Poster: Unseen Threats: The Privacy Risks of Data Collection in Government Fleet Vehicles

Bruce Chojnacki, Zachary Daher, Alexander Master
United States Military Academy
{bruce.chojnacki, zachary.daher, alexander.master}@westpoint.edu

***Abstract*—Data collection and transmission in connected vehicles pose privacy concerns when the vehicles are part of a government-operated fleet. U.S. Army leaders and personnel rely on the General Services Administration's (GSA) fleet vehicles for their day-to-day duties. These connected vehicles may introduce privacy risks to individuals employed in a national security context by collecting and transmitting sensitive data. This study investigates connected vehicles belonging to the GSA fleet. Our objective is to analyze the data collected by these vehicles, capture the data, and analyze their transmissions to external parties.**

Introduction. Auto manufacturers improve their products by incorporating hardware and software into connected vehicles (internet-enabled vehicles with intelligent autonomous onboard systems). These enhancements enable connected vehicles to gather and transmit significant data (Figure 1).

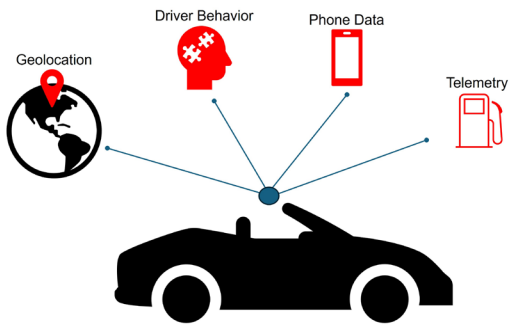

Figure 1. Data Collected by a Connected Car

Collecting and transmitting this data can be a privacy and mission risk for the U.S. Army. The Army relies on the General Services Administration (GSA) for fleet vehicles supporting VIP movements and operational missions. The users of connected cars may unknowingly allow the collection and transmission of sensitive data, enabling adversaries to exploit the data for intelligence gathering, digital surveillance, or cyberspace operations.

Research Objectives. This study investigates the information collected and transmitted by connected vehicles in the GSA fleet. We focused on identifying privacy risks associated with these vehicles using network and radio frequency analysis tools to monitor outbound transmissions. Distinguishing differences between government fleet vehicles and commercially available cars (if any) will be one of our key outcomes. Our team utilized Spectrum Guard Pro, Onboard Diagnostic (OBD) tools, and Wireshark to detect and analyze data collection and transmission. These tools allowed for the investigation of radio frequency channels, including Wi-Fi, Bluetooth, and cellular networks. We aimed to identify potential privacy concerns and recommend strategies to mitigate risks.

Scope of Automotive Data Collection. There are many technical methods for connected vehicles to gather data about drivers and their driving behaviors from onboard systems and sensors. When drivers use an account on their infotainment system or an onboard connection service (i.e., AT&T Connected Car), they may expose their name, address, and contact information, which could be shared with a third party. Many drivers connect their phones to their connected vehicles via Bluetooth or USB. Connected vehicles can access phone data, such as contact lists, call histories, and text messages. If this data is retained by the connected vehicle or transmitted outside the car, it can pose a privacy issue. Driving behavior is also recorded, capturing details such as the rate of acceleration, braking intensity, steering inputs, and instances of speeding, which can reveal individual driving styles [1]. These behaviors can negatively impact a driver's insurance rates if shared with their insurance company [2]. Many car insurance companies now offer programs that install data collection devices in a driver's car, providing an incentive to lower rates when the driver operates the vehicle safely.

Connected vehicles use geolocation data to offer drivers navigation routes and road conditions. GPS maintains a history of past routes for the driver's convenience. Some models of connected vehicles even provide predictive navigation. Tesla has an Automatic Navigation feature that analyzes a driver's usual driving routes to automatically input a route when the driver enters their car to commute to work in the morning [3]. Many connected vehicles also save a user's financial information, including credit card data. Drivers use this information to make in-car purchases, subscriptions, or EV charging. Additionally, connected vehicles have internal and external cameras that capture video when the car is both stationary and in motion.

Data Weaponization. Connected vehicles pose real-world risks. They are data-rich targets with network capabilities that enable remote access. A malicious actor may target a connected vehicle to collect information, steal financial data, or exploit vulnerabilities. Commercial entities may aggregate data that can be used to target individuals or organizations [4].

Methodology. Our study sought to determine what data connected vehicles collect about drivers through sensors, onboard systems, and connected devices. We aimed to find out whether connected vehicles store this data and what they do with it. Furthermore, we wanted to determine if connected vehicles transmit this data through any of their built-in transmission systems, including Wi-Fi, Bluetooth, or cellular. Lastly, we aimed to identify where this data is being sent.

Our methodology involved working from the exterior to the interior of the connected vehicles. First, we isolated the vehicle to prevent any collateral interference and collection. Then, we scanned the car to analyze radio transmissions. We connected to the vehicle's wireless and physical access points (Figure 2).

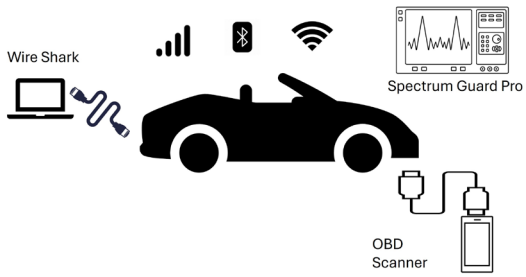

Figure 2. Data Collection

Electromagnetic Spectrum Analysis. We analyzed the electromagnetic spectrum (EMS) and determined which frequencies were used by the connected vehicles. We utilized a Spectrum Guard Pro, a portable spectrum analyzer that detects and logs electromagnetic signals. This process enabled our team to classify the detected signals into the wireless technologies that the connected vehicles employ, including Wi-Fi, Bluetooth, cellular (LTE/5G), proprietary radio frequency protocols for key fobs, or tire pressure monitoring systems (TPMS). Comparing baseline measurements (e.g., car running) with measurements taken after specific actions or the connection of external devices helps to characterize vehicle EMS emissions.

Network Packet Capture with Wireshark. After determining a connected vehicle's transmission capabilities, we connected devices to the access points. Using Wireshark, we conducted packet sniffing and protocol analysis. For Wi-Fi analysis, we examined unencrypted packets and metadata and determined whether vehicle telemetry, geolocation, mobile device information, and/or driver behavior metrics were being transmitted. Additionally, we investigated whether destination information could be identified.

Bluetooth Analysis. We monitored Bluetooth traffic for sensitive or destination information. We connected to vehicles' infotainment systems via Bluetooth to capture handshake protocols or data streams to determine if personal information (e.g., contact lists and call logs) was transmitted.

On-Board Diagnostic (OBD) Port Analysis. This port is mainly used to diagnose issues in a car during maintenance. We used an Autel Maxisys MS919 (commercial device) connected to the OBD port to capture and analyze data.

Preliminary Results. Our study showed that GSA fleet vehicles do not transmit unencrypted sensitive information over Wi-Fi or Bluetooth. However, a risk exists for passive surveillance through unique signals broadcast by connected vehicles, such as Wi-Fi SSIDs and MAC addresses. There are Bluetooth connection artifacts that reside in vehicle infotainment systems. Typically, a fleet vehicle user does not erase their Bluetooth artifacts when returning a car from use. This information can be used to link a specific driver to a car. In our tests, we have not yet found that driver information was being transmitted to manufacturers or third parties.

Future Work. We plan to investigate the data transmitted over LTE/5G cellular networks by employing man-in-the-middle exploitation to characterize the types of data transmitted and determine first-party versus third-party exposures. Future work will involve intercepting vehicle communication using a private cellular base station. Extracting data from vehicle infotainment systems will enhance our efforts.

REFERENCES

[1] SAE International, "Driver Identification Using Vehicle Telematics Data" Jan. 2017. [Online]. Available: https://www.sae.org.

[2] The New York Times, "Carmakers' Driver-Tracking Insurance" *The New York Times*, Mar. 11, 2024. [Online]. Available: https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html.

[3] Teslarati, "Tesla introduces new Automatic Navigation destination feature in software 2023.26" *Teslarati*, 2023. [Online]. Available: https://www.teslarati.com/tesla-automatic-navigation-destination-feature-2023-26/.

[4] Fox et al., "Death by a Thousand Cuts: Commercial Data Risks to the Army" Technical Report, Army Cyber Institute. Dec. 2023. Available: https://cyber.army.mil/Portals/3/Documents/2023_ACI_Commercial_Data_Report.pdf.