Ph.D. Position: Integrating Vehicular Safety and Cyber Security to System Design

Supervision

Ludovic Apvrille and Dominique Blouin, Télécom Paris, Institut Polytechnique de Paris, France

Context and Problem

Automotive systems are increasingly depending on intricate system architectures and a variety of external services to deliver advanced features, spanning from driving assistance to infotainment and remote tolling, among others. The successful deployment of these sophisticated services necessitates the integration of an expanding assortment of hardware devices, notably communication devices such as Bluetooth, Wi-Fi, and 5G technologies, in conjunction with an increasing number of software components. This increase in functionality not only expands the range of capabilities but also significantly broadens the vehicle's attack surface. Consequently, this growth engenders new and potentially more complex cyber security challenges that need to be addressed.

Analyzing the safety risks presented by these novel components is a task of paramount significance [1, 2, 3, 4]. Risk analysis involves recognizing the role fulfilled by various assets and discerning how they might be impacted by attacks that could subsequently engender safety issues. Typically, the ramifications of potential attacks are classified within four distinct categories: Safety, Financial, Operational, and Privacy (SFOP).

However, the growing complexity of a vehicle's architecture poses significant challenges when attempting to evaluate these impacts [7]. This is particularly true when considering scenarios where an attacker might simultaneously compromise multiple services/assets or gain comprehensive control over a specific component, such as an Electronic Control Unit (ECU) or a communication channel.

This emergent complexity underscores the necessity for robust and dynamic risk assessment models capable of effectively capturing and addressing these multifaceted cybersecurity concerns.

This problematic will be tackled in the scope of the Connected Cars and Cyber Security (C3S-2) research chair, which gathers industrial partners and research teams of Télécom Paris. This Ph.D. is part of a track of this chair called “risk analysis”.

Scientific Contribution

To better support SFOP, we believe a first contribution would be to better capture the interactions between the different system components. This would facilitate and improve the understanding of how a successful cyber-attack might propagate throughout a system and influence its various services.

A promising direction to explore is the utilization of a Model-Based Approach [5, 7], serving as a unified framework to bridge the gap between hardware, electrical, electronic, and physical architectures. Leveraging this model, the goal is to provide automated analysis capabilities to ascertain how various attacks might impact the system in terms of SFOP. Safety is obviously of utmost importance and will be the first target of the analysis, in particular determining which ASIL (Automotive Safety Integrity Level) an attack can reach could be a first objective. The ASIL is established by performing a risk analysis of a potential hazard (possibly due to an attack) by considering the severity, exposure, and controllability of the vehicle operation scenario where the hazardous event could occur.

In order to construct the appropriate modeling and analysis environment, it will be crucial to define and evaluate diverse attack models and scenarios. Essentially, the devised model should be capable of encapsulating the Functional and Operational Architectures, and augmenting them with Cybersecurity and SFOP attributes.

Various types of SFOP impact analysis could be executed at multiple levels, including systems, features, and components. Furthermore, these innovative models and analysis techniques could serve as a shared platform to enhance the OEM's risk analysis at the system/feature level in synergy with the supplier's risk analysis at the component/sub-component level. This coordinated approach can foster a more holistic understanding of risks, facilitating more effective mitigation strategies across all levels of system architecture.

This model shall permit to address the challenges of a dynamic evaluation of the ASI Level of an attack taking into account the side effects of the trigger of multiple failures / EICPS at the same time.

Expected Work

1. State of the art on risk analysis techniques.
2. Understand the architecture of vehicular systems and practice with modeling environments.
3. Define a modeling and analysis technique for simple attack scenarios.
4. Extend the technique to more complex system components and attack scenarios.
5. Evaluate the technique on vehicular sub-systems provided by the partner of the C3S2 chair.
6. Publish the work in A-ranked journals and conferences.

Administrative Aspects

- Scholarship provided by Télécom Paris
- Ph.D director: Prof. Ludovic Apvrille (Télécom Paris)
- Co-director : Dr Dominique Blouin (Télécom Paris)
- Duration: 36 months
- Starting date: September 2023

Candidate Profile and Skills

- Master’s degree in engineering or equivalent in computer science.
- Prerequisites: the candidate should have followed courses in the field of system design (particularly for embedded systems) and should have basic knowledge of formal methods.
- Programming languages skills: C/C++, Java.
- Some knowledge of model-driven engineering techniques would be a plus
- Good level of spoken and written English

Application

• Contact: Ludovic Apvrille (ludovic.apvrille@telecom-paris.fr), Dominique Blouin (dominique.blouin@telecom-paris.fr)

• Documents to include in the application: resume, cover letter, grades transcripts, recommendation letter(s).

References

1. C. Schmittner, Z. Ma and E. Schoitsch, "Combined safety and security development lifecylce," 2015 IEEE 13th International Conference on Industrial Informatics (INDIN), Cambridge, UK, 2015, pp. 1408-1415, doi: 10.1109/INDIN.2015.7281940.,

2. Siwar Kriaa, Ludovic Pietre-Cambacedes, Marc Bouissou, Yoran Halgand, "A survey of approaches combining safety and security for industrial control systems," Reliability Engineering & System Safety, Volume 139, 2015, Pages 156-178, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2015.02.008.

3. Izuakor, Christine. “Understanding the Impact of Cyber Security Risks on Safety.” International Conference on Information Systems Security and Privacy (2016).

4. E. Lisova, I. Sljivo and A. Causevic, "Safety and Security Co-Analyses: A Systematic Literature Review," 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 2019, pp. 833-833, doi: 10.1109/COMPSAC.2019.00122.

5. 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)*

6. 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.

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