Shin, Hyoung-Kee Choi*
Sungkyunkwan Univ.

요 약

본 논문은 에어갭 트랜잭션 기반 하드웨어 지갑의 트랜잭션과 펌웨어 업데이트 과정을 분석하여 발생할 수 있는 공격 가능성을 제시한다. 트랜잭션 서명은 QR 코드를 통해 오프라인으로 처리되며, 펌웨어는 WebUSB 를 통해 암호화된 형태로 전달된다. 분석 결과, 세션키 노출과 펌웨어 다운그레이드 취약점이 확인되었고, 향후 부트로더의 우회를 거쳐 악성 펌웨어의 설치 가능성을 제시한다.

Ⅰ. 서 론

암호화폐의 자산 가치가 증가함에 따라, 사용자의 개인키를 안전하게 보관할 수 있는 하드웨어 지갑의 중요성이 강조되고 있다[1]. 이러한 지갑은 인터넷과의 직접적인 연결을 차단한 에어갭 환경을 도입하여, 트랜잭션 서명 과정에서도 비밀키가 외부로 노출되지 않도록 설계된다. 이와 같은 격리 구조는 소프트웨어 기반 공격을 차단하는 데 효과적이며, 공격자가 키를 탈취하기 위해 물리적인 접근을 강제한다.

일부 기기에는 anti-tamper 기술이 적용되어 있어, 디버깅 인터페이스나 테스트 핀을 통한 하드웨어 해킹 시도가 어렵다[2]. 하지만 펌웨어 업데이트 과정을 악용한 공격은 여전히 이루어질 수 있다.

본 논문에서는 Keystone 3 하드웨어 지갑의 에어갭 트랜잭션과 펌웨어 업데이트 절차를 분석하고, 이를 바탕으로 발생할 수 있는 보안 취약점 및 공격 가능성을 제시함으로써, 에어갭 장치의 실질적인 보안 수준을 평가한다.

Ⅱ. 본론

하드웨어 지갑의 안정성을 분석하기 위해, 대상 기기의 키 생성 과정, 트랜잭션 처리 방식, 그리고 펌웨어 업데이트 절차에 대해 기술적 분석을 수행하였다.

1. 하드웨어 지갑의 키 생성 과정 분석

암호화폐의 소유와 전송에는 개인키가 필요하며, 이는 유출 시 자산 탈취로 직결된다. 따라서 개인키를 생성하고 안전하게 보관하는 것은 암호화폐 사용자의 보안에서 중요하다.

하드웨어 지갑은 BIP39 표준으로 12 개 혹은 24 개의 단어로 구성된 니모닉 문구가 생성하고, PBKDF2-HMAC-SHA512 함수를 거쳐 512 비트의 시드가 생성된다[3]. 이 시드는 BIP32 표준을 기반으로 다수의 주소와 키 쌍이 생성된다[4]. 대상 기기인 Keystone 3 는 사용자의 시드 정보를 하드웨어키로 암호화하여 보안칩에 저장한다.

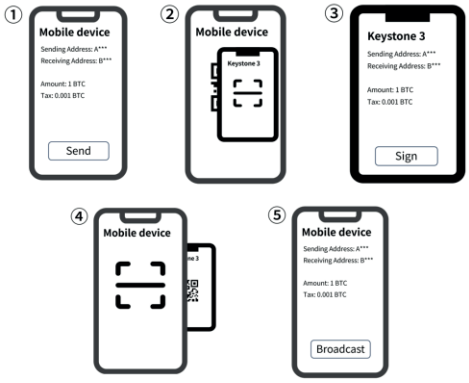

그림 1. 트랜잭션 수행 과정

2. 에어갭 트랜잭션 과정 분석

에어갭 트랜잭션은 인터넷과 분리된 상태로 동작하므로, 하드웨어 지갑은 블록체인 네트워크의 최신 상태를 실시간으로 확인하거나 트랜잭션을 구성하는 기능을 자체적으로 수행할 수 없다. 그러므로 모바일 디바이스와 같이 외부 네트워크에 연결된 장치가 트랜잭션을 생성해야 한다. 이후 하드웨어 지갑은 해당 트랜잭션 정보를 QR 코드 등 오프라인 매체로 전달받아 서명을 수행하며, 이때 기기에 저장된 BIP32 시드로부터 파생된 개인키가 사용된다[5].

그림 1 의 트랜잭션 수행 과정은 다음과 같다:

① 모바일 디바이스가 트랜잭션을 구성하여 Uniform Resource (UR) [6] 인코딩 형식으로 QR 코드를 생성
② 하드웨어 지갑이 QR 코드를 인식하여 트랜잭션을 취득
③ 하드웨어 지갑이 트랜잭션을 서명하여 UR 인코딩 형식으로 QR 코드를 생성
④ 모바일 디바이스가 QR 코드를 인식하여 서명된 트랜잭션을 취득
⑤ 모바일 디바이스가 트랜잭션을 네트워크로 분산

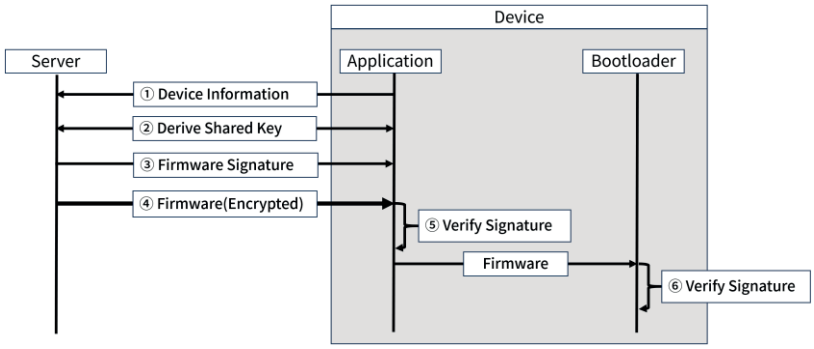

그림 2. 펌웨어 업데이트 과정

3. 펌웨어 업데이트 과정 분석

Keystone 3 의 펌웨어 업데이트는 보안을 위해 네트워크 기반 직접 업데이트를 차단하고, 공식 웹사이트의 WebUSB API 를 통해서만 수행된다. WebUSB API 는 브라우저에서 USB 장치와 직접 통신할 수 있도록 만든 표준으로, 안전한 펌웨어 전송 경로를 제공한다[7]. 이는 공격자가 임의의 펌웨어를 주입하지 못하도록 하기 위한 설계이다.

그림 2 의 펌웨어 업데이트 과정은 다음과 같다:

① Keystone 3 디바이스 정보 수집
② Eliptic Curve Diffie-Hellman (ECDH) 세션키 교환
③ 펌웨어의 해시 및 서명 디바이스에 전달
④ AES256 암호화된 펌웨어 전송
⑤ 복호화 후 해시·서명 검증
⑥ 부트로더가 서명 최종 검증

업데이트를 수행한 결과, ②단계에서 생성된 ECDH 세션키가 ④단계 중 브라우저에 노출되는 문제가 확인되었다. 또한 펌웨어 전송을 중단하면 디바이스가 세션키를 초기화하지 않아, 공격자가 동일한 키로 임의 펌웨어를 전달할 가능성이 생겼다. 그러나 ⑤단계 서명 검증과 ⑥단계 부트로더 검증 절차로 인해 서명되지 않은 바이너리는 설치되지 않았다.

4. 공격 가능성 분석

Keystone 3 의 펌웨어 다운그레이드를 통해 서명 검증을 우회할 수 있다. 실험 대상의 버전(1.8.2)에는 ⑤단계 검증 절차가 포함되어 있지만, 초기 버전(예: 1.1.0)에는 해당 로직이 없었다. 이로 인해 공격자는 구버전으로 다운그레이드한 뒤, 서명 없이 임의의 펌웨어를 로딩할 수 있다.

부트로더 로직을 우회하거나 변경하는 가능성도 존재한다. Keystone 3 는 ⑥단계에서 서명 확인 절차를 포함하고 있으나, 만약 공격자가 디바이스에 직접 접근해 부트로더를 수정할 경우 이 절차도 우회될 수 있다. 이와 관련하여 ARM SoC 를 대상으로 UART 부트모드를 활성화한 선행 연구가 있다[8]. 또한, 실제 하드웨어 지갑인 Ledger Nano S 기기의 부트로더를 우회하여 임의의 펌웨어를 설치하는 공격이 시연된 바가 있다[9].

Ⅲ. 결론

본 논문에서는 에어갭 환경을 갖춘 하드웨어 지갑을 대상으로 트랜잭션 처리 및 펌웨어 업데이트 과정을 분석하였다. 이를 통해 발생 가능한 공격 시나리오를 정리하였으며, 향후 연구에서는 부트로더 검증 절차를 우회하여 실제로 악성 펌웨어가 설치될 수 있음을 입증할 계획이다.

ACKNOWLEDGMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과 임 (No. RS-2024-00398745, 디지털 환경에서의 증거인멸행위 증명 및 대응 기술 개발)

참 고 문 헌

[1] Hardware Wallet Market Size and Trends, https://www.coherentmarketinsights.com/market-insight/hardware-wallet-market-5101

[2] Staat, Paul, et al. "Anti-tamper radio: System-level tamper detection for computing systems." 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022.

[3] BIP 0032, https://en.bitcoin.it/wiki/BIP_0032

[4] BIP 0039, https://en.bitcoin.it/wiki/BIP_0039

[5] Ever Wondered What Your Hardware Wallet Inputs and Outputs? , https://blog.keyst.one/ever-wondered-what-your-hardware-wallet-inputs-and-outputs-9b33b4cedafd

[6] Uniform Resources (UR), https://github.com/BlockchainCommons/Research/blob/master/papers/bcr-2020-005-ur.md

[7] WebUSB API, https://wicg.github.io/webusb/

[8] Bittner, Otto, et al. "The forgotten threat of voltage glitching: a case study on Nvidia Tegra X2 SoCs." 2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC). IEEE, 2021.

[9] Thomas Roth, Dmitry Nedospasov, and Josh Datko. (2018) Hacking the most popular cryptocurrency hardware wallets. Video. [Online]. Available: https://media.ccc.de/v/35c3-9563-wallet_fail