SAE INTERNATIONAL®

WCX™

APRIL 18-20, 2023
DETROIT

A First Look at Android Automotive Privacy

Mert D. Pesé

Assistant Professor in School of Computing

Director of TigerSec Laboratory

TigerSec Laboratory
@ Clemson University

CLEMSON UNIVERSITY

Android Automotive OS (AAOS) on the Rise!

Android Automotive goes mainstream: A review of GM's new infotainment system

It has four screens, three operating systems, and many of the usual car problems.

RON AMADEO - 1/6/2023, 7:20 AM

Source: https://arstechnica.com/gadgets/2023/01/android-automotive-goes-mainstream-a-review-of-gms-new-infotainment-system/

March 13, 2023 09:22 AM

Porsche in talks with Google about integrating software

Reuters

Source: https://europe.autonews.com/automakers/porsche-talks-google-over-software-deal-ceo-says

VW will support Android Automotive for the "lifetime" of a car—15 years

It's the answer to a question we've been pondering for some time.

JONATHAN M. GITLIN - 3/22/2023, 1:16 PM

Source: https://arstechnica.com/cars/2023/03/android-infotainment-will-be-supported-for-at-least-15-years-vw-says/

Android Apps Taking Over Cars, Making Android Auto and CarPlay Feel Outdated

Home > News > Coverstory

25 Feb 2023, 09:20 UTC • By: Bogdan Popa

Source: https://www.autoevolution.com/news/android-apps-taking-over-cars-making-android-auto-and-carplay-feel-outdated-210918.html

More than 15 car brands pledged to use AAOS

AAOS market share expected to grow from 1% in 2022 to 18% by 2027

Android Auto vs Android Automotive (AAOS)

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

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

AAOS: The Next Generation of Infotainment

TRANSPO / GM / ELECTRIC CARS

GM is cutting off access to Apple CarPlay and Android Auto for its future EVs

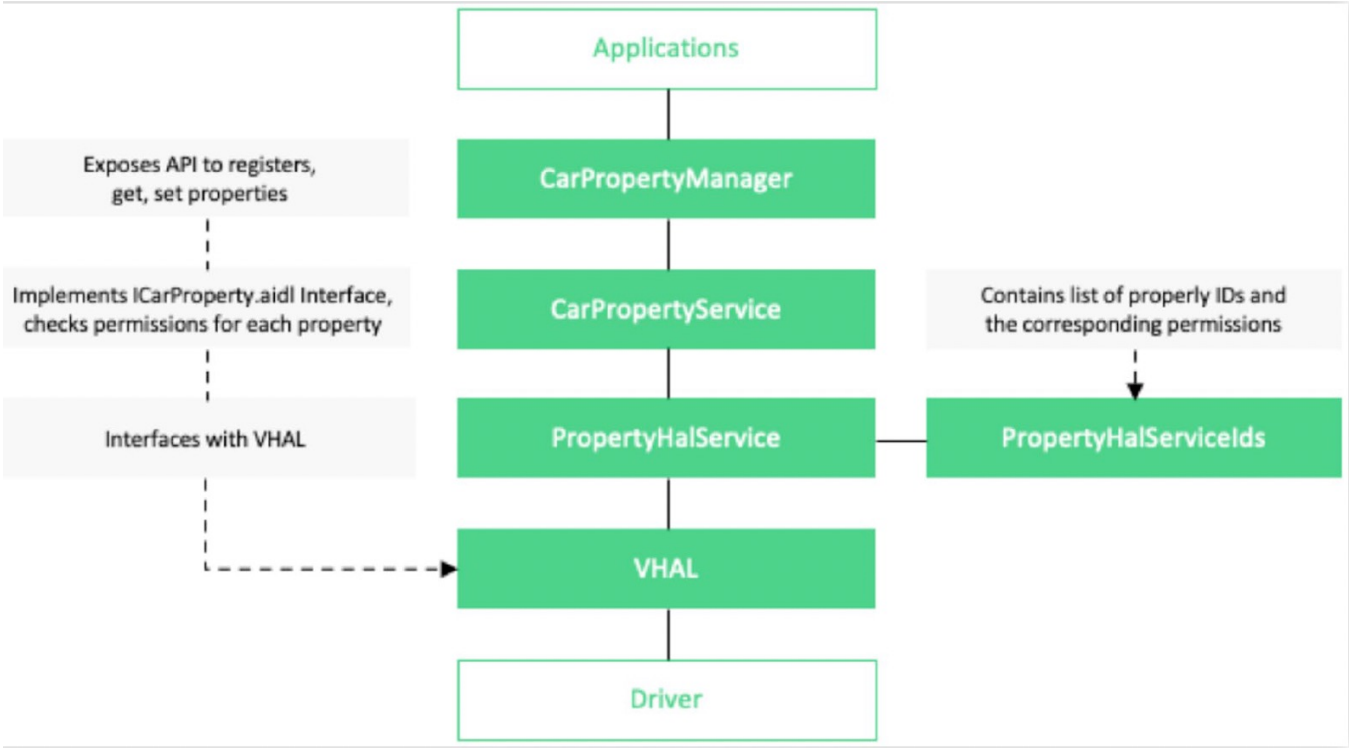
The 2024 Chevy Blazer EV will be the first GM vehicle to restrict access to Apple CarPlay and Android Auto. Image: GM

/ Starting with the 2024 Chevy Blazer EV, General Motors' electric vehicles will restrict Apple CarPlay and Android Auto in favor of a native Google infotainment system.

By ANDREW J. HAWKINS / @andyjayhawk
Mar 31, 2023, 1:21 PM EDT | 251 Comments / 251 New

Source: https://www.theverge.com/2023/3/31/23664814/gm-ev-restrict-apple-carplay-android-auto-google

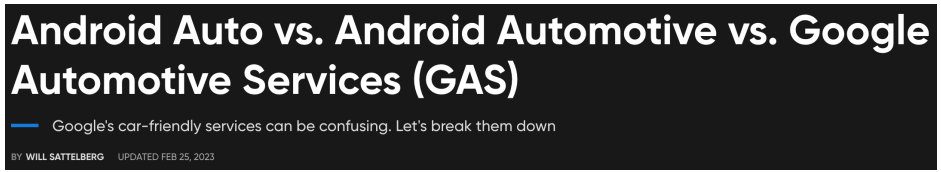
AAOS System Architecture



Source: https://www.androidautomotivebook.com/android-automotive-andphysical-car-interaction/

AAOS App Ecosystem

- Different kinds of Android apps (APKs) installed on Infotainment (IVI) devices
  - **AOSP** (**A**ndroid **O**pen **S**ource **P**roject): APKs baked into base AAOS builds, usually dependencies of other APKs
    - Examples: *com.android.carrierconfig*, *com.android.car.systemupdater*
  - **Google**: Part of GAS (Google Automotive Services), OEM can choose to include them on their vehicles
    - Majority of OEMs choose to use them to offer premium in-car experience
    - Examples: *com.google.android.carassistant*, *com.google.android.apps.maps*



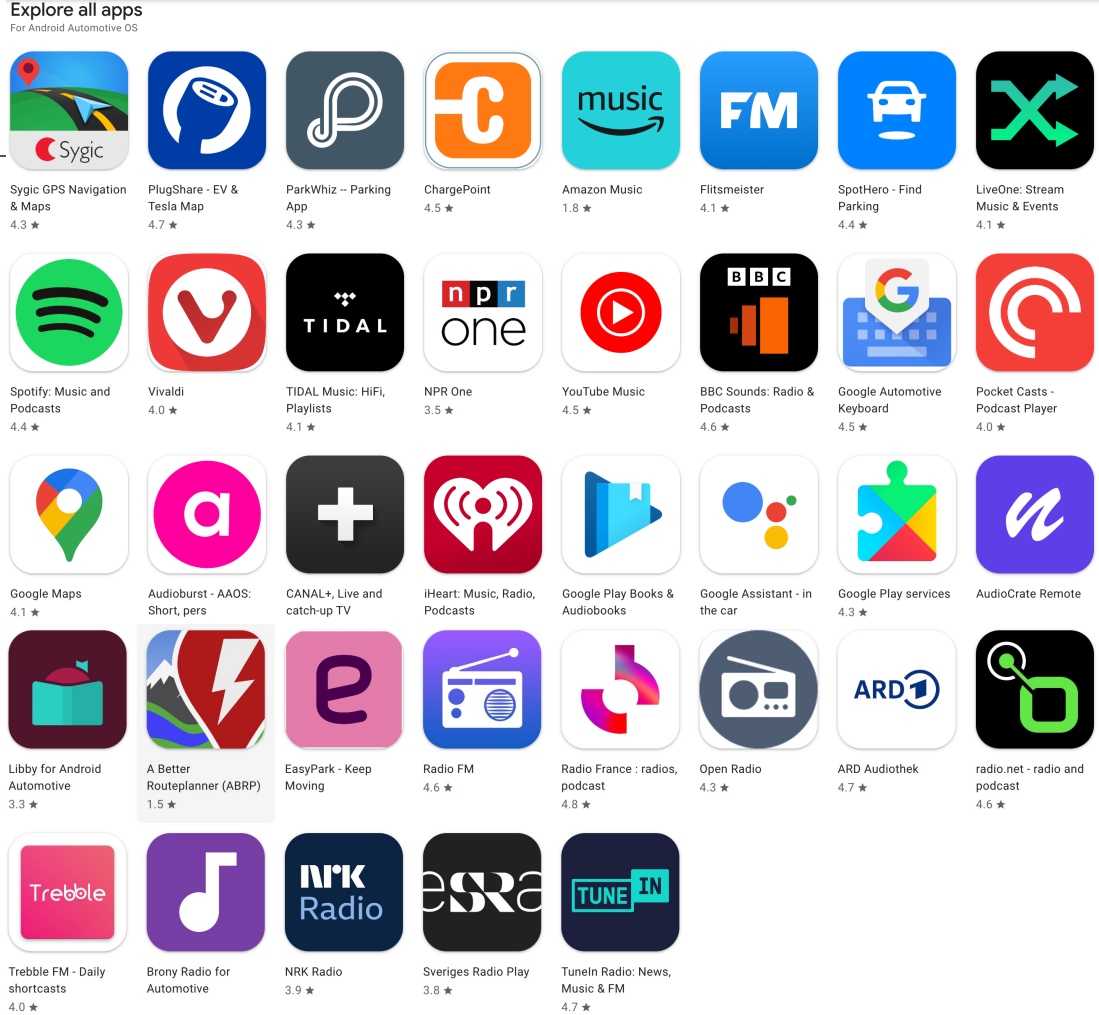
Source: https://www.androidpolice.com/android-auto-vs-android-automotive-vs-google-automotive-services/

AAOS App Ecosystem

- Different kinds of Android apps (APKs) installed on Infotainment (IVI) devices
  - **OEM**: Provided by car manufacturer, only part of production build on their vehicles, custom themes
    - Examples: *com.polestar.audiosettings*, *com.polestar.abrp.production.android*
  - **Third-party**: Found on Google Play Store, developed by independent third-party app developers, shared across different production builds of OEMs
    - Examples: *com.parkwhiz.driverApp*, *com.amazon.mp3.automotiveOS*

Third-Party APKs

- 55 APKs developed by independent app developers
- 37/55 APKs generically available for all production builds
- Different categories
  - Maps & Navigation
  - Music & Audio
  - News & Magazines
  - Entertainment
  - Productivity
  - Tools



Android 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 ☺

Android Permission Model

- 31 dangerous permissions in Android
- 2 car-specific dangerous permissions
  - CAR_SPEED
  - CAR_ENERGY
- Permissions can be mapped to more coarse-grained permission groups
  - 11 permission groups
  - Our focus in this paper
- Permissions defined in Android Manifest (part of every APK)

Dangerous Permissions	Permission Group
READ_CALENDAR WRITE_CALENDAR	CALENDAR
CAR_ENERGY	CAR_MONITORING
CAMERA	CAMERA
READ_CONTACTS WRITE_CONTACTS GET_ACCOUNTS	CONTACTS
ACCESS_FINE_LOCATION ACCESS_COARSE_LOCATION ACCESS_MEDIA_LOCATION ACCESS_BACKGROUND_LOCATION CAR_SPEED	LOCATION
RECORD_AUDIO	MICROPHONE
READ_PHONE_STATE ACCESS_NETWORK_STATE	PERSISTENTID
READ_PHONE_NUMBERS CALL_PHONE ANSWER_PHONE_CALLS ADD_VOICEMAIL USE_SIP READ_CALL_LOG WRITE_CALL_LOG PROCESS_OUTGOING_CALLS	PHONE_CALL
ACTIVITY_RECOGNITION BODY_SENSORS	SENSOR
SEND_SMS RECEIVE_SMS RECEIVE_WAP_PUSH RECEIVE_MMS	SMS
READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	STORAGE

AAOS Permission Model

- 111 car-specific permissions in AAOS (selection below)

Permission Name	Protection Level	Description
READ_CAR_DISPLAY_UNITS	Normal	Allows an application to read the display units for distance, fuel, tire pressure, EV battery and fuel consumption.
CONTROL_CAR_DISPLAY_UNITS	Normal	Allows an application to control the display units for distance, fuel, tire pressure, EV battery and fuel consumption.
CAR_ENERGY_PORTS	Normal	Allows an application to read the vehicle fuel and charge port status.
CAR_INFO	Normal	Allows an application to read the vehicle car basic information. For example, it allows an application to read the vehicle Make, Model, Model Year, fuel capacity, fuel type, EV battery capacity, EV connection type, fuel door location and driver seat location.
CAR_EXTERIOR_ENVIRONMENT	Normal	Allows an application to read the vehicle exterior environment information. For example, it allows an application to read the vehicle exterior temperature and night mode status.
CAR_POWERTRAIN	Normal	Allows an application to read the vehicle powertrain information. For example, it allows an application to read the vehicle current gear, ignition state or parking brake status.

Permission Name	Protection Level	Description
READ_CAR_POWER_POLICY	Normal	Allows an application to get the current power policy or to be notified of power policy change.
CAR_SPEED	Dangerous	Allows an application to read the vehicle speed.
CAR_ENERGY	Dangerous	Allows an application to read the vehicle energy information.
CAR_IDENTIFICATION	signature|privileged	Allows an application to read the VIN information.
CAR_MILEAGE	signature|privileged	Allows an application to read the vehicle mileage information.
CAR_ENGINE_DETAILED	signature|privileged	Allows an application to read the vehicle engine information. For example, it allows an application to read the engine oil level, oil temperature, coolant temperature and RPM.
CAR_VENDOR_EXTENSION	signature|privileged	Allows an application to access the vehicle vendor channel to exchange vendor-specific information.
READ_CAR_INTERIOR_LIGHTS	signature|privileged	Allows an application to read the vehicle interior lights state.
CAR_NAVIGATION_MANAGER	signature|privileged	Allows an application to access CarNavigationStatusManager to report navigation data. This information may be displayed by the vehicle in the instrument cluster, head-up display or other locations.

Data Collection and Privacy

- APKs collect and transmit data to application backend
- Only data that is declared in permissions can be collected
- Collection of driver data subject to privacy regulations
  - GDPR (**G**eneral **D**ata **P**rotection **R**egulation)
  - CCPA (**C**alifornia **C**onsumer **P**rivacy **A**ct)
  - CPRA (**C**alifornia **P**rivacy **R**ights **A**ct)
- GDPR is EU-based, most comprehensive privacy regulation to date
- OEMs are data controllers and subject to increased compliance obligations

OEMs sell cars worldwide, GDPR compliance is important

Android Manifests and Privacy Policies

Example: com.parkwhiz.driverApp

- GDPR requires data

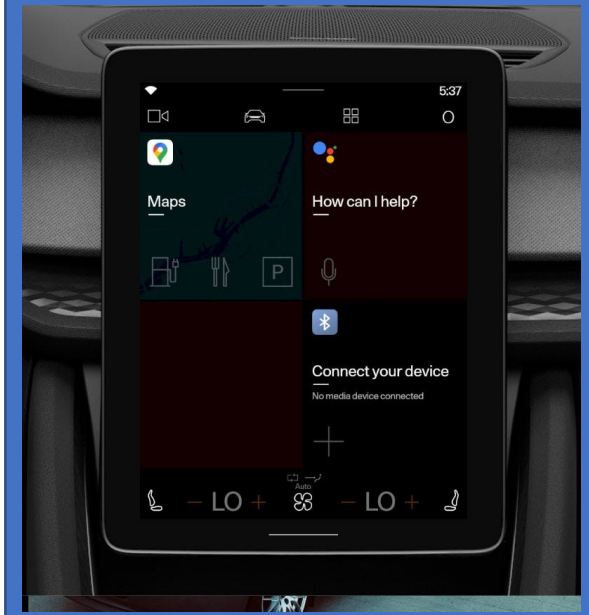
Google does not check content of privacy policy URL

Mismatch between declared permissions in Manifest and stated privacy policy in Play Store URL!

- GDPR requires this as well

Experimental Design

APK Acquisition



Manifest Analysis

APKTOOL

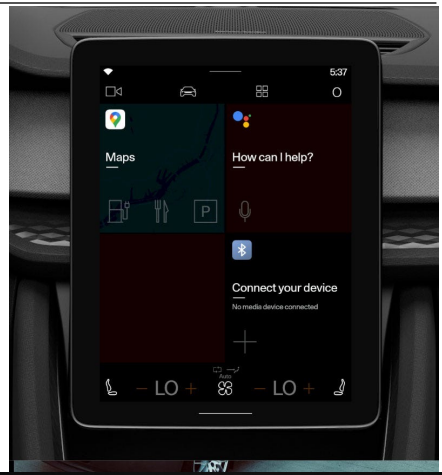
```
$ unzip testapp.apk
Archive:  testapp.apk
 inflating: AndroidManifest.xml
 inflating: classes.dex
 extracting: res/drawable-hdpi/ic_launcher.png
 inflating: res/xml/literals.xml
 inflating: res/xml/references.xml
 extracting: resources.arsc
```

Privacy Policy Analysis

APK Acquisition

Android Debug Bridge

- 55 third-party APKs
  - 37 generic (can be found across all GAS production builds)
  - 16 Polestar 2
  - 2 Volvo XC40
- **Problem**: APKs cannot be found on Mirror websites
- **Solution**: Scrape APKs from production builds using adb (**A**ndroid **D**ebug **B**ridge)
- Use two publicly available non-rooted emulator devices
  - Polestar 2 (Geely Group)
  - Volvo XC40 (Geely Group)



Manifest Analysis

- **Recall**: Permissions declared in AndroidManifest.xml
- APKs are container format that can be decompiled using tools such as **apktool**

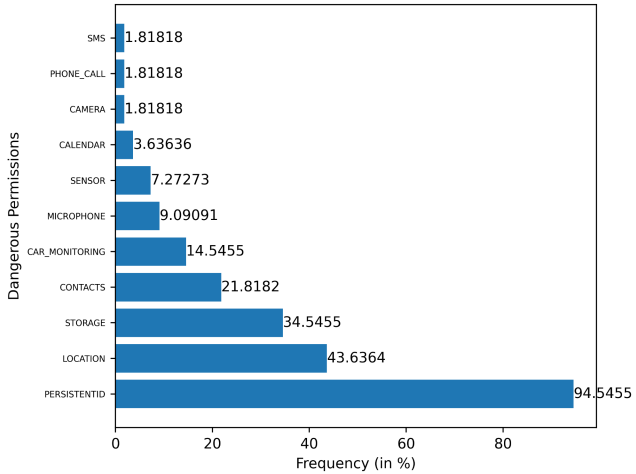
```
$ unzip testapp.apk
Archive:  testapp.apk
 inflating: AndroidManifest.xml
 inflating: classes.dex
 extracting: res/drawable-hdpi/ic_launcher.png
 inflating: res/xml/literals.xml
 inflating: res/xml/references.xml
 extracting: resources.arsc
```

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="20819482" android:versionName="13.5.4" android:compileSdkVersion="31" android:compileSdkVersionCodename="12" p
  xmlns:android="http://schemas.android.com/apk/res/android"
  xmlns:dist="http://schemas.android.com/apk/distribution">
    <uses-sdk android:minSdkVersion="29" android:targetSdkVersion="30" />
    <dist:module dist:instant="false" />
    <uses-feature android:name="android.hardware.type.automotive" android:required="true" />
    <uses-feature android:name="android.software.car.templates_host" android:required="true" />
    <uses-feature android:name="android.hardware.wifi" android:required="false" />
    <uses-feature android:name="android.hardware.screen.portrait" android:required="false" />
    <uses-feature android:name="android.hardware.screen.landscape" android:required="false" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="androidx.car.app.MAP_TEMPLATES" />
    <uses-permission android:name="android.permission.BLUETOOTH" android:required="false" />
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN" android:required="false" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <queries>
        <intent>
            <action android:name="android.car.template.host.RendererService" />
        </intent>
        <provider android:authorities="androidx.car.app.connection" />
        <package android:name="com.venmo" />
        <package android:name="com.paypal.android.p2pmobile" />
        <intent>
            <action android:name="android.intent.action.VIEW" />
            <category android:name="android.intent.category.BROWSABLE" />
            <data android:scheme="https" />
        </intent>
    </queries>
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.WAKE_LOCK" />
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE" />
    <uses-feature android:glEsVersion="0x00020000" android:required="true" />
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE" />
    <application android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:name="com.arrive.android.auto.app.AutoApplicatio
```

android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
androidx.car.app.MAP_TEMPLATES	unknown	Unknown permission	Unknown permission from android reference

Manifest Analysis

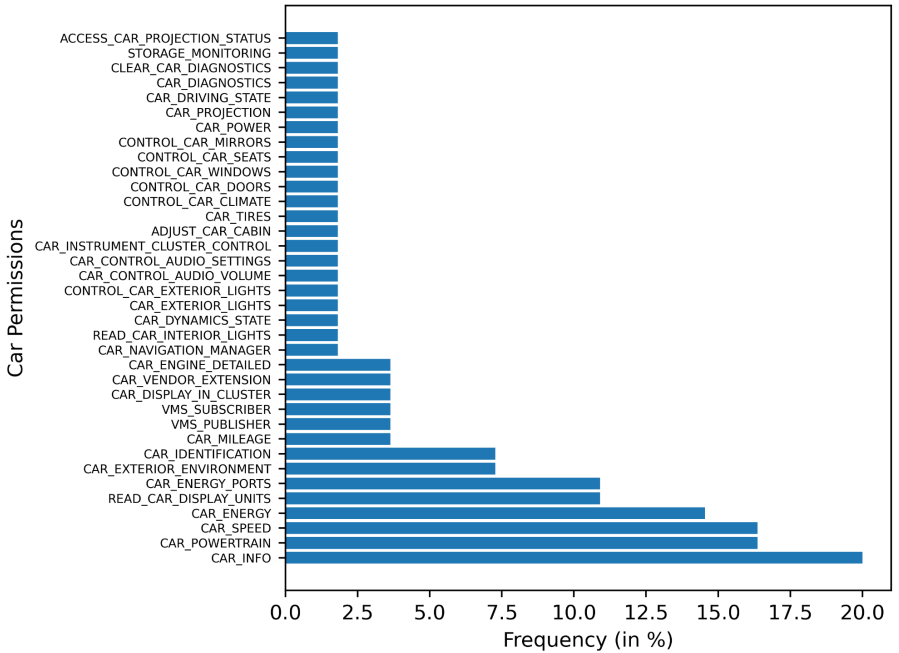
- **Recall**: 31 dangerous permissions, 2 car-specific
- SMS, PHONE_CALL, CAMERA, CALENDAR seem interesting due to lack of these capabilities on AAOS builds



Dangerous Permissions	Permission Group
READ_CALENDAR WRITE_CALENDAR	CALENDAR
CAR_ENERGY	CAR_MONITORING
CAMERA	CAMERA
READ_CONTACTS WRITE_CONTACTS GET_ACCOUNTS	CONTACTS
ACCESS_FINE_LOCATION ACCESS_COARSE_LOCATION ACCESS_MEDIA_LOCATION ACCESS_BACKGROUND_LOCATION CAR_SPEED	LOCATION
RECORD_AUDIO	MICROPHONE
READ_PHONE_STATE ACCESS_NETWORK_STATE	PERSISTENTID
READ_PHONE_NUMBERS CALL_PHONE ANSWER_PHONE_CALLS ADD_VOICEMAIL USE_SIP READ_CALL_LOG WRITE_CALL_LOG PROCESS_OUTGOING_CALLS	PHONE_CALL
ACTIVITY_RECOGNITION BODY_SENSORS	SENSOR
SEND_SMS RECEIVE_SMS RECEIVE_WAP_PUSH RECEIVE_MMS	SMS
READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	STORAGE

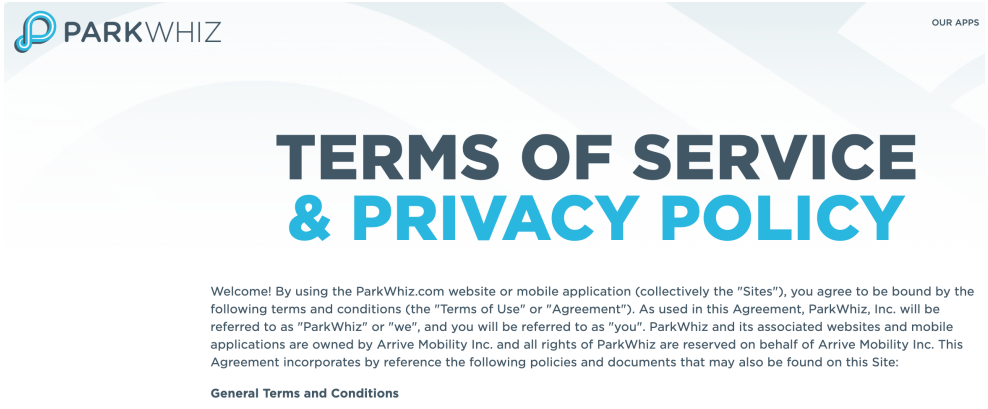
Manifest Analysis

- 14/55 APKs use car-specific permissions
  - Most APKs media apps
  - Our focus in this paper
- 1 in 5 APKs use CAR_INFO
  - Normal (“zero”) permission
  - Make, Model, Year of vehicle
- 1 in 6 APKs use CAR_SPEED
  - Dangerous permission



Privacy Policy Analysis

- Only dangerous permissions need to be included in natural language policy text
- Manual extraction of permission groups
  - Low number of APKs
  - To reduce subjectivity: Second human reviewer
- Include indirect references
  - Example: Creating data log will require *STORAGE* permission group



Permission Analysis for Dangerous Protection Level

Package Name	Permission Declared	LOCATION	CAMERA	CALENDAR	STORAGE	MICROPHONE	SENSOR	CONTACTS	PERSISTENTID	CAR_ENERGY	CAR_SPEED	GDPR	CCPA	# Discrepancies
	Manifest	X	X	X	X	X	X			X	X			3
com.polestar.abrp.production.android	Privacy Policy	X			X		X			X	X	X		
	Manifest	X							X	X				1
com.polestar.easypark.production.android	Privacy Policy	X							X					
	Manifest	X			X		X			X				2
com.sygic.aura	Privacy Policy	X								X		X		
	Manifest	X						X			X			2
com.xatori.Plugshare	Privacy Policy	X							X			X	X	
	Manifest	X												0
com.parkwhiz.driverApp	Privacy Policy	X											X	
	Manifest	X								X	X			1
com.coulombtech	Privacy Policy	X	X		X						X		X	
	Manifest	X		X	X	X	X	X	X					5
nl.flitsmeister	Privacy Policy	X							X					
	Manifest	X			X			X	X					1
com.spothero.spothero	Privacy Policy	X						X	X				X	
	Manifest	X			X		X	X	X	X	X			3
com.google.android.apps.maps	Privacy Policy	X			X		X		X				X	
	Manifest	X								X	X			1
com.polestar.driver.journey.log.production.android	Privacy Policy	X									X	X		
	Manifest													0
com.polestar.spacewarp.production.android	Privacy Policy	X								X	X			
	Manifest	X							X	X	X			4
com.polestar.p2performancepack.production.android	Privacy Policy													
	Manifest								X					0
com.polestar.web.production.android	Privacy Policy								X			X		
	Manifest	X							X	X	X			2
net.vonforst.evmap	Privacy Policy	X							X					

Findings

- Only 3/14 AAOS APKs (**21%**) have complete description of all requested dangerous permissions in privacy policies
  - Compares to 31% for mobile Android apps [1]
  - *CAMERA*, *CALENDAR*, *MICROPHONE* requested, but never defined in Manifest ➔ Probably legacy artifacts from mobile versions of APK

- Discrepancies range from 0 to 5 permissions per APK
  - **16%** of dangerous permissions never mentioned in privacy policies
  - **36%** of car-specific dangerous permissions never mentioned in privacy policies

Findings

- **38%** of normal (“zero”) car-specific permissions are sometimes mentioned in privacy policies
  - Technically not required

- 5/14 APKs (**36%**) declare signature permissions
  - However, third-parties only restricted to normal and dangerous permissions!
  - Explanation: 4 APKs signed with OEM (e.g., Polestar) or Google key
  - 1 APK unaccounted (*com.sygic.aura*)

- 5/14 APKs (**36%**) mention GDPR or CCPA in privacy policies

Conclusion

- Third-party app developers are not very consistent nor transparent in explaining sensitive permissions to users
- Over 78% of AAOS apps have inconsistencies in privacy policy
- At least two apps overprivileged

Next Step:

Analyze permission usage in APK source code using static and dynamic analysis techniques.

Contact Info

Thank You!

Mert D. Pesé
Clemson University
821 McMillan Rd, Clemson, SC 29634
www.mpese.com
mpese@clemson.edu

References

[1] Rahman, M.S., Naghavi, P., Kojusner, B., Afroz, S. et al., “PermPress: Machine Learning-Based Pipeline to Evaluate Permissions in App Privacy Policies,” IEEE Access 10 (2022): 89248-89269.