Sujet de stage de Master 2 recherche 2015-2016

Etudes des liens entre modèles de faute induite par des attaques physiques à différents niveaux et analyse des effets de l'optimisation de code sur les modèles de faute et les contremesures associées.

Encadrement :
Thanh-Ha Le (MORPHO)
Emmanuelle Encrenaz et Karine Heydemann (LIP6/UPMC)

Mots clés : attaques physiques, modèles de fautes, protection de code, code source, code assembleur, compilation

Contexte et objectif

Les attaques physiques de systèmes embarqués tels que les cartes à puces ont pour but de déjouer les mécanismes de sécurité embarqués, par exemple pour obtenir des données sensibles. Au moyen d'attaques par injection de faute, il est possible de perturber le flot d'exécution d'un programme embarqué. Dans un environnement aux ressources limitées (CPU, mémoire), le challenge est alors de mettre en oeuvre des contremesures appropriées et performantes afin de renforcer la sécurité de ces implémentations.

Les études d'impacts des injections de faute(s) mettent en évidence des effets sur le flot de contrôle et/ou sur les données d'un programme [1,2]. La compréhension des effets des injections permet d'élaborer des modèles de faute à différents niveaux d'abstraction (RTL, assembleur, code source)[3,4]. Les modèles de fautes à bas niveau sont plus proches de la réalité des attaques physiques.

Les contremesures logicielles sont ou peuvent être conçues au niveau du code source, du code assembleur ou du code binaire pour un modèle de fautes donné. Un problème important est la mise en correspondance des modèles de fautes et des contremesures associées entre les différents niveaux.

De surcroît, il est difficile de transposer une exigence de sécurité au niveau du code source en une exigence sur le code assembleur ou binaire. A l'opposé, une faute matérielle peut avoir des impacts multiples au niveau assembleur, de même une faute assembleur peut avoir des impacts multiples au niveau du code source, en fonction du compilateur et des optimisations utilisées pour compiler le code en langage de la cible.

C'est pourquoi, il est difficile de statuer du niveau de criticité d'une faute observée à bas niveau, et qu'il est nécessaire d'établir un lien avec l'architecture haut-niveau.

L'objet du stage est dans un premier temps d'étudier les conséquences fonctionnelles des injections de fautes à différents niveaux d'abstraction à l'aide de jeux de code tests. Dans un second temps, les effets des optimisations de code applicables par le compilateur sur les modèles de faute à ces différents niveaux et sur des contremesures associées seront analysés. Le but est d'établir des liens entre les modèles de faute et robustesse des contremesures associées à ces différents niveaux en considérant les effets possibles de la compilation.

Déroulement

D'une durée de 6 mois, le stage se déroulera en co-encadrement Morpho (Osny) - LIP6 (Jussieu, Paris). Le stagiaire sera amené à travailler sur les 2 localisations associées, avec une répartition adaptée au rythme du stage.

Contact : karine.heydemann@lip6.fr
emmanuelle.encrenaz@lip6.fr
thanh-ha.le@morpho.com

[1] A. Dehbaoui, A.-P. Mirbaha, N. Moro, J.-M. Dutertre, and A. Tria. *Electromagnetic Glitch on the AES Round Counter*. In E. Prouff, editor, COSADE, volume 7864 of LNCS, pages 17-31. Springer, 2013.

[2] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz. *Electromagnetic Fault Injection: Towards a Fault Model on a 32-bit Microcontroller.* In Workshop on Fault Diagnosis and Tolerance in Cryptography 2013, pages 77-88. IEEE, 2013.

[3] I. Verbauwhede, D. Karaklajic, and J. Schmidt. *The fault attack jungle - A classification model to guide you.* In L. Breveglieri, S. Guilley, I. Koren, D. Naccache, and J. Takahashi, editors, 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011, Tokyo, Japan, pages 3-8. IEEE, 2011.

[4] L. Rivière, M-L Potet, T-H Le, J. Bringer, H. Chabanne and M. Puys. *Combining High-Level and Low-Level Approaches to Evaluate Software Implementations Robustness Against Multiple Fault Injection Attacks.* In 7th International Symposium on Foundations and Practice of Security, FPS 2014, Montreal, QC, Canada, pages 92-111, 2014.