Analyse de vulnerabilités : Automatisation du raisonnement sur les attaques par canaux auxiliaires et injection de fautes

Frédéric Recoules and Sébastien Bardin

CEA, List

frederic.recoules@cea.fr sebastien.bardin@cea.fr
https://binsec.github.io/

Alors que l'analyse de programmes se concentre usuellement sur des fautes « basiques » de type violation mémoire (ex : buffer overflows), les attaquants ont à leur disposition d'autres vecteurs d'attaques plus avancés, comme des attaques par canaux auxiliaires (ex : temps, cache, consommation énergétique) ou des attaques par injection de fautes. Les outils d'analyse de programme pour la sécurité commencent désormais à prendre en compte ce type de vecteurs d'attaque.

La plateforme d'analyse de code binaire BINSEC [1] développée au CEA propose des extensions récentes pour prendre en compte certains canaux cachés (via de l'analyse symbolique relationnelle [2]) et certains modèles d'injection de fautes (fautes symboliques [3]). Le but de ce stage sera de faire un état de l'art afin de comprendre quelles classes d'attaques physiques peuvent actuellement être prises en compte par les outils d'analyse de programme de type exécution symbolique (on pourra par exemple considérer les attaques par consommation énergétique ou par contention de port), d'identifier des limitations de BINSEC sur ce sujet et de proposer des piste d'améliorations.

Éléments logistiques. Le stage sera hébergé sur le site Nano-INNOV à Saclay. Le stage sera co-encadré par Frédéric Recoules et Sébastien Bardin.

Postuler. Pour candidater ou pour obtenir plus d'information, merci de prendre contact par mail avec les encadrants.

Références

[1] Binsec. https://binsec.github.io/.

[2] Lesly-Ann Daniel, Sébastien Bardin, and Tamara Rezk. Binsec/rel : Symbolic binary analyzer for security with applications to constant-time and secret-erasure. *ACM Trans. Priv. Secur.*, 2023.

[3] Soline Ducousso, Sébastien Bardin, and Marie-Laure Potet. Adversarial reachability for program-level security analysis. In Thomas Wies, editor, *Programming Languages and Systems*, 2023.