커넥티드카 앱을 통한 차량 권한 탈취 가능성 실증 연구

CSOS 학부연구생 정연수

INDEX

01 연구 배경

02 연구 개요

03 분석 과정

04 악성 시나리오

05 연구 결과

01 연구 배경

연구 배경

❖ 자동차의 공격 표면 확대

- 자동차의 전장화
- V2X 개념과 SDV 플랫폼 등장
- 끊임없이 통신하는 디지털 시스템으로 변화

❖ Connected Car App (CCA)

- 커넥티드 카 서비스 제공 목적
- 차량 제어 / 모니터링 / 공유 등 차량에 대한 강력한 권한

02 연구 개요

연구 개요

❖ 목적

- 공식 CCA의 취약점을 악용한 차량 권한 탈취 시나리오 실증

❖ 분석 대상

Type	Name	Version
Car	AVANTE(CN7)	2022
Mobile Device (pure)	Galaxy S21	Android 14
Mobile Device (rooting)	Galaxy A23	Android 14
App	Bluelink	ver. 3.922

※ Bluelink는 2025/06 기준 마이현대app으로 서비스 통합되었습니다.

연구 개요

❖ 주요 분석 도구

Name		Description
static	adb	Tool for checking dynamically loaded dex files
	apktool	APK file unpacking and repacking tool
	jd-gui	App source code viewer
Dynamic	Python	Tool for attaching Frida to Bluelink
	Frida	Hooking Tool for bypassing root detection logics
	Chrome Devtools	Tool for analysis target API’s process

03 분석 과정

분석 환경 구축

❖ 루팅된 디바이스에서 블루링크 실행

- 결과: 비정상 종료

분석 환경 구축

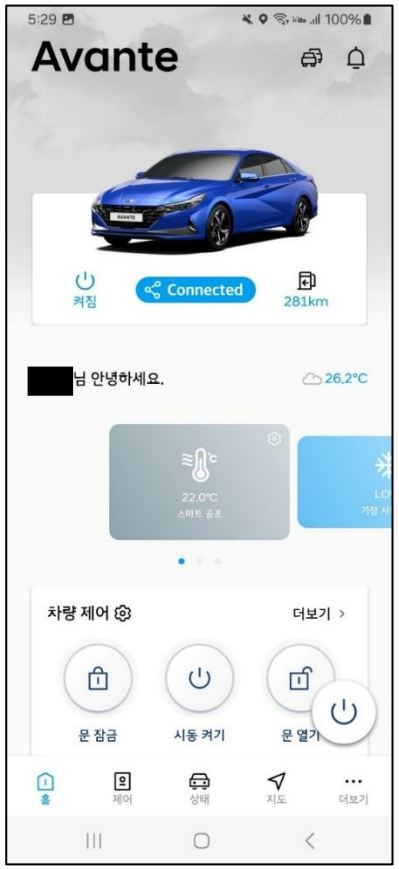
❖ 루팅된 디바이스에서 블루링크 실행

- 결과: 비정상 종료

❖ 루팅 탐지 로직 우회 필요성

- jd-gui 로 루팅 탐지 로직 식별
- Python & Frida 로 동적 후킹을 통한 우회

Hooking



분석 환경 구축

❖루팅 탐지 로직 우회 과정

시간의 흐름

Index	Type	Tool	Behavior	Result
1	S	jd-gui	Analyze Original Dex file	Find rooting detection logic 1
2	D	frida	Hooking Logic 1	Execute App in rooted device
3	D	adb	Analyze Dynamic Dex Loading	Get Dynamic Dex Loading files
4	S	jd-gui	Analyze Dynamic Dex files	Find rooting detection logic 2
5	D	frida	Hooking Logic 2	Execute features in app

TYPE [S : Static, D : Dynamic]

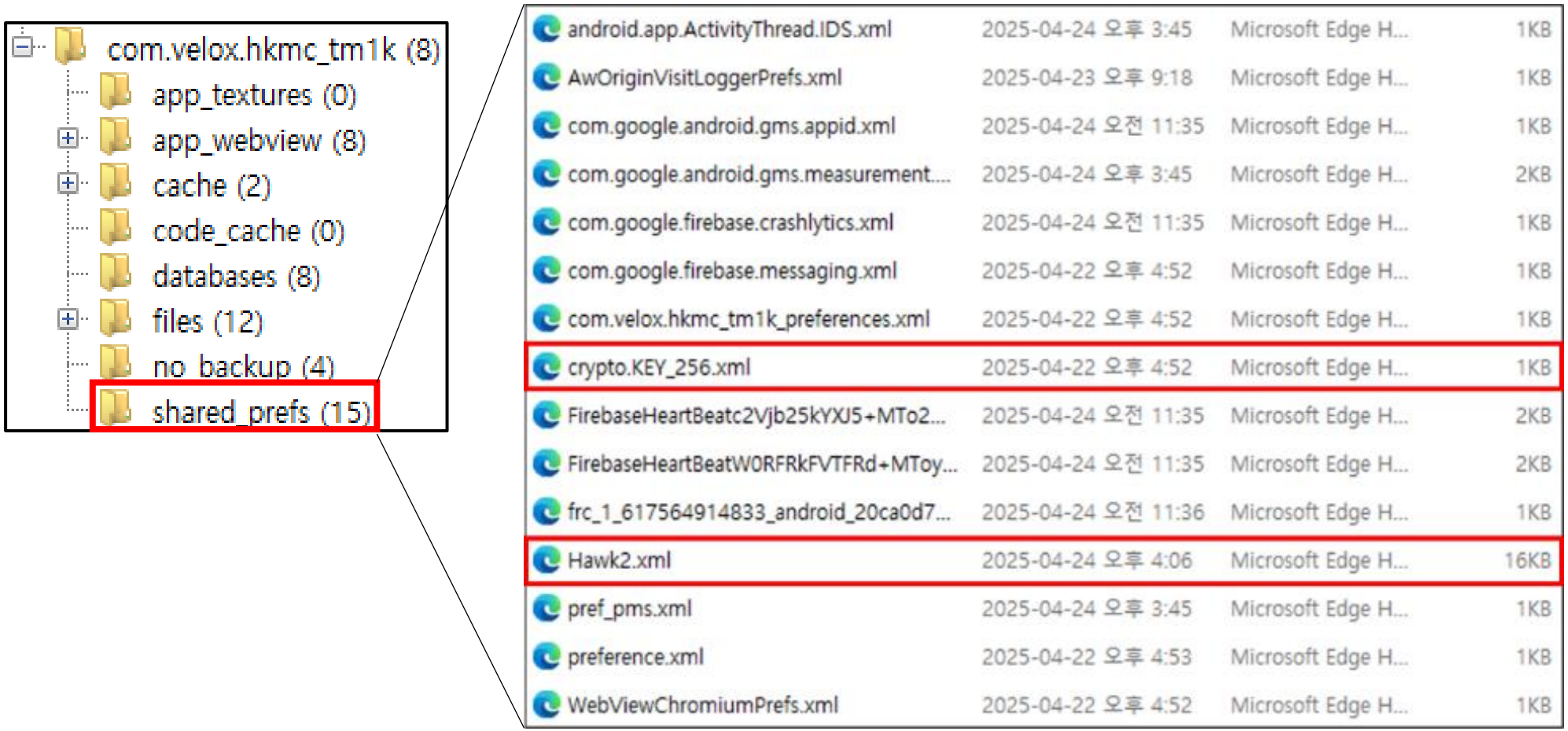
기능 작동 교차 검증

❖ 참고: Bluelink User Manual

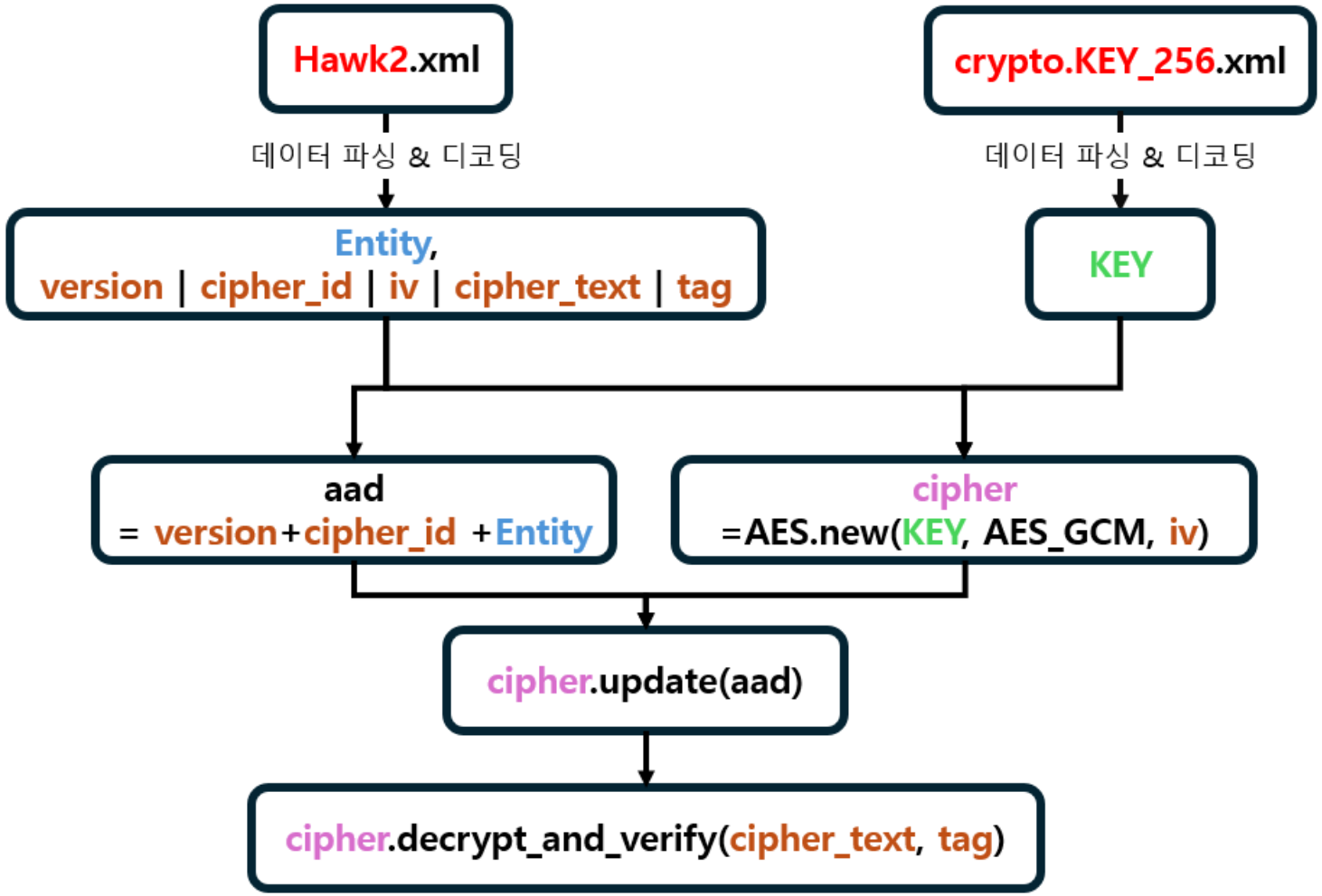
Category	Target	Features	S21 (pure)	A23 (rooting)
Control	Engine	Start	X	X
		Stop	X	X
	Doors	Lock	O	O
		Unlock	O	O
	ETC	Light	O	O
Map		sendToCar	O	O
More		carSharing	O	O

부주의한 키 관리

❖ 앱 데이터 구조



사용자 데이터 복호화


Hawk2.xml
crypto.KEY_256.xml
데이터 파싱 & 디코딩
데이터 파싱 & 디코딩
Entity,
version | cipher_id | iv | cipher_text | tag
KEY
aad
= version+cipher_id +Entity
cipher
=AES.new(KEY, AES_GCM, iv)
cipher.update(aad)
cipher.decrypt_and_verify(cipher_text, tag)

차량 공유 API

❖ Input

- 전화번호
- 공유 비밀번호(PIN, 4자리)

❖ Output

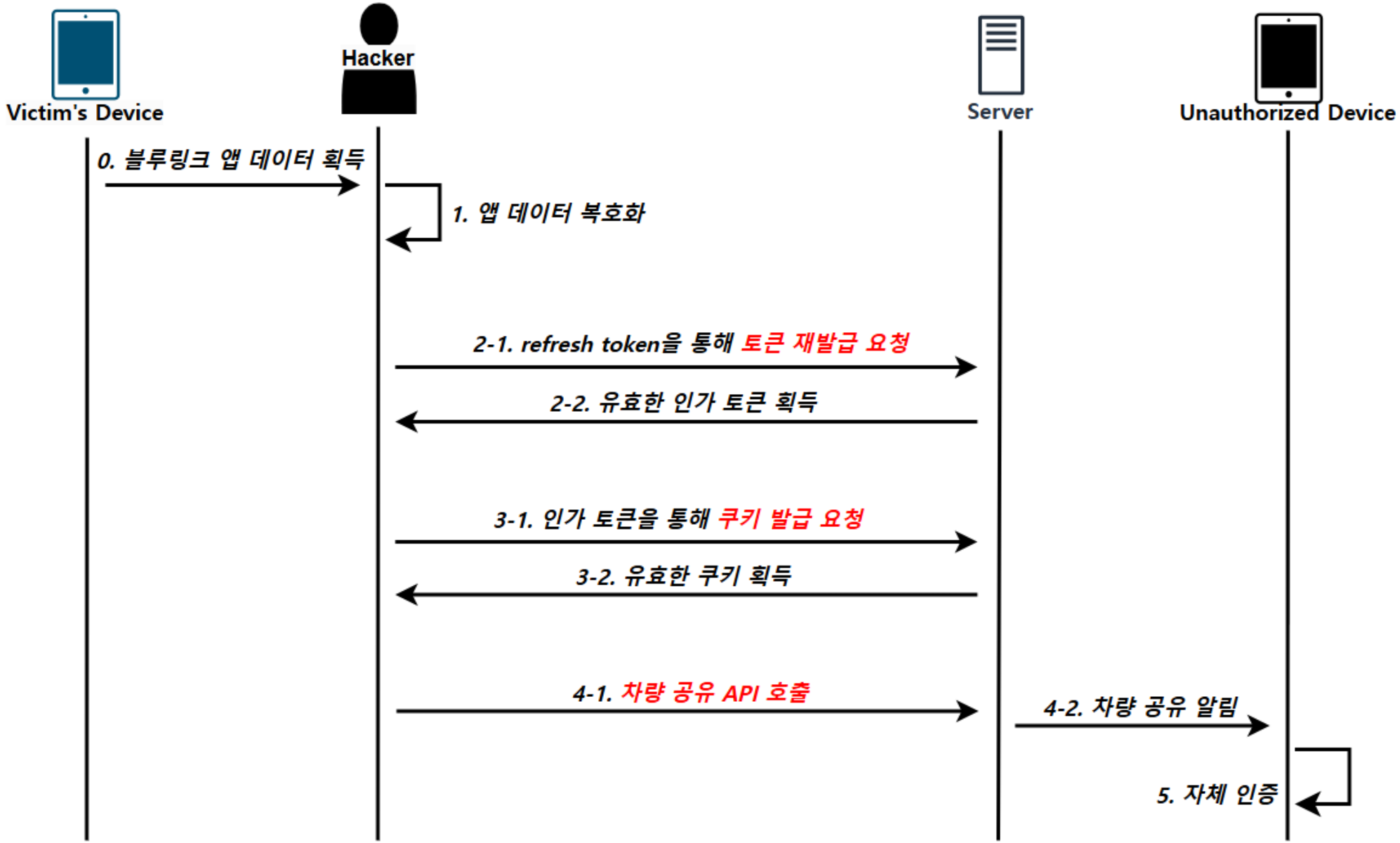
- 선택한 계정으로 '차량 공유' 알림 전송

❖ Need

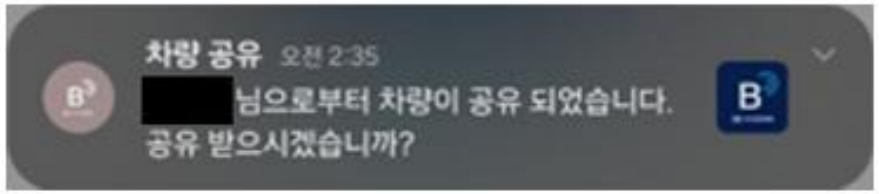
- 유효한 **인가 토큰**
- 유효한 특정 **쿠키**

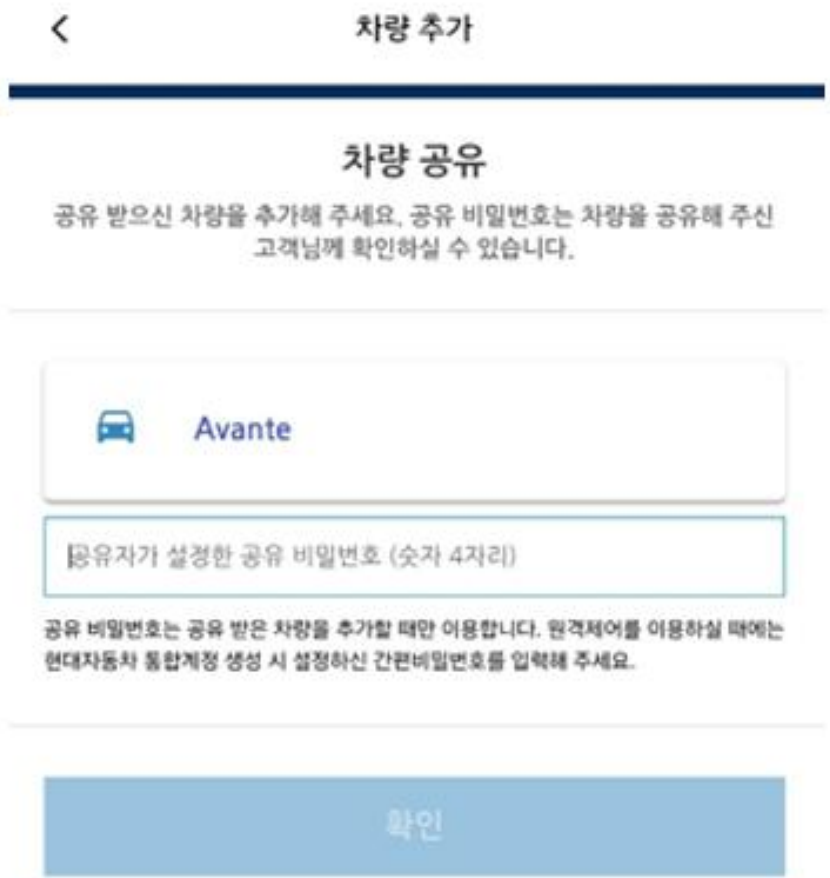
04 악성 시나리오

악성 시나리오


Victim's Device
Hacker
Server
Unauthorized Device
0. 블루링크 앱 데이터 획득
1. 앱 데이터 복호화
2-1. refresh token을 통해 토큰 재발급 요청
2-2. 유효한 인가 토큰 획득
3-1. 인가 토큰을 통해 쿠키 발급 요청
3-2. 유효한 쿠키 획득
4-1. 차량 공유 API 호출
4-2. 차량 공유 알림
5. 자체 인증

악성 시나리오


차량 공유 오전 2:35
[redacted]님으로부터 차량이 공유 되었습니다.
공유 받으시겠습니까?


차량 추가
차량 공유
공유 받으신 차량을 추가해 주세요. 공유 비밀번호는 차량을 공유해 주신 고객님께 확인하실 수 있습니다.
Avante
공유자가 설정한 공유 비밀번호 (숫자 4자리)
공유 비밀번호는 공유 받은 차량을 추가할 때만 이용합니다. 원격제어를 이용하실 때에는 현대자동차 통합계정 생성 시 설정하신 간편비밀번호를 입력해 주세요.
확인


2:51
99%
차량 및 서비스 설정
가입 정보
차량공유 관리
공유 추가
프로필 등록 사용자 (2/2)
[redacted]
등록 해제
[redacted]
정연수 [redacted]
공유 중지
등록 해제
공유 중인 사람이 없습니다.
홈
제어
상태
지도
더보기

05 연구 결과

연구 결과

❖ 의의

- 모바일 디바이스의 권한 탈취가 차량 권한 탈취로 이어질 수 있음을 보임.

❖ 한계

- 전제 조건이 충족되기 어려움.

Thank you

Q&A