한국융합보안학회 2025년 추계학술대회 논문집

# 공공 USB 충전 인프라의 취약성과 안드로이드 주스재킹 연구

성민욱[1]*, 유한영[1], 홍영재[1] ,이병천[1]

중부대학교[1]

# Vulnerabilities of Public USB Charging Infrastructure: A Study on Android Juice Jacking

Minwook Seong[1]*, Hanyoung You[1], Youngjae Hong[1] , Byoungcheon Lee[1]

요약: 스마트폰 사용자가 공항이나 지하철 등의 공용 USB 충전 포트를 이용할 때, 충전 케이블을 통해 악성코드가 설치되거나 데이터가 몰래 복제되는 이른바 주스 재킹(Juice Jacking) 공격의 위험성이 대두되고 있다 본 연구에서는 안드로이드 스마트폰 환경을 중심으로 주스재킹 공격의 원리와 사례를 분석한다. 특히 공개 소스(open-source)를 활용한 악성코드로 실제 공격 시나리오를 구현함으로써, 사용자가 무심코 충전 케이블을 연결했을 때 초래될 수 있는 보안상의 피해를 살펴본다. 끝으로 이러한 공격에 대비하기 위한 대응 방안과 예방책을 제시한다.

Key Words: Juice Jacking(주스재킹), USB Charging Security(USB 충전 보안), Android Malware(안드로이드 악성코드), Mobile Device Security(모바일 기기 보안)

## 1. 서론

공공장소의 USB 충전 포트는 스마트폰 배터리 소모가 잦은 현대인에게 필수적인 편의 시설로 자리 잡았다. 그러나 USB 케이블은 전원 공급과 데이터 전송 기능을 동시에 수행하도록 설계되었기에, 이러한 공용 충전 인프라가 보안상 취약점으로 악용될 수 있다. 이른바 '주스재킹(Juice Jacking)'은 악의적으로 조작된 충전기나 케이블에 기기를 연결했을 때, 사용자 모르게 데이터를 탈취하거나 악성코드를 설치하는 사이버 공격 기법을 지칭한다.

주스재킹의 잠재적 위험성은 2011년 미국 데프콘(DefCon) 해킹 컨퍼런스에서 처음으로 대중에게 알려졌다. 당시 무료 충전소로 위장한 키오스크는 연결된 기기에 경고 메시지를 띄워 공용 포트의 위험을 환기시켰다. 이후 2013년 블랙햇(Black Hat) 보안 컨퍼런스에서는 '막탄스(Mactans)'라는 공격 시연을 통해, 악성 충전기에 연결하는 것만으로 1분 내에 기기가 악성 앱에 감염될 수 있음이 입증되었다. 이러한 초기 연구들은 단순한 충전 행위가 신용카드 정보 유출이나 랜섬웨어 감염과 같은 심각한 보안 사고로 이어질 수 있음을 명확히 보여주었다.

한편, 이러한 위협에 대응하여 스마트폰 운영체제(OS) 제조사들은 보안 기능을 대폭 강화했다. 최신 스마트폰은 낯선 기기와 USB로 연결될 때 "이 기기를 신뢰하시겠습니까?"와 같은 명시적인 사용자 동의를 얻도록 절차를 개선하여, 임의의 데이터 접근을 차단하고 있다. 이 때문에 현재까지 주스재킹이 실제 환경에서 성공했다는 공식적인 보고는 확인되지 않고 있다. 그럼에도 불구하고, 미국 FBI와 같은 기관들은 잠재적 위험을 근거로 공항 등 공공장소의 USB 포트 사용 자제를 지속적으로 권고하며 2023년에도 관련 경고를 갱신한 바 있다.

본 논문은 이러한 배경을 바탕으로, 현재의 보안 기술 환경에서 안드로이드 스마트폰을 대상으로 한 주스재킹 공격의 구체적인 방법론을 분석하고, 그 잠재적 영향과 현실적인 보안 대책을 심도 있게 다루고자 한다.

## 2. 본론

### 2.1 주스재킹 공격 원리

주스재킹 공격은 전력 공급과 데이터 전송이라는 USB의 이중적 기능을 악용하는 데서 출발한다. 사용자가 스마트폰을 충전기에 연결하면 전력 공급과 함께 데이터 통신 채널이 열리게 되는데, 공격자는 이 과정에서 형성되는 암묵적인 신뢰 관계를 파고든다. 겉보기에는 평범한 충전 과정처럼 보이지만, 이면에서는 악성 페이로드(payload)를 주입하거나 기기에 저장된 민감 정보를 유출하는 것이다.

공격의 양상은 크게 두 가지로 나타난다. 하나는 연락처, 사진, 인증 정보와 같은 민감 데이터를 무단으로 복제하는 '데이터 탈취'이며, 다른 하나는 트로이목마나 랜섬웨어 등의 악성 앱을 설치하여 기기를 원격으로 제어하거나 지속적인 정보 유출을 시도하는 '악성코드 주입'이다. 이러한 공격은 사용자가 인지하기 어려운 백그라운드에서 은밀하게 이루어지므로 치명적인 보안 침해로 이어질 수 있다.

특히 안드로이드 운영체제는 개방적인 플랫폼 특성상 공격 표면이 상대적으로 넓어 다양한 악용 시도가 가능하다. 일례로, P2P-ADB 공격 기법은 USB OTG(On-The-Go) 기능을 이용해 공격자의 기기를 피해자의 기기에 직접 연결하여, 잠금 상태의 스마트폰을 해제하고 구글 계정 토큰과 같은 핵심 데이터를 탈취할 수 있음을 실증한 바 있다. 이처럼 주스재킹은 USB 연결을 매개로 스마트폰의 보안 통제를 우회하는

다양한 시나리오를 포괄하며, 사용자가 케이블을 연결하는 행위 자체가 잠재적인 공격의 기회가 될 수 있다[1].

2.2 공격 구현 사례 및 실험 계획

본 연구에서는 주스재킹 공격의 실효성을 검증하기 위해, 공개된 오픈소스 악성코드를 이용한 공격 시연 환경을 구축한다. 실험 시나리오는 공격자가 라즈베리파이와 같은 소형 컴퓨터를 악성 충전 스테이션으로 위장하고, 사용자가 스마트폰을 연결하면 사전에 준비된 악성코드가 자동으로 전송 및 설치되도록 설계하였다.

공격 페이로드로는 안드로이드 원격관리 도구(RAT, Remote Administration Tool)인 'AndroRAT'을 활용한다[2]. AndroRAT은 본래 학술 연구 목적으로 개발된 오픈소스 툴이지만, 강력한 원격 제어 기능으로 인해 사이버 범죄에 악용되어 왔다. 이 악성코드는 사용자 모르게 앱을 설치하거나 쉘 명령 실행, Wi-Fi 비밀번호 수집, 화면 캡처 등 광범위한 악성 행위가 가능하다[2].

본 실험에서는 AndroRAT을 일부 수정한 악성 앱(APK)을 제작하여, USB 디버깅 옵션이 활성화된 안드로이드 기기를 공격 대상으로 삼는다. 공격 스테이션은 기기가 연결되면 ADB(Android Debug Bridge)를 통해 장치를 인식하고, 'adb install' 명령어로 악성 앱을 강제 설치하는 방식으로 작동한다. 최신 안드로이드 버전에서는 ADB 연결 시 사용자 확인을 요구하므로, 본 실험 환경에서는 사용자가 '허용'을 누를 수밖에 없는 사회공학적 상황을 가정한다. 악성 앱 설치가 완료되면, 공격자는 C&C(Command & Control) 서버를 통해 감염된 기기에 원격으로 접속하여, 개인정보 탈취, 위치 추적, 추가 명령 실행 등 2차 공격을 수행할 수 있다. 본 구현 실험은 사용자가 신뢰할 수 없는 USB 포트에 기기를 연결하는 일상적인 행위가 어떤 구체적인 보안 위협으로 이어질 수 있는지 실증적으로 보여주는 것을 목표로 한다.

2.3 대응 및 방어 대책

주스재킹은 사용자의 단순한 충전 행위만으로도 악성 행위가 개입될 수 있다는 점에서 예방 중심의 접근이 요구된다.

가장 확실한 방어책은 사용자 수준에서 시작된다.

공공 USB 포트 사용을 지양하고, 개인 AC 어댑터나 보조 배터리를 활용하는 것이 최선이며, 부득이한 경우 데이터 전송을 물리적으로 차단하는 USB 데이터 차단기(일명 'USB 콘돔')를 사용하는 것이 효과적이다[3].

또한 USB 디버깅과 같은 개발자 옵션을 비활성화하고, 신뢰할 수 없는 기기에 대한 접근 허용 요청을 무분별하게 승인하지 않는 기본적인 보안 수칙을 생활화해야 한다.

운영체제 수준에서도 기술적 개선이 필요하다.

'초이스재킹(ChoiceJacking)'과 같이 사용자 동의 절차 자체를 무력화하는 지능형 공격 기법이 보고되고 있으므로[4], 이에 대응하기 위한 OS 프로토콜의 근본적 강화, 데이터 전송 경로 모니터링, 악성 행위 탐지 기술의 내재화가 요구된다.

나아가 공항·지하철 등 공공 충전 인프라에는 신뢰성 있는 인증 체계와 관리 표준이 마련되어야 하며, 사용자의 보안 인식을 제고하기 위한 공공 캠페인 및 교육 프로그램이 병행되어야 한다.

## 3. 결론

본 연구는 충전이라는 일상적 행위를 악용한 주스재킹(Juice Jacking) 공격의 개념을 분석하고, 안드로이드 환경에서의 공격 구현과 대응 전략을 고찰하였다.

현재까지 공식적인 피해 사례는 보고되지 않았으나, 구형 기기와 낮은 보안 인식은 여전히 잠재적 위협 요인으로 남아 있다.

향후 연구에서는 OS 수준의 능동형 방어 기술과 공공 인프라의 보안 표준화 방안, 그리고 사용자의 보안 인식 제고를 위한 실증적 교육 프로그램 개발이 필요하다.

본 연구가 이러한 기술적·정책적 논의의 기반이 되길 기대한다.

## 참고문헌

[1] Singh, D., Biswal, A. K., Samanta, D., Singh, D., and Lee, H. N., “Juice Jacking: Security Issues and Improvements in USB Technology,” Sustainability, Vol. 14, No. 2, 2022, Article 939.

[2] Zhang, V., Gu, J., and Shen, S., “New AndroRAT Exploits Allow for Permanent Rooting,” Trend Micro Research, Feb. 2018.

[3] Kumar, Y., “Juice Jacking – The USB Charger Scam,” Cybersecurity and Public Sufferings Conference, St. Petersburg, 2020

[4] M. S. Ahmad, et al., “Choicejacking: Interactively attacking and repairing authentication-bypass vulnerabilities in android,” in Proc. 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 1435-1542.