Vulnérabilités matérielles des smartphones face aux verrous de la synchronisation

Sujet de Stage

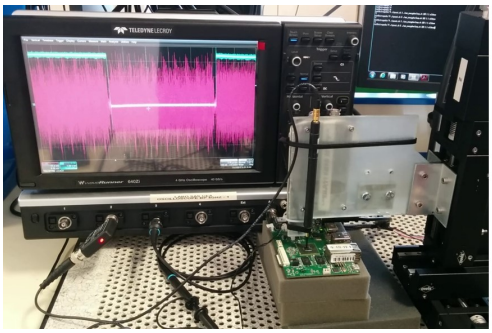
Description

L'objectif du stage est d'étudier le potentiel des attaques physiques pour contourner des fonctions de sécurité d'un téléphone mobile de type smartphone. Les chemins d'attaques à explorer tireront profit d'un accès physique au System-On-Chip réalisant ces fonctions de sécurité. Par exemple, l'analyse des émanations électromagnétiques ou la perturbation par illumination laser ou électromagnétique sont des moyens efficaces pour extraire des secrets ou contourner des mécanismes de sécurités de microcontrôleurs.

Figure 1: Contexte du stage: attaques physiques sur smartphone

Des travaux de l'équipe SAS ont permis de montrer que les attaques physiques peuvent être une menace pour les mécanismes de sécurité des Systems-On-Chip. L'analyse d'émissions permet potentiellement d'extraire un secret d'une enclave comme la TrustZone [1]. L'injection de fautes par perturbation électromagnétique peut permettre de réaliser une élévation de privilèges en s'authentifiant avec un mot de passe illégitime [2]. Cependant, la mise en place de ces attaques nécessite une bonne synchronisation entre le banc d'attaque et le code logiciel en cours d'exécution. Cette synchronisation est un verrou pour l'exploitation de vulnérabilité matérielles sur smartphone.

La mission de ce stage consiste à développer des outils ou proposer des chemins d'attaques permettant d'améliorer la synchronisation entre les bancs d'attaque et la cible.



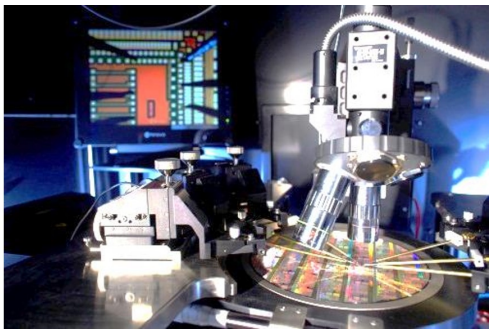


Figure 2: Exemples de bancs d'attaque physique à Gardanne: par écoute électromagnétique et par perturbation laser

Ce sujet de stage s'inscrit dans le contexte du projet H2020 EXFILES. Ce projet réuni des académiques, des industrielles et des forces de l'ordre de 7 pays européens. Les travaux effectués dans le cadre de ce stage permettront de compléter les outils d'analyse forensique existants.

Figure 3: Projet H2020 EXFILES (vidéo)

Le laboratoire LSOSP (Laboratoire de Sécurité des Objets et Systèmes Physiques) 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 Driss Aboulkassimi (CEA), Simon Pontié (CEA) et Olivier Potin (EMSE).

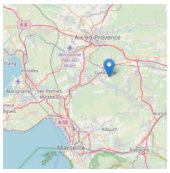


Figure 4: Campus Georges Charpak Provence: (lien)

Plus d'informations:

- https://www.simon.pontie.fr/sujet-stage/exfiles/index.html
- https://www.emploi.cea.fr/Pages/Offre/detailoffre.aspx?idOffre=14604
- https://exfiles.eu/, présentation vidéo https://vimeo.com/441318313
- https://www.simon.pontie.fr/
- https://www.leti-cea.fr/

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.

La poursuite de ce stage par une thèse est envisageable.

Le stage démarrera en 2021.

Candidature

Les candidatures sont fermées depuis le 15 novembre 2020.

Bibliographie

[1] P. Leignac, O. Potin, J.-M. Dutertre, J.-B. Rigaud, et S. Pontie, « Comparaison of side-channel leakage on Rich and Trusted Execution Environments », in *6th Workshop on Cryptography and Security in Computing Systems*, 2019, p. 19-22. https://hal.archives-ouvertes.fr/hal-02380360/ https://dx.doi.org/10.1145/3304080.3304084.

[2] C. Gaine, D. Aboulkassimi, S. Pontie, J.-P. Nikolovski, et J.-M. Dutertre, « Electromagnetic Fault Injection as a New Forensic Approach for SoCs », in *2020 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2020, p. 1-6. https://hal.archives-ouvertes.fr/cea-03155307/ https://dx.doi.org/10.1109/WIFS49906.2020.9360902.