Analyse automatisée de binaires à la recherche de vulnérabilités matérielles

Théo De Castro Pinto*[1]

[1]Laboratoire Bordelais de Recherche en Informatique – Université de Bordeaux, Centre National de la Recherche Scientifique : UMR5800 / URA1304, École Nationale Supérieure d'Électronique, Informatique et Radiocommunications de Bordeaux (ENSEIRB) – France

Résumé

Les cartes à puce et autres appareils embarqués mettent les développeurs face à un problème de taille : les attaques physiques. Parmi celles-ci, certaines visent à modifier le comportement de la puce (temporairement ou non) grâce à une perturbation physique (laser, glitch ou autre). Ces dernières, qui peuvent être multiples au cours d'une seule exécution, sont difficiles à détecter et même si des contre-mesures existent, elles peuvent être insuffisantes ou disparaitre à la compilation. Pour ces raisons une analyse des binaires générés est nécessaire, afin de détecter la présence (ou non) de vulnérabilités face à ces attaques. Cette analyse est généralement effectuée à la main. Ce papier présente un outil d'aide à la recherche de vulnérabilités matérielles pour du code binaire. Il s'appuie sur l'outil Binsec. Il permet de détecter des vulnérabilités dans un binaire en fonction d'un schéma d'attaque et d'une cible à atteindre. Il s'agit de résultats préliminaires obtenus lors d'un stage de Master. Ce papier présente aussi quelques problématiques de recherche qui seront abordées au cours de la thèse.

*Intervenant