Sujet de Thèse

Approche orientée modèle pour la conception de systèmes embarqués à la fois sûrs, sécurisés et efficaces

Model-Based Approach to Design Safe, Secure and Efficient Embedded Systems

Directeur de Thèse : Ludovic Apvrille
Co-directeur de thèse : Renaud Pacalet
Département Communication et Électronique
Institut Mines Télécom / Télécom ParisTech
450 route des Chappes – 06904 Sophia-Antipolis Cedex
Téléphone : +33 (0) 4 9300 8406
Email : `ludovic.apvrille@telecom-paristech.fr`

Mots clés : Ingénierie dirigée par les modèles, sécurité, sûreté de fonctionnement, SysML, vérification formelle
Keywords : Model-driven engineering, security, safety, SysML, formal verification

Résumé français

Les attaques régulièrement publiées sur les systèmes embarqués démontrent le besoin de mieux sécuriser ces systèmes avant qu'ils ne soient mis sur le marché, c'est à dire lors de leur conception. L'environnement SysML-Sec [1] de Telecom ParisTech a été proposé pour répondre au besoin de conception des systèmes sécurisés à l'aide d'une approche orientée modèles et de preuves. Toutefois, SysML-Sec ne considère pas suffisamment la phase de partitionnement logiciel/matériel pendant laquelle les principales décisions d'architecture sont prises. La thèse s'intéresse donc à la conception de l'architecture par itération sur les exigences de sécurité, les attaques et les architecture candidates. Elle consistera à définir cette itération, puis à enrichir la méthodologie et les modèles de SysML-Sec, et enfin à implémenter ces extensions dans l'outil support à SysML-Sec : TTool [2]. La thèse se déroulera dans le cadre d'un projet Européen appelé "Aquas", qui est en cours de démarrage. Le projet fournira notamment des études de cas industrielles qui serviront de point de départ aux travaux autour de SysML-Sec et TTool.

La thèse s'effectuera au LabSoC, un laboratoire de Telecom ParisTech situé à Sophia-Antipolis (Côte d'Azur).

English summary

Attacks on embedded systems are frequently published : they demonstrate the need to better secure embedded systems before they are on the market, i.e. during their design process. The SysML-Sec [1] environment – developed by Telecom ParisTech – offers a model-driven approach to design secure embedded systems and perform security proofs. However, SysML-Sec does not fully address the hardware / software partitioning stage during which main system architectural decisions are taken. In particular, it does not offer any support to efficiently iterate between system requirements, threats, and candidate architectures. The Ph.D. candidate will thus need to propose extensions to SysML-Sec, and to implement these extensions within the TTool [2] toolkit supporting SysML-Sec. The Ph.D. work will be part of a European project – named Aquas - that will start presently. The project is expected to provide industrial case studies that will serve as starting points for the project.

The laboratory of the Ph.D. is called "LabSoc" – a lab of Telecom ParisTech, a French Engineering School – and is located in Sophia Antipolis on the French Riviera.

Context and Motivation

Many recent attacks targeted security vulnerabilities on embedded devices such as the Tesla hack [5], mobile&smart phones [9], avionics [6], drones [10], and smart objects such as the Fitbit [3]. These security vulnerabilities leave users susceptible to personal injury, theft of personal information, or financial damage. Finding security flaws in these systems is difficult, as their complexity is further increased by their heterogeneous nature ; one must analyze both hardware and software components, and the consequent interactions. Moreover, correcting these security flaws might be difficult once the system has been released - and sometimes impossible - if the flaws cannot be corrected by software update only. As commonly stated, these kinds of issues should be discovered early in the development process.

The SysML-Sec [1] methodology was introduced to handle the design of such complex systems, in terms of safety, performance, and security [4]. SysML-Sec [1] extends UML for the design of embedded systems. One of its important early development phases is the hardware / software partitioning phase, which distributes functions to be realized by the system among processing nodes. This phase explores candidate hardware / software architectures and decides on the "best" architecture according to several criteria such as cost of the platform and its performance. To better address embedded system security, the choice of architecture should also be based on the ability of the architecture to support security features for secure communication.

Security properties of the components of the architecture itself should be modeled based on attacker capabilities. For example, communication buses and memories can be internal and secure against an external attacker, and functions mapped to the same processor using an on-die memory can consider their message exchanges secure. On the contrary, external buses can be spied on. The chosen architecture also affects where encryption algorithms need to be executed and where cryptographic materials need to be stored to fulfill security requirements.

Objective

The objective of the Ph.D. thesis is to propose a new model-driven method to capture, within different views, requirements, attacks and the candidate system architecture, and to propose a method to efficiently iterate between the different views (requirements, attacks, architecture), while considering all together safety, security and performance properties. Last but not least, the proposition will be define according to case studies provided within a

European project, and in particular railway-based systems.

Verification will also play a key role since proposed models shall always be verifiable from a safety, security and performance point of view. We do not expect to (fully) redevelop verification techniques and tools in the thesis, but rather to define the necessary techniques to perform the proofs from models - including model transformation techniques -, and how the proposed method can rely on existing approaches. However, if existing techniques are insufficient, extensions to existing verification techniques should also be proposed.

Finally, the contributions shall be integrated within the SysML-Sec [1] modeling environment, and within the support toolkit (TTool [2]).

State of the art

Many works address the modeling of security during software design only. SecureUML enabled the design and analysis of secure systems by adding mechanisms to model role-based access control [8]. Authorization constraints are expressed in Object Constraint Language (OCL) for formal verification. The proposed thesis should focus on security models focusing on protecting against several kinds of attackers (eg., an external attacker) and not only on access control. Also, in contrast to formula-based constraints or queries, we expect the Ph.D. thesis to rely mostly on graphical elements (operators, annotations).

Another work [11] proposed modeling security in embedded systems with attack graphs to determine the probability that data assets could be compromised. While their approach is also UML-based, they focus on estimating probabilities of success for attacks, while ours focuses on verifying adequate placement of security mechanisms, with regards to requirements (safety, security, performance) and threats

UMLsec [7] is a UML profile for expressing security concepts, such as encryption mechanisms and attack scenarios. It provides a modeling framework to define security properties of software components and of their composition within a UML framework. It also features a rather complete framework addressing various stages of model-driven secure software engineering from the specification of security requirements to tests, including logic-based formal verification regarding the composition of software components. However, UMLSec does not take into account the HW/SW Partitioning phase necessary for the design of IoTs.

Work plan

First year

The first year will be dedicated to understanding the issues in the modeling and verification of safe, secure and efficient embedded systems. It may start by making a complete overview of the bibliography on modeling and proofs techniques for security, safety and performance. Another way to start will be to consider the case studies of the Aquas project, and to use the current modeling environments (SysMLSec [1], TTool [2], but also e.g. Capella) to better understand the limitations of these environments. While safety and performance constraints have been studied for a long time in model-driven approaches, there are only few contributions for handling security alone, or for handling security along the two other constraints (safety, performance).

The result of the first year should be a set of proposals on how security could be better taken into account, and how its impact on safety and performance could be better evaluated. As previously explained, the focus of the research will be on the preliminary development stages of a system : requirements, threats and hardware / software architecture, and how they can efficiently interact with later ones.

Second year

Following the set of proposals given at the end of the first year, these proposals will be prototyped in a modeling and verification environment (TTool [2]), and evaluated using the case studies of Aquas. The evaluation metrics must be listed, e.g., relevance of models, scalability, ease-of modeling, efficiency of verification, maintainability, etc. First demonstrations and publications will be performed.

Third year

Publications are commonly written during the third year. The third year work will also include finalizing the modeling and verification environment, and writing the Ph.D. thesis manuscript. The latter should include a formalization of the modeling environment, and of the model transformations used for verification.

Since the work will be performed in the scope of a European project (Aquas), the Ph.D. candidate is expected to attend the different meetings (teleconferences, in-person meetings) during all three years.

Expected results

The main outcome of the thesis will be an innovative model-driven approach for handling security, safety and performance in the preliminary development stages of complex embedded systems. The results will be in the form of :

- Meta-models describing the informal semantics of the diagramming elements
- A methodology that explains how to efficiently use the different (new) modeling views
- A formal description of the diagrams, and a formal description of the model-to-formal-code transformations
- An evaluation of the overall approach
- An extension to TTool [2] in order to support the new diagrams and transformations
- Publications in the notable conferences of the domain (e.g., MODELS)
- Deliverables in the Aquas project

Work Environment

The Ph.D. candidate will be part of "LabSoC", a lab in the "Communication and Electronics" department of TELECOM ParisTech, a high-level French engineering school. The doctoral school is "ED STIC" of Université Paris Saclay. The lab is located in Sophia Antipolis, around 30 minutes from Nice.

The LabSoC has about 15 members, with 5 professors or assistant professors, one part-time engineer, and 9 Ph.D. students. The main research topic of LabSoC is the design and analysis of embedded systems, including smart objects and Internet of Things.

International opportunities

The Ph.D. candidate will actively participate in a European project called Aquas. The project goal is to develop synergies between industrial and academics - more than 20 partners - on how to deal with safety, security

and performance constraints when developing complex embedded systems. More precisely, the Ph.D. candidate will consider case studies provided by industrial partners of the projects in the domain of trains for example.

Collaborations

Apart from the collaborations within the Aquas project, the Ph.D. candidate will have the opportunity to interact with other Ph.D. students of LabSoC involved in other industrial contracts (Nokia, VEDECOM).

Dissemination

We expect the Ph.D. student to actively participate in writing the deliverables of the Aquas project. Also, the Ph.D. student will publish his/her contributions to international conferences of the domain, either for tools demonstrations or paper presentation : DATE, Models, Modelsward, etc. Last but not least, publications should include journal articles during at least the last year of the Ph.D.

Confidential work

No

Références

[1] Sysml-sec website : http://sysml-sec.telecom-paristech.fr.

[2] Ttool website : http://ttool.telecom-paristech.fr.

[3] Axelle Apvrille. Geek usages for your Fitbit Flex tracker Hack.lu, Luxemburg, October 2015. Slides at framadrive.org/index.php/s/Wk6nxAKMpVTdQl4, October 2015.

[4] 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*, Angers, France, February 2015. SCITEPRESS Digital Library.

[5] Lucian Constantin. Researchers hack Tesla Model S with remote attack. http ://www.pcworld.com/article/ 3121999/security/researchers-demonstrate-remote-attack-against-tesla-model-s.html, 2016.

[6] Andrei Costin and Aurélien Francillon. Ghost in the air (traffic) : On insecurity of ads-b protocol and practical attacks on ads-b devices. *Black Hat USA*, pages 1–12, 2012.

[7] Jan Jürjens. Umlsec : Extending uml for secure systems development. In *Proceedings of the 5th International Conference on The Unified Modeling Language*, UML '02, pages 412–425, London, UK, UK, 2002. Springer-Verlag.

[8] Torsten Lodderstedt, David A. Basin, and Jürgen Doser. Secureuml : A uml-based modeling language for model-driven security. In *Proceedings of the 5th International Conference on The Unified Modeling Language*, UML '02, pages 426–441, London, UK, UK, 2002. Springer-Verlag.

[9] D. Maslennikov. Russian cybercriminals on the move : profiting from mobile malware. In *The 20th Virus Bulletin Internation Conference*, pages 84–89, Vancouver, Canada, October 2010.

[10] Nils Rodday. Hacking a Professional Drone. Slides at www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf, March 2016.

[11] Maria Vasilevskaya and Simin Nadjm-Tehrani. *Quantifying Risks to Data Assets Using Formal Metrics in Embedded System Design*, pages 347–361. Springer International Publishing, Cham, 2015.