Proposition de recherche doctorale

Improving Software Security via Symbolic Execution

Mots clés :

- **Directeur de thèse** : aurelien FRANCILLON
- **Co directeur de thèse** : aurelien FRANCILLON
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire de recherche d'EURECOM
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Sciences et technologies de l'information et de la communication

Résumé du projet de recherche (Langue 1)

Symbolic execution has been used for bug finding with great success; it is particularly useful in cases where simpler methods like random testing cannot reach relevant parts of a program under test. However, despite considerable improvements, the technique still suffers from scalability problems which make it unsuitable for many use cases in practice. Moreover, symbolic execution of firmware, i.e., software running inside embedded devices, poses a set of additional challenges. In my doctoral studies, I plan to advance the state of the art in symbolic execution with the goal of providing software developers a tool that can detect faults in software before it is released. Specifically, I would like to focus on the interaction between symbolic execution engines and SMT solvers, as well as the symbolic interpreter. I believe that tighter interaction between symbolic execution and the underlying reasoning engine can alleviate some of the scalability problems we are currently facing, and there is potential in optimizing the code execution step. I hope thereby to contribute to the field of software and firmware security at large.