INSTITUT POLYTECHNIQUE DE PARIS

Postdoctoral project: Simulation/co-simulation/emulation to model systems and threats

Contact : Gregory Blanc, Télécom SudParis (gregory.blanc@telecom-sudparis.eu)

Object : Postdoctoral project proposal

Project : CERES

Duration : 18 months

Motivation:

The CERES project takes place within the Interdisciplinary Center for Defence and Security Studies (CIEDS) of Institut Polytechnique de Paris (IP Paris). In particular, the project aims at contributing to different system security phases: 1) specification of the expected security properties to define complete policies, i.e., able to be deployed and ensuring a complete risk coverage; 2) deployment of policy enforcement points; 3) verification of the mechanisms efficiency through a rigorous and reproducible validation approach, that is relying on a methodology generic enough to be applied to several security mechanisms, ensuring stability through time and enabling the comparison of results. Case studies may cover both a constellation of connected devices or a building information and management system. For each of them, several layers of modelisation are considered from abstracting operations to demonstrating an isolated prototype, and even its integration to a complete system (long-term objective).

The postdoctoral researcher work will focus on CERES workpackge 1, which aims at modeling both systems and threats to systems, in the context of the security study of complex systems. We will later rely on existing formalisms (e.g., attack graphs) enriched with the produced formalisms and adapted to the case of complex systems. We will consider the modeling of testbed environments and attacks, going from abstract descriptions extracted from threat intelligence to concrete executions such as the deployment of a botnet into a target system.

Proposed work:

The activities focus on the study of diverse modeling approaches and formalisms to find the best tradeoff between the realism of the systems and attacks representation on one hand, and the feasibility of the simulations on the other hand:

- state of the art on architecture description langages for modeling building managment systems, including security aspects
- state of the art of attack modeling and formalisms
- state of the art of assessment/certification methodologies
- state of the art of testbed technologies
- development of models and tools
- definition of a data-driven methodology

Candidate profile:

Ph.D in computer science with experience in one of the following topics: network security, cyber-physical systems, model-driven engineering. Programming and systems/networks administration skills are advisable.