**Effective Cybersecurity in Modern Vehicles**

Cars are heavily integrated with computing technology, almost more so than the motor or features of the car itself. How can a user stay safe and private with the cloud of digitized information surrounding them? What information goes to and from different vehicles on the road, to any applications controlling the vehicle or integrated in the infotainment systems, and what stays within the vehicle? All this data can be maladapted by corporations, governments, hackers, and abusers to track and harass their victims. However, there are organizations present to counteract malicious factors. The goal is to explore existing automotive cybersecurity research, add to current vehicle data security models, develop awareness of the hazards associated with highly computerized automotive systems, yet inspire reassurance with the efforts in place to secure data produced by modern vehicles.

The information that vehicles produce and use is put into different categories. There is data that is given and received to a device inside a vehicle, to other road users, and to different cloud-based services. For instance, a cell phone inside a vehicle might be using a music streaming service, which connects to the infotainment center. Also, there are different nodes throughout an automobile that create and send data to each other. For example, the fuel tank might have an electronic sensor that sends information to the main electronic control unit (ECU), which then sends a reading to the dashboard. There are also several different types of data transfers, such as transfers within the car itself, sending information to another entity, receiving information from an entity, and passing data back-and-forth. A panel of researchers in Europe devised a model to aid privacy by limiting what information is sent in each direction. While data transfers within a vehicle do not necessarily need any sort of filtering, data sent to and from outside sources should be encrypted, sent as raw data, or a combination of both. Also, limiting the types of information sent based on the source is helpful. For example, an outside device like a key fob doesn’t need tire pressure information. In this way, automobile privacy is top priority. (Pape et al., 2023)

Automotive manufacturers and other third-party corporations are insatiably hungry for road users’ data and are willing to sell it out or hand it over to legal entities, even though they aren’t safeguarding it properly. General Motors with OnStar fell into multiple class-action lawsuits because they were giving data about driving habits to insurance companies, which sent users’ insurance rates skyrocketing (Bronstad, 2024). Furthermore, GM, Kia, and Nissan claim that they can collect biometric data from users. That information is easily hackable, with automakers like Toyota, Volkswagen, and Honda who have gotten hit with multiple data breaches (Caltrider et al., 2023). Also, law enforcement can access user data without a warrant, they just need probable cause (Beggin, 2022).

The technology that makes modern vehicles so convenient can be manipulated by abusers. In 2022, a woman by the name of Christine Dowdall escaped an abusive marriage in her Mercedes-Benz C300, but found her ex-husband was tracking her location via the vehicle’s location software. When she found out, she petitioned the company to limit her ex-husband’s access to the software, even citing her restraining order against him and the court ruling that she be the sole user of the car. However, since his name was on the loan and title, there was nothing they would do. Other victims of abuse have come forward with similar stories, even stating an abuser would go so far as to manipulate functions of the car, such as heating, air conditioning, and the motor itself (Hill, 2024). Legal and ownership paperwork makes cybersecurity abuse complicated.

Thankfully, the NHTSA has already researched a lot of automotive cybersecurity concepts since 2012 as cars have grown more technologically advanced. The organization has collaborated with Original Equipment Manufacturers, other government agencies, industry experts, and other computer manufacturers to find the best solutions. To expand their knowledge, they moved the automotive industry to create numerous Information Sharing and Analysis Centers (ISAC) in the private sector. These divisions were put in place so manufacturers can exchange data relating to cybersecurity and keep vehicle users safe (NHTSA, 2016). Also, United States lawmakers, like Senator Edward J. Markey, are petitioning automakers to become more ethical with data practices. In a multi-page letter to multiple automotive manufacturer CEOs, the senator cited numerous articles and lawsuits to create a conversation about data privacy. He posed questions about the types of data collected, privacy policies that outlined user consent, cybersecurity standards, and what was given to law enforcement (Markey, 2023). There are many people and organizations who want to keep automotive information safe and secure.

In conclusion, automotive cybersecurity is a crucial component of road safety. Vehicles can glitch, companies can invasively track user data and give it to other entities, and abusers can stalk their victims with vehicle data. All vehicle users need to be aware of the extensive computing technology in their cars. Thankfully, automotive manufacturers, industry professionals, and government road safety agencies are working together to mitigate problems with vehicle data privacy.

**Timetable**

A close-up of a data

Description automatically generated

**References**

NHTSA. (2016). NHTSA and Vehicle Cybersecurity.

Hill, K. (2024, October). The spy in your car. *Reader’s Digest*, 68–75.

Pape, S., Syed-Winkler, S., Garcia, A. M., Chah, B., Bkakria, A., Hiller, M., Walcher, T., Lombard, A., Abbas-Turki, A., & Yaich, R. (2023a). A systematic approach for Automotive Privacy Management. *Proceedings of the 7th ACM Computer Science in Cars Symposium*, 1–12. https://doi.org/10.1145/3631204.3631863

Bronstad, A. (2024, May 28). *“a lot of outrage”: Privacy suits allege GM Steers driver data to insurers*. Law.com. <https://www.law.com/2024/05/28/a-lot-of-outrage-privacy-suits-allege-gm-steers-driver-data-to-insurers/>

Caltrider, J., Rykov, M., & MacDonald, Z. (2023, September 26). *After Researching Cars and Privacy, Here’s What Keeps Us up at Night*. Mozilla Foundation. https://foundation.mozilla.org/en/privacynotincluded/articles/after-researching-cars-and-privacy-heres-what-keeps-us-up-at-night/

Beggin, R. (2022, January 4). *Police Don’t Need a Warrant to Pull Personal Data from Cars*. Governing. https://www.governing.com/security/police-dont-need-a-warrant-to-pull-personal-data-from-cars

Markey, E. J. (2023, December 1). Senator Markey Letter to Automakers on Privacy. *Senator Edward Markey of Massachusetts*. Retrieved November 25, 2024, from https://www.markey.senate.gov/imo/media/doc/senator\_markey\_letter\_to\_automakers\_on\_privacy.pdf.