Partitionnement dynamique à grain fin contre des attaques par canaux auxiliaires exploitant les mémoires caches

Vianney Lapôtre*[1]

[1]Laboratoire Lab-STICC – Lab-STICC, UMR CNRS 6285 – Laboratoire Lab-STICC - CNRS, UMR 6285 Centre de Recherche Christiaan Huygens Rue de Saint-Maudé CS 7030 - 56321 Lorient CEDEX - FRANCE, France

Résumé

Les mémoires caches permettent d'accélérer considérablement les accès mémoire en stockant temporairement des données au plus proche du cœur d'exécution. Cependant, le partage de ces ressources ouvre la porte à des attaques par canaux auxiliaires. Ces attaques sont principalement exploitées pour extraire des informations sensibles, telles que des clés de chiffrement. Cette menace, bien étudiées en considérant des processeurs haute performance modernes, a conduit à la conception de contremesures complexes, parfois inapplicables aux systèmes embarqués ou engendrant un surcoût trop élevé. C'est la raison pour laquelle nous proposons, dans nos travaux, une contremesure basée sur un partitionnement à grain fin, qui permet à une application de verrouiller dynamiquement ses données en mémoire cache. Une fois les données verrouillées, aucune application ne peut inférer les accès réalisés sur celles-ci. Cette solution apporte des garanties de sécurité pour des sections de programmes critiques tout en engendrant un faible surcoût temporel grâce à une solution hybride matérielle et logicielle.

*Intervenant