Binsec/Rel : Exécution Symbolique Relationnelle Efficace pour Analyse de Binaire Constant-Time

Lesly-Ann Daniel*[1], Sébastien Bardin[1], and Tamara Rezk[2]

[1]CEA LIST – Université Paris Saclay – France
[2]Inria Sophia Antipolis – Institut National de Recherche en Informatique et en Automatique – 2004 route des Lucioles BP 93 06902 Sophia Antipolis, France

Résumé

Constant-time est une contre-mesure aux attaques temporelles qui interdit les branchements et les accès mémoires dépendants des secrets. Cette contre-mesure n'est généralement pas préservée par le compilateur et requiert donc de raisonner au niveau binaire. Or, les outils d'analyse dédiés à constant-time raisonnent actuellement à un plus haut niveau (C ou LLVM), approximent la sémantique du programme, ou ne passent pas à l'échelle. Nous concevons une technique d'analyse efficace au niveau binaire qui ne fait pas d'approximation sur la sémantique du programme, permettant à la fois de trouver des bugs ou de faire de la vérification bornée pour constant-time. Celle-ci s'appuie sur l'exécution symbolique relationnelle, à laquelle nous ajoutons des optimisations dédiées. Nous proposons un prototype, Binsec/Rel et réalisons des expériences sur un ensemble de 338 binaires cryptographiques, démontrant le passage à l'échelle de notre technique. De plus, en utilisant Binsec/Rel, nous avons automatisé et étendu une étude existante sur la préservation de constant-time par les compilateurs. Nous avons ainsi découvert des violations introduites par les compilateurs qui étaient hors de portée des outils d'analyse pour LLVM, soulignant l'importance de raisonner au niveau binaire.

*Intervenant