2018-7185 Reconstruction de code à partir de fuites par canaux auxiliaires H/F

Informations générales

Description de l'entité	Le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) est un organisme public de recherche. Acteur majeur de la recherche, du développement et de l'innovation, le CEA intervient dans le cadre de ses quatre missions : . la défense et la sécurité . l'énergie nucléaire (fission et fusion) . la recherche technologique pour l'industrie . la recherche fondamentale (sciences de la matière et sciences de la vie). Avec ses 16000 salariés -techniciens, ingénieurs, chercheurs, et personnel en soutien à la recherche- le CEA participe à de nombreux projets de collaboration aux côtés de ses partenaires académiques et industriels.
Description de l'unité	Le Leti, institut de recherche technologique de Cea Tech, a pour mission de créer de la valeur et de l'innovation avec ses partenaires industriels. Il fait le lien entre la recherche fondamentale et la production de micro et nanotechnologies dans le but d'améliorer la qualité de vie de chacun. Fort d'un portefeuille de 2.800 brevets, le Leti façonne des solutions avancées pour améliorer la compétitivité de ses partenaires industriels: grands groupes, PME ou startups. Localisé à Grenoble (38), le Leti compte plus de 1 800 chercheurs et a des bureaux aux US et au Japon. Le LSOSP, Laboratoire sécurité des objets et des systèmes physiques, mène des activités de R&D dans le domaine des technologies de sécurité et de protection de la vie privée. Il analyse et caractérise les risques auxquels sont soumis les systèmes électroniques et les composants; il conçoit des contre-mesures s'appuyant notamment sur des techniques cryptographiques mais aussi sur des modifications dans l'architecture des systèmes pour intégrer les technologies nécessaires (composants, codes embarqués, interfaces ou protocoles de communications...). Il caractérise l'efficacité des contremesures intégrées dans des composants, des objets (communicants) et des systèmes cyberphysiques afin de résister aux attaques au niveau de leur structure, de leurs fonctions ou de leur utilisation.
Délai de traitement	2 mois

Description du poste

Site	Grenoble
Lieu	17, avenue des martyrs, 38000 GRENOBLE
Domaine	Composants et équipements électroniques
Contrat	Stage
Intitulé de l'offre	Reconstruction de code à partir de fuites par canaux auxiliaires H/F
Sujet de stage	Reconstruction de code à partir de fuites par canaux auxiliaires
Durée du contrat (en mois)	6 mois
Description de l'offre	Lorsque les processeurs effectuent des calculs, ils émettent une empreinte bien particulière à travers différents phénomènes physiques : la consommation, le rayonnement électromagnétique, le bruit acoustique, etc. Les attaques par canaux auxiliaires permettre d'extraire des informations sensibles manipulées par un processeur à partir de ces données physiques. Ces attaques visent la plupart du temps à retrouver les clés cryptographiques. Mais il a également été montré [1, 2, 3] que ces fuites permettent de reconstruire le code exécuté par un processeur simple (type microcontrôleur). L'objectif de ce stage est d'étudier la faisabilité de ces attaques sur des processeurs plus complexes (pipeline important, avec des fonctionnements prédictifs, etc.) et d'identifier les éléments d'architectures responsables des fuites (caches, décodage, ALU). Une première partie du stage consistera à mettre une ou plusieurs méthodes de l'état de l'art sur un système simple comme une carte Arduino. Pour cela, le candidat aura accès aux bancs de caractérisation électromagnétique du laboratoire. Dans un deuxième temps, ces méthodes de reconstruction seront portées vers des systèmes plus complexes : un STM32 puis éventuellement une carte Raspberry Pi. Cette deuxième partie du stage sera plus exploratoire que la première et n'aboutira pas forcément sur des attaques fonctionnelles. Il faudra alors chercher à comprendre dans quelle mesure l'architecture permet de limiter (ou non) ce type d'attaques.

	Le stage aura lieux dans le Laboratoire de Sécurité des Objets et des Systèmes Physiques (LSOSP), une équipe de chercheurs du CEA Tech Leti (www.leti-cea.fr) basé sur Grenoble (France). Le candidat y rejoindra l'équipe du projet Nanotrust qui développe un processeur sécurisé pour l'internet des objets. Références ----------
	[1] Goldack, M., & Paar, I. C. (2008). Side-channel based reverse engineering for microcontrollers. Master's thesis. [2] Eisenbarth, T., Paar, C., & Weghenkel, B. (2010). Building a side channel based disassembler. In Transactions on computational. [3] Strobel, D., Bache, F., Oswald, D., Schellenberg, F., & Paar, C. (2015). Scandalee: a side-channel-based disassembler using local electromagnetic emanations. In Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition.
Moyens / Méthodes / Logiciels	Linux, programmation bas niveau en C/C++, Python
Profil du candidat	Le candidat doit avoir quelques notions d'architecture des processeurs. Les aspects expérimentaux du stage nécessitent une certaine autonomie. Le candidat doit être à l'aise sous Linux, maitriser la programmation bas niveau en C (éventuellement C++) et avoir quelques connaissances en Python. Des connaissances de bases sur les attaques par canaux auxiliaires et en machine learning sont un plus. Merci de bien vouloir transmettre votre candidature directement à Thomas HISCOCK : thomas.hiscock@cea.fr

Critères candidat

Langues	Anglais (Courant)
Diplôme préparé	Bac+5 - Diplôme École d'ingénieurs
Formation recommandée	Master 2 ou 3ème année d'école d'ingénieur

Demandeur

Disponibilité du poste	01/02/2019