Embarcabilité des mécanismes de détection dans des objets connectés

Mars 2023

1 Introduction

Dans le cadre du PEPR Cybersécurité, et plus spécifiquement dans le contexte du projet Superviz, qui se focalise sur la Supervisation et l'Orchestration de la Sécurité, le LAAS-CNRS et l'institut Eurecom proposent un sujet de post-doctorat visant à concevoir et implémenter des mécanismes innovants de détection d'intrusions embarqués dans des objets connectés.

2 Contexte

La diversité et le nombre des protocoles de communication sans fils présents dans l'IoT rendent leur surveillance très difficile. Comme pour n'importe quelle communication sans fils, les attaques sont relativement faciles à perpétrer car elles ne nécessitent aucune connexion à un point spécifique du réseau (à l'inverse des réseaux filaires), il suffit pour l'attaquant d'être à portée radio. La surveillance des réseaux IoT via des sondes pose le problème du déploiement pour couvrir tout le réseau, notamment dans un environnement professionnel (type usine connectée du futur) qui peut être très étendu. Par conséquent, compléter la surveillance par des mécanismes de détection sur les objets eux-mêmes semble une piste intéressante. Cependant, il faut considérer que les objets ont souvent des ressources limitées (puissance de traitement, énergie), il faut donc des mécanismes légers adaptés.

3 Objectifs

Il s'agira ici de proposer des mécanismes de détection d'intrusion légers qui puissent être embarqués sur le contrôleur radio des objets eux-mêmes. Des travaux dans ce cadre ont démarré au LAAS-CNRS et des mécanismes embarqués dans les contrôleurs BLE ont été développés. Il s'agit ici de poursuivre ce travail dans le cadre d'un post-doc, de façon à généraliser cette approche.

4 Approche envisagée

Les mécanismes de détection qui ont été mis en œuvre dans le cadre du BLE détectent les principales attaques connues de nos jours. Leur intégration est d'autant plus efficace qu'il est possible de tirer profit des informations des couches basses du protocole. Seules les primitives de réception et d'émission nativement intégrées dans le firmware du contrôleur radio des objets ont été modifiées pour remonter des métriques essentielles à la détection des attaques. Dans cette proposition de post-doc, nous souhaitons poursuivre ces travaux sous plusieurs angles :

- en automatisant autant que possible l'insertion de ces mécanismes dans le firmware des objets,
- en étudiant la possibilité d'intégrer les mécanismes de détection à la fois dans le contrôleur mais aussi dans la partie système d'exploitation de l'objet quand cela est possible (approche hybride),
- en les étendant à d'autres protocoles de l'IoT.

Une autre piste intéressante pour ce post-doc consiste à imaginer comment il est possible d'implanter une supervision distribuée de réseaux IoT à l'aide de ces mécanismes de détection locaux sur les objets et de mécanismes supplémentaires de corrélation d'alertes entre les objets. Il s'agit ici de déterminer à la fois les moyens de communication permettant aux détecteurs locaux de communiquer entre eux et/ou avec une entité centrale, et de concevoir les mécanismes de corrélation adaptés à ce type d'environnement.

Pour tester ces mécanismes, on pourra avantageusement tirer profit de l'outil Mirage1, développé au LAAS, qui permet de réaliser de l'audit de protocoles de communication des réseaux IoT.

5 Contact

Guillaume Auriol guillaume.auriol@laas.fr;

Vincent Nicomette vincent.nicomette@laas.fr;

Romain Cayre romain.cayre@eurecom.fr;

Aurelien Francillon aurelien.francillon@eurecom.fr