Using Formal Methods for Bug Evaluation and Prioritization

Guilhem Lacombe*[1,2] and Sébastien Bardin[3]

[1]CEA LIST – CEA/ DRT/LIST – France
[2]Université Paris-Saclay – Université Paris-Saclay,Sorbonne Universités – France
[3]CEA, List, Université Paris-Saclay – CEA-LIST – France

Résumé

As bug-finding methods improve, bug-fixing capabilities are exceeded, resulting in an accumulation of potential vulnerabilities. There is thus a need for efficient and precise bug prioritization based on exploitability. Most current approaches rely on imprecise heuristics or opaque machine learning, while there is a distinct lack of developments on the side of formal methods. We aim to raise awareness for the advantages of using formal methods to automatically prioritize bugs. In particular, our works on evaluating attacker control over vulnerabilities ("Attacker Control and Bug Prioritization", accepted at USENIX Security 2025) and bug reliability ("Quantitative Robustness for Vulnerability Assessment", PLDI 2024) demonstrate the feasibility and effectiveness of this idea.

*Intervenant