Unseen Threats: Weaponization of Privacy Data in Government Fleet Vehicles

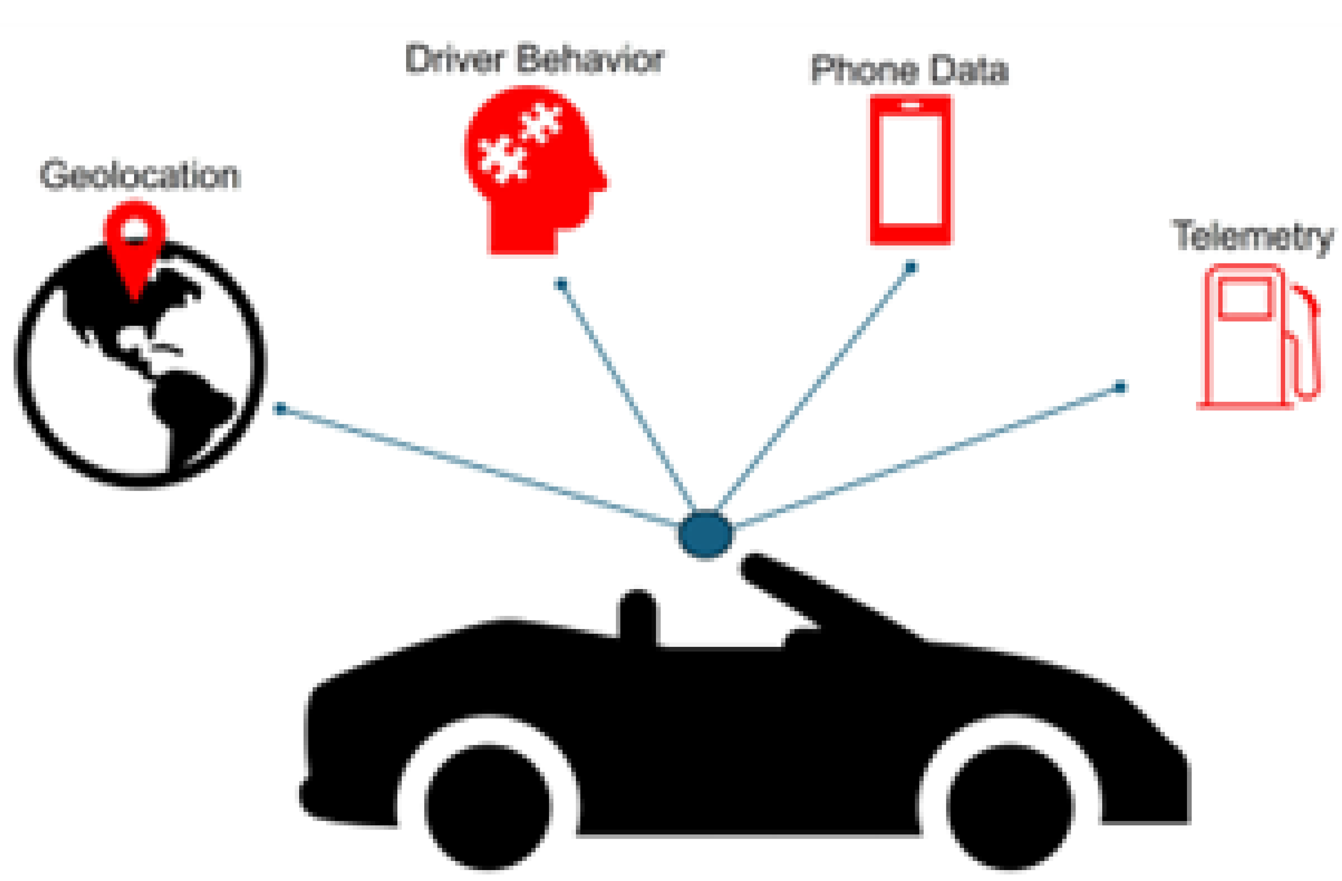
CDT Zachary Daher
Advisor: LTC Bruce Chojnacki

ABSTRACT

Automobile manufacturers produce connected vehicles with improved hardware and software capabilities each year. The vehicles offer safety and convenience features for drivers and passengers, like predictive navigation and text-to-voice capabilities. Collecting user data enables the provision of many of these features. This data includes vehicle telemetry, geolocation, mobile device information, and driver behavior metrics. While gathering this data from drivers enables futuristic and convenient features, it also presents privacy risks. The extent of this data collection is unclear to many drivers, and many may not know that their data is being collected to begin with. These drivers may also be unaware that manufacturers and third parties could use this data.

BACKGROUND

Drivers may not know their data is being collected. Data collection and transmission become even more concerning when connected vehicles are part of a government-operated fleet. Army leaders and personnel rely on General Services Administration (GSA) vehicles for daily operations, and even if they are aware of potential data exploitation, they have little choice but to use them. In a national security context, these connected vehicles can pose serious privacy and security risks by collecting and transmitting sensitive information. This data could be intercepted or exploited by foreign adversaries, potentially undermining the U.S. Army's operations and mission.

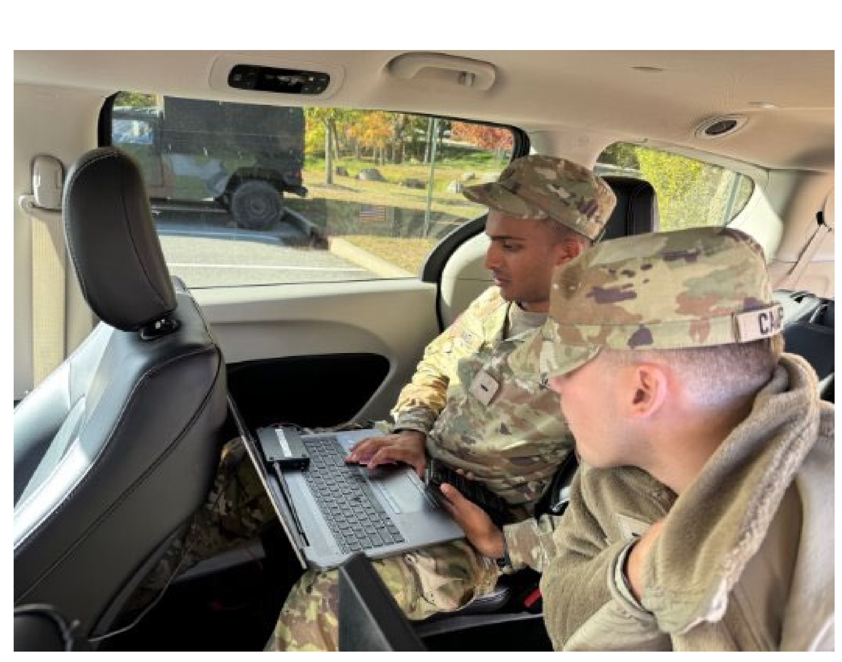


Military Analogy:

You are setting up a platoon ambush. The PL and PSG split off to recon the objective, leaving the rest of the unit at the ORP. Everything is supposed to stay quiet, disciplined, and tactical.

As soon as the PL steps off, one soldier starts yelling out grid coordinates. Loud. Repeatedly. No one else says anything — but now the enemy knows *exactly* where we are.

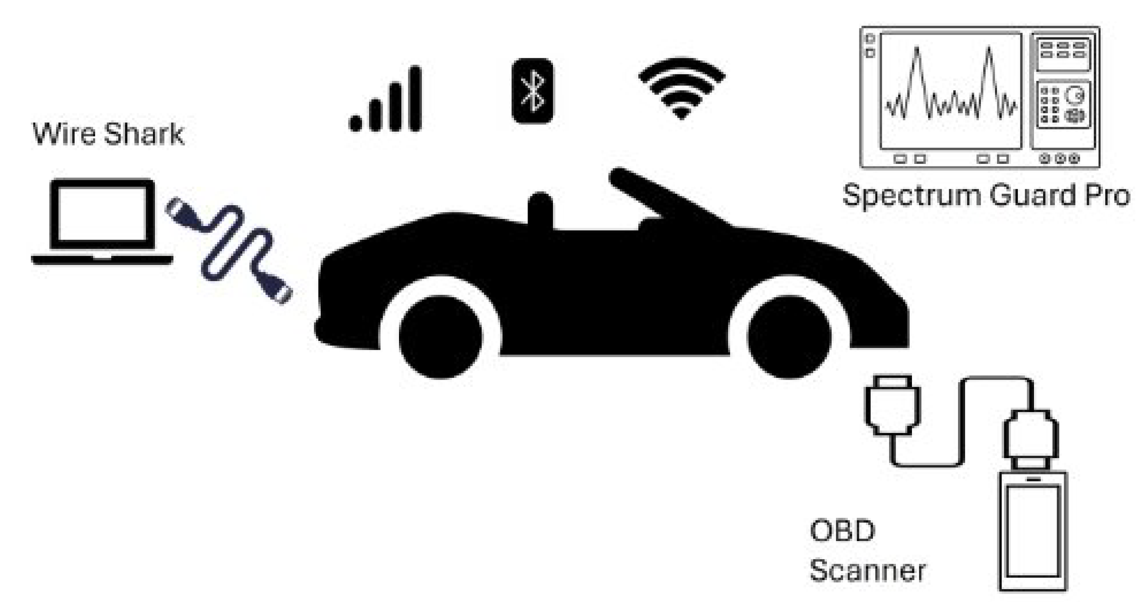
This is what connected vehicles are doing, and the PL (Army and policymakers) NEED to be aware that cars are giving away information without our knowledge. They are broadcasting SSIDs, MAC addresses, Bluetooth device names — even when we think everything's silent.



METHODOLOGY

We began by isolating each vehicle in a semi-remote area and used Faraday bags to avoid signal interference, then scanned for electromagnetic signals using a Spectrum Guard Pro to identify active frequencies and communication technologies. Next, we used Wireshark to capture and analyze network packets transmitted over the vehicle's wireless networks, examining unencrypted Wi-Fi and Bluetooth traffic for any signs of telemetry, location data, or personal user information.

For physical access, we connected an Innova 1000 OBD2 scanner to each vehicle's diagnostic port to retrieve standard data such as VIN, engine metrics, and sensor readings, without modifying vehicle systems. In cars without a traditional OBD port, we connected via Ethernet to capture diagnostic network traffic. This multi-layered approach—combining RF analysis, wireless packet capture, and onboard diagnostic access—provided a comprehensive look into the data practices of connected vehicles.



RESULTS

Our findings and data evaluation revealed no transmission or storage of unencrypted sensitive user data, including geolocation, mobile device information, or driver behavior metrics. However, every vehicle retained Bluetooth artifacts from previous users—including device names like "Ian's iPhone" and unique Bluetooth MAC addresses, which are persistent identifiers tied to individual devices. These artifacts pose a privacy concern, especially in shared or recycled government vehicles. Additionally, all cars broadcast Wi-Fi SSIDs—the public names of their wireless networks—and unique MAC addresses, creating a digital fingerprint for each car. This means that even without accessing the vehicle, someone could passively track its presence across different locations by simply logging repeated sightings of the identical SSID or MAC. This is what we refer to as long-term identification: the ability to follow or profile a specific vehicle over time without direct interaction. While physical access through OBD or Ethernet ports revealed only standard diagnostics, such as battery status or tire pressure, these systems—and the wireless broadcasts—could be exploited. For example, attackers could scrape Bluetooth histories to identify and target previous users, or use SSIDs and MACs to build location patterns of high-value vehicles. Our results make it clear: although the cars didn't leak apparent personal data, they continuously emit low-level signals that, when aggregated, could expose user identities, patterns, or movements.

CONCLUSION AND FUTURE WORK

As connected vehicles grow in capability and adoption, GSA fleet managers and policy makers must implement stronger contracting rules to safeguard Army personnel data, starting with user options to disable data collection, reset broadcast identifiers, and regularly purge stored user data. The Army must not assume connected vehicle data practices are benign; proactive policy, user education, and technical safeguards are critical to protecting operational security.

We recommend investigating the data transmitted over 4G/5G cellular networks. The connected vehicle's onboard Wi-Fi cannot provide an internet connection unless it is connected to an internet access point, which is typically not shared outside of the car parked at a residential location. The onboard 4G/5G transmitters can provide an internet connection. Given this, future work will focus on intercepting the communication between vehicles and mobile/cellular towers. We recommend procuring a private cellular base station or repeater. This will enable the analysis of the packet transmissions before they are encrypted (see Figure 4). This will enable the analysis of data packets by destination IP addresses and content. This will also provide insight into the applications within connected vehicles that send data and the triggers for when the data is sent. This work will require an isolated location or a Faraday cage capability to limit collateral collection.

Another option for future work is to acquire a connected vehicle that can be disassembled. One approach could be to physically extract the vehicle's infotainment system and electronic control unit to perform hardware exploitation, determining any data storage on the systems and what data is transmitted outside the car. While this could reveal a significant level of data, it will require more expertise and specialized equipment.