Titre : « Platforme de sécurité légère pour l'Internet des objets »

L'émergence de l'Internet des Objets (IoT- *Internet of Things*) comme nouveau paradigme mène vers une vie de plus en plus connectée. Des milliers d'appareils, de personnes et, éventuellement, de services devraient être interconnectés et seraient amener à échangés de données et d'informations utiles. Bien que ce nouveau paradigme continue à créer de nouvelles opportunités, l'IoT présente également des défis fondamentaux liés à la sécurité, à la confidentialité et le respect de la vie privée. Pour établir des connexions sécurisées entre des personnes, des objets et des services, la sécurité doit être omniprésente. La sécurité physique et la cybersécurité doivent travailler en collaboration pour protéger les réseaux, les applications, les appareils, les données et les utilisateurs, qui sont les éléments essentiels de l'IoT. A cause de l'augmentation du nombre d'appareils connectés, l'émergence du « *Big Data »* et de l'automatisation, les données exploités par les systèmes d'information doivent être traitées de manière aussi sécurisée que possible.

Dans ce contexte, ce stage de fin d'étude portera sur l'analyse de la sécurité dans le domaine de l'IoT dont le but est de fournir une vue d'ensemble sur les concepts, les techniques, les applications, ainsi que les principaux axes de recherche dans ce domaine. En effet, la gestion et le déploiement des politiques de contrôle d'accès (*Access Control Policies*) se reposent sur des architectures standardisées et fiables. Néanmoins, ces architectures peinent encore et présentent des limitations pour la prise en charge de l'évolution et le changement éventuel du contexte dans la gestion du contrôle d'accès. Le contrôle d'accès selon le contexte (*Context-sensitive Access Control*) permet de prendre des décisions concernant les permissions d'accès en prenant en considération des changements d'états liés à l'environnement de l'utilisateur ou à de l'objet physique (lieu, situation, niveau de confiance ou réputation des entités environnantes, etc.). Par conséquent, l'objectif principal de ce travail est de développer un *proof-of-concept* pour un schéma de sécurité allégée, mettant en œuvre un protocole pour le contrôle d'accès en se basant sur le concept de clés numérique *(Tokens* en anglais*)*.

Après une analyse de l'état de l'art qui portera sur les aspects de sécurité, de confidentialité et le respect de la vie privée liés à l'écosystème de l'Internet des objets, le stagiaire travaillerait sur les aspects suivants :

• Analyse des risques et de vulnérabilités liés à un scénario spécifique (serrure connectée dans un *Smart Hotel*, *Smart Home*, etc.).

• Conception d'un schéma/architecture pour le contrôle d'accès basé sur le contexte avec des stratégies de sécurité spécifiques afin de fournir des clés numériques pour donner/retirer l'accès aux ressources numériques/physiques dans le cadre de l'Internet des objets (IoT).

• Implémentation d'un scénario de démonstration utilisant une application de téléphone Android pour accéder en toute sécurité à un périphérique IoT intelligent (verrou intelligent ouvert, récupération d'informations sensibles, etc.).

Mots-clés : Internet des objets, sécurité des réseaux informatique, protection de la vie privée, contrôle d'accès, Infrastructure à clé publique (PKI).

Encadrants : Prof. Sidi Mohammed Senouci et Dr. Ayoub MESSOUS, Université de Bourgogne, Nevers

Date de début : Début 2019.

Durée : 5 à 6 mois

Lieu du stage : Laboratoire DRIVE à Nevers, Université de Bourgogne, France.

Profil recherché : Une formation initiale requise de niveau BAC+5 (dernière année d'études d'ingénieur ou de master 2) en informatique ou en télécommunications, avec de bonnes connaissances en mathématiques et une connaissance approfondie de la sécurité des réseaux, ainsi que des compétences pratiques en programmation et en développement (Java, Android, Arduino). Avant tout, le candidat doit être dynamique, doté de compétences en communication et en travail d'équipe, motivé pour apprendre rapidement et travailler efficacement sur des problèmes de recherche.

Processus de sélection : Les candidats potentiels sont priés d'envoyer leur CV et leurs derniers relevés de notes (éventuellement des lettres de recommandation) à :

Prof. sidi-mohammed.senouci@u-bourgogne.fr

Dr. ayoub.messous@u-bourgogne.fr