2018-7180 Conception et développement d'un outil intelligent pour les attaques par perturbation 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 Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) mène des activités dans le domaine de l'évaluation sécuritaire de systèmes électroniques, de composants de logiciels embarqués, soit dans le cadre de schémas de certification, par exemple celui piloté par l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), soit à la demande directe d'industriels.
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	Conception et développement d'un outil intelligent pour les attaques par perturbation H/F
Sujet de stage	Conception et développement d'un outil intelligent pour les attaques par perturbation
Durée du contrat (en mois)	6 mois
Description de l'offre	La cryptographie embarquée sur les cartes à puce peut être vulnérable à des attaques par perturbation qui peuvent modifier le fonctionnement d'une puce. Ainsi des erreurs de chiffrement peuvent être obtenues pendant l'exécution perturbée d'un algorithme cryptographique. L'exploitation de ces erreurs permet de remonter à la clé secrète suivant plusieurs techniques. La plus ancienne, parue en 1997 et appelée Differential Fault Analysis (DFA), tire parti des relations entre les résultats erronés et les résultats corrects. D'autres méthodes, plus récentes, utilisent des outils statistiques et/ou s'appuient sur l'analyse des sorties non erronées. L'objectif du stage est d'étudier les différentes attaques proposées par la littérature et d'analyser leur faisabilité à partir des données habituellement obtenus par le CESTI par des campagnes de tests par perturbation. Le stagiaire pourra développer un outil regroupant les méthodes les plus intéressantes et proposer si besoin d'élargir leur champ d'application. Ce développement se fera en collaboration avec l'équipe laser du CESTI afin de parvenir à un outil adapté à leurs besoins. Plusieurs algorithmes de cryptographie seront considérés et un intérêt particulier sera consacré à la recherche de nouvelles attaques.
Moyens / Méthodes / Logiciels	Cryptographie, C/C++
Profil du candidat	Vous êtes étudiant en école d'ingénieur ou en Master 2. Vous avez des connaissances en : - cryptographie, - C/C++ Merci de bien vouloir transmettre votre candidature directement à Cécile DUMAS : cecile.dumas@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