CERES Research Internship: Security Modelling and Assessment

Institut Polytechnique de Paris

Internship start: February 2022

Keywords — modelling, security metrics, risk assessment

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. 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 levels of abstractions to endow different actors with situational awareness. Incidentally, the modelling 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.

The security posture of an entity often translates into a security policy that defines, based on a prior cyber-risk assessment, the procedures, tools and people that will enforce security actions, both preventive and reactive. It unravels within a cybersecurity lifecycle where regular audits (both organizational and technical) and trainings are performed to ensure security readiness. Any new information (alert, incident) or evolution of the protected system, or the security information system should be taken into account as soon as possible to understand the relevance of the security policy.

This internship aims to survey the state of the art of security models, in particular of complex systems. Past formalisms and approaches have enabled to model risk interdependencies between the information system and the system to protect [1], to evaluate the impact of security measures on the system to protect [2], or the business assets [3]. This internship aims at combining (or unifying) different approaches to reach an awareness of the cybersecurity situation, in a way that is resilient to changes, by taking into account additional sources of information, such as logs or threat intelligence. Additionally, predictive approaches could also be developed by leveraging machine learning methods on security data sources.

Activities

- survey of security models
- study and implementation of a subset of approaches

- development of a limited cybersecurity situational awareness system
- integration of different data sources (logs, threat intel)
- *(optional) development of a predictive module*

Practical information

The internship will take place jointly at SAMOVAR and LTCI laboratories, Institut Polytechnique de Paris, in Palaiseau. It will be 5 to 6 months long.

Applicants are about to complete their Master 2 level degree (or equivalent engineering school degree) and should have the following skills:

- strong knowledge in a modern programming language
- skills in system modelling, or at least practice in modelling languages
- knowledge in cybersecurity risk modelling

The internship topic is linked to a Ph.D offer in the context of the CERES project (funded by the French Agency for Defense Innovation (AID)). **Applicants MUST be European nationals and WILL be subjected to a defense authorization process before starting**. Applications (resume, motivation letter, academic transcripts, recommendation letters) must be sent to `gregory.blanc[at]telecom-sudparis.eu`, `jean.leneutre[at]telecom-paris.fr` and `olivier.levillain[at]telecom-sudparis.eu`.

References

[1] Ziad Ismail, Jean Leneutre, David Bateman, and Lin Chen. Managing security risks interdependencies between ict and electric infrastructures: A game theoretical analysis. In *Game theory for security and risk management*, pages 223–250. Springer, 2018.

[2] Gustavo Gonzalez-Granadillo, Hervé Debar, Grégoire Jacob, Chrystel Gaber, and Mohammed Achemlal. Individual countermeasure selection based on the return on response investment index. In *Proc. of MMM-ACNS'12*. Springer, 2012.

[3] A. Motzek, G. Gonzalez-Granadillo, H. Debar, J. Garcia-Alfaro, and R. Möller. Selection of Pareto-efficient response plans based on financial and operational assessments. *EURASIP Journal on Information Security*, 2017.