Ph.D. proposal: Threat models for long-term automotive architectures

Supervision by Télécom Paris: Ludovic Apvrille, Guillaume Duc

Supervision by Renault / Ampère: Jean-Baptiste Mangé

Context and problematic

For the past fifteen years, cybersecurity has gradually been integrated into automotive engineering. To date, numerous sectors, such as IS/IT, production, after-sales, regulatory management, procurement, and legal, are involved in the secure design of vehicles. To support the integration of these various sectors and the changes brought about by cybersecurity, existing processes and work methods have been used and adapted without necessarily focusing on overall coherence across the entire chain.

At the same time, transformations brought about by the Software Defined Vehicle—such as continuous integration or the increased adaptability of the software and electronic platform—exacerbate cybersecurity issues but also highlight or intensify this lack of coherence.

Added to these internal transformations is a regulatory context particularly focused on the long-term operational cybersecurity (about 20 years after a given model's production has ceased), which presents a major challenge in managing a highly diverse range of products simultaneously, both in terms of workload and in terms of the operational knowledge of the existing teams. Thus, they may find themselves tasked with assessing a cybersecurity issue on a vehicle model designed before their arrival, based on potentially outdated tools, methods, and practices.

A viable approach to addressing this issue involves initially standardizing the internal activities of automotive actors involved in the ICMS chaire (e.g., Ampere/Renault). Following standardization, these activities should be optimized to ensure seamless compatibility with external stakeholders, including competitors, threat intelligence sources, regulatory bodies, and the broader cybersecurity community.

Contribution and objectives

To effectively address the previously identified challenges, it is essential to develop and evaluate new methodologies that can integrate cybersecurity throughout the product development cycles [1, 2, 3, 4, 5]. Crucially, these methodologies must facilitate a clear separation between the modeling of threats—considered during the design phase—and the risk assessments conducted on implementations.

The criteria to evaluate the relevance of the defined methods are:

- Its definition of a global and collaborative approach to threat assessment that facilitates exchanges with competitors, authorities, and suppliers (holistic method).
- Its Ability to rapidly update the risk assessment in case of a threat evolution.
- It Ability to rapidly update the end-to-end risk assessment in case of a vulnerability.
- A complete delegation of impact scoring to the business units owning the concerned assets.

- A full integration of cybersecurity attributes into the objects of MBSx (Model Based System Engineering or Software).
- An integration of attack scenarios into the digital twin models of vehicles.
- A good modularity and complementarity of risk analyses (inter and intra components, both onboard and offboard).

Expected work

In the context of this thesis, to achieve these objectives, it is proposed to work on two distinct stages.

The **first stage** involves setting up the data model for the following areas:

- theoretical threats (attacker profile, motivation, modus operandi)
- real threats (attacker, tactics, techniques, kill-chain)
- vulnerabilities (public or private, with or without CVSS scoring)
- definition of attack paths from risk analyses
- mapping of elementary steps with CTI (Cyber Threat Intelligence) data
- system modeling MBSx

This stage will allow the doctoral candidate to cover the complete cycle of cybersecurity activities and, as a result, to acquire solid knowledge of all these activities. More generally, a related work covering these different aspects will be performed, starting for instance from the references given below, and from any references provided by the chaire's members.

Based on these technical and scientific foundations, the doctoral candidate will construct the data-based method that enables various stakeholders—both external, such as authorities, competitors, or the cyber community, and internal, such as automotive engineering teams, the PSIRT (Product Security Incident Response Team), IT management, or production sectors—to identify the developments needed on repositories, interfaces, and tools handling these data.

The method definition will also take into account the format of external input data considered as "imposed" and the format of expected output data for sharing with external actors, for example, the cyber community, competitors, or authorities. This is a key point to ensure the challenge of having a common method.

The second stage involves implementing the identified key aspects of the method within a more precise scope to be defined by the doctoral candidate and the supervising team (the scope not covered will need to be addressed by the existing teams independently from this Ph.D.).

For example, the doctoral candidate will have the opportunity to develop the **modeling of attack paths in the end-to-end architecture** (ranging from embedded systems to disembarked systems), or to **implement artificial intelligence processing for recalculating risks based on the evolution of threats provided by CTI**, or **to establish a common repository for managing threats through a concerted design among manufacturers**, or any other topic identified during the first stage.

Research activities will take place within a lab of Télécom Paris, in collaboration with the automotive engineering cybersecurity teams of the partner of chaire ICMS. In particular, Ampere/Renault will offer a complete immersion with the operational staff handling development, upstream projects or research, as well as serial production.

In parallel, the Ph.D. candidate will have to publish its work in A-rank journals and conferences.

Administrative aspects

- Ph.D. scholarship by Télécom Paris
- Ph.D director: Prof. Ludovic Apvrille (Télécom Paris)
- Co-supervisor:
- Co-supervisor: Dr Patricia Guitton-Ouhamou (Renault / Ampere)
- Duration: 36 months
- Starting: September 2024

Profile and required skills

- Master's degree, engineer or equivalent in computer science
- Pre-requisites: the candidate should have taken courses in the field of system design and/or cybersecurity (particularly for embedded systems)
- Programming languages skills: C/C
- Good level of spoken and written English

How to apply?

- Contact: Ludovic Apvrille (ludovic.apvrille@telecom-paris.fr
- Documents to include in the application: resume, cover letter, grades transcripts, recommendation letter(s). Incomplete applications will be rejected.

References

1. E. Schoitsch, A. Skavhaug, and J. Hauge, "SafEUr – Safety and Security by Design for Interconnected Mixed-Critical Cyber-Physical Systems – A project outline," in Proc. 4th Workshop on Critical Automotive Applications: Robustness and Safety, CARS, 2015.

2. H. Martin, D. Pilgrim, E. Torkilsheyggi, and A. R. Cavalli, "Safe and Secure Feature Interactions in Embedded Systems: A Systematic Literature Review," IEEE Access, 2020.

3. *Yuri Gil Dantas,* Vivek Nigam, "Automating Safety and Security Co-design through Semantically Rich Architecture Patterns. ". *ACM Trans. Cyber Phys. Syst. 7(1): 5:1-5:28 (2023)*

4. L. Apvrille, L. W. Li, "Harmonizing Safety, Security and Performance Requirements in Embedded Systems", Proceedings of the Design Automation and Test in Europe conference (DATE), March 25-29, Firenze, Italy.

5. Ludovic Apvrille, Letitia LI, Annie Bracquemond, "Design and Verification of Secure Autonomous Vehicles", Proceedings of the 12th European ITS Congress, Strasbourg, France, June 2017.