

주스 재킹(Juice Jacking) 연구와 삼성 DeX 기반 신규 공격 시나리오

USB 충전 포트를 통한 데이터 탈취 위협과 DeX 기능 악용 공격 시나리오 연구

T.ACE 유한영 성민욱 홍영재



목차

1. 연구 배경 및 목표

- 공공장소 USB 충전 포트의 보편화
- 데이터 탈취 시 파급력 증대
- 현실적 공격 시나리오 발굴 목표

2. 주스 재킹의 개념

- 주스 재킹이란?
- 주스 재킹의 공격 원리
- 가능한 공격 유형
- 주스 재킹의 한계점

3. 기존 연구 및 한계점 분석

- Choice Jacking (초이스 재킹)
- Bluetooth/HID 모듈 활용
- 승인 팝업 우회 기법
- 기술적/현실적 한계

4. 새로운 접근법: DeX-Jacking

- 삼성 DeX 기능 취약점
- 화면 이원화 & 독립 실행 환경
- 은밀한 데이터 탈취 가능성

5. 공격 시나리오 실증

- 실험 장비 구성
- 시연 영상
- 특이점 분석

6. 보안 위협 및 대응 방안

- 스마트폰 편의 기능에 보안 취약성
- 제조사 및 사용자 대응 방안

연구 배경 및 목표

보안 위협의 증가

- 2019년 미국 LA 검찰과 2023년 FBI·FCC까지 공공 USB 포트 사용에 대한 경고 발표
- 공공장소 USB 충전 포트가 보편화되면서 주스 재킹 위협 증가
- 사용자들의 충전 포트에 대한 무분별한 신뢰

연구 목표

- 기존 주스 재킹 공격의 현실적 한계를 검증
- 주스 재킹의 현실적인 공격 시나리오 발굴
- 보안적 시사점 도출 및 대응 방향 제안

지하철역 무료 충전기 쓰면 '악성코드' 감염?... '주스 재킹' 주의보

공공 와이파이 사용 중 개인정보 입력 금지
"공공장소 비치된 충전기 가급적 이용 자제"

박민정 기자 mftth@kgnews.co.kr | 등록 2025.06.15 14:45:05



IT·산업 입력 2024.07.22 14:18

공공장소 USB 충전 해킹 '주스재킹' 주의보

국가사이버안보센터, 글로벌 보안 동향 발표

시스코 이메일 취약점, 새로운 백도어 배포, 공공장소 USB 충전기 해킹 등 6건

카페·공항 속 충전기가 해킹 통로?... '주스 재킹' 다시 고개

연합뉴스 | 2025.09.23 (화) 15:17

1 2

공공 장소의 USB 충전기를 통한 해킹 수법 '주스 재킹'과 '초이스 재킹'의 위험이 다시 주목받고 있다. 전문가들은 여행철 공용 충전기 사용 자제와 함께 보안 강화 조치를 촉구했다.

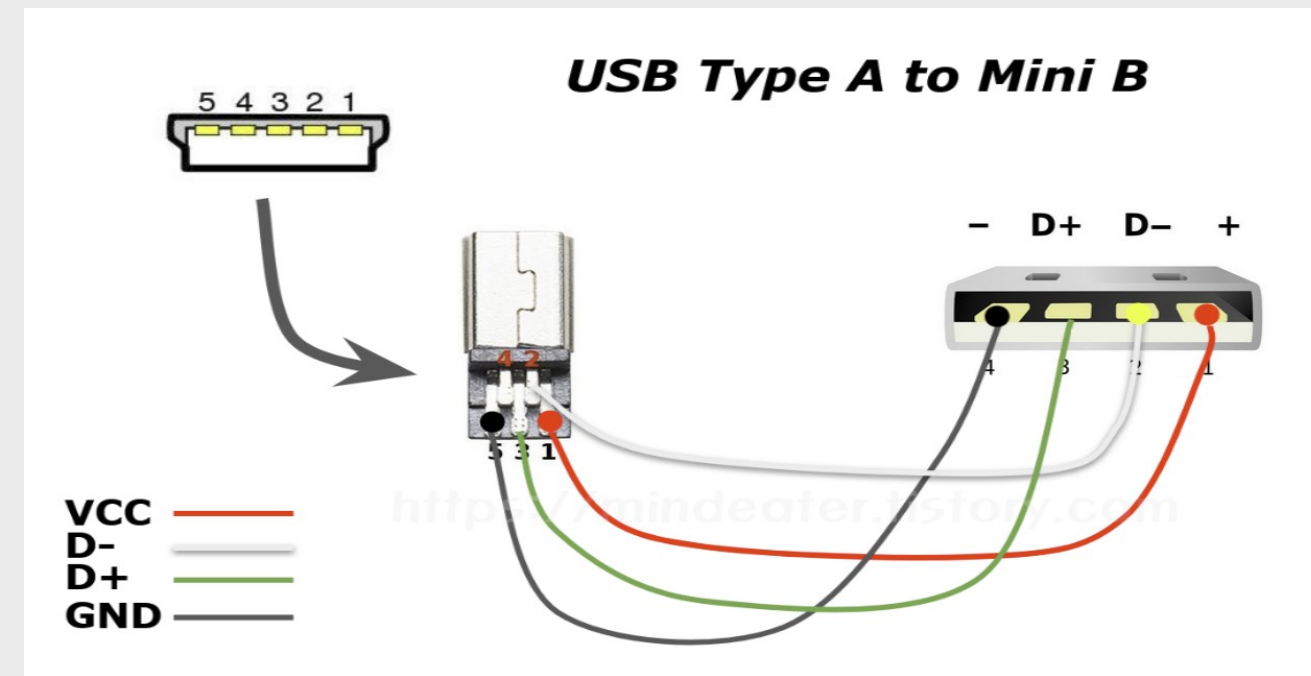
주스 재킹의 개념

주스 재킹(Juice Jacking)이란?



- 충전 포트(USB)를 통해 데이터 핀에 접근하여 악성코드를 설치하거나 데이터를 탈취하는 공격
- 동일한 USB 케이블이 전원(Vbus/GND)과 데이터(D+/D-) 전송을 모두 지원하는 구조를 가진 특성 악용

USB 케이블의 구조와 공격 원리



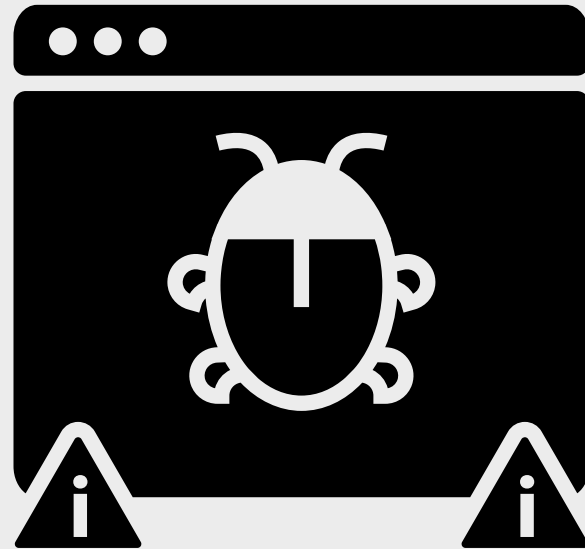
- USB 케이블은 전원 핀(VCC/GND)과 데이터 핀(D+/D-)으로 구성
- 전원(VBUS) + 데이터(D+/D- 등)"를 같은 케이블/포트로 동시에 제공
- 공격자는 데이터 경로를 열어 사용자 승인 유도, 취약점 악용, 악성 주변 기기 행세를 노림

주스 재킹의 공격 유형



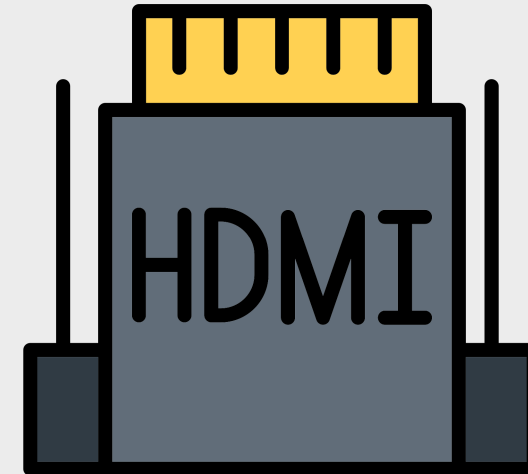
데이터 탈취

- 개인 데이터 복사
- 민감 정보 추출 (연락처, 사진)
- 계정 정보 및 비밀번호 탈취



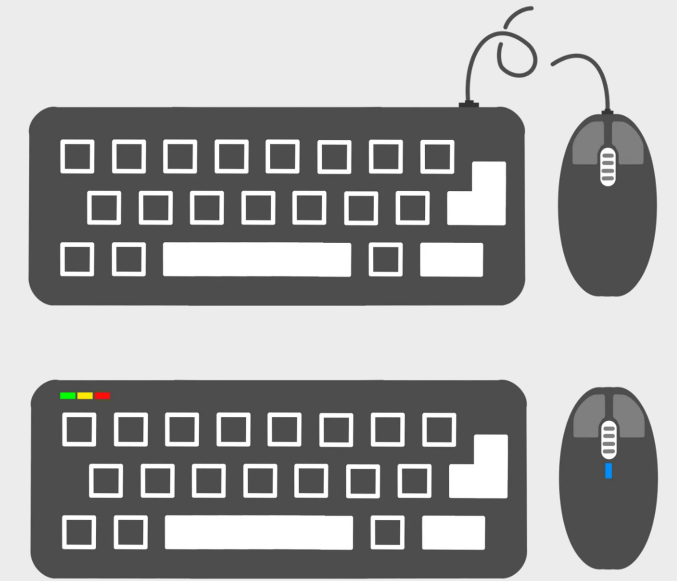
악성 앱 설치

- 스파이웨어 설치
- 원격 제어 악성코드 주입
- 랜섬웨어



화면 미러링

- HDMI를 이용한 화면 복제
- 사용자 입력 정보 모니터링
- 비밀번호, 결제 정보 등 탈취



입력 장치 위장

- 키보드/마우스처럼 인식
- 사용자 입력처럼 명령 주입
- 드라이버 설치 없이 즉시 인식



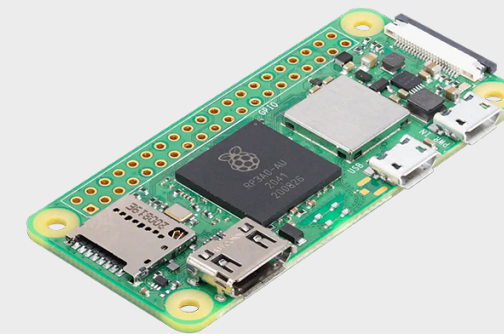
운영체제(OS)의 보안 정책 강화

"이 기기를 신뢰하시겠습니까?" 팝업 우회

최신 스마트폰 운영체제는 USB 연결을 단순한 충전 행위가 아닌 잠재적인 보안 위협으로 인식하여, 전원 공급과 데이터 통신을 명확히 분리하고 기본적으로 충전 전용 모드로 동작하도록 설계되어 있다. 이로 인해 USB를 통해 파일 전송, 입력 장치 인식, 디버깅 등의 데이터 통신을 시도할 경우 운영체제가 강제로 “이 기기를 신뢰하시겠습니까?”와 같은 사용자 승인 팝업을 표시하며, 사용자가 직접 이를 허용하지 않는 한 모든 데이터 채널은 논리적으로 차단된다.

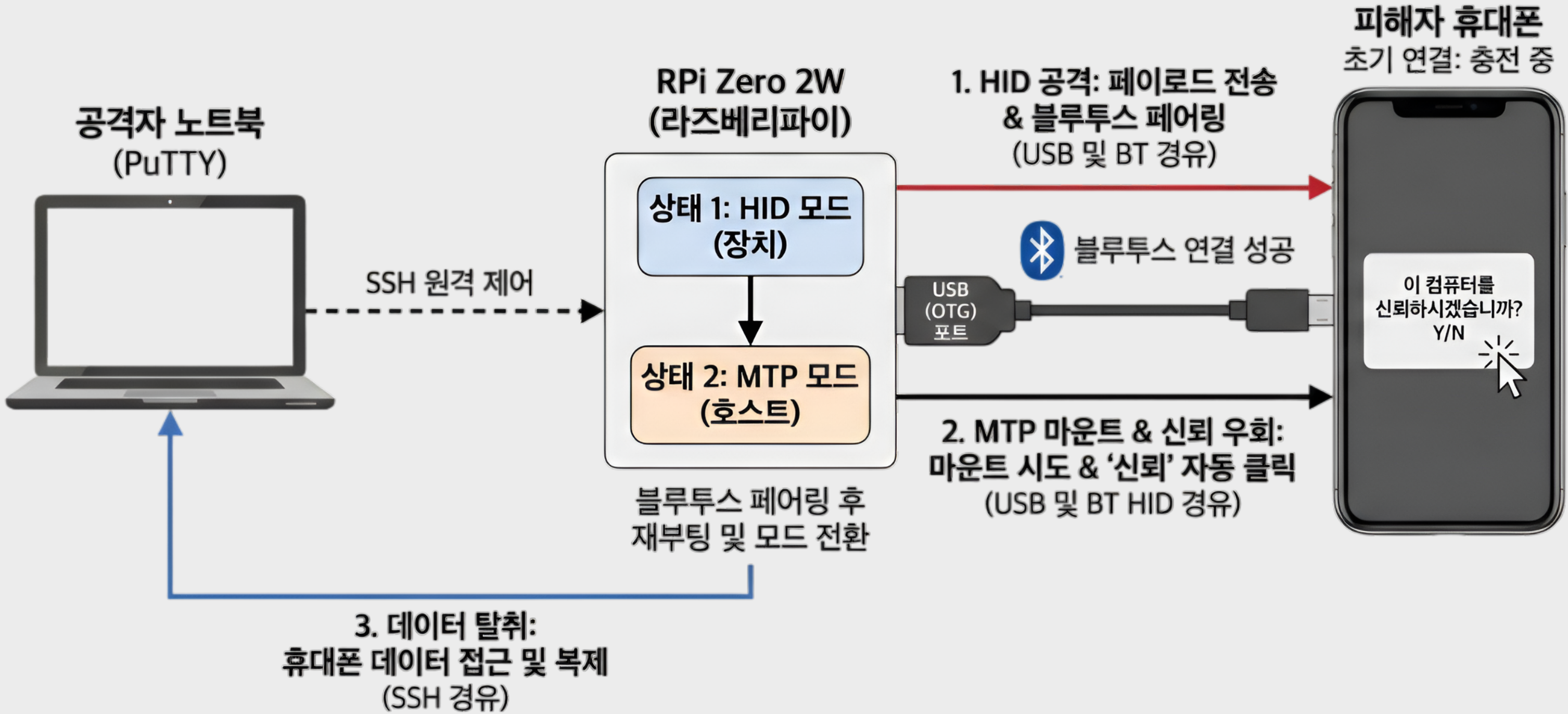
기존 연구 : Choice-Jacking

주스 재킹 공격 시나리오의 기존 접근법

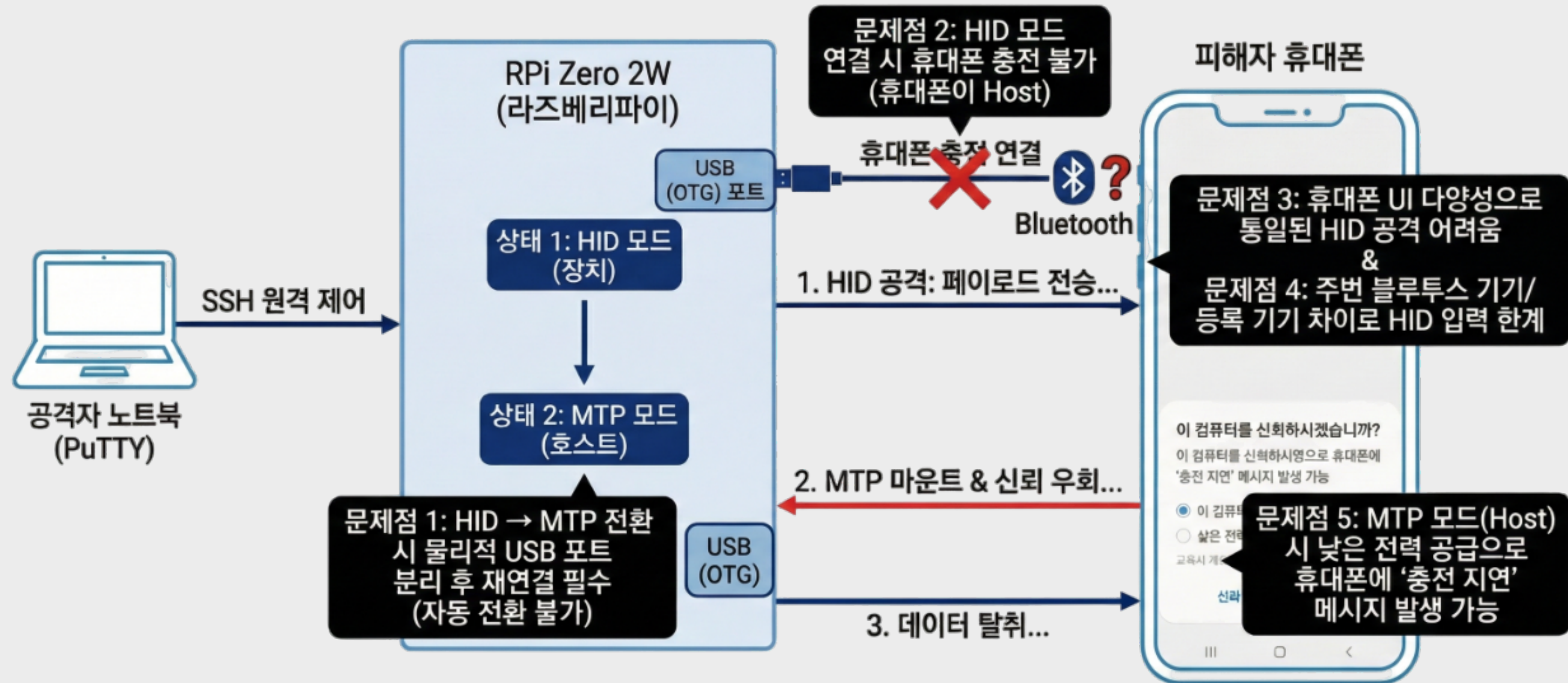


-
- Choice Jacking(선택 강요) 기법: 블루투스 HID(키보드/마우스)를 에뮬레이션하여 사용자 몰래 '허용' 버튼을 누르게 하는 방식
 - 공격 원리: 충전 중 MTP 연결 팝업이 뜨면 HID 장치가 자동으로 '허용' 버튼을 클릭하도록 설정
 - 실험 장비 구성: Raspberry Pi Zero 2W + HID Script + MTP 프로토콜 사용
 - 테스트 환경: Android 13, One UI 5.1 버전 Galaxy Note 20 사용

기존 연구 시나리오 구성도



기존 연구 시나리오 문제점



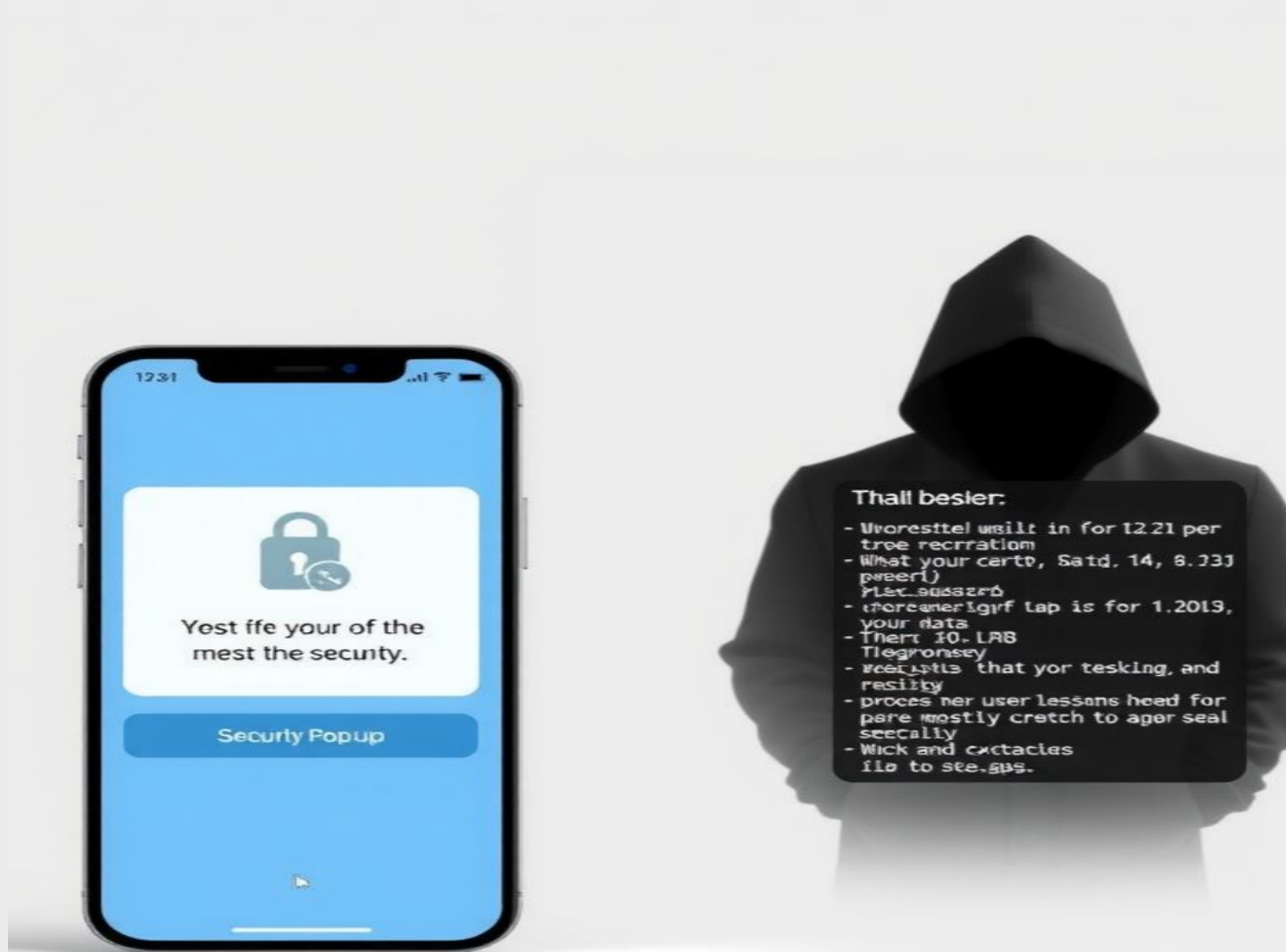
한계 극복 시도 (1)

제조사/기종별 상이한 UI로 인해 좌표 기반 클릭 불가능

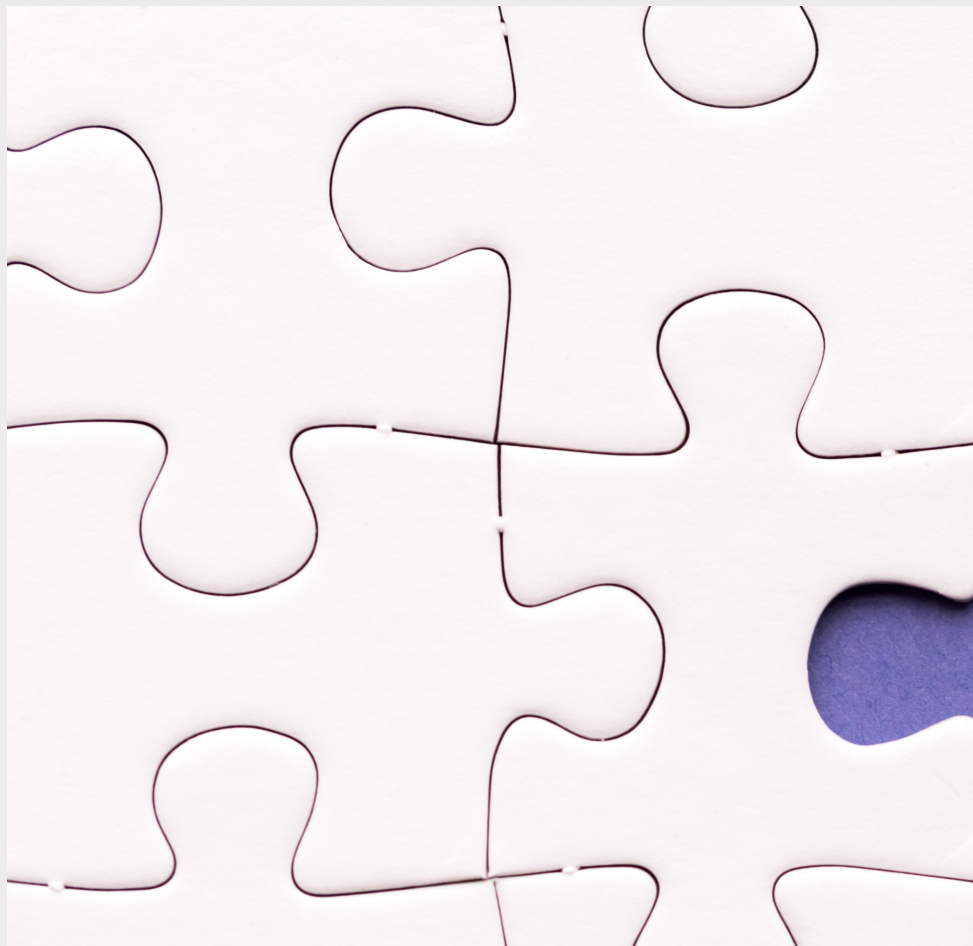
- Universal Shortcut (단축키 활용): 좌표 클릭 대신 Windows Key + I (설정창) 또는 Search Key 활용
- 빅스비(AI) 텍스트 명령을 HID로 입력하여 "블루투스 설정 열어줘" 실행 → UI 무관하게 설정 창 진입 성공

사용자마다 블루투스 등록 기기가 다름

- Reverse Navigation (역순 탐색 알고리즘) : 등록된 기기 리스트(가변적)를 건너뛰고, 하단의 '연결 가능한 기기'(고정적 위치)부터 역순으로 탐색하여 공격자 기기 선택 정확도 향상



한계 극복 시도 (2)



전력 공급 약화 문제

- 데이터 라인과 전원 라인을 물리적으로 분리하는 Y자 케이블 사용
- 전원을 따로 공급할 수 있는 전원 허브를 사용하여 HID 연결
- 공격 수행 중에도 스마트폰에 지속적인 전원 공급 → 사용자 의심 회피

HID → MTP 모드 전환 충돌

- 이원화된 공격 장비 사용 : 지속적인 입력 신호 및 팝업 담당 기기, 데이터 탈취 담당 기기를 따로 분리하여 사용 (기기 간 충돌 방지 및 물리적 재부팅 없이 즉각적인 공격 수행 가능)

기존 공격 방식의 한계점

기술적 한계

- 안드로이드 16/UI 8.0 이상에서 보안 강화
- 팝업이 아닌 생체 인식 요구
- 권한 승인 방식의 변경으로 기존 공격 무력화

시간적 한계

- 블루투스 페어링에 약 20초 소요
- 페어링 과정 중 충전 중단 현상 발생
- 공격 성공까지 시간 지연으로 의심 유발

은닉성 부족

- 화면 제어권이 공격자에게 넘어감
- 사용자가 이상 징후를 즉시 포착 가능
- 은밀성 요건 충족 실패

실용성 문제

- 현실 환경에서 적용 어려움
- 사용자 인지 가능성 높음
- 공격 성공률 저하

블루투스를 이용한 시나리오(Choice Jacking)는 현실에서 사용하기 힘든 공격

새로운 접근법 : DeX-Jacking

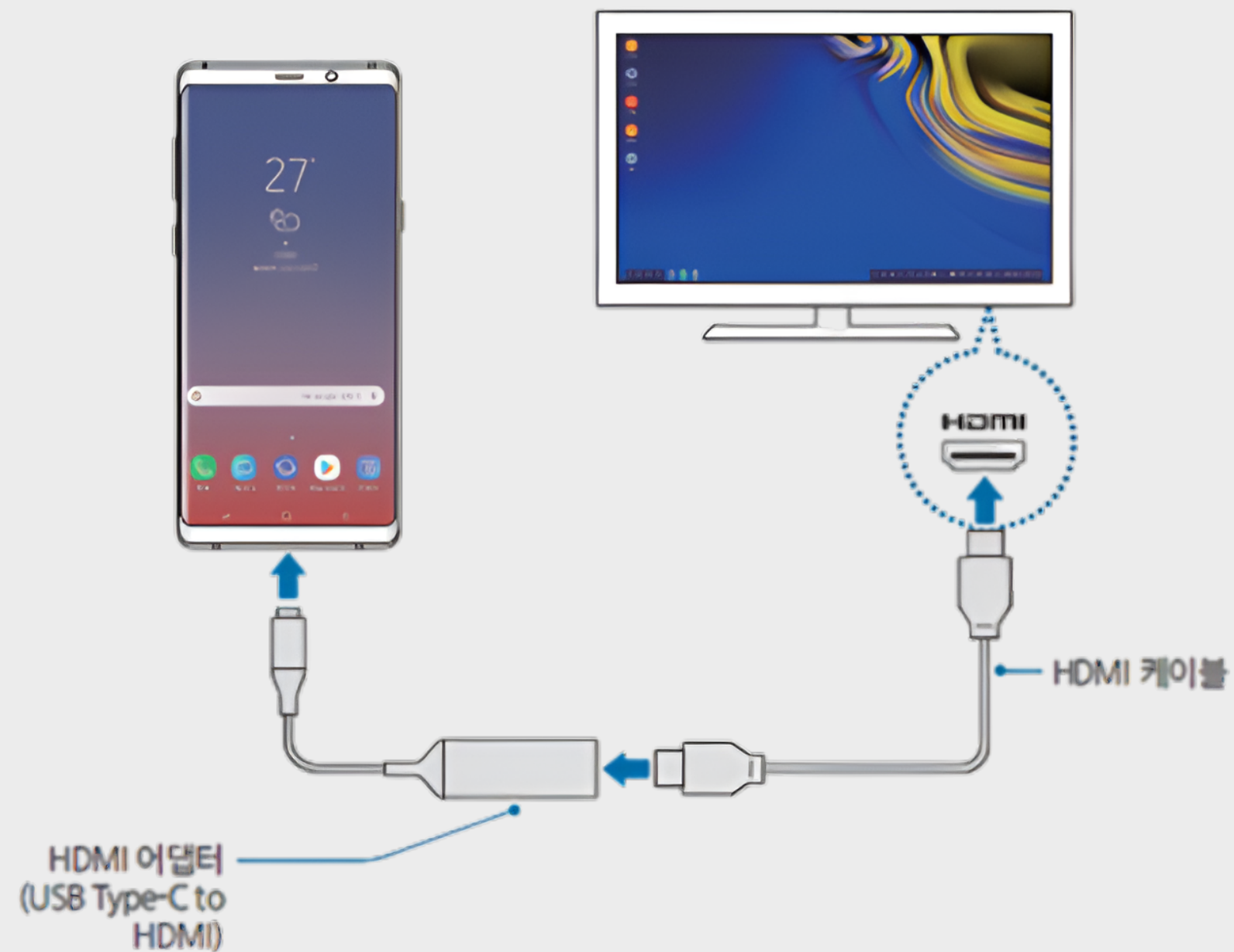
제조사 고유 기능(DeX)을 악용한 은밀한 공격 시나리오



소프트웨어 취약점을 파고드는 대신, 스마트폰 제조사의 편의 기능을 역으로 악용하는 방향으로 접근법을 전환했습니다. 기존 우회 방식의 한계를 극복하기 위해 정상적인 기능의 설계 의도를 벗어난 활용에 주목했습니다.

삼성 갤럭시 기종의 Samsung DeX 기능에 주목했습니다. 이 기능은 화면 이원화 및 독립 실행 환경을 제공하여, 스마트폰 본체 화면과 외부 모니터 화면에 서로 다른 내용을 동시에 표시할 수 있습니다.

DeX의 취약 지점 (1)



1. 외부 디스플레이 자동 실행

- HDMI 모니터에 연결하면 별도 인증 없이 DeX 모드로 자동 전환
- 휴대폰이 잠금 해제 상태일 경우 사용자 승인 없이 즉시 실행
- 아무 인증과 경고 없이 두 번째 화면을 열어 공격 환경 구성 가능

2. 허술한 경고 체계

- 사용자 편의를 위한 설계가 보안 취약점으로 작용
- 하단에 '외부 디스플레이에 연결됨' 아이콘이 잠깐 표시 (2~3초)
- 상단바의 작은 아이콘 외에 지속적인 경고나 기록이 거의 없음

DeX의 취약 지점 (2)



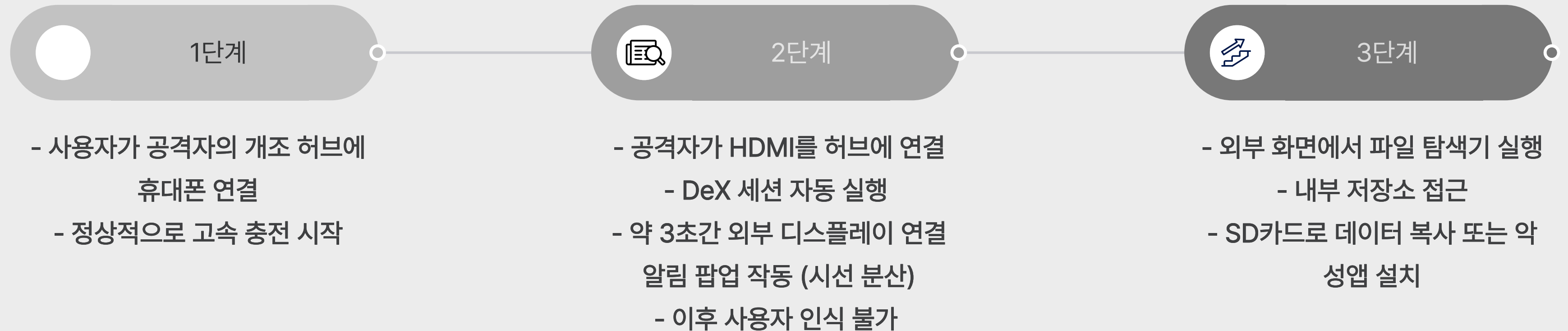
3. 독립 작동 환경

- 휴대폰 본체와 DeX 화면의 입력이 완전히 분리되어 처리됨
- 공격자의 마우스/키보드 조작이 휴대폰 화면에 영향을 주지 않음
- 사용자가 휴대폰을 정상적으로 사용하는 동안에도 공격 가능
- 입력 장치가 DeX 화면에만 영향을 주어 사용자 조작과 충돌하지 않음

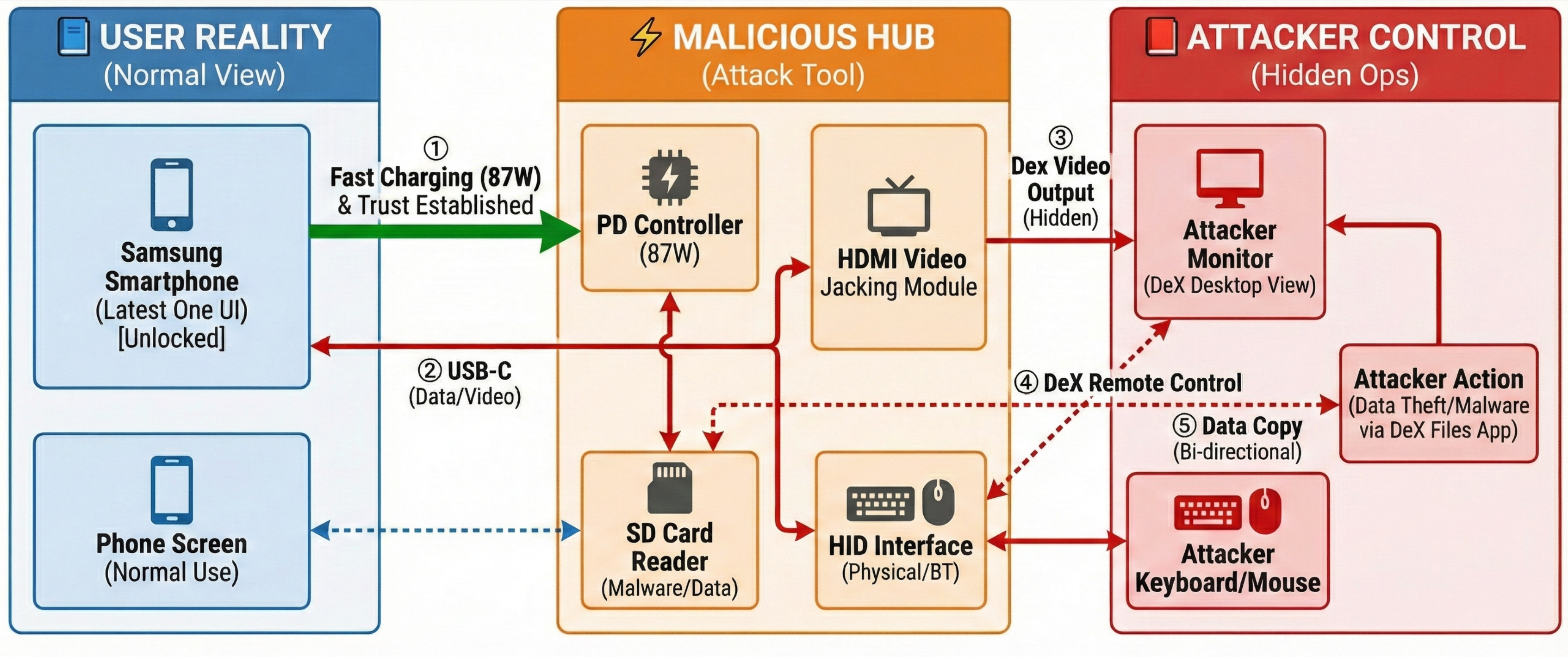
4. 입력 장치 공유

- 공격자가 USB 허브에 키보드/마우스를 연결하면 DeX 화면에서만 작동
- 사용자의 휴대폰 화면에는 어떠한 입력 흔적도 나타나지 않음
- 별도의 블루투스 페어링 과정이 필요 없어 사용자 인지 불가능

DeX-Jacking 공격 흐름



DeX-Jacking 구성도



공격 시나리오 검증

Hardware

- C-Type 멀티 허브 (PD 충전 + HDMI + USB 포트 + SD 포트)
- 정상 충전 표시를 위한 PD 프로토콜 지원 필수

Storage

- 대용량 SD 카드 (데이터 탈취용)
- 악성 APK 파일 저장 및 설치 + 데이터 탈취 가능

Input

- USB 연결 HID 장치 (물리적 연결)
- 블루투스 페어링 과정 없이 즉시 인식

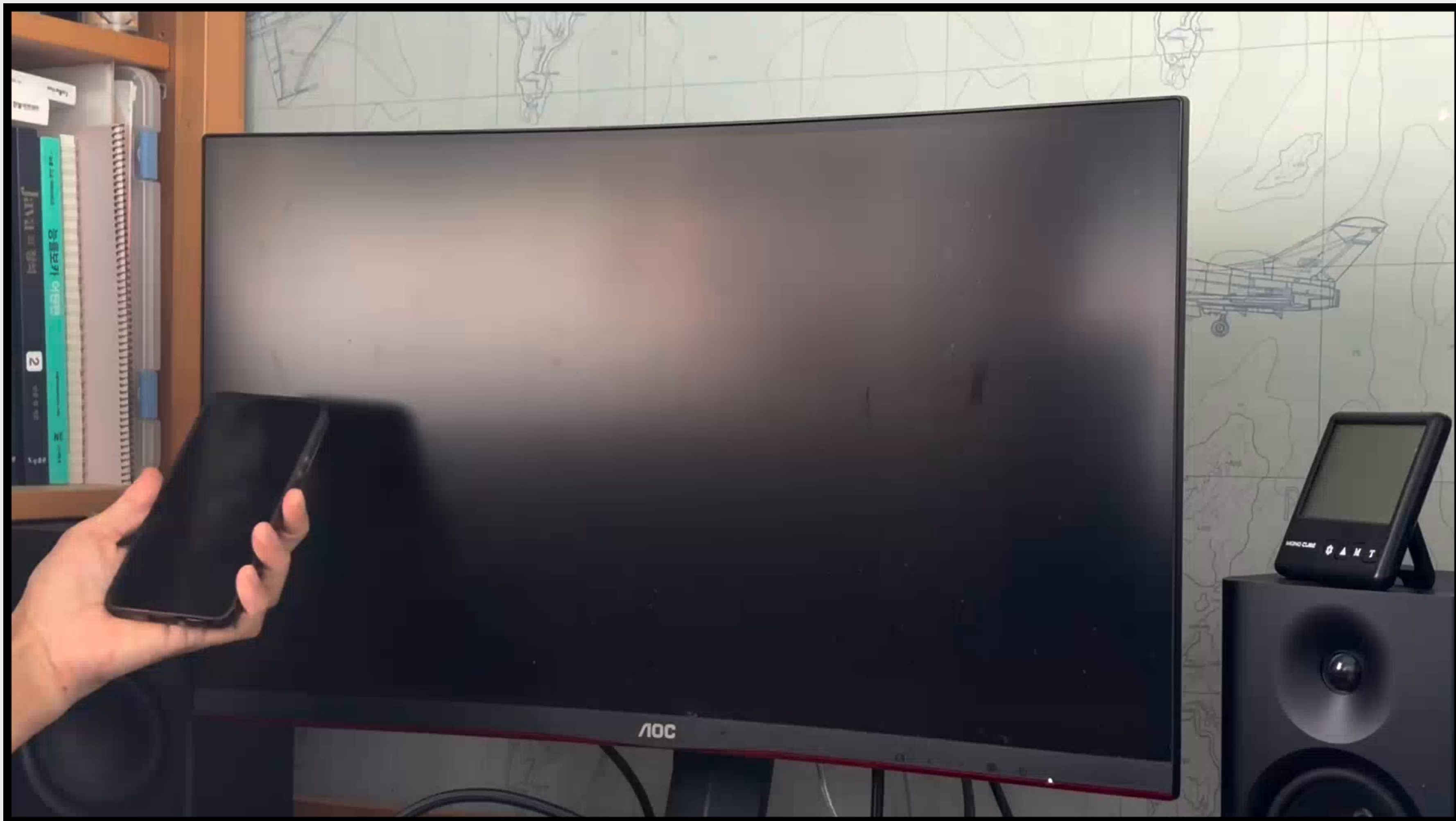
우회 기법

- MTP 대신 SD카드 마운트 방식 사용
- '신뢰' 팝업 우회로 사용자 승인 과정 생략

공격 흐름

- 연결 → DeX 자동 실행 → 데이터 접근 → 파일 복사 → 연결 해제
- 전 과정 사용자 인지 어려움 (초기 연결 문구만 시선 분산 필요)





DeX-Jacking 특징

기존 주스 재킹 / 미러링 기반 공격

- MTP 신뢰/허용 팝업, 권한 승인 등 소프트웨어 취약점 공략 (운영체제(OS) 보안 정책 우회에 의존)
- 스마트폰 화면을 외부 디스플레이에 그대로 복제 (미러링 구조 사용)
- 앱 실행, 설정 변경, 데이터 이동 과정이 사용자 화면에 그대로 노출 (은밀한 공격이 어려움)
- 제조사, OS 버전, UI 구성 차이에 따라 공격 스크립트 수정 필요

VS

Dex-Jacking (확장형 공격)

- 취약점 공격이 아닌 제조사 정상 기능(Feature) 악용 (최신 Android 버전에서도 동작)
- 스마트폰과 외부 디스플레이가 독립적으로 작동하는 특성 활용
- 사용자는 스마트폰 화면만 보는 반면, 공격자는 외부 디스플레이에서 별도 작업 수행 가능
- HDMI 출력 + DeX 환경에서 동일한 UI 제공 (사용자 기기 설정, 테마, 앱 배치와 무관하게 공격 가능)

보안 위협 평가

편의 기능의 보안 취약점화

- 스마트폰 편의 기능의 설정 미비가 심각한 보안 구멍으로 작용
- 제조사가 사용자 편의를 위해 도입한 자동 연결 기능이 악용
 - 듀얼스크린 기능이 공격자에게 은신처 제공
 - 보안과 편의성 사이의 균형점 재고 필요

기업 환경에서의 위험성

- 기업 기밀을 다루는 임직원이 출장 중 특히 위험
- 공항 라운지나 호텔의 DeX 도킹 스테이션 사용 시 위험
- 악의적 장치에 의해 업무 자료가 순식간에 탈취 가능
 - 기업 정보 유출로 인한 경제적 손실 가능성

현실적 위협으로의 전환

- 기존 주스 재킹은 이론적 난이도로 인해 실제 위협 낮게 평가
 - 본 연구는 공격 난이도를 현실적으로 낮춤
 - '충분히 발생 가능한 위협'으로 전환

사용자 인지 불가능성

- 사용자가 공격 진행 상황을 인지하기 어려움
 - 일반적인 보안 인식으로는 탐지 불가능
- 충전 중 정상 사용이 가능하여 의심 여지 없음
- 공격 후에도 흔적이 미미하여 사후 발견 어려움

제조사 대응 방안

추가 인증 절차 도입

- 외부 디스플레이 연결 시 추가 인증 필요
- 휴대폰 잠금 해제 상태에서도 별도 확인 요구
- 생체인증 옵션 제공

DeX 실행 보안 강화

- DeX 모드 진입 시 명시적 사용자 승인 필수화
- 자동 실행 기능에 보안 레이어 추가
- 중요 데이터 접근 시 추가 인증

UI 개선

- DeX 활성화 중임을 명확히 인지시키는 인터페이스 개선
- 휴대폰 화면에 지속적인 표시
- 직관적 상태 표시 아이콘 개발

사용자 알림 강화

- 외부 디스플레이 연결 시 강력한 경고 배너 표시
- 주기적 알림으로 사용자 주의 환기
- 연결 상태 로그 기록 강화

사용자 대응 방안

신뢰성

- 공공장소의 USB 포트 사용 시 각별한 주의
- 신뢰할 수 있는 장소의 충전 설비만 이용

개인 장비

- 개인 충전기 또는 보조 배터리 항상 휴대
- 자신의 충전 케이블 사용 권장

보호 장치

- 데이터선이 제거된 전용 케이블 사용
- 휴대폰 설정에서 '충전만' 옵션 사용

주의 관찰

- 승인 팝업이 갑자기 나타나면 즉시 의심
- 충전 중 비정상적 동작 즉시 케이블 분리

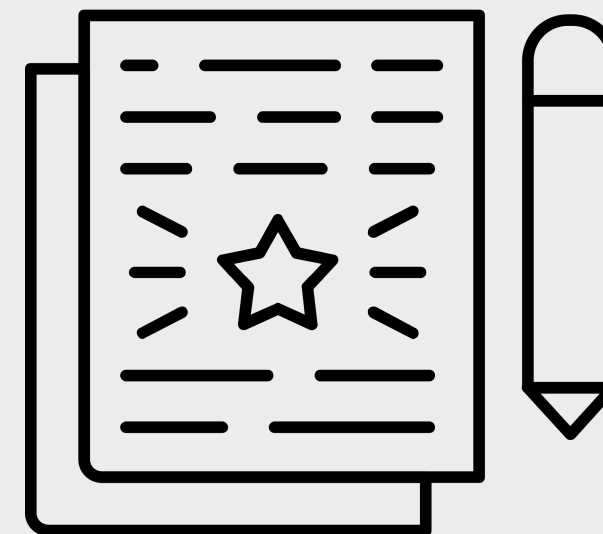
정기 점검

- 의심스러운 앱 설치 여부 점검
- 보안 업데이트 항상 최신 상태 유지

결론

본 연구에서는 주스 재킹 공격의 개념과 기존 시나리오의 한계를 분석하고, 이를 극복할 수 있는 새로운 복합 공격 기법('DeX-Jacking')을 제안 및 실증했습니다. USB 데이터 통신 차단 팝업, 블루투스 HID 조작, 영상 미러링 등 각각의 우회 시도들이 지닌 약점을 보완하기 위해, 삼성 스마트폰의 DeX 기능을 악용한 현실적 시나리오를 구현한 것이 핵심입니다.

실험 결과, 최신 보안 정책을 우회하면서도 사용자가 공격 진행을 눈치채지 못할 정도의 은밀성을 확보할 수 있음을 확인하였습니다. 이는 스마트폰의 편의 기능과 보안성의 트레이드오프에 대해 경각심을 일깨워줍니다. 제조사가 제공하는 생산성 기능이라 해도 적절한 보안 고려 없이 자동화되어 있다면 충분히 공격에 악용될 수 있습니다.





THANK YOU!

감사합니다!

T.ACE | 유한영 성민욱 홍영재