Poster: PRIDRIVE: An Advanced Privacy Analysis Tool for Android Automotive

Bulut Gozubuyuk, Mert D. Pesé
Clemson University
{bgozubu, mpese}@clemson.edu

***Abstract*—Android Automotive OS (AAOS) has emerged as a key player in the the In-Vehicle Infotainment (IVI) sector, influencing over 100 million vehicles. This paper introduces an innovative privacy analysis tool in this domain. Utilizing a combination of static analysis, dynamic analysis, and Deep Packet Inspection (DPI), the tool automatically measures the data collected from the vehicle by Original Equipment Manufacturers (OEMs) which can have an impact on drivers' privacy.**

Introduction. As AAOS extends its presence in connected vehicles, ensuring robust privacy protection becomes critical. Our tool is specifically designed to address this challenge, offering a comprehensive analysis of privacy dynamics within AAOS. In an environment where sensitive data leaks pose significant privacy threats, such as the potential inference of vehicle speed from accessible engine data [2], our tool provides an essential safeguard. Unlike Android Auto and Apple CarPlay, AAOS runs directly within vehicles, interfacing with the Electronic Control Unit (ECU) and the IVI and this amplifies the importance of managing privacy risks [3]. Our tool is not merely an analytical asset but a pivotal instrument for advancing privacy standards in the automotive industry.

Background. AAOS is based on the Android Open Source Project (AOSP) [1]. Its direct integration with the CAN bus underscores the importance of the Vehicle Hardware Abstraction Layer (VHAL). The latter defines OEMs' implementable properties, including key vehicle properties such as tire pressure and engine RPM, each accompanied by detailed metadata. The Android permission model, with its install time, runtime, and special permissions categories, delineates various access levels to these features. Our study employed tools such as *logcat* for system logging, *Frida Toolkit* for application behavior analysis, *mitmproxy* and *Wireshark* for network monitoring, forming a comprehensive approach to measure collected data by OEMs and evaluate AAOS's privacy landscape.

Method. The tool starts by setting up an Android emulator with a production image from an automaker and securing root access using a Magisk module. Network traffic analysis is a crucial component, achieved by reconfiguring the emulator to accept a modified mitmproxy CA certificate, which allows mitmproxy to intercept all network communications. Wireshark is also employed for detailed protocol analysis. On the application front, the Frida server is installed on the emulator for dynamic analysis of application activities. Furthermore, the tool collects all APK files from the emulator into a system dump, enabling static analysis by automatically decompiling APKs with jadx. Dynamic analysis involves using Frida-Trace to log VHAL system calls associated with these APK files. The tool gathers logcat information and utilizes tcpdump, ensuring a comprehensive data collection. The JSON output below from the tool illustrates how each app involves specific property IDs.

Listing 1. JSON output example

```
"App1Name": {
    "VHAL_PROPERTY1_ID": {
        "description": "VHAL_PROPERTY1_DESCRIPTION",
        "occurrences": PROPERTY1_OCCURENCE_COUNT
    },
    "VHAL_PROPERTY2_ID": {
        ...
},
"App2Name": {
    ...
```

Table I shows the count of vendor VHAL properties and custom OEM permissions after running our tool with four real-world OEM emulator images as input.

TABLE I
NUMBER OF CUSTOM PERMISSIONS AND PROPERTIES DEFINED BY OEMS

Platform	Custom VHAL Properties	Custom Permissions
OEM A	753	225
OEM B	436	338
OEM C	193	34
OEM D	156	21

Conclusion. Our tool can effectively analyze data from different emulators, focusing on the unique Android permissions of OEMs, their specific vendor VHAL property IDs, and usage frequencies. It can also examine network behaviors and runtime logs of all APKs in the study. While data collection alone does not imply privacy concerns, our tool's analysis marks a significant step in scrutinizing AAOS's privacy aspects which serves as a foundation for future research in this area.

REFERENCES

[1] "Android automotive," https://source.android.com/docs/automotive.
[2] M. Pese, K. Shin, J. Bruner, and A. Chu, "Security analysis of android automotive," *SAE International Journal of Advances and Current Practices in Mobility*, vol. 2, no. 2020-01-1295, pp. 2337–2346, 2020.
[3] M. D. Pese, "A first look at android automotive privacy," SAE Technical Paper, Tech. Rep., 2023.

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25024
www.ndss-symposium.org