Évaluation de la sécurité des objets connectés dans l'Internet des Objets

Rémi GASCOU
INSA Toulouse - FRANCE
gascou@etud.insa-toulouse.fr
remi@gascou.net

Jérôme Kompé Miarivelo MAMPIANINAZAKASON
INSA Toulouse - FRANCE
mampiani@etud.insa-toulouse.fr
jerome.kompe@gmail.com

Abstract

Un des enjeux majeurs de l'Internet des Objets (IdO) est aujourd'hui la sécurisation des appareils. Il est essentiel d'être capable de détecter si un objet connecté est compromis ou attaqué. Dans le projet étudiant de M1 décrit dans cet article, nous proposons une méthode originale permettant de détecter les attaques ou les compromissions d'un objet connecté. Cette méthode consiste en la création d'un dispositif d'audit, équipé de capteurs divers, qui permet de collecter des données qui sont ensuite utilisées en entrée d'un Système de Détection d'Intrusion (SDI). Deux pistes sont envisagées pour la détection d'intrusion, l'une basée sur des heuristiques l'autre basée sur des algorithmes de machine learning de détection d'anomalies. Nous testons notre SDI basé à la fois sur des mesures physiques et sur des analyses du réseau, sur un objet connecté incluant des vulnérabilités courantes dans l'IdO.

1 Contexte

De nombreux objets connectés voient le jour et sont massivement utilisés dans notre vie professionnelle et personnelle. Le développement de ces objets se fait de façon très rapide et intègre des fonctionnalités de plus en plus variées (on trouve aujourd'hui des réfrigérateurs connectés, des brosses à dents connectées, etc ...), au détriment de leur sécurité. Les problématiques de sécurité sont en effet très souvent ignorées ou reléguées au second plan. Ces lacunes s'expliquent par deux facteurs : le manque de formation en sécurité des développeurs et des concepteurs, et les politiques de réduction des coûts. Afin d'améliorer la sécurité de ces objets, il est donc nécessaire de prendre en compte cet aspect dès leur phase de conception mais aussi d'avoir accès à des dispositifs d'audit capable de détecter des modifications de l'environnement physique ou réseau pouvant résulter d'une attaque visant l'appareil à analyser.

C'est à cette seconde problématique que notre projet étudiant de M1 se consacre. Dans ce projet, nous proposons de développer un dispositif original non-intrusif de détection basé sur des heuristiques et sur de la détection d'anomalies grâce à des algorithmes de machine learning. Ce dispositif se base sur la collecte d'informations physiques (lumière, chaleur, son, etc) et la collecte de traces de communication réseaux impliquant l'objet.

Nous avons réalisé un état de l'art sur les attaques et les vulnérabilités couramment rencontrées dans l'Internet des Objets [1] ainsi qu'un état de l'art sur les Systèmes de Détection d'Intrusion pouvant être utilisés pour détecter de telles attaques. [2].

Dans ce projet, nous considérerons tous les comportements non prévus dans le comportement de l'objet comme des attaques. Dans la suite de cet article, nous présentons les réalisations faites jusqu'à présent dans ce projet : la conception et la réalisation d'un objet connecté vulnérable (section 2.1) ainsi que le dispositif d'audit (section 2.2).

2 Réalisation

2.1 Développement d'un objet connecté vulnérable

Afin de tester notre méthode de détection dans des cas proches de la réalité, nous avons conçu une serrure connectée en utilisant une Rasbperry Pi 3 B+.

2.1.1 Fonctionnalités

La serrure connectée peut être contrôlée à partir d'un téléphone portable afin d'effectuer des actions basiques comme verrouiller et déverrouiller la porte. Suite à nos recherches sur les vulnérabilités couramment exploitées dans les objets connectés, nous avons implémenté dans notre appareil une API conforme à l'architecture REST pour contrôler la serrure. Les utilisateurs peuvent ainsi, à l'aide d'une requête HTTP, verrouiller et déverrouiller la porte, réinitialiser l'appareil, mais aussi activer le mode debug qui exécute un serveur telnet.

2.1.2 Vulnérabilités

Pour commencer, nous nous sommes basés sur la faille la plus basique et rendue célèbre par le botnet Mirai [3] : les identifiants par défaut.

Ensuite, nous avons profité de l'architecture REST, et de son transfert de données non chiffrées, basé sur le protocole HTTP. Cela, permet aux attaquants d'intercepter des données sur le réseau (identifiant, jeton de connexion, etc.), ou également de rejouer les paquets.

Un attaquant connaissant le modèle de notre serrure pourrait en activer le mode débug pour lancer le service telnet afin de l'attaquer par force brute.

Ces appareils sont aussi vulnérables à des attaques de type Man-in-the-middle (MiTM), dans laquelle l'attaquant peut intercepter les communications entre l'utilisateur légitime et l'objet. Il pourrait ainsi les modifier, les lire ou simplement ne pas relayer les requêtes.

Pour terminer, la majeure partie des appareils connectés sont sensibles au déni de service. De telles attaques peuvent prendre plusieurs formes, par exemple les attaques de SYN ou ICMP flooding, afin de saturer toutes les ressources de l'appareil par l'envoi de requêtes massives, ou encore les requêtes de déconnexion au point d'accès Wifi, afin que l'appareil soit déconnecté du réseau.

2.1.3 Scénarios

Les scénarios suivants décrivent un cas d'utilisation normal (légitime), et un cas anormal (attaque).

Un scénario légitime - Utilisation courante : L'utilisateur ouvre la porte à 7h00 le matin et la referme à 7h01. Il part au travail, et à son retour, il ouvre à nouveau la porte à 18h30, et la referme à 18h31.

Un scénario d'attaque - SYN flooding : L'attaquant accède au réseau Wifi de la victime, en utilisant par exemple la faille Key Reinstallation Attacks (KRACK), et réalise une découverte réseau pour trouver l'adresse de la serrure connectée. Lorsque l'utilisateur légitime ouvre la porte l'attaquant lance une attaque de déni de service (DoS) par SYN flooding contre la serrure. L'utilisateur légitime ne peut donc plus entrer chez lui car la serrure est inaccessible.

2.2 Dispositif de détection

Le but principal de notre projet est de créer un Système de Détection d'Intrusions (SDI) capable de détecter les attaques les plus courantes visant les objets connectés ou leurs conséquences.

2.2.1 Mesures Physiques et Réseau

Dans notre SDI, nous utilisons à la fois des mesures physiques et des mesures du trafic réseau. Sur le plan des mesures physiques, nous utilisons un capteur de température infrarouge, une caméra, un capteur de lumière et un microphone. Sur le plan de l'analyse réseau, nous enregistrons différents paramètres sur le trafic, tels que le type et le nombre de paquets reçus et émis.

2.2.2 Heuristique

Une méthode simple de détection se basant sur une heuristique fonctionne très bien sur des attaques simples telles que le Dénis de Service Distribué (DDoS). Au niveau physique, nous pouvons nous attendre à une augmentation de la température du contrôleur de la carte réseau. Au niveau du réseau, nous pouvons nous attendre à un trafic très élevé en direction de l'objet. Dans le cas d'une attaque `SYN`-storm ou `ACK`-storm par exemple, une heuristique simple consisterait à compter le nombre de paquets entrant et le comparer à une valeur seuil de comportement normal. Ces heuristiques sont très efficaces pour détecter des attaques simples et bruyantes, mais perdent en efficacité face à des attaques plus complexes et discrètes.

2.2.3 Machine Learning - Détection d'anomalies

Afin de détecter des comportements plus complexes, nous utilisons des algorithmes de machine learning axés sur la détection d'anomalies. Ce travail est actuellement en cours et nous pouvons simplement donner ici les pistes sur lesquelles nous travaillons. Nous étudions actuellement les algorithmes de type "one-class classifier" (en particulier One-class SVM), dans lesquels le classifieur est entraîné avec des traces correspondant uniquement à des données légitimes. En phase de test, il peut ensuite identifier des comportements comme anormaux (scénario d'attaque) comme étant des déviations des comportements légitimes appris lors de la phase d'apprentissage.

3 Conclusion

Pour ce projet nous avons développé un Système de détection d'intrusions ainsi qu'un objet connecté vulnérable similaire aux produits du marché.

Après avoir testé des scénarios légitimes et d'attaque sur notre dispositif, nous étudions désormais les algorithmes de machine learning afin d'intégrer les plus efficaces dans notre contexte à notre système de détection d'intrusion.

Références

[1] J. K. M. MAMPIANINAZAKASON and al, "Internet of things security, a state of the art," January 2019. [Online]. Available : https://remigascou.github.io/uploads/2019/seciot/IoT_attacks_a_State_of_the_Art.pdf

[2] R. GASCOU and al, "Security assessment of connected objects in the internet of things," January 2019. [Online]. Available : https://remigascou.github.io/uploads/2019/seciot/Security_assessment_in_the_IoT_a_State_of_the_art.pdf

[3] M. Antonakaki, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *USENIX Security Symposium*, 2017. [Online]. Available : https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf