2018-7186 Implémentation d'un protocole de tunnel léger avec de la cryptographie asymétrique 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	Implémentation d'un protocole de tunnel léger avec de la cryptographie asymétrique H/F
Sujet de stage	Implémentation d'un protocole de tunnel léger avec de la cryptographie asymétrique pour l'IoT
Durée du contrat (en mois)	6 mois
Description de l'offre	Dans le cadre du Programme Usage des technologies de Liaison et Soutien aux Entreprises (PULSE) de l'IRT Nanoelec, le LSOSP a développé un prototype de tunnel cryptographique léger dans le but de permettre la sécurité des communications de l'IoT quel que soit le protocole utilisé. Cette première version du prototype était basée sur de la cryptographie symétrique. Dans l'exécution de sa mission, le stagiaire devra : 1. réaliser un état de l'art, dans une permiere partie, sur les tunnels cryptographiques et plus particulièrement les versions de tunnels légers. Dans une deuxième partie, l'état de l'art s'intéressera notamment aux algorithmes de chiffrement légers (ex : Trivium, Chacha...) en mettant en perspective leurs propriétés cryptographiqes (clés, IV, attaques...) et leurs apports au niveau de l'implémentation (consommation, débit...), 2. qualifier l'architecture actuelle vis à vis de l'état de l'art, 3. enrichir le tunnel léger actuel avec des nouveaux protocoles d'authentification en utilisant de la cryptographie asymétrique, 4. mettre en place des moyens de caractérisation de la performance du tunnel léger (benchmark). L'implémentation de ce prototype pourra ensuite être portée sur différentes cibles matérielles (composants électroniques sécurisés ou non), ainsi que sur des protocoles de communication variés pour en faire la démonstration.

Profil du candidat	Le stagiaire fera partie intégrante de l'équipe programme PULSE. A ce titre, il sera placé sous le tutorat de Christophe VILLEMAZET. Etudiant en troisième année d'école d'ingénieur ou deuxième année de master Le stagiaire devra posséder des compétences en sécurité, programmation et logiciels embarqués. Il devra faire preuve d'ouverture d'esprit, d'autonomie et d'initiative en étant force de propositions. Il intégrera une équipe d'ingénieurs pluridisciplinaires (environ 33 personnes). Merci de bien vouloir transmettre votre candidature directement à Christophe VILLEMAZET : christophe.villemazet@cea.fr

Critères candidat

Langues	Anglais (Intermédiaire)
Diplôme préparé	Bac+5 - Diplôme École d'ingénieurs
Formation recommandée	Etudiant en 3ème année d'école d'ingénieur ou 2ème année de master

Demandeur

Disponibilité du poste	01/02/2019