MINES
Saint-Étienne

Objet : Proposition Post-Doc ou Ingénieur de recherche

Dossier suivi par :
Nom : Potin
Prénom : Olivier

Tél : 0442616737

N / Ref :

PJ : 0

Attaques matérielles sur TEE

Le développement en masse des services mobiles nécessitant l'utilisation des données privées reste encore à ce jour balbutiant en grande partie dûe à la difficulté de mettre en place un environnement de confiance aux utilisateurs comme aux fournisseurs de ces services. De plus, les smartphones représentent des cibles de grande valeur pour les hackers car ils contiennent les vies numériques de nombreux utilisateurs et leurs données personnelles. Aussi, on observe ces dernières années une augmentation très importante de la fraude sur mobile (vol d'identité, vol de données financières,...) et du nombre de logiciels malveillants sur les sites de téléchargements (+614% de 2012 à 2013 selon une étude de Juniper, 2013). Face à ces enjeux, il y a donc un besoin urgent de développer et déployer des solutions de sécurité De nombreuses technologies ont pour objectif de fournir des briques de sécurité utilisables dans les terminaux Mobile. Parmi les plus prometteuses le **Trusted Execution Environement (TEE)** supportée notamment par Gemalto et Trustonic sur la base soit d'une solution mixte logicielle/matérielle incluant la **TrustZone** d'ARM ou bien purement logicielle dite **White-Box Crypto**, offre de réelles perspectives dans l'IoT, les Télécoms, la banque électronique... pour lutter efficacement contre la prolifération de logiciels malveillants et la fraude constatée sur les mobiles.

Objectifs :

L'objectif des travaux sera par conséquent de procéder à des attaques matérielles et logicielles sur un **TEE** pour en évaluer la sécurité. Lors d'une première phase, le candidat aura la charge de mettre en place ces attaques, de mettre à niveau les bancs EM/LASER et les méthodologies d'attaques pour répondre à la problématique TEE (circuits complexes, multi-threading, multicœurs, désynchronisation…). Dans une seconde phase, le candidat proposera des contre-mesures pour les attaques ayant réussies afin de les tester et d'arriver à des solutions parfaitement caractérisées du point de vue sécuritaire.
Ces travaux se dérouleront dans le cadre du projet TEEVA (Trusted Electronic EVAluation) développé en partenariat avec GEMALTO, TrustedTonic, le Laboratoire Hubert Curien, le LIRMM et MSE.

Lieu :

Le candidat effectuera ses travaux au Campus Georges Charpak Provence de Gardanne (CGCP), 5ème centre de recherche et formation de L'École Nationale Supérieure des Mines de Saint-Étienne (MSE) dans le département Systèmes et Architectures Sécurisés (SAS).

Durée :

10 mois
(possibilité d'extension de la durée selon l'évolution du projet TEEVA)

Compétences :

- Environnement de développement des systèmes embarqués (C / C++, Assembleur, compilateur…)
- Processeurs ARM (La connaissance de l'architecture Trustzone serait un plus)
- Attaques matérielles par LASER ou EM de type DFA, CPA…
- Notion de cryptographie
- Anglais, Capacité de rédaction, méthodologie, …

Candidature :

La candidature sera envoyée à Olivier Potin (Enseignant-Chercheur MSE) à l'adresse olivier.potin@mines-stetienne.fr. Elle comportera un CV détaillé, une lettre de motivation et des lettres de recommandation éventuelles.