Exploitation des vulnérabilités matérielles des dispositifs mobiles comme nouvelle approche pour l'analyse Forensic

Sujet de Thèse

Description

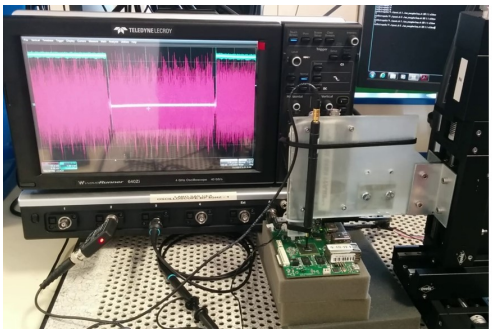
L'objectif de cette thèse est d'étudier et d'exploiter les vulnérabilités matérielles des dispositifs mobiles pour contourner les fonctions de sécurité d'un téléphone mobile de type smartphone, ou extraire des secrets. Les chemins de vulnérabilités à explorer tireront profit d'un accès physique au System-On-Chip réalisant des fonctions de sécurité. Par exemple, l'analyse des émissions électromagnétiques ou la perturbation par illumination laser ou électromagnétique sont des moyens efficaces pour extraire des secrets ou contourner des mécanismes de sécurités.

Figure 1: Contexte de la thèse: attaques physiques sur smartphone

Des travaux récents de l'équipe SAS ont permis de mettre en évidence que les vulnérabilités physiques peuvent être une menace pour les mécanismes de sécurité actuellement disponibles sur des Systems-On-Chip. L'analyse d'émissions électromagnétiques permet potentiellement d'extraire un secret d'une enclave de sécurité telle que 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]. À travers

cette thèse nous étudierons trois verrous qui limitent aujourd'hui le potentiel des vulnérabilités physiques sur Smartphone : la microarchitecture complexe des SoCs, la pile logicielle complexe des smartphones, et la synchronisation temporelle et spatiale des perturbations pour contourner un mécanisme de sécurité. En effet, la mise en œuvre de ces attaques nécessite la mise en place de bancs de test offrant une bonne synchronisation avec le code logiciel en cours d'exécution. Cette synchronisation est un verrou majeur, voire le premier à lever pour ouvrir de nouvelles pistes permettant l'exploitation des vulnérabilités matérielles sur smartphone.

Dans un premier temps, le doctorant ou la doctorante identifiera de nouvelles méthodes pour résoudre la problématique de la synchronisation du banc de test par perturbation pour l'exploitation d'injection de fautes sur Systems-On-Chip. Dans un second temps, les travaux de thèse viseront à développer de nouvelles méthodes pour contourner les verrous précédemment identifiés afin de rendre possible et réalisable l'exploitation des techniques de caractérisation sécuritaire par perturbation et par analyse de canaux auxiliaires sur téléphones mobiles pour l'extraction de données.



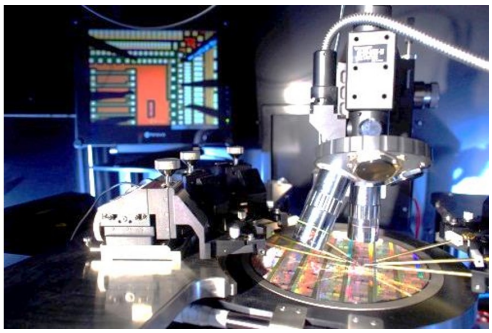


Figure 2: Exemples de bancs d'attaque physique à Gardanne: par écoute électromagnétique et par perturbation laser

Ce sujet de thèse s'inscrit dans le contexte du projet H2020 EXFILES dont le consortium est constitué de 14 partenaires : académiques, industriels et des forces de l'ordre de 7 pays européens. Les travaux effectués dans le cadre de cette thèse permettront de compléter les outils d'analyse Forensics existants. Par ailleurs, l'un des problèmes majeurs de l'exploitation des techniques de perturbation par injection de fautes à des fin FORENSIQUE, réside dans le taux de reproductibilité des résultats obtenus. En effet, en fonction des conditions expérimentales de réalisation du test, un banc d'injection EM ne permet pas de fournir les mêmes résultats sur la même cible par exemple en cas de variation de quelques degrés de la température de la salle de test, ou si la sonde d'injection EM a été déplacée puis remise à sa position initiale, etc. Le doctorant devra donc explorer et proposer des pistes d'automatisation des méthodes de tests afin de garantir un fort taux de reproductibilité indépendamment des conditions de test et de la cible analysée.

Le laboratoire LSOSP (Laboratoire de Sécurité des Objets et Systèmes Physiques) accueillera le/la doctorant sur son site de Gardanne (13) au sein de l'équipe de recherche

Figure 3: Projet H2020 EXFILES (vidéo)

commune entre le CEA et l'EMSE: SAS "Systèmes et Architectures Sécurisés". Cette équipe dispose d'équipements de pointe avec des bancs de caractérisation sécuritaire matérielle au niveau de l'état de l'art international. Située sur le campus Georges Charpak Provence à Gardanne, entre Aix-En-Povence et Marseille. La thèse sera dirigée par Jessy Clédière et co-encadrée par Driss Aboulkassimi et Simon Pontié.

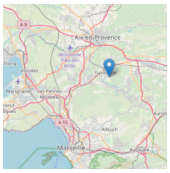


Figure 4: Campus Georges Charpak Provence: (lien)

Plus d'informations:

- https://www.simon.pontie.fr/sujet-these/exfiles/index.html
- https://exfiles.eu/, présentation vidéo https://vimeo.com/technikon/exfiles-francais
- 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 pourra avoir suivi un cursus Mathématique, Informatique ou Électronique. Une expérience en lien avec l'analyse de vulnérabilités matérielles n'étant pas obligatoire, mais appréciable.

La thèse démarrera en octobre 2021.

Candidature

Les candidatures sont fermées depuis le 15 avril 2021.

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.