

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



A dark blue background featuring a dense grid of white circuit board traces and component pads, creating a high-tech, electronic theme.

01

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

A dark blue background featuring a dense grid of white circuit board traces and component pads, creating a high-tech, electronic theme.

02

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.

❖ 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	

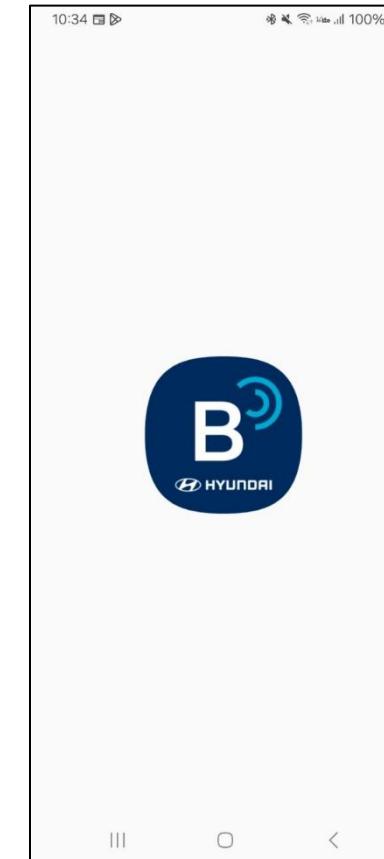
A dark blue background featuring a dense grid of white circuit board traces and component pads, creating a technical and futuristic feel.

03

분석 과정

- ❖ 루팅된 디바이스에서 블루링크 실행

- 결과: 비정상 종료



분석 환경 구축

❖ 루팅된 디바이스에서 블루링크 실행

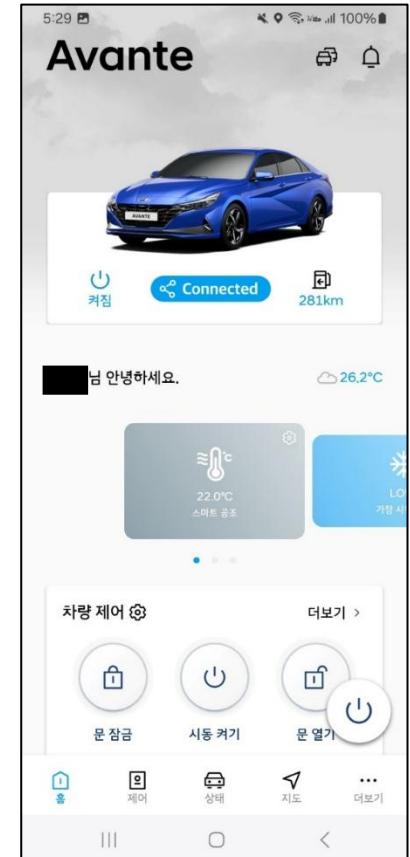
- 결과: 비정상 종료

❖ 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

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]

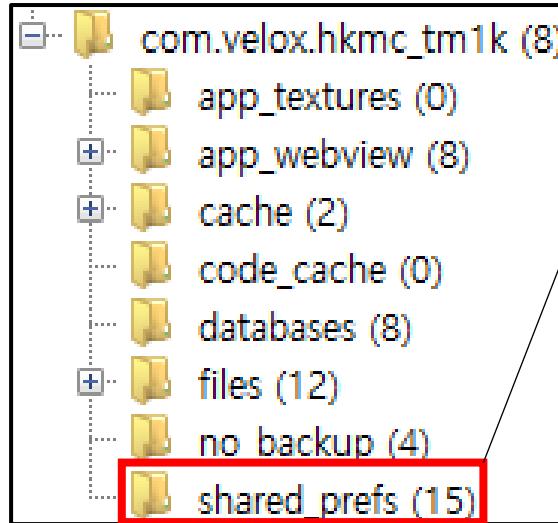
기능 작동 교차 검증

❖ 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

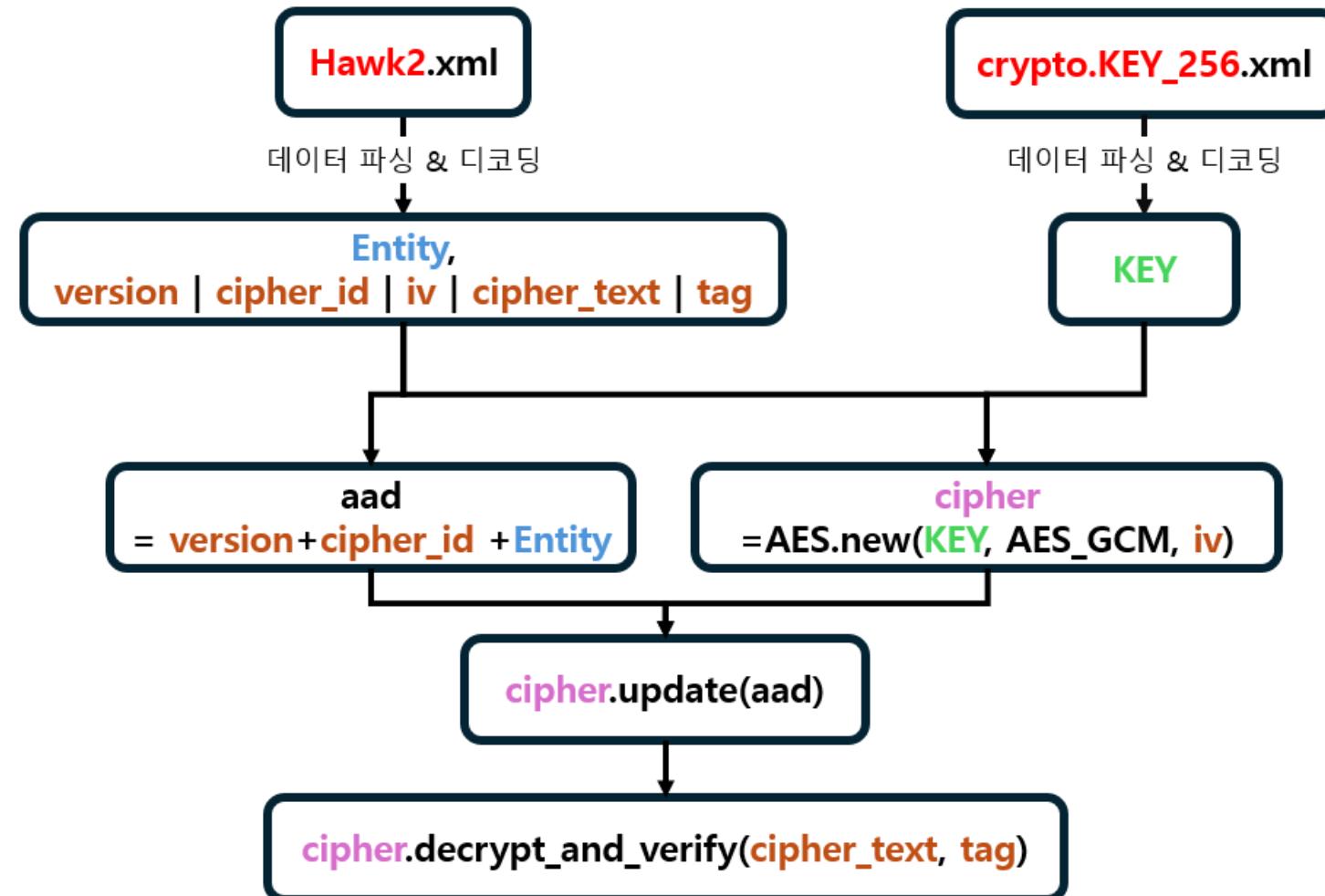
부주의한 키 관리

❖ 앱 데이터 구조



android.app.ActivityThread.IDS.xml	2025-04-24 오후 3:45	Microsoft Edge H...	1KB
AwOriginVisitLoggerPrefs.xml	2025-04-23 오후 9:18	Microsoft Edge H...	1KB
com.google.android.gms.appid.xml	2025-04-24 오전 11:35	Microsoft Edge H...	1KB
com.google.android.gms.measurement....	2025-04-24 오후 3:45	Microsoft Edge H...	2KB
com.google.firebaseio.crashlytics.xml	2025-04-24 오전 11:35	Microsoft Edge H...	1KB
com.google.firebaseio.messaging.xml	2025-04-22 오후 4:52	Microsoft Edge H...	1KB
com.velox.hkmc_tm1k_preferences.xml	2025-04-22 오후 4:52	Microsoft Edge H...	1KB
crypto.KEY_256.xml	2025-04-22 오후 4:52	Microsoft Edge H...	1KB
FirebaseHeartBeatc2Vjb25kYXU5+MTo2...	2025-04-24 오전 11:35	Microsoft Edge H...	2KB
FirebaseHeartBeatW0RFRkFVTFRd+MToy...	2025-04-24 오전 11:35	Microsoft Edge H...	2KB
frc_1_617564914833_android_20ca0d7...	2025-04-24 오전 11:36	Microsoft Edge H...	1KB
Hawk2.xml	2025-04-24 오후 4:06	Microsoft Edge H...	16KB
pref_pms.xml	2025-04-24 오후 3:45	Microsoft Edge H...	1KB
preference.xml	2025-04-22 오후 4:53	Microsoft Edge H...	1KB
WebViewChromiumPrefs.xml	2025-04-22 오후 4:52	Microsoft Edge H...	1KB

사용자 데이터 복호화



내차 공유

내차 공유를 위한 정보를 등록해 주세요.

* 공유받는 사람 휴대폰 번호

공유받는 사람 휴대폰 번호 +

● 공백 특수기호 없이 숫자만 입력하세요.

* 공유 비밀번호

공유 비밀번호(숫자 4자리)

차량을 공유 받으실 분께 지정하신 일시 공유 비밀번호를 알려주세요. 공유 비밀번호를 입력하신 후 차량을 이용하실 수 있습니다.

내차 공유

❖ Input

- 전화번호
- 공유 비밀번호(PIN, 4자리)

❖ Output

- 선택한 계정으로 '차량 공유' 알림 전송

❖ Need

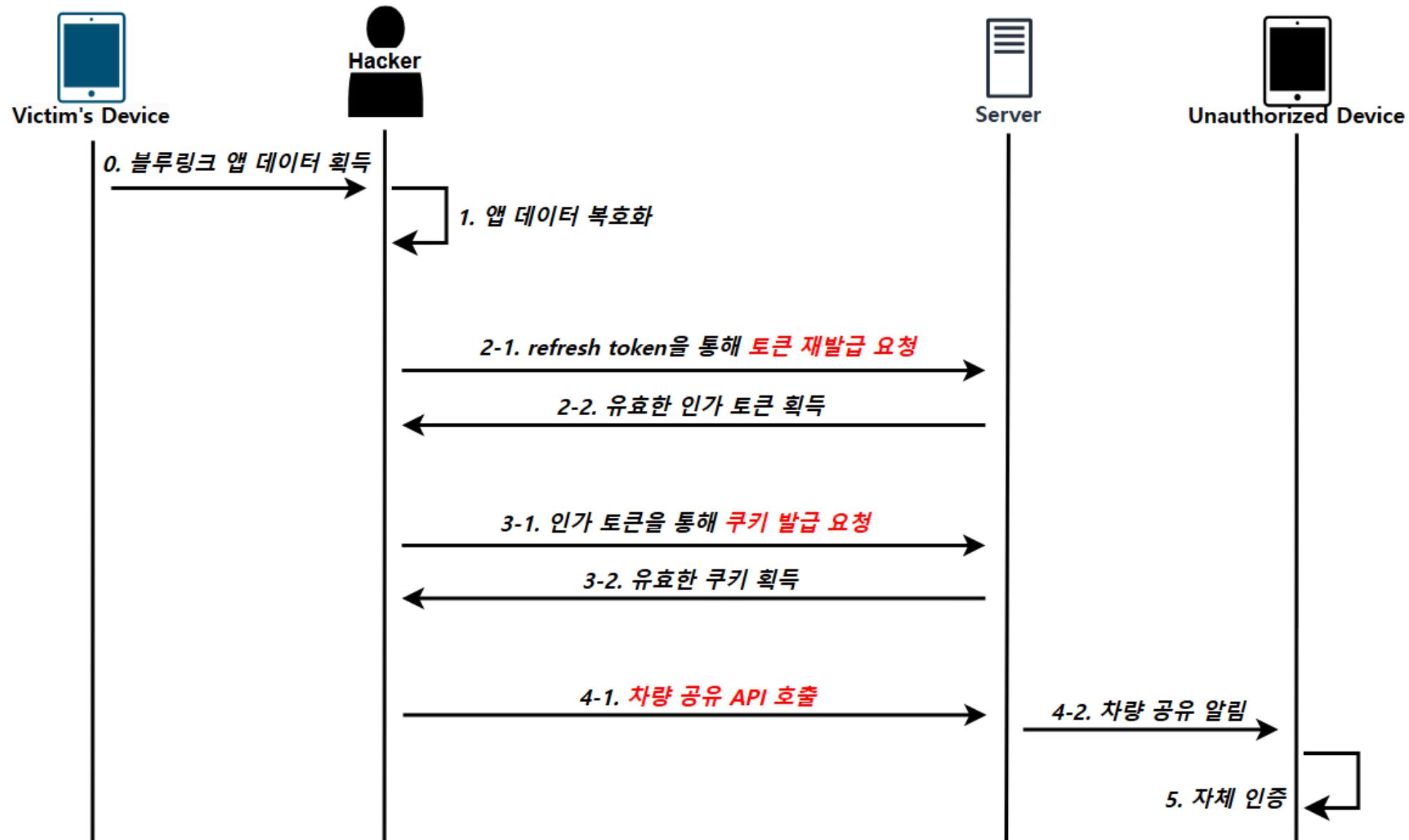
- 유효한 인가 토큰
- 유효한 특정 쿠키

A dark blue background featuring a dense grid of white circuit board traces and component pads, creating a technical and futuristic aesthetic.

04

악성 시나리오

악성 시나리오



악성 시나리오

The composite screenshot displays four mobile application screens:

- Top Left:** A dark-themed notification card from a service like B-Car. It shows a profile icon with a 'B' and the text "차량 공유 오전 2:35" (Car Sharing, 2:35 AM). Below it is a message: "님으로부터 차량이 공유 되었습니다. 공유 받으시겠습니까?" (A vehicle has been shared with you. Would you like to accept it?).
- Top Right:** A settings screen titled "차량 및 서비스 설정" (Vehicle and Service Settings) with a battery level of 99%. It includes sections for "가입 정보" (Registration Information) and "차량공유 관리" (Car Sharing Management), with a red box highlighting the latter.
- Middle Left:** A screen titled "차량 추가" (Add Vehicle) under "차량 공유" (Car Sharing). It shows a car icon and the model "Avante". Below it is a text input field labeled "[공유자가 설정한 공유 비밀번호 (숫자 4자리)]" (Shared by user's shared password (4-digit number)). A note below states: "공유 비밀번호는 공유 받은 차량을 추가할 때만 이용합니다. 원격제어를 이용하실 때에는 현대자동차 통합계정 생성 시 설정하신 간편비밀번호를 입력해 주세요." (The shared password is used only when adding a vehicle received through sharing. When using remote control, please enter the password set during the creation of the Hyundai Motor Group integrated account.).
- Middle Right:** A detailed view of "차량공유 관리" (Car Sharing Management) showing two users associated with the vehicle. The first user is listed as "차량 소유자" (Vehicle Owner) with a redacted name and phone number, and a "등록 해제" (Unregister) button. The second user is listed as "정연수" with a redacted phone number, and buttons for "공유 중지" (Stop Sharing) and "등록 해제" (Unregister).

A dark blue background featuring a dense grid of white circuit board traces and component pads, creating a technical and futuristic aesthetic.

05

연구 결과

❖ 의의

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

❖ 한계

- 전제 조건이 충족되기 어려움.

Thank you

Q&A

