
Revisiting Program Analysis through the Security Lens

Sébastien Bardin*¹

¹CEA LIST – Univ. Paris-Saclay – France

Résumé

Symbolic Execution emerged in the mid-2000 and was rapidly adopted by the research community as a tool of choice for bug hunting. In this talk, we consider security concerns and binary-level vulnerability issues. We will show some challenges symbolic execution faces in this field of application, and report on several results and achievements carried out within the BINSEC group to adapt Symbolic Execution to these challenges. We will especially focus on the problems of robust reachability (trying to define and find meaningful bugs) and adversarial reachability (considering an active code-level attacker).

*Intervenant