Postdoctoral project: IoT Traffic Generation Platform

Contact : Gregory Blanc, Département RST (gregory.blanc@telecom-sudparis.eu)

Objet : Proposition de sujet postdoctoral

Cadre : CEF VARIoT

Durée : 24 mois

Motivation :

Le projet VARIoT (2018-EU-IA-0100) répond à un appel CEF Telecom sur la plateformes publiques de données ouvertes (Public Open Data). En particulier, les partenaires s'attaquent au problème particulier de la collection et du partage de données sur la cybersécurité de l'Internet des Objets (IoT). L'objectif principal de VARIoT est de créer un service permettant de fournir des données directement exploitables (manuellement et automatiquement) afin d'assurer la sécurité de l'Internet des Objets. Ces données seront mises à disposition du public sur le portail EDP (European Data Portal) ainsi que sur d'autres plateformes telles MISP (Malware Information Sharing Platform). Les résultats du projet incluent, entre autres : une base de données des vulnérabilités des objets connectés et leurs exploits, une base de jeu de données de trafic réseau d'objets connectés (à la fois légitime et malveillant), une base de modèles de détection de trafic d'objets connectés, des outils de supervision et de collection de données réseau des objets connectés, des interfaces de partage.

La contribution de Télécom SudParis se concentre sur l'Activité 4 que nous pilotons. L'objectif de cette activité est de créer une base de jeux de données concernant le trafic des objets connectés, dans leur fonctionnement nominal, ainsi qu'une fois compromis. Les jeux de données de trafic à proprement parler seront générés sur une plateforme hébergé à Télécom SudParis. Cette plateforme intègre de nombreux objets connectés et sont manipulés par le personnel de Télécom SudParis dans des cas d'usage naturels (maison connectée) afin de générer des données réalistes. Les données d'objets compromis seront générées par la compromission de ces objets et leur observation dans un environnement virtualisé et isolé. La collection de ces données permettront aussi leur analyse afin de générer des modèles comportementaux de trafic légitimet et malveillant.

Travaux proposés :

Les travaux tournent autour de la mise en place et la maintenance d'un environnement de génération et de collecte de trafic réseau des objets connectés, ainsi que le formatage, le stockage, la sécurisation et la présentation de ces données:

- déploiement et développement d'une plateforme d'objets connectés
- mise en place d'un framework de génération et de collection de trafic
- déploiement et développement d'une plateforme de collection et de stockage sécurisé des données de trafic, et d'analyse et d'apprentissage des comportements
- déploiement et développement d'une plateforme sécurisée de génération de trafic d'objets compromis

Profil recherché :

Candidat(e) doit avoir un doctorat en informatique et une expérience dans l'un des domaines suivants: sécurité réseau, IoT, programmabilité des réseaux (SDN, NFV, etc.), analyse de logiciels malveillants. Des compétences en administration systèmes et réseau sont aussi souhaitables.