Post-doc Position (12 months)

A model-driven approach for handling vulnerabilities in critical embedded systems after they have been released

Ludovic Apvrille - Telecom Paris - Sophia-Antipolis
ludovic.apvrille@telecom-paris.fr
Philippe Jaillon - Mines Saint-Etienne - Saint Etienne
philippe.jaillon@emse.fr

11 septembre 2020

1 Context and problematic

It is a common practice to consider safety aspects when designing embedded systems. Recent contributions propose to also handle cyber security aspects. For instance, in its CAPE program (Continuous assessment in polymorphous environments), the H2020 European project SPARTA (https ://www.sparta.eu/) targets the interaction between safety, security and performance both from a system engineering perspective but also from a more practical point of view within the design of concrete systems (e.g. motor drives, space based systems, etc.).

In the previous H2020 European project AQUAS, interests for cybersecurity aspects have been studied within model-driven engineering approaches and languages, e.g. in SysML-Sec where safety and security verification can be lead from the same models [1]. SysML-Sec is supported by the TTool framework [2].

Yet, most of these approaches consider only high-level security vulnerabilities (e.g. a bus can be spied at), thus without caring with more concrete hardware attacks, and the impact of the latter on system safety. Moreover, model-driven approaches mostly address how the system should be built according to the current state of the art. Said differently, they only consider known attacks and vulnerabilities when designing the system.

Obvisouly, new vulnerabilities which could possibly impact systems safety might be discovered once the system has been released. Using Model-driven approach in this context can surely help supporting the process to identify a good fix, that is identifying the right countermeasures that will resolve the latest issue while ensuring all previous requirements . Similarly, when the system has been released, new updates are generally used to add new functionalities or remove superseded functionalities. Safety, security and performance of the system must be assessed before a patch is applied to running systems.

The proposed post-doctorate intends to study how the upgrade of a system can be driven in a safe, secure and efficient way using a model-driven approach. This work will be carried out in the scope of the CAPE program of the H2020 SPARTA project.

2 Expected work

To achieve the previously described issues, the post-doc should focus on the following stages :

1. Learn how SysML-Sec can be used to design a safe and secure embedded system.
2. Perform a bibliographical study on critical system updates
3. Propose new model-based methods and tools to handle system updates
4. Play an active role in the SPARTA project. In particular, the rover developed in the scope of the project might be used to practise with the defined techniques.

3 Skills

Prior knowledge of embedded systems (i.e., software and hardware architectures) is an asset. Programming skills in Java or C is preferable. No prior knowledge of UML is necessary.

4 Practical information

The Post-doc will be located in Telecom Paris, Sophia-Antipolis, on the French Riviera. Based on the candidate preference, location could be also in Gardanne or in Saint-Etienne. This will be discussed during the interview.

Regular meetings will be organized with Mines Saint-Etienne and Telecom Paris.

5 How to apply ?

Send the following elements - in **pdf** format, if possible - by email to ludovic.apvrille@telecom-paris.fr and to philippe.jaillon@emse.fr. Incomplete applications won't be taken into

account.

— CV, including your list of publications and a summary of your Ph.D.
— Cover letter
— Reference letters. At least one reference letter is necessary (e.g. Ph.D. supervisor)

Références

[1] L. Apvrille and L. W. Li. Harmonizing safety, security and performance requirements in embedded systems. In *Design, Automation and Test in Europe (DATE'2019)*, Florence, Italy, 2019.

[2] TTool. "The TURTLE Toolkit". In *http ://ttool.telecom-paris.fr*.