

The Importance of Automotive Cybersecurity

Wayne Ricks, Jr.

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Dr. Patricia Oliver

April 16, 2024

Abstract

For years to come, there will always be a need for cybersecurity specialists to reinforce or implement protocols to deter attackers from accomplishing their goal. With the continuous evolution of technology influencing the world around us, it should be little to no surprise that we would eventually see vehicles becoming more advanced as time marches on. Along with these vehicles becoming more reliant on digital infrastructure, the risk of insider threats and data breaches is ever-present. The same way there is a need for protection towards keeping sensitive data safe can be said about automotive cybersecurity. Automotive cybersecurity refers to the protection over vehicular systems such as electronics and communication networks against any malicious attacks using a variety of protocols. With cybersecurity already being an interdisciplinary career field, how do these disciplines intertwine in a way that can help strengthen cybersecurity within the automotive industry?

Keywords: Automotive Cybersecurity, Cybersecurity Management System (CSMS), Mitigation, Cyber Threat, Secure Communication,

Computer Science Discipline

Computer science plays a pivotal role in strengthening automotive cybersecurity by providing the technical foundation and expertise needed to implement security measures and practices throughout the vehicle's life. One significant contribution of computer science to automotive cybersecurity is its alignment with international standards such as ISO 21434. This standard provides a framework for integrating cybersecurity into the development processes of automotive systems, emphasizing risk assessment, threat modeling, and security validation (Vaibhav 2024). By leveraging computer science principles, automotive manufacturers can align with ISO 21434 guidelines to establish Cybersecurity Management Systems (CSMS) effectively. According to a report made by Klaus Kainrath, CSMS are required to be in all vehicles made after July 2022 until July 2024, stating “Additionally, Cybersecurity Management Systems (CSMS) have been mandatory for all newly developed vehicle types in the EU since July 2022 – a mandate which will be extended to all new vehicles in general by July 2024” (Burkacky, Pototzky, Deichmann, Klein, Scherf 2020). By designing and implementing CSMS systems, computer science professionals facilitate the systematic identification, assessment, and mitigation of cybersecurity risks within automotive systems and networks. This way, they can help protect cars from hackers and keep people's private information safe, making sure that both passengers and their vehicles stay safe as the world of cars gets more connected and automated. Computer science skills are also imperative when it comes to creating secure ways for cars to get software updates and security patches over the air. Using methods, such as secure boot processes and cryptography, can limit the likelihood of anyone intercepting or manipulating the updates.

Manufacturers, such as Ford, use these methods as a way to decrease the number of trips taken to dealerships and to ensure the integrity of their updates. Cryptographically signed OTA updates can be viewed as another form of a digital signature, which comes directly from the manufacturer, verifying that there is an update ready to be installed. By implementing the proper protocols and methods of mitigating risk, manufacturers can always stay one step ahead in the ever-evolving war on technology.

Automotive Engineering Discipline

Automotive engineering and cybersecurity are like two peas in a pod, working together to make sure cars are safe, reliable, and secure in today's super-connected world. Automotive engineering is all about designing, building, and testing vehicles, using mechanical, electrical, and software engineering to do it. Cybersecurity, on the other hand, is about keeping cars safe from hackers and making sure everything inside them stays private and secure. The two fields are so connected that you really can't have one without the other. Automotive engineers need to think about cybersecurity as they design cars, and cybersecurity experts need to know how cars work to keep them safe. This means that automotive engineering has to change to include cybersecurity as a main focus, not just an afterthought. It's not just about making cars that go fast and use less gas anymore; it's also about making sure they can't be hacked and won't give away your personal info. A report made by the collaboration of writers from McKinsey and Company states that these new automotive technologies, housing data the way a computer would, can bring unwanted attention towards them; "These innovations...turn modern cars into information clearinghouses while also making them tempting targets for cyberattacks." (Burkacky, Deichmann, Klein, Pototzky, Scherf 2020). In order to minimize the likelihood of an attack, automotive engineers design secure vehicle architectures that isolate critical systems from

non-critical ones and implement defense-in-depth strategies to mitigate cyber threats. The use of secure hardware modules, such as Trusted Platform Modules (TPM), helps protect cryptographic keys and sensitive data, ensuring their integrity and confidentiality (Denning et al., 2019).

Another way engineers combat these attacks is by integrating hardware-based security mechanisms, such as secure elements and tamper-resistant modules, into vehicle components to protect against physical attacks and tampering. This form of protection may seem a bit lackluster, but not all hackers can remotely access a vehicle. By integrating measures such as these, manufacturers can enhance the cybersecurity posture of vehicles, mitigate cyber risks, and ensure the safety and security of drivers and passengers.

Ergonomics Discipline

In the context of automotive cybersecurity, ergonomics plays a crucial role in shaping the design and usability of onboard interfaces, controls, and driver-assist systems to mitigate security risks and enhance user awareness and response to cyber threats. Ergonomics also focuses on designing systems and interfaces that optimize human interaction and performance within the vehicle environment, considering factors such as user comfort, accessibility, and efficiency. In a report made by the collaboration of writers discussing human factors in autonomous vehicles, they state that humans are the main factors that lead to cyberattacks, “Because human failure is the most common reason for a successful cyberattack, human-factor researchers and psychologists might improve AV cybersecurity by researching how to decrease the probability of a successful attack.” (Linkov, Václav, et al 2019). Since human-error is the main reason for these cyberattacks, the most optimal way to decrease this likelihood is to have people educated about cybersecurity and spread the awareness to others. Training materials designed with ergonomics in mind tend to be more engaging, effective, and accessible, leading to improved cybersecurity

awareness and behavior. Additionally, ergonomics plays a vital role in the physical construction of the vehicle, taking into consideration the variety of consumers that may show interest.

Physical ergonomics address the design of vehicle interiors and seating arrangements to optimize driver comfort and reduce fatigue. By integrating ergonomics into the design of the car's controls and interfaces, auto engineers can make it easier for drivers to stay aware of their surroundings, lower the chances of them making mistakes, and help prevent cybersecurity issues caused by user errors, misconfigurations, or malicious actions. Furthermore, ergonomics are responsible in designing the alerts, notifications, and feedback systems for cybersecurity technology, to make them clear, easy to understand, and actionable for drivers. This way, they can handle any cybersecurity threats that come up without getting distracted from the main job of driving. Overall, the incorporation of ergonomics principles into automotive cybersecurity increases user-friendliness, effectiveness, and safety of security measures, ultimately resulting in a more secure and resilient automotive ecosystem.

Conclusion/Common Ground

Ergonomics, computer science, and automotive engineering intersect in the domain of automotive cybersecurity, forming a collaborative framework that enhances security measures within the automotive industry. Computer science provides the technical expertise and tools necessary to develop robust cybersecurity solutions to protect vehicles from cyber threats. Ergonomics contributes to automotive cybersecurity by ensuring the design of intuitive and user-friendly interfaces and controls that facilitate driver awareness and response to cybersecurity alerts and threats, thereby reducing the risk of human error and enhancing overall system resilience. Additionally, automotive engineering integrates cybersecurity considerations into the design and development of vehicles, maximizing secure software and hardware

technologies to fortify onboard systems against cyberattacks. By harnessing the synergies between these disciplines, stakeholders can enhance the safety, security, and reliability of modern vehicles in an increasingly connected and digitized automotive landscape.

References

- Burkacky, Pototzky, Deichmann, Klein, Scherf “Automotive Cybersecurity: Mastering the Challenge | McKinsey.” *W*www.mckinsey.com, www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge
- Denning, D., Bailey, M., & Denning, D. (2019). *Secure Architectures for Vehicular Networks and Embedded Systems*. CRC Press.
- Galis, M. (2024, March 13). *The Future Of Security Compliance: How Emerging Vehicle Technologies Are Setting New Rules*. Forbes. Retrieved March 30, 2024, from <https://www.forbes.com/sites/forbestechcouncil/2024/03/13/the-future-of-security-compliance-how-emerging-vehicle-technologies-are-setting-new-rules/?sh=6811c2636dff>
- Hill. “Automotive Supply Chain Vulnerable to Attack as Cybersecurity Regulation Looms.” *CSO Online*, www.csoonline.com/article/652299/automotive-supply-chain-vulnerable-to-attack-as-cybersecurity-regulation-looms.html.
- Kainrath, “Automotive Cybersecurity - Challenges for Developers.” *Magna*, www.magna.com/stories/inside-automotive/2023/cybersecurity-in-the-automotive-industry.
- Kukkala, Vignesh, Pasricha. “Roadmap for Cybersecurity in Autonomous Vehicles” 2201.10349.pdf (arxiv.org)
- Linkov, Václav, et al. “Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research.” *Frontiers in Psychology*, vol. 10, 3 May 2019, <https://doi.org/10.3389/fpsyg.2019.00995>.
- Vaibhav (2024, January 2). *Automotive Cybersecurity: The Foundation of Next-Generation Vehicle Technology*. Embitel. Retrieved April 1, 2024, from <https://www.embitel.com/blog/embedded-blog/automotive-cybersecurity-the-foundation-of-next-generation-vehicle-technology>