Master internship Topic

Modeling and Verification of Cybersecurity Constraints with the TTool software

Prof Ludovic APVRILLE
Télécom Paris, LabSoC team
450 routes des Chappes, F-06904 Sophia-Antipolis Cedex, France
Email: ludovic.apvrille@telecom-paris.fr

June 12, 2023

1 Context and Problem Statement

The design of embedded systems is complex due to the numerous requirements and the presence of hardware and software components [3]. Not only must the designer ensure that the system will always behave safely, but he must also take into account real-time performance and cybersecurity constraints.

Currently, our approach to designing safe embedded systems is based on modeling and verification techniques, particularly on the SysML-Sec profile [1]. SysML-Sec is supported by the free and open-source TTool software [2]. We believe that systematic modeling and the use of verification techniques (simulation, formal proof) help detect errors earlier in the system design cycle, including considering possible attacks on these systems and associated countermeasures.

2 Objectives

Therefore, **the main objective of this internship work is to contribute to the modeling and verification techniques of the free software "TTool"**, with a focus on cybersecurity aspects. These contributions will be **made available to the public** via the TTool website.

3 Expected Work

To achieve these objectives, the work will focus on the following steps:

1. Understand SysML-Sec modeling and the principles of attack and countermeasure modeling.
2. Create new models of embedded systems highlighting the capabilities of SysML-Sec. In particular, examples from automotive and avionic systems will be made, and the associated tutorial enriched.
3. Propose new security modeling patterns. Currently, the tool offers fairly simple patterns, based on basic cryptographic primitives: it would be interesting to define new higher-level patterns (secure channel ensuring such property, firewall, intrusion detection, etc.).
4. Code these patterns in TTool, along with the associated tests.
5. Update the documentation related to the verification of SysML-Sec cybersecurity.

4 Required Skills

- Mandatory: Java development, knowledge of *gitlab*, mastery of the Linux terminal
- Optional but recommended: cybersecurity, UML/SysML modeling

5 How to apply?

Send your CV, grades and recommandations, all in pdf format, to ludovic.apvrille@telecom-paris.fr

References

[1] L. Apvrille, L. W. Li, and A. Bracquemond. Design and verification of secure autonomous vehicles. In *12th European ITS Congress*, Strasbourg, France, June 2017.

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

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