TELECOM ParisTech

Une école de l'IMT

Ph.D. Proposal for C3S

Model-based Joint Analysis of Safety and Security

Ludovic APVRILLE, Guillaume DUC, Dominique BLOUIN
Telecom ParisTech
Equipes LabSoC / SSH
450 routes des Chappes, F-06904 Sophia-Antipolis Cedex, France
46 rue Barrault, F-75634 Paris Cedex 13, France
Email: firstname.lastname@telecom-paristech.fr

June 1, 2018

1 Context and problematic

The omnipresent connectivity across so many of our objects has improved our daily lives, from adding conveniences by allowing us to track appliances (such as fridges, detectors, etc) [6], adding conveniences and improving safety in our daily commutes (internet connectivity, car monitoring, emergency braking, etc) [13], monitor our personal health (fitbits, glucose monitors) [3] or of children (Mimo, trackers) [8], to helping medical professionals with menial tasks, monitoring patients or administer treatment (delivery robot, insulin delivery, etc) [11]. For all the benefits due to these connected devices, malfunctions may lead to grave impacts on personal privacy or safety.

The design of embedded systems is complicated by the many different requirements and the presence of both hardware and software components [4]. Not only must we assure that the system will always behave safely and is protected against attackers, we must also consider the real-time performance for timing-critical devices, the cost and size of the architecture, power consumption as many of these devices have limited battery life [5]. While many safety and security standards exist [9], they are written in text, and it is uncertain if the designer has taken them into account, where modeling and verification is mathematical and objective [7]. We propose that we can directly check if each standard is fulfilled if they are written as requirements that are refined until they can be directly tested (i.e. latency $<$ value). It is more assuring to test a mathematical statement rather than a high-level idea "safety should be a consideration".

Currently, our approach to designing safe and secure embedded systems relies on modeling and verification techniques: SysML-Sec [2]. SysML-Sec is fully supported by the free and open-source TTool. We assume that systematic modeling and formal verification helps detect flaws earlier, and can analyze absolutely every possible situation, which individual safety or security tests cannot do. There exist many other design methods and tools, each which analyze some aspects of design, but none that really cover within the same modeling and verification approach the interaction between faults/hazards (safety) and attacks (security) while elaborating the HW/SW architecture of a system. Yet, while our approach already supports an analysis phase (requirements, fault and attack trees) and a partitioning phase in which hardware and software are jointly designed, the method on how to have smart interactions between all these models is still unclear, especially when it comes to respect development standards.

2 Objectives

Therefore, **the main objective of the Ph.D is to study methods, models and tools that could offer a smart interaction between requirements, fault and attack trees, and HW/SW partitioning.** This includes the study on how to integrate domain-specific development standards (e.g., ISO 26262) into a model-driven approach that can handle both safety and security aspects in the first development stages. Finally, a prototyping tool supporting the proposals will be implemented. “Smart” means that the proposal should minimize negative side effects.

An interesting aspect is to find fault and attack countermeasures that minimize negative side-effects on the system. For instance, adding an encryption mechanism to counter an attack on a bus increases transmission delay, and therefore increases the possible faults — encryption mechanisms could themselves include HW or SW bugs —. Similarly, using redundancy HW to decrease the probability that a result cannot be computed because of a failure increases the attack surface of the system. As a result, clear modeling rules, following e.g. automotive standards, must clearly explain how to interact between antagonist design choices. The Ph.D. should clearly show if the support offered by fault and attack trees can help find these compromises.

This work will obviously be driven from partners of the “C3S chaire”. It will be based on our previous contributions with Automotive partners, e.g. the European FP7 project EVITA [10] and the VEDECOM institute [12] [1].

3 Expected work

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

1. Understand the methods currently in use for safe or secure systems within the partners of the “C3S chaire”. More generally a biblio on model-driven approaches for designing embedded systems will be studied, with a focus on fault and attack trees.

2. Learn how to make system modeling with TTool and SysML-Sec. You will practice with a case study provided by the Chaire committee.
3. From the first work, study how fault and attack trees could be used together to better identify relevant HW/SW architectures. This includes methodological work as well as modeling extensions (find new operators in trees e.g. ways to express countermeasures linked in the two kinds of trees).
4. A deep bibliographical study must then be done on modeling techniques for safe and secure embedded systems, as well as on standards for automotive systems.
5. Propose an enhanced methodology and modeling extensions. This could be additional operators in trees e.g. ways to express countermeasures in the two kinds of trees, with a way to link countermeasure in fault and attack trees.
6. Propose a way to integrate current contributions with current automotive standards, implement and evaluate your proposal.

4 Skills

- Excellent skills in software engineering (principle of Model-Driven engineering) and embedded architectures (i.e. hardware/software architectures)
- Skills in safety and 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-paristech.fr. Incomplete applications won't be taken into account. Selected candidates will be evaluated on technical skills and on their research capabilities (e.g. reviewing a paper).

- CV
- Cover letter
- Reference letters. At least one reference letter from your Master internship supervisor is necessary.
- Grades obtained during the master, and ranks.

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] 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.

[3] Tom Davenport and John Lucker. Running on data: Activity trackers and the internet of things. https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-16/internet-of-things-wearable-technology.html, 2015.

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

[5] Paul Kocher, Ruby Lee, Gary McGraw, and Anand Raghunathan. Security as a new dimension in embedded system design. In *Proceedings of the 41st Annual Design Automation Conference*, DAC '04, pages 753–760, New York, NY, USA, 2004. ACM. Moderator-Ravi, Srivaths.

[6] pymnts.com. Can a connected refrigerator anchor the iot household? https://www.pymnts.com/intelligence-of-things/2017/can-a-connected-refrigerator-anchor-the-iot-household/, May 2017.

[7] Jose Fran Ruiz, Rajesh Harjani, Antonio Mana, Vasily Desnitsky, Igor Kotenko, and Andrey Chechulin. A methodology for the analysis and modeling of security threats and attacks for systems of embedded components. In *Parallel, Distributed and Network-Based Processing (PDP), 2012 20th Euromicro International Conference on*, pages 261–268. IEEE, 2012.

[8] Safety.com. The top 40 best wearable tech products for kids and families. https://www.safety.com/best-wearables, 2017.

[9] Erwin Schoitsch. Design for safety and security of complex embedded systems: A unified approach. In *Proceedings of the NATO Advanced Research Workshop on Cyberspace Security and Defense: Research Issues*, pages 161–174. Springer, 2005.

[10] H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann. C2x communication: Securing the last meter. In *The 4th IEEE International Symposium on Wireless Vehicular Communications: WIVEC2011*, San Francisco, USA, September 2011.

[11] Cadie Thompson. As healthcare costs rise and patients demand better care, hospitals turn to new technologies. http://www.businessinsider.fr/us/how-hospitals-are-using-iot-2016-10/, 2016.

[12] VEDECOM. Institut français de recherche partenariale publique-privée et de formation dédié à la mobilité individuelle décarbonée et durable. http://www.vedecom.fr/.

[13] Wired. How connectivity is driving the future of the car. https://www.wired.com/brandlab/2016/02/how-connectivity-is-driving-the-future-of-the-car/, 2016.