A Survey of Recent Automotive Software Security Vulnerabilities: Trends and Attack Vectors

Srijita Basu, Miroslaw Staron, Jennifer Horkoff, Magnus Almgren,
Christian Berger and Tomas Olovsson
Computer Science and Engineering, Chalmers | University of Gothenburg

1 Motivation and Work Done

Development and use of Autonomous Vehicles (AVs) have grown significantly in the last few years. According to a report by McKinsey & Company [1], by 2035, autonomous vehicles could generate a revenue of $300 to $400 billion. However, the increased level of connectivity (e.g. updating High Definition maps, reporting vehicle status, etc.) in AVs leads to varied and increased security concerns. For example, 187 vulnerabilities and exploits related to autonomous vehicles have been reported between 2010 and 2019 [2]. Such a high number of vulnerabilities is a serious issue, as security attack on cars can lead to safety risks and ultimately to accidents. In the last three years, these numbers have seen extensive growth, and, in addition, a number of new attack vectors were discovered. These vectors cover a wide range: from internal vehicular networks (CAN, LIN, FlexRay, etc.), ECU units, and OBD ports – prone to physical/local attacks – and External Applications, Infotainment Systems, Wi-fi/Cellular Networks – prone to remote/network attacks.

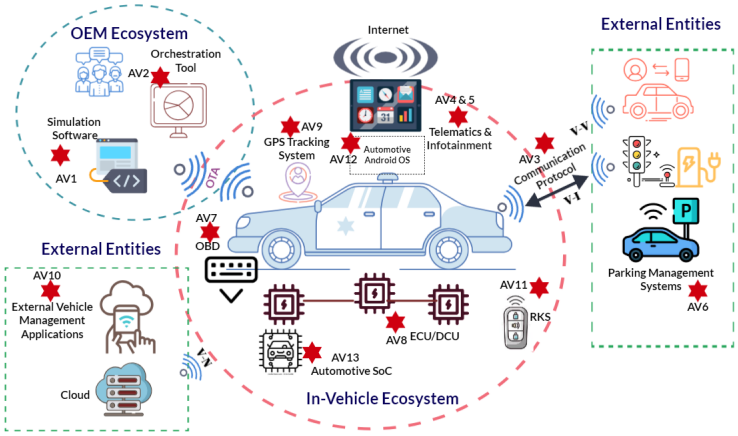

Figure 1: Attack Vectors in an Automotive Ecosystem

Observing the attack patterns identified in [2], we see the number of remote attacks highly surpassed the number of local attacks. This highlights a very crucial issue: an attacker need not have physical access to the AV to launch an attack. The attacker can relatively easily contaminate the system using vulnerable software or unprotected network channels. Under such circumstances, our study tries to answer the following vital research questions in context of AVs, focusing on developments in the last three years: i) Which types of software has become more vulnerable (e.g., infotainment systems/RKS software, Parking Management Software/Fleet Management Software)? ii) Which software product (by name e.g., Grafana Telematics Dashboard) has seen the most vulnerabilities? iii) In which part of the software development life cycle has the maximum number of vulnerabilities been introduced? iv) Which CAPEC mechanism, i.e., attack mechanisms that are commonly used to exploit the identified vulnerabilities, has been the most popular? v) Which are the most vulnerable packages/libraries being used in the automotive software industry?

These answers shall be used to formulate automotive software vulnerability metrics that will assist testing teams to identify the spatiotemporal weaknesses of the system, including both weak entities and weak phases of the connected vehicle ecosystem.

In our work, we conduct an exploratory survey to identify and analyze the automotive software vulnerabilities related to AVs in the last three years, i.e. 2022 to 2024 (till date). We started from [3], a study which focuses on different GitHub repositories associated with Automotive Software. Using the National Vulnerability Database (NVD), we found a set of existing vulnerabilities in some of the repositories from [3]. In addition to targeting these specific repositories, keyword searches (Telematics, Simulation, Infotainment, ECU, etc.) were performed to identify further vulnerabilities. Moreover, several vulnerability scanning tools were applied to check whether these tools could identify and report the vulnerabilities found in the previous step. We associated each of the vulnerabilities found with relevant attack vectors, as shown in Fig. 1 and use this information to reveal the entities of the automotive ecosystem where security should be strengthened. Results are summarized in the following section.

2 Results and Conclusion

The following analyses were performed on the surveyed data. *i) CVSS Severity Statistics*, *ii) Trend Statistics*, *iii) Overall Attack Vector Statistics* (depicted in Fig. 2, answering the first research question i.e. type of software showing more vulnerabilities), *iv) Attack Vector Statistics: as per Product*, and *v) Attack Vector Statistics: as per Software Development Phase.*

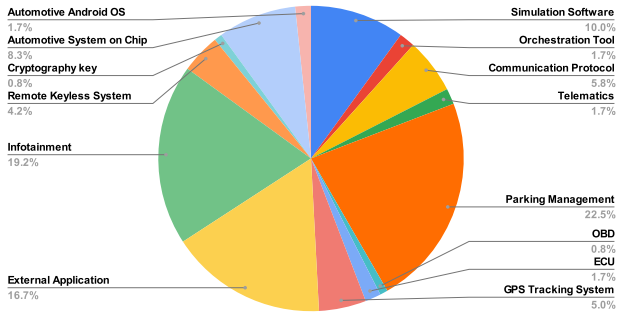

Figure 2: Overall Attack Vector Percentage (2022-2024)

The results are quite concerning as not only were 125 new vulnerabilities identified in some of the most popular automotive software products, but almost 47% out of those had high severity scores. Additionally, the scanning tools detected a large number of vulnerable software packages that are being used in the automotive software development. The various facets of this analysis help to understand the security loopholes from different dimensions (e.g., prioritizing the automotive entities according to their proximity to the identified attack vectors, identifying the part of the SDLC and thereby the organization roles that should be more active in finding and fixing vulnerabilities). We envision that our results will help the automotive software testing team to prioritize the testing process of software entities and mitigate the underlying risk in a reduced time.

References

[1] J. Deichmann, E. Ebel, K. Heineke, R. Heuss, M. Kellner, and F. Steiner, 2023. Autonomous driving's future: Convenient and connected, McKinsey & Company.

[2] M. Gülsever, 2019. A Study on Vulnerabilities in Connected Cars.

[3] S. Kochanthara, Y. Dajsuren, L. Cleophas, and M. van den Brand, 2022 May. Painting the landscape of automotive software in GitHub. In Proceedings of the 19th International Conference on Mining Software Repositories (pp. 215-226).