

2018-7162 Étude d'architectures de réseaux neuronaux pour les attaques par canaux auxiliaires H/F



Informations générales

Description de l'entité	<p>Le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) est un organisme public de recherche.</p> <p>Acteur majeur de la recherche, du développement et de l'innovation, le CEA intervient dans le cadre de ses quatre missions :</p> <ul style="list-style-type: none">. 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). <p>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.</p>
Description de l'unité	<p>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.</p> <p>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.</p>
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	Étude d'architectures de réseaux neuronaux pour les attaques par canaux auxiliaires H/F
Sujet de stage	Étude d'architectures de réseaux neuronaux pour les attaques par canaux auxiliaires
Durée du contrat (en mois)	6 mois
Description de l'offre	<p>La cryptographie embarquée sur les cartes à puce peut être vulnérable à des attaques par canaux auxiliaires qui consistent à analyser les signaux récupérés pendant l'exécution de l'algorithme cryptographique. Cette analyse repose sur de nombreuses méthodes, souvent basées sur des outils statistiques, et vise essentiellement à classifier les signaux selon la valeur d'une clé secrète manipulée lors de leur acquisition. De nos jours, la tâche de classification est de plus en plus réalisée à l'aide de méthodes d'apprentissage automatiques (Machine Learning en anglais) et d'apprentissage profond (Deep Learning), qui s'avèrent très efficaces dans de nombreux domaines (reconnaissance d'image, traitement automatisé du langage, vision par ordinateur, etc.). L'exploitation de ces méthodes dans le domaine des attaques sur carte à puce est un fervent (et récent) sujet de recherche, pour l'instant limitée à certains types d'analyse/attaque.</p> <p>L'objectif du stage est d'étudier et proposer des architectures d'apprentissage profond adaptées à d'autres attaques connues de la littérature, pour lesquelles aucun outil Deep Learning n'a encore été exploré. Pourtant des résultats préliminaires prometteurs ont été observés par notre équipe. Le stagiaire participera ainsi à l'enrichissement de la suite d'outils d'attaque du CESTI. Il sera d'ailleurs amené à proposer une stratégie pour tester ses avancées et les comparer avec l'état de l'art, à travers la mise en place d'un ensemble de signaux appropriés (simulés ou acquis) et/ou l'exploitation de signaux publics. Le stage pourrait aboutir sur une publication des travaux du candidat à conférences locales ou internationales.</p>
Moyens / Méthodes / Logiciels	Python / C/C++ / Keras/Tensoflow
Profil du candidat	<p>Vous êtes étudiant en 3ème année d'école d'ingénieur ou en Master 2.</p> <p>Vous avez des connaissances en :</p> <ul style="list-style-type: none">- cryptographie,

- apprentissage profond (Deep Learning),
- Python,
- C/C++.
La maîtrise d'un système d'apprentissage profond (Keras, Tensorflow en particulier) est un plus.

Merci de bien vouloir transmettre votre candidature directement à Eleonora CAGLI : eleonora.cagli@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
------------------------	------------