4.10. SEROIF_

Titre du projet : Sécurisation des réseaux d'objets interconnectés et de l'information pour l'industrie du futur

Porteur du projet : Sébastien PILLEMENT
Etablissement : Université de Nantes, Polytech Nantes
Laboratoire : IETR (UMR 6064) équipe SysCom
Partenaires :

Université de Nantes IETR Lab	Méndez Real	Maria
Polytechnique Montréal	Langlois	Pierre
Polytechnique Montréal	Nicolescu	Gabriela

Mots clés : IoT industriel, sécurité, cloud

Verrous scientifiques ou technologiques : Amélioration de la sécurité des communications dans le cadre de l'internet des objets. Sécurisation de bout en bout des éléments de la chaîne (du capteur au serveur).

Etat : Début en novembre 2019, fin prévue actuellement en Décembre 2021.

Nature des mobilités : Compte tenu de la crise sanitaire de la COVID 19 les collaborations n'ont pas pu démarrer sur ce projet. Une première visite des collègues Canadiens était prévue en juin 2020, mais a été annulée.

Impact de la collaboration internationale : Cf ci-dessus

4.10.1. Résumé du projet :

Dans le cadre de l'industrie du futur, il faudra garantir la disponibilité des informations au sein du système complet (i.e. des capteurs aux serveurs de calcul). L'objectif général du projet est de proposer de nouvelles approches pour sécuriser les réseaux d'objets interconnectés contre les attaques de déni de service visant l'interruption du service ou même les pannes de batterie des objets. Ces attaques sont aujourd'hui particulièrement importantes et posent des problèmes autour de l'authentification des objets et des requêtes. Trois objectifs scientifiques sont identifiés : 1. Analyser les similarités et différences des contraintes de sécurité des réseaux d'objets interconnectés et des réseaux informatiques traditionnels. 2. Mettre en place des modèles d'attaques de déni de service pour les réseaux d'objets interconnectés. 3. Proposer de nouvelles solutions pour assurer la disponibilité des réseaux d'objets interconnectés et des centres de calcul incluant à la fois des solutions d'authentification des objets et requêtes ainsi que de gestion du flot de communication pour la détection de patrons de messages et de requêtes potentiellement malicieux.

Le premier résultat attendu du projet est la mise en place d'une collaboration à long terme par la mise en réseau de nos laboratoires de Polytechnique Montréal et de l'IETR Nantes. Cette collaboration sera lancée par le biais de semaines de travail conjointes à Nantes et à Montréal lors du déplacement des équipes (cinq périodes d'une semaine au total sur deux ans). Nous organiserons des séminaires scientifiques entre nos deux laboratoires.

Sur le plan scientifique, des modèles d'attaques et des solutions de sécurité seront développés. L'idée principale du projet vise à considérer l'ensemble de la chaîne IoT (du capteur au centre de calcul) pour proposer différentes stratégies globales de sécurisation des données.

4.10.2. Résultats scientifiques du projet :

4.10.2.1. Résumé

4.10.2.2. Les publications réalisées :

4.10.2.3. Dissémination :

4.10.2.4. Equipement et ressourcement