Étude de la sensibilité des System-on-Chip aux attaques par illumination laser et application à l'extraction de secrets cryptographiques.

Sujet de Stage

Description

L'objectif du stage est d'étudier le potentiel des attaques par illumination laser pour extraire des secrets cryptographiques d'un téléphone mobile de type smartphone. En effet, les photocourants induits par l'illumination laser du silicium d'un circuit peut mener à la perturbation de celui-ci. Dans certains cas, cette perturbation peut être utilisée a des fin d'exfiltration de secret cryptographique.

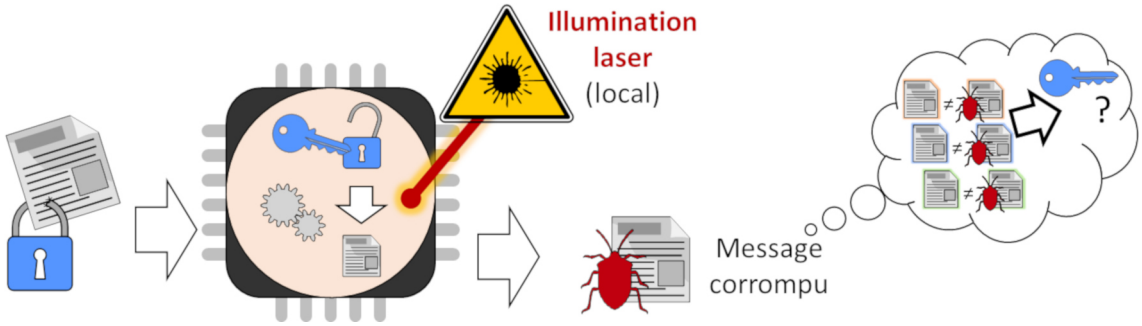

Figure 1: Une illumination laser perturbant un déchiffrement

Des chemins d'attaque par injection de fautes ont été identifiés dans la littérature pour extraire le secret utilisé par des implémentations de cryptographie (ex. [1]). Certains de ces chemins d'attaque nécessitent la modification de l'état d'un bit à un instant précis (ex. [2]). La mise en oeuvre d'un contrôle aussi fin lors d'une attaque par injection de fautes semble possible pour des cibles de type micro-contrôleur mais représente un défi pour des cibles complexes telles qu'un System-On-Chip.

Des travaux de l'équipe SAS ont permis de montrer que d'autres types d'attaques par perturbation permettent de contourner des mécanismes de sécurité sur un System-on-Chip [3]. Pour les attaques par illumination laser, il a été démontré dans la littérature que, dans certaines situations, elles peuvent permettre de contourner des mécanismes de sécurité sur ces cibles [4]. Néanmoins, les phénomènes mis en jeu et la complexité de la micro-architecture de ce type de cibles rend le contrôle de la faute injectée par l'attaquant difficile [5].

Ce stage a donc pour but de répondre aux questions suivantes:

- Existe-t-il une zone spatiale du silicium d'un System-on-Chip produisant un modèle de fautes particulier lors d'une illumination laser (ex: bit-flip) ?
- Quelle méthodologie peut permettre d'accélérer la recherche d'une telle zone ?

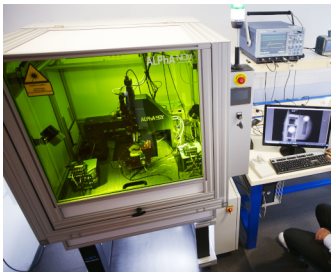

Figure 2: Banc laser bi-spot permettant d'illuminer deux zones d'un circuit

- Le contrôle des fautes produites est-il suffisant pour la mise en oeuvre attaques par injection de fautes proposées dans littérature contre les implémentations de cryptographie?

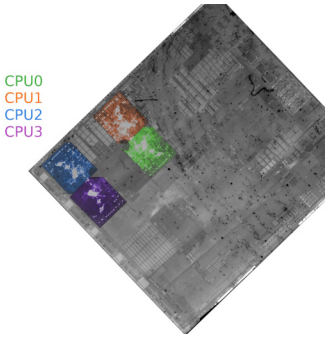

Figure 3: Identification des 4 coeurs de CPU d'un Système-on-Chip par photoémission. (Clément Gaine)

Ce sujet de stage s'inscrit dans le contexte du projet Horizon Europe POLIIICE: https://poliiice-project.eu/

Le laboratoire LSCO (Laboratoire de Sécurité des COmposants) accueillera le/la stagiaire sur son site de Gardanne au sein de l'équipe de recherche commune entre le CEA et l'EMSE: SAS "Systèmes et Architectures Sécurisés". Cette équipe dispose d'équipements de pointe avec des bancs d'attaque physique au niveau de l'état de l'art international. Elle est située entre Aix-En-Povence et Marseille à Gardanne sur le campus Georges Charpak Provence. Le stage sera encadré par Simon Pontié (CEA) et Driss Aboulkassimi (CEA).

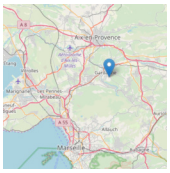

Figure 4: Campus Georges Charpak Provence: (lien)

Plus d'informations:

- https://www.simon.pontie.fr/sujet-stage/poliiice/index.html
- https://www.simon.pontie.fr/
- https://www.cea.fr/cea-tech/leti/Pages/formations/stages-alternances.aspx
- https://www.emploi.cea.fr/offre-de-emploi/emploi-extraction-de-secrets-cryptographiques-par-illumination-laser-d-un-system-on-chip-h-f_29070.aspx

Entité de rattachement

Le Leti, institut de recherche technologique de Cea Tech, a pour mission d'innover et de transférer les innovations à l'industrie. Son cœur de métier réside dans les technologies de la microélectronique, de miniaturisation des composants, d'intégration système, et d'architecture de circuits intégrés, à la base de l'internet des objets, de l'intelligence artificielle, de la réalité augmentée, de la santé connectée. Le Leti façonne des solutions différenciantes, sécurisées et fiables visant à augmenter la compétitivité de ses partenaires industriels par l'innovation technologique. L'institut est localisé à Grenoble avec deux bureaux aux USA et au Japon, et compte 1800 chercheurs.

Profil recherché

Le candidat/La candidate devra être en dernière année de Master d'un cursus Mathématique, Informatique, Électronique ou Cybersécurité.

Une expérience en lien avec les attaques physiques n'étant pas obligatoire, mais appréciable.

Le stagiaire/La stagiaire sera rémunéré(e) en fonction des grilles salariales CEA.

Le stage démarrera en 2024.

Candidature

Les candidatures sont fermées depuis le 30 novembre 2023.

Bibliographie

[1] P. Ravi, A. Chattopadhyay, J. P. D'Anvers, et A. Baksi, « Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results », *ACM Transactions on Embedded Computing Systems*, 2022.

[2] J. Hermelink, P. Pessl, et T. Pöppelmann, « Fault-enabled chosen-ciphertext attacks on Kyber », in *Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22*, 2021, p. 311-334.

[3] C. Fanjas, D. Aboulkassimi, J. Clédière, et S. Pontie, « Exploration of System-on-Chip Secure-Boot Vulnerability to Fault-Injection by Side-Channel Analysis », in *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2023. http://www.dfts.org/program.htm.

[4] A. Vasselle, H. Thiebeauld, Q. Maouhoub, A. Morisset, et S. Ermeneux, « Laser-induced fault injection on smartphone bypassing the secure boot », in *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2017, p. 41-48.

[5] T. Trouchkine, « SoC physical security evaluation », Theses, Université Grenoble Alpes [2020-....], 2021.