Sujet de thèse : Architecture numérique pour l'identification de failles de sécurité et contre-mesures matérielles / logicielles : application à l'expertise criminalistique

CONSORTIUM : La thèse sera en collaboration entre SAFRAN IDENTITY and SECURITY, l'équipe ASTRE du Laboratoire ETIS, et, l'IRCGN – Institut de Recherche Criminelle de la Gendarmerie Nationale.

ETIS – UMR8051	**IRCGN**	**SAFRAN IDENTITY and SECURITY**
Pr. Olivier ROMAIN (directeur thèse)	Thomas SOUVIGNET	Emmanuel PROUFF
Dr. Jordane LORANDEL	Matthieu REGNERY	

CONTEXTE

La sécurité des téléphones mobiles et tablettes devient un enjeu essentiel, de préservation des données personnelles pour les uns, et d'exploitation de ces données pour les autres. Les fabricants intègrent cette sécurité de manière très disparate. Certains (i.e. Apple) sécurisent très fortement, même si la confidentialité des données reste non prouvée.

Les smartphones sont majoritairement la cible d'attaques logicielles et de nombreuses contre-mesures ont été développées par les fabricants. Ainsi, les terminaux les plus sécurisés sont de moins en moins vulnérables, notamment lorsqu'ils sont verrouillés par un mot de passe. L'angle d'attaque retenu pour cette thèse est la mémoire, volatile ou non. La plupart des données sont stockées sur cette mémoire qui est souvent reconnue comme périphérique de confiance par défaut. Si l'authenticité et l'intégrité des différents programmes lancés au démarrage de l'appareil sont souvent vérifiés, ce n'est pas forcément le cas au cours de l'utilisation du terminal. Ces failles peuvent être la clé d'un accès aux données de plateformes non vulnérables à ce jour.

Les objectifs scientifiques de cette thèse portent :

- La mise en œuvre d'une méthodologie d'attaques non intrusives.
- L'identification des contre-mesures.
- Le benchmarking sur un banc dédié.

Une telle étude n'a encore jamais été menée et n'a fait l'objet d'aucune publication. Ainsi l'innovation de la méthode et la surface d'attaque découverte représenteront des avancées significatives en matière de sécurité. Si le concept rejoint les attaques de l'homme du milieu décrites par Ross Anderson, les supports et la mise en œuvre sont novateurs. Par ailleurs, les plateformes visées chiffrent les données sur les supports de stockage. Ainsi les attaques ne pourront porter sur le contenu mais sur les metadata, comme l'emplacement dans la mémoire, le moment de l'utilisation ou la fréquence d'accès.

La stratégie de recherche envisagée est la suivante :

1. Etude théorique et pratique des différentes technologies utilisées dans le stockage des données. Ces technologies sont RAM, Flash, eMMC, PCI Express et UFS (Universal Flash Storage). Dans un premier temps recherche documentaire et appropriation des différentes spécifications. Dans un deuxième temps, manipulations d'utilisation.
2. Recherche des architectures numériques (FPGA, GPU, multi-cœurs, …) pouvant être compatibles avec les technologies étudiées en vue de réaliser un banc d'attaque. Preuve de concept de fonctionnement de l'architecture choisie.
3. Attaque en rejeu de données sur une cible.
4. Etude de contre-mesures SW/HW aux failles découvertes.

L'accès a des données protégées, et par conséquent la découverte de failles de sécurité et leur exploitation intéresse particulièrement le domaine de l'expertise criminalistique. En effet, les experts doivent en permanence trouver des moyens d'extraire les données de supports protégés pour lesquels les codes de verrouillage ne sont pas disponibles. Les contre mesures associées intéressent Safran I&S pour la sécurisation des plateformes.

MODALITE DE CANDIDATURE : Envoyer Lettre de motivation + CV + relevés de notes + copie diplôme ou attestation **avant le 1er décembre 2016** à Jordane.Lorandel@u-cergy.fr

COMPETENCES ATTENDUES

Electronique, architecture FPGA, programmation embarquée, sécurité matérielle, protocole hardware, sécurité système. Un étudiant ayant participé à un Hackathon serait un plus.

Remarque : Compte tenu du sujet et consortium, une enquête de moralité sera menée sur le candidat retenu