CERES – PhD Thesis Position

A Model-Based Systems Engineering Approach for Assessing the Security of Cyber-physical Systems

Team R3S
SAMOVAR, Télécom SudParis
Institut Polytechnique de Paris

Team ACES
LTCI, Télécom Paris
Institut Polytechnique de Paris

Start Date: As soon as possible

Context and General Objectives

Cyber-physical systems (CPSs) have been receiving increasing interest from both researchersand industrial practitioners. These are smart embedded systems e.g., vehicles, aerospace systems, medical systems, or industrial control systems, that encompass computational (i.e., hardware and software) and physical components, seamlessly integrated and closely interacting to sense the changing state of the real world. These systems involve a high degree of complexity at numerous spatial and temporal scales and highly networked communications integrating computational and physical components.

However, interconnecting the cyber and physical worlds, increases the attack surface and gives rise to new impactful security threats. The security of cyber-physical systems is a major challenge for their designers and maintainers. To address this challenge, a methodology able to specify expected security requirements properties of a system, deploy enforcement points and verify their efficiency, is necessary. Such a methodology should allow to model complex (systems of) systems at several level of abstraction to enable situational awareness to different actors in term of cybersecurity. Incidentally, the modeling should expose hints (metrics or interfaces) that an evaluator can instrument to check the efficiency of security measures to protect the system under test.

Therefore, the main objective of this work is two-fold: i) propose methodologies and tools to accurately model cyber-physical systems, as well as the security requirements, threats and remediations that apply to them, so that operators can gain different levels of insights and interact with it at increasing levels of accuracy; ii) design methodologies to assessthe security of the system under test security or its resilience to threats in the presence or absence of remediations with fine control over the inputs and conditions of the assessment environment, including metrics, probes, injection points, datasets (both legitimate and malicious activities).

This work is part of the CERES project, within the framework of the CIEDS (Interdisciplinary Center for Defense and Security Studies) of the Institut Polytechnique de Paris. It is partially funded by the French Agency for Defense Innovation (AID), ministry of armed forces.

State Of the Art, Envisioned Approach, and Expected Results

Several research studies propose semi-formal or formal models of security threats corresponding to multi-step attack scenarios in complex systems like cyber- physical systems. Most are based on a symbolic model of the attack process that can rely on different formalisms: trees, graphs, transition systems (automata, Petri nets), logical theories, etc. Amongst those, one of the most used formalism to model and rea son about these attacks scenarios is *Attack Graphs* (for a recent survey, see for instance [8]).Given a description of the architecture of the analyzed system and the knowledge of the existing vulnerabilities on the various components of this system, the attack graphsrepresent all the attack scenarios in the form of a graph. An attack scenario, correspondingto a path of the attack graph, is represented as a sequence of atomic actions (an injection of SQL code, the exploitation of a buffer overflow, a dictionary password attack, etc.)performed by the attacker, and considering causal dependencies and feasibilityconstraints in the attack scenario. The nodes of an attack graph represent possible states ofa system during the attack. The edges correspond to changes of states due to an attacker's actions. The generation of an attack graph proceeds in three main phases: 1) architecturemodeling, 2) security information collection; and 3) attack graph building. Attack graphs can then be used to perform security analysis both offline (computation of security metrics, selection of an optimal security hardening policy) or online (ongoing attack scenario prediction, selection of reactive security countermeasures).

The existing research on attack graph generation is mainly "non-model-based". It is rarely based on a formal description of the system model (describing architecture and connectivity, components and behaviors, assets, defenses, vulnerabilities, and atomic attacks), and hence cannot be fully automated and is therefore time-consuming and error prone. When this is the case, the models used are ad-hoc and difficult to integrate in a classical system engineering process (i.e., cannot be automatically derived from existing models ofthe architecture of the system).

Today, *Model-Based Systems Engineering (MBSE)* has become an important paradigm for the development of cyber-physical systems. MDE is a software development methodology thatfocuses on creating and exploiting domain models, which are conceptual models of all the topics related to a specific problem. Amongst others, current popular modeling languages used in *MBSE* are the Systems Modeling Language (SysML), the Unified Modeling Language, the Modeling and Analysis of Real-Time and Embedded systems (MARTE) and the Architecture Analysis and Design Language (AADL) (see for instance [10] for a presentation and comparison of these languages). Recently, MBSE approaches for security have been proposed (see [7] for a survey). However, to the best of our knowledge, no approach for security fully integrates multi-step attack scenario modeling. Some works on the topic considers models allowing the representation of attack trees or graphs [2, 4]. However, they do not specify all the necessary models to generate the attack scenario model.

Therefore, an integrated approach that is based on complete and accurate models and that is automated (to a certain extent) in generating multi-step attack scenarios for CPS is highly desired. Based on the existing expertise on MBSE and attack modeling in the team, we plan to propose such a methodology and related tools for MBSE support and multi-step attack scenario modeling (again possibly based on attack graphs, though not mandatory). As an initial step, such a methodology could borrow from [12] that proposes a modeling language extension to represent security concepts and metrics throughout the systems modeling life cycle. Such an approach will have to tackle a well-known problem related to attack graph generation: it may suffer from the state explosion problem occurring (most notably when the number of vulnerabilities in the target system grows large). A possible way to avoid this problem is to take inspiration from the work in [9] that proposes a parallel and distributed memory-based algorithm to generate an attack graph.

To complete the picture, a complementary field of study is the modeling of tests environments and their representativity. This aspect is often in conflict with the feasibility of the tests as they could exceedingly complexify the model and its computability. A number of innovations are expected to extend or surpass the state of the art in testbeds [5, 13], cyber-ranges [1, 3, 6] and other product security evaluation platforms [11].

The approach we want to develop will be validated through a case study related to the domain of smart buildings. Domain specific characteristics could be captured using a modeling language dedicated to building systems such as *Realestatecore*[1]. Furthermore, digital twin models could be extracted using language such as Azure *Digital Twin Definition Language (DTDL)* [2].

Tasks

- Contribute to a state of the art on existing security analysis approaches and tools.
- Develop an architecture-centric model-based methodology to assess the security of cyber-physical systems orchestrating the relevant analysis tools selected from the state of the art.
- Select the most appropriate modeling languages to describe the architecture of smart buildings and other viewpoints (requirements, attack scenarios, etc.) as required by the methodology.
- Prototype and evaluate the methodology on our smart building case study.

Application

Applications should be sent as soon as possible and will be followed by a (remote) interview, if accepted. Potential candidates MUST hold a master's degree in computer science and ideally have experience in one or several domains related to cybersecurity, model-based engineering, test and verification, testbeds, as well as a strong motivation for research. The candidate should send by email the following items to ALL contacts:

- Detailed resume.
- A copy of the latest diploma.
- Letters of recommendation or a list of referees (people that would recommend the candidate).

Incomplete applications will not be considered.

Contacts

- Gregory Blanc (gregory.blanc@telecom-sudparis.eu)
- Dominique Blouin (dominique.blouin@telecom-paris.fr)
- Jean Leneutre (jean.leneutre@telecom-paris.fr)
- Olivier Levillain (olivier.levillain@telecom-sudparis.eu)

References

[1] A. Furfaro et al. A Cloud-based platform for the emulation of complex cybersecurity scenarios. *Future Generation Computer Systems*, 89:791–803, 2018.

[2] L. Apvrille and Y. Roudier. SysML-Sec Attack Graphs: Compact Representations for Complex Attacks. In *The Second International Workshop on Graphical Models for Security (GraMSec 2015)*, volume 9390, pages 35–49, Verona, Italy, July 2015. Springer, LNCS.

[3] E. de Souza, O. Ardakanian, and I. Nikolaidis. A Co-simulation Platform for Evaluating Cyber Security and Control Applications in the Smart Grid. In *Proc. of ICC'20*, pages 1–7. IEEE, 2020.

[4] W. Depamelaere, L. Lemaire, J. Vossaert, and V. Naessens. Cps security assessment using automatically generated attack trees. 2018.

[5] D.S. Fowler et al. Towards a Testbed for Automotive Cybersecurity. In *Proc. of ICST'17*, pages 540–541. IEEE, 2017.

[6] M. Ficco and F. Palmieri. Leaf: an open-source cybersecurity training platform for realistic edge-IoT scenarios. *Journal of Systems Architecture*, 97:107–129, 2019.

[7] J. Geismann and E. Bodden. A systematic literature review of model-driven security engineering for cyber-physical systems. *J. Syst. Softw.*, 169:110697, 2020.

[8] K. Kaynar. A taxonomy for attack graph generation and usage in network security. *J. Inf. Secur. Appl.*, 29(C):27–56, aug 2016.

[9] K. Kaynar and F. Sivrikaya. Distributed attack graph generation. *IEEE Trans. Dependable Secur. Comput.*, 13(5):519–532, sep 2016.

[10] F. Kordon, J. Hugues, A. Canals, and A. Dohet. *Embedded Systems: Analysis and Modeling with SysML, UML and AADL.* ISTE. Wiley, 2013.

[11] MITRE. Engenuity.

[12] D. Naouar, J. E. Hachem, J.-L. Voirin, J. Foisil, and Y. Kermarrec. Towards the integration of cybersecurity risk assessment into model-based requirements engineering. In *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pages 334–344, 2021.

[13] Y. Yang et al. Cybersecurity testbed for IEC 61850 based smart substations. In *Proc. of PESGM'15*, pages 1–5. IEEE, 2015.

[1] https://www.realestatecore.io/introduction/

[2] https://learn.microsoft.com/en-us/azure/digital-twins/concepts-model