Research engineer or post doc. position
12 months

A platform for supporting security modeling and verification

Ludovic APVRILLE
Telecom Paris
Equipe LabSoC
450 routes des Chappes, F-06904 Sophia-Antipolis Cedex, France
Email: firstname.lastname@telecom-paris.fr

February 28, 2025

1 Context and problematic

The design of embedded systems is inherently complex due to the diverse set of safety and security requirements, as well as the integration of both hardware and software components sourced from multiple partners [4]. Ensuring that the system operates safely under all conditions and remains resilient against attacks is crucial. Additionally, compliance with domain-specific standards (e.g., ISO 26262) must be considered. Challenges encountered during the integration phase can significantly affect the product's time-to-market and quality, potentially leading to costly maintenance efforts such as product recalls or urgent security patches.

A promising solution is to capture all system components using a unified formalism that allows for the evaluation of safety, cybersecurity, and performance in a consistent manner. Studies have shown that maintaining the entire modeling process within a

single toolkit reduces rework at each iteration [5]. To achieve this, we build upon our existing approach for designing safe and secure embedded systems: SysML-Sec [1], W-Sec [6], and its supporting tool, TTool [2]. However, neither SysML-Sec nor W-Sec were originally designed with emerging threats in mind. We believe that an improved modeling and verification approach is necessary, as outlined in the following section.

2 Objectives

The solution we aim to explore in this work is, first, **to define modeling techniques that more effectively capture cybersecurity requirements, attack trees, and security mechanisms**, thereby improving the representation of recent threats—including those targeting both information systems and embedded systems. To achieve this, we propose identifying the gap between the capabilities currently supported by TTool and the latest advancements in attack modeling. Additionally, AI could be leveraged to enhance the representation of security aspects, as already partially investigated by our research team [3].

A second contribution is **to develop simulation and verification techniques applicable to the proposed models**, ensuring their robustness and alignment with real-world security challenges.

Finally, we intend to **design comprehensive tutorials—including hands-on labs—to support students, engineers, and researchers in getting started with our toolkit and deepening their expertise in system security**.

This research will be conducted within the framework of the "TCE: Train Cyber Expert" project.

3 Expected work

To achieve the previously described issues, the work should focus on the following stages:

1. Understand the methods currently in use for safe or secure systems. More generally, a bibliography on model-driven approaches for designing secure embedded systems will be updated with latest papers of the field.
2. Learn how to perform simulations and verifications with TTool and SysML-Sec. You will practice with toy and industrial case studies.
3. Propose a new modeling and verification approach for security, and implement it in TTool: in this position, you are expected to make important implementation contributions to TTool.
4. Apply your techniques to case studies provided by the CME partners.

4 Skills

- Excellent skills in software engineering (principle of Model-Driven engineering) and embedded architectures (i.e. hardware/software architectures)
- Skills in security are appreciated.
- No prior knowledge of UML is necessary.

5 How to apply?

Send the following elements - in **one pdf** file - by email to ludovic.apvrille@telecom-paris.fr. Incomplete applications won't be taken into account. Selected candidates will be evaluated on technical skills (e.g. programming in C or Java) and on their research capabilities (e.g. reviewing a paper).

- CV, including your list of publications
- Reference to your Ph.D. manuscript
- Cover letter
- Reference letters. A reference letter from the Ph.D. supervisor is encouraged.
- Grades obtained during the master, and ranks.

References

[1] L. Apvrille and Y. Roudier. SysML-Sec: A Model Driven Approach for Designing Safe and Secure Systems. In *3rd International Conference on Model-Driven Engineering and Software Development, Special session on Security and Privacy in Model Based Engineering*, France, February 2015. SCITEPRESS Digital Library.

[2] Ludovic Apvrille. Webpage of TTool. In *http://ttool.telecom-paristech.fr/*, 2015.

[3] Alan Birchler De Allende, Bastien Sultan, and Ludovic Apvrille. From attack trees to attack-defense trees with generative ai & natural language processing. In *Proceedings of the ACM/IEEE 27th International Conference on Model Driven Engineering Languages and Systems*, MODELS Companion '24, page 561–569, New York, NY, USA, 2024. Association for Computing Machinery.

[4] Thomas A Henzinger and Joseph Sifakis. The embedded systems design challenge. In *International Symposium on Formal Methods*, pages 1–15. Springer, 2006.

[5] National Instruments. Best practices for embedded software testing of safety compliant systems. http://www.ni.com/white-paper/13671/en/, 2016.

[6] Bastien Sultan, Ludovic Apvrille, Philippe Jaillon, and Sophie Coudert. W-sec: A model-based formal method for assessing the impacts of security countermeasures. In Luís Ferreira Pires, Slimane Hammoudi, and Edwin Seidewitz, editors, *Model-Driven Engineering and Software Development*, pages 203–229, Cham, 2023. Springer Nature Switzerland.