CERES – Thesis proposal #1 on Security Modelization and Assessment

Team R3S
SAMOVAR, Télécom SudParis
Institut Polytechnique de Paris

Team ACES
LTCI, Télécom Paris
Institut Polytechnique de Paris

Context

Information systems are increasingly complex and spreading in every sector, often built from off-the-shelf components, with little to no security guarantees whatsoever. In order to regain its sovereignty, a State needs to build its cybersecurity posture from certified software and hardware stacks, security-wise. To that end, a methodology is necessary to specify expected security properties of a system, deploy enforcement points and verify their efficiency. Our objective is to model complex (systems of) systems at several level of abstraction to enable situational awareness to different actors. Incidentally, the modelization should expose metrics or interfaces that an evaluator can instrument to verify the ability of security measures to protect the system under test. Yet, the extent and diversity of the inputs, although restricted to a given scope of evaluation, is entirely left to the creativity of the evaluator.

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

Objectives

The objective of this thesis is two-fold: i) propose ways to accurately model a process, a function, a system, and a system of systems, as well as the security threats and remediations that apply to them, so that operators can gain different levels of insights and interact with it, with increasing levels of realism; ii) design methodologies to assess the system under test's security or 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). A number of innovations are expected to extend or surpass the state of the art in testbeds [3,6], cyberranges [1,2,4] and other product security evaluation platforms [5].

Proposal

In this thesis, state-of-the-art modelizations of complex systems will be first studied in depth and compared to apprehend current limitations and discuss open problems. In particular, we will focus on modelizations enabling actors to comprehend threats and their impacts on the system under test, such as attack graphs. An attempt will be made to

extend such models through data enrichment to accommodate more complex systems or attacks.

Another field of study is the modelization of test environments and their realism. This aspect is often in conflict with the feasibility of the tests as they could exceedingly complexify the model and its computability.

Finally, in terms of assessment, the thesis aims at formalizing existing methodologies, and providing a reproducible approach. Reliability and comparability are two important properties for assessing the properties of a security mechanism. Additionally, the approach will drive the generation of test cases in a way that maximize coverage while still enabling explainability.

Application

We are open to applications to be reviewed as soon as possible, and followed by an (remote) interview, if accepted. Potential candidates MUST hold a Master-level degree or equivalent (e.g., a French *diplôme d'ingénieur*) and have experience in domains related to this thesis offer (cybersecurity, modelization, test and verification, testbeds) as well as a strong motivation for research. The candidate SHOULD provide the following items as an application package by email to ALL points of contact:

- up-to-date resume (CV);
- a copy of the latest degree (or ongoing if completion date is September 2021);
- letters of recommendation, or a list of references (people that would recommend the candidate).

Incomplete packages will not be reviewed.

Contacts

- Gregory Blanc (`gregory.blanc@telecom-sudparis.eu`)
- 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] 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.

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

[4] 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.

[5] MITRE. Engenuity.

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