Ph.D. proposal: Integrating Vehicular Safety and Cybersecurity to Systems and Architecture Design

Supervision by Télécom Paris: Ludovic Apvrille, Dominique Blouin

Supervision by Renault / Ampère: Pierpaolo Cincilla, Patricia Guitton-Ouhamou

Context and problematic

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 augmentation 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, cybersecurity challenges that need to be addressed.

Analyzing the safety risk 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 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.

Contribution

To accurately evaluate the SFOP impacts within these intricate environments, one approach could be to refine the formalization of interactions among different system components. This would facilitate an improved understanding of how a successful cyberattack 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 level can an attack reach could be a first objective. The ASI Level depends on the Severity, Controllability and Exposure.

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 analyses 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, ideally leading to "security by design".

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. Learn Renault's Model-Based System Engineering design flows
3. Understand the architecture of vehicular systems, and practice with modeling environments
4. Define a model and analysis technique for simple attack scenarios
5. Extend to more system components and more complex attack scenarios
6. Evaluate on vehicular sub-systems provided by the partner of the chaire ICMS
7. Publish your work in A-rank journals and conferences

Administrative aspects

- Ph.D. scholarship by Télécom Paris
- Ph.D director: Prof. Ludovic Apvrille (Télécom Paris)
- Co-director: Dr Dominique Blouin (Télécom Paris)
- Co-supervisor: Dr Pierpaolo Cincilla (Renault / Ampere)
- Co-supervisor: Dr Patricia Blouin (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 (particularly embedded systems) and should have knowledge of the basis of formal methods.
- Programming languages skills: C/C++, Java
- Good level of spoken and written English

How to apply ?

- 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. 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. L. Piètre-Cambacédès, and M. Bouissou, "Beyond CVSS: From Vulnerability Assessment to Vulnerability Management," in Proc. 2nd International Symposium for ICS & SCADA Cyber Security Research, 2014.

3. R. R. Hansen, M. S. Lund, and J. H. H. Rafn, "SysML-based Safety Assessment: Aligning System and Safety Engineering," in Proc. 7th IFIP WG 13.2 International Conference, HCSE, 2016.

4. 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.

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