ARMY CYBER INSTITUTE

WHITE PAPER

Vehicle Privacy in the GSA Fleet

Date: December 16, 2024
Authors: CDT Ian Campbell, CDT Zach Daher, CDT Heainz Manoj
LTC Bruce Chojnacki
Approved by: Professor Robert Barnsby, ACI Director
Contact: bruce.chojnacki@westpoint.edu

Executive Summary

Modern vehicles increasingly collect and transmit driver and passenger data including biometrics, personal identifiers, telemetry, and driving behavior. This data poses significant privacy and security risks, especially for military personnel. Research conducted at the United States Military Academy examined vehicles' wireless data transmissions and on-board data collection using Wireshark, Spectrum Guard Pro, and On-Board Diagnostic tools. The study highlighted potential vulnerabilities in cellular data, Wi-Fi, and Bluetooth transmissions. Recommendations include technical research into LTE data, advanced analysis of onboard data repositories, education for personnel on mitigating privacy risks, and policy updates.

Key Points

- Types of Data Collected:
  - Modern vehicles collect information about a driver's geolocation, driving behaviors, biometric data (in-car cameras), personal identifiers, and phone data (calls, texts) through wired and Bluetooth connections.
  - Data from sensors, such as tire pressure, engine diagnostics, environmental data, and vehicle speed, can also be logged and transmitted.
- Lack of Awareness of Vehicle Privacy Policies:
  - Vehicle users, including military personnel, lack awareness of privacy risks due to complex and unclear manufacturer policies.
  - GSA fleet vehicle assignments operate similarly to renting a car. Users often do not know what type of vehicle they will be operating and are not given the opportunity to review or agree to any privacy policy.
- Risks over Wi-Fi and Bluetooth:
  - Vehicles broadcast Wi-Fi signals with unique MAC addresses and ESSIDs when hotspots are enabled, creating tracking risks.
  - Data from personal devices (phones) can be collected by a vehicle when connected through both wired and wireless connections.
- Potential LTE/5G Privacy Risks:
  - Cellular networks likely carry sensitive data from the vehicle to manufacturers and data brokers. This data is difficult to analyze due to the encryption of cellular transmissions.
  - Most vehicles made after 2019 have onboard SIM cards and connect to cellular networks.

Recommendations

- Technical Investigations:
  - Analyze LTE/5G cellular transmissions with a private base station to identify the data being transmitted and the destination.
  - Conduct hardware analysis by accessing vehicle on-board memory, infotainment systems, and Electronic Control Units (ECUs).

- Educational Initiatives:
  - Train personnel to disable onboard Wi-Fi hotspots.
  - Train personnel to remove data collected by the vehicle from the user's Bluetooth phone connection when returning a vehicle.
  - Educate personnel about vehicle privacy settings.

- Policy Updates
  - Develop contracting policies to limit/restrict manufacturer's ability to collect data on vehicles in the GSA fleet.
  - Require the disclosure of data collection on vehicles in the GSA fleet from manufacturers.