SECURITY ANALYSIS OF ANDROID AUTOMOTIVE

Mert D. Pesé and Kang G. Shin, University of Michigan
Josiah Bruner, Georgia Institute of Technology
Amy Chu, Harman International

Agenda

Introduction

Related Work

Threat Model and Background

Security Analysis

Recommendations

Next Generation of IVIs

ALEX DAVIES GEAR 05.26.15 08:00 AM

ANDROID AUTO: THE FIRST GREAT IN-CAR INFOTAINMENT SYSTEM

Source: https://www.wired.com/2015/05/android-auto-first-great-car-infotainment-system/

Google Unveils Android Automotive OS on the 2020 Polestar 2 EV

By Ryan Whitwam on May 3, 2019 at 2:15 pm | 4 Comments

11 SHARES

Source: https://www.extremetech.com/mobile/290792-google-unveils-android-automotive-os-on-the-2020-polestar-2

Android Auto vs Android Automotive

Android Auto

- Runs **outside** vehicles (on phone)
- Phone connection required, since mirroring
- **Cannot** use data from IVN
- Only restricted to media and messaging apps

Source: https://www.funzen.net/2019/11/20/how-android-auto-works-everything-you-need-to-know/

Android Automotive

- Runs **inside** vehicles (on IVI)
- **No** phone connection required
- **Can** use data from IVN
- Richer 3rd party apps possible

Source: https://www.engadget.com/2019-05-04-android-automotive-hands-on.html/

\+ Restricted Permissions
\+ Restricted Attack Surfaces
\- Phone Integration

\+ No Phone
\- More Attack Surfaces
\- Access to IVN data
→ Data Injection & Privacy

Agenda

Introduction

Related Work

Threat Model and Background

Security Analysis

Recommendations

Related Work

Android Auto

- Static analysis of infotainment apps in Google Play Store
- Vulnerabilities limited to operational damage, but also driver safety (distraction)
- Study found 60% of all apps have some sort of vulnerability
  - 25% of all apps have JavaScript vulnerabilities

Android Automotive

- Focus on third-party app analysis
- Developed tool for vehicle-specific code analysis
- PoC attacks for driver disturbance, availability, privacy

Agenda

Introduction

Related Work

Threat Model and Background

Security Analysis

Recommendations

Classification of Attacks

Attack Landscape is changing...

First-Generation Attacks (~2010-2015)	Second-Generation Attacks (~2015-2020)	Third-Generation Attacks (~2020-?)
Using physical interfaces	Using wireless interfaces (e.g., IVI and TCU)	Using app eco-system on IVIs

Scalability

Risk / Damage Potential

Classification of Attacks

... so is the risk.

Infrastructure Vulnerabilities

- Network
- OS
- Runtime Environment
- Hypervisor
- Backend

Can be patched

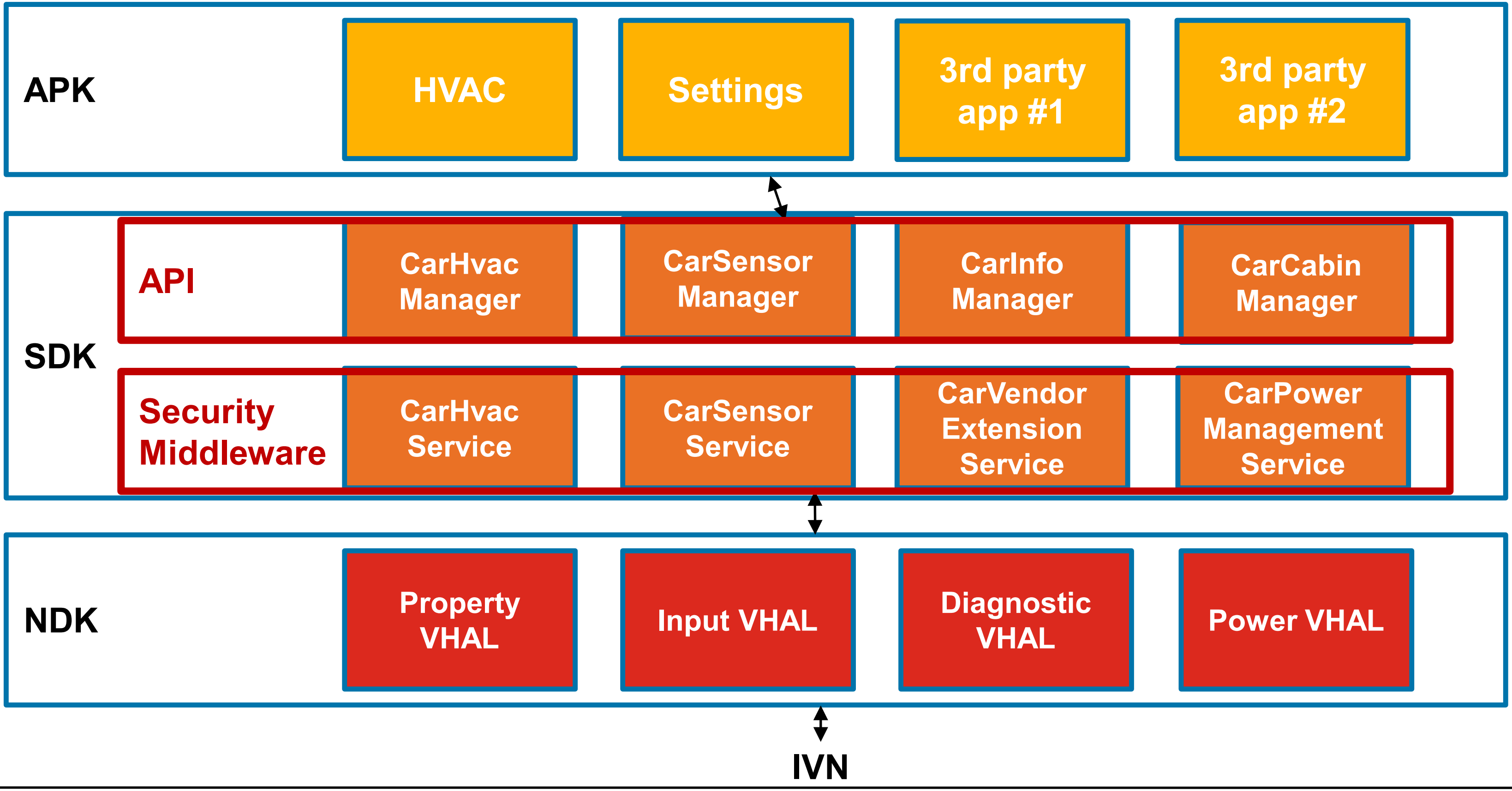
(Programming) Framework Design Vulnerabilities

- APIs
- Permission Model
- Unauthorized Access to IVN

Far-reaching impact, significant disruption once adapted system

Early analysis and disclosure to Google is vital!

Architecture



Permission Model

Four levels of protection level

- **Normal:** No explicit consent needed
- **Dangerous:** Explicit user consent required
- **Signature:** Cryptographically signed with platform certificate
- **signature|privileged:** Cryptographically signed or pre-installed

Third-party applications only have access to normal and dangerous permissions ☺

Permission Model

47 permissions defined in android.car.permission as of October 2019

Permission Name	Protection Level
READ_CAR_DISPLAY_UNITS	Normal
CONTROL_CAR_DISPLAY_UNITS	Normal
CAR_ENERGY_PORTS	Normal
CAR_INFO	Normal
CAR_EXTERIOR_ENVIRONMENT	Normal
CAR_POWERTRAIN	Normal
CAR_SPEED	Dangerous
CAR_ENERGY	Dangerous
BIND_VMS_CLIENT	Signature
BIND_PROJECTION_SERVICE	Signature
BIND_INSTRUMENT_CLUSTER_RENDERER_SE RVICE	Signature
BIND_CAR_INPUT_SERVICE	Signature

CAR_MOCK_VEHICLE_HAL	signature|privileged
READ_CAR_STEERING	signature|privileged
CAR_IDENTIFICATION	signature|privileged
CAR_MILEAGE	signature|privileged
CAR_TIRES	signature|privileged
CAR_ENGINE_DETAILED	signature|privileged
CAR_DYNAMICS_STATE	signature|privileged
CAR_VENDOR_EXTENSION	signature|privileged
CAR_PROJECTION	signature|privileged
ACCESS_CAR_PROJECTION_STATUS	signature|privileged
CONTROL_CAR_SEATS	signature|privileged
CONTROL_CAR_MIRRORS	signature|privileged
CONTROL_CAR_WINDOWS	signature|privileged
CONTROL_CAR_DOORS	signature|privileged
CONTROL_CAR_CLIMATE	signature|privileged

Vehicle Properties

Implemented by VHAL

Vendor-extendable Android module to abstract vehicle data for SDK, APK

Mapping properties to CAN signals provided by DBCs

```
VEHICLEPROPERTY_INVALID = 0x0
VEHICLEPROPERTY_INFO_VIN = 0x11100100
VEHICLEPROPERTY_INFO_MAKE = 0x11100101
VEHICLEPROPERTY_INFO_MODEL = 0x11100102
VEHICLEPROPERTY_INFO_MODEL_YEAR = 0x11400103
VEHICLEPROPERTY_INFO_FUEL_CAPACITY = 0x11600104
VEHICLEPROPERTY_INFO_FUEL_TYPE = 0x11410105
VEHICLEPROPERTY_INFO_EV_BATTERY_CAPACITY = 0x11600106
VEHICLEPROPERTY_INFO_EV_CONNECTOR_TYPE = 0x11410107
VEHICLEPROPERTY_INFO_FUEL_DOOR_LOCATION = 0x11400108
VEHICLEPROPERTY_INFO_EV_PORT_LOCATION = 0x11400109
VEHICLEPROPERTY_INFO_DRIVER_SEAT = 0x1540010a
VEHICLEPROPERTY_PERF_ODOMETER = 0x11600204
VEHICLEPROPERTY_PERF_VEHICLE_SPEED = 0x11600207
VEHICLEPROPERTY_ENGINE_COOLANT_TEMP = 0x11600301
VEHICLEPROPERTY_ENGINE_OIL_LEVEL = 0x11400303
VEHICLEPROPERTY_ENGINE_OIL_TEMP = 0x11600304
VEHICLEPROPERTY_ENGINE_RPM = 0x11600305
VEHICLEPROPERTY_WHEEL_TICK = 0x11510306
VEHICLEPROPERTY_FUEL_LEVEL = 0x11600307
VEHICLEPROPERTY_FUEL_DOOR_OPEN = 0x11200308
VEHICLEPROPERTY_EV_BATTERY_LEVEL = 0x11600309
VEHICLEPROPERTY_EV_CHARGE_PORT_OPEN = 0x1120030a
VEHICLEPROPERTY_EV_CHARGE_PORT_CONNECTED = 0x1120030b
VEHICLEPROPERTY_EV_BATTERY_INSTANTANEOUS_CHARGE_RATE = 0x1160030c
VEHICLEPROPERTY_RANGE_REMAINING = 0x11600308
VEHICLEPROPERTY_TIRE_PRESSURE = 0x17e00309
VEHICLEPROPERTY_GEAR_SELECTION = 0x11400400
VEHICLEPROPERTY_CURRENT_GEAR = 0x11400401
VEHICLEPROPERTY_PARKING_BRAKE_ON = 0x11200402
VEHICLEPROPERTY_PARKING_BRAKE_AUTO_APPLY = 0x11200403
VEHICLEPROPERTY_FUEL_LEVEL_LOW = 0x11200405
VEHICLEPROPERTY_NIGHT_MODE = 0x11200407
VEHICLEPROPERTY_TURN_SIGNAL_STATE = 0x11400408
VEHICLEPROPERTY_IGNITION_STATE = 0x11400409
VEHICLEPROPERTY_ABS_ACTIVE = 0x1120040a
VEHICLEPROPERTY_TRACTION_CONTROL_ACTIVE = 0x1120040b
```

Agenda

Introduction
Related Work
Threat Model and Background
Security Analysis
Recommendations

EVITA Security Threats

Create PoC attacks based on severity classification of EVITA

Security threat severity class	Aspects of security threats			
	Safety	**Privacy**	**Financial**	**Operational**
0	No injuries	No unauthorized access to data	No financial loss	No impact on operational performance
1	Light or moderate injuries	Anonymous data only (no specific driver of vehicle data)	Low-level loss (≈ € 10)	Impact not discernible to driver
2	Severe injuries (survival probable); light/moderate injuries for multiple vehicles	Identification of vehicle or driver; anonymous data for multiple vehicles	Moderate loss (≈ € 100); low losses for multiple vehicles	Driver aware of performance degradation; indiscernible impacts for multiple vehicles
3	Life threatening (survival uncertain) or fatal injuries; severe injuries for multiple vehicles	Driver or vehicle tracking; identification of driver or vehicle for multiple vehicles	Heavy loss (≈ € 1000); moderate losses for multiple vehicles	Significant impact on performance; noticeable impact for multiple vehicles
4	Life threatening or fatal injuries for multiple vehicles	Driver or vehicle tracking for multiple vehicles	Heavy losses for multiple vehicles	Significant impact for multiple vehicles

Attack #1: Privacy

Goal: Malicious 3rd party app obtains privacy-sensitive driver information

Speed has *dangerous* permission

– Explicit user consent necessary

Gear position and RPM have *normal* permission

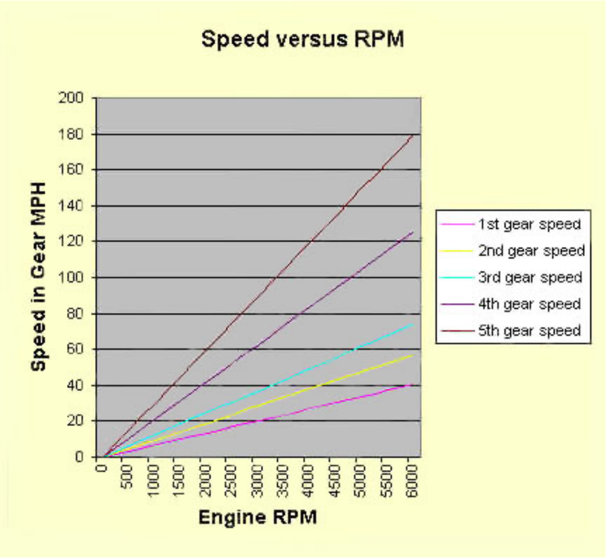
– Can be read by any app without user consent

Speed = f(gear, RPM)

Dangerous permission is circumvented

– More examples possible

– Physical signals have certain relationships with each other...



Source:http://homepages.bw.edu/~katchins/csc131common/a_papers/student2/gearmath.htm

Attack #2: Financial/Operational

Goal: Malicious 3rd party app breaks instrument cluster

CONTROL_CAR_DISPLAY_UNITS has *normal* permission

- Display units for distance, fuel, tire pressure, EV battery, fuel consumption can be modified

Examples: Switch from min. to max. fuel level, force TPMS light to come on etc.

- Bound by 1 Hz frequency (1 change per second)

Financial damage: Needle will break eventually

Operational damage: Driver realizes something is wrong with tires and brings car to dealership/tire shop

Source: https://www.cornwalllive.com/news/uk-world-news/how-far-can-you-drive-697463

Attack #3: Safety

Goal: Malicious 3rd party app accelerates the vehicle instead of displaying value on instrument cluster

Not all CAN signals mapped to vehicle properties

- Acceleration/Gas pedal does not need to be read/written

Option #1: Reverse engineering of the IVI FW

- DBCs and mapping table are stored on IVI
- Change mapping
- Reflash

Option #2: Access via ADB shell

Source: https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Agenda

Introduction
Related Work
Threat Model and Background
Security Analysis
Recommendations

Recommendations

Fine-grained permission model

- Problem: Multiple properties summarized in one permission
- Assign unique permission for property
- Quantify privacy risk of each property, assign protection levels accordingly

Further standardization from Google

- Problem: Vendors given too much free space for implementation design
- Google should define security recommendations and standardize more modules
- Example: DBC mapping without physically storing DBC file, use lookup table in Trusted Execution Environment (TEE)

Recommendations

Separation of domains in IVN architecture

- Problem: IVI might control other (safety-critical) ECUs
- Implement access control, e.g., by firewall, in gateway

Protection against runtime attacks

- Problem: Android still suspectible to Return-Oriented Programming (ROP) attacks, can lead to buffer overflows
- Vendor-specific C/C++ code (device drivers, etc.) most vulnerable

Restrict ADB shell access (USB and WiFi!)

- Disable USB debugging by default in production
- Never allow default user to run as root

THANK YOU

Mert D. Pesé
University of Michigan – Ann Arbor
2260 Hayward Street, Ann Arbor, MI 48109-2121, U.S.A

mpese@umich.edu