Audit d'un système IoT par test d'intrusion

Jonathan Tournier
CITI-Lab, INSA-Lyon
F-69621 Villeurbanne, France
AlgoSecure
57 bd Marius Vivier Merle, Lyon
jonathan.tournier@algosecure.fr

François Lesueur,
Frédéric Le Mouël
CITI-Lab, INSA-Lyon
F-69621 Villeurbanne, France
{prénom}.{nom}@insa-lyon.fr

Laurent Guyon,
Hicham Ben-Hassine
AlgoSecure
57 bd Marius Vivier Merle, Lyon
{prénom}.{nom}@algosecure.fr

***Résumé*—L'explosion du secteur de l'Internet des Objets, reposant majoritairement sur des technologies de communication sans fil, soulève de nombreuses problématiques de sécurité. Ceci est notamment dû à leur caractère hétérogène, à leurs réseaux peu cloisonnés et une mise sur le marché hâtive. Nous proposons dans le cadre de cette thèse une méthode permettant d'évaluer la sécurité d'un système d'objets connectés utilisant des modes de communication sans fil, ceci afin de renforcer la sécurité du système d'information dans son ensemble. Notre méthodologie se base sur une approche éprouvée dans l'IT classique : le test d'intrusion.**

I. Introduction

L'Internet des Objets (*Internet of Things* - IoT) consiste en une interconnexion de plusieurs milliers d'objets entre eux. Ceux-ci peuvent être des capteurs ou tout autre objet ayant la capacité de se connecter, d'interagir et d'échanger de l'information dans leur environnement. Le nombre d'objets connectés ne cesse d'augmenter pour atteindre en 2017 plusieurs milliards d'objets [1].

L'IoT est employé dans de nombreux domaines comme celui de la santé, de l'industrie ou encore de la domotique. Aussi, pour profiter pleinement des fonctionnalités de leurs objets, les utilisateurs n'hésitent pas à renseigner des données personnelles et critiques. Cependant, la forte croissance de l'IoT associée à la forte concurrence du domaine implique un développement rapide et une mise sur le marché parfois précoce, reléguant souvent la sécurité au second plan. Par conséquent, une compromission de ces objets peut entraîner une fuite de données critiques voire une atteinte directe à la vie des utilisateurs, comme par exemple le cas des pacemaker Abbott [2]. Ces objets compromis ayant accès à Internet peuvent également servir à d'autres attaques de plus grande ampleur telles que le botnet Mirai [1].

L'objectif de cette thèse est double :

— proposer une méthodologie pour évaluer la sécurité d'un système IoT ;
— renforcer la sécurité des systèmes d'information (SI) accueillant de l'IoT.

L'évaluation, par la mise en évidence des problèmes liés à l'IoT, permet de définir des solutions pour limiter les impacts sur le système d'information.

1. http://www.gartner.com/newsroom/id/3598917
2. https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

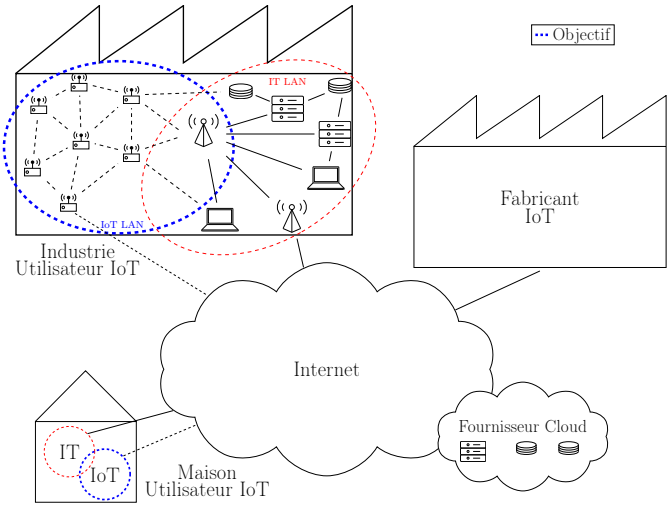

Figure 1. Écosystème IoT.

Parmi les solutions d'évaluation et d'amélioration de la sécurité d'un réseau classique, le test d'intrusion est basé sur l'analyse offensive afin d'éprouver la sécurité d'un système complexe en exécutant une attaque réelle [2] dans un contexte maîtrisé. Cependant, le test d'intrusion dans sa forme conventionnelle n'est pas adapté aux contraintes et exigences de l'IoT. En effet, la différence de ressources entre les objets, l'hétérogénéité des systèmes, l'échelle du réseau, les topologies rencontrées ainsi que l'arrivée de nouveaux protocoles soulèvent de nouveaux problèmes et nécessitent une modification des techniques actuelles pour les résoudre.

Cet article est structuré comme suit. Dans la section 2, nous exposons notre vision de l'IoT. La section 3 résume notre démarche visant à adapter la méthodologie de test d'intrusion classique IT à un environnement IoT. Les section 4 et 5 notre approche sur deux étapes de la méthodologie. La section 6 conclut l'article et en évoque les travaux futurs.

II. Notre vision de l'IoT

Nous définissons l'IoT comme un système complexe, composé d'objets connectés entre eux, et interconnectés avec le réseau des technologies de l'information (IT) de chaque acteur-utilisateur, soit directement soit par le biais d'Internet (Figure 1). Ces objets peuvent communiquer avec différents

acteurs externes au travers des réseaux IT auxquels ils sont connectés. Le SI est ainsi composé d'une combinaison d'éléments IT et IoT.

Ainsi, la compromission d'un seul de ces objets pose non seulement des risques sur le système IoT en lui-même, mais aussi sur le système IT auquel il est relié. Ceci est dû en grande partie à une gestion souvent permissive du cloisonnement entre ces deux systèmes. De plus, l'interconnexion de ces objets à Internet (soit directement soit au travers du réseau IT classique) augmente la zone d'impact d'une compromission. Il est en effet possible depuis un tel objet compromis d'attaquer des acteurs externes [1].

Un attaque ciblée contre le réseau IT peut également utiliser le réseau IoT qui lui est connecté comme pivot afin de lancer une attaque vers d'autres acteurs.

III. Notre approche de test d'intrusion pour l'IoT

Il existe deux types de test d'intrusion [2] (aussi appelé *pentest*) qui se différencient par le niveau d'information connu au démarrage : les *pentests* dits "boîte noire" pour lesquels aucune information préalable n'est connue et les *pentest* dits "boîte blanche" durant lesquels l'équipe d'audit dispose de toutes les informations nécessaires (comptes utilisateurs, documents d'architecture). Nous nous attachons dans ce travail à la version dite "boite noire".

Un test d'intrusion conventionnel suit une méthodologie classiquement définie en plusieurs étapes[3] : collecte d'information, modèle de menace, analyse des vulnérabilités, exploitation, post-exploitation et enfin restitution des résultats. Cependant, à notre connaissance, il n'existe aucune mise en oeuvre spécifique de cette méthodologie pour la réalisation de tests d'intrusion sur des systèmes d'objets connectés. C'est pourquoi nous proposons une adaptation de certaines étapes de la méthodologie standard pour répondre aux spécificités des environnements IoT.

Dans cet article, nous traitons les étapes de collecte d'information et d'analyse de vulnérabilités de la méthodologie. En effet, nous pensons que les autres étapes sont sensiblement similaires à celles d'un *pentest* IT classique, où seulement quelques adaptations d'outils semblent nécessaires pour être utilisés dans un environnement IoT. Donc, les sections suivantes présentent les deux étapes, avec l'approche telle que décrite pour le cas d'un test d'intrusion classique, puis notre approche afin d'adapter la solution pour qu'elle puisse convenir à un environnement constitué d'objets connectés.

IV. Collecte d'information

Dans le contexte d'un test d'intrusion conventionnel, cette étape est dédiée au recueil des informations nécessaires à l'évaluation de la surface d'attaque potentielle.

Dans notre contexte, elle consiste plutôt à identifier les propriétés de communication du réseau IoT. Elles ont principalement trait à la topologie du réseau, au protocole de communication permettant l'échange de données, et aux différents types d'objets déployés dans le réseau. Ainsi, nous

3. http://www.pentest-standard.org/index.php/Main_Page

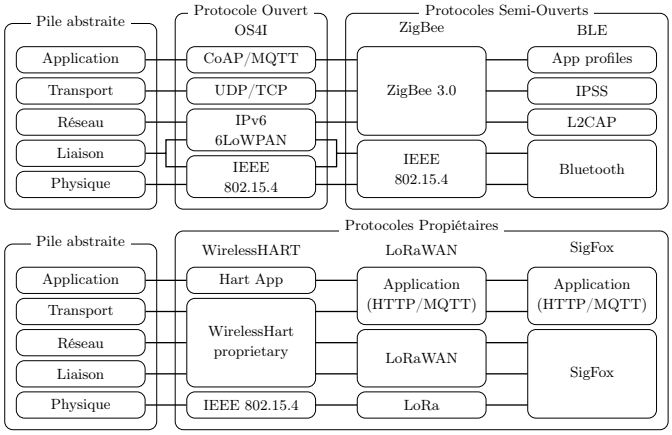

FIGURE 2. Comparaison des protocoles IoT.

avons divisé en deux parties cette étape avec dans un premier temps une analyse des réseaux IoT et dans un second temps la modélisation de ces derniers.

A. Réseaux IoT

La première approche consiste à déterminer l'environnement dans lequel l'audit se déroule par découverte de la topologie déployée et du protocole utilisé.

Topologies: Les topologies existantes se regroupent en 4 catégories : étoile, arbre, mesh (P2P) et cellulaire.

Protocoles: Les protocoles IoT permettent aux objets de pouvoir communiquer entre eux et ainsi d'échanger des données. Il est donc important de comprendre leur fonctionnement au travers d'une étude comparative. Nous avons fait le choix d'étudier les protocoles suivants et représentés en Figure 2 : ZigBee, Z-Wave, BLE, WirelessHart, une pile ouverte OS4I, LoRaWAN et SigFox. Afin de pouvoir les comparer entre eux, nous avons défini un modèle générique sur lequel nous les avons tous reportés. Notre comparaison s'appuie sur 5 critères : la portée, l'ouverture, l'intéropérabilité, les topologies supportées et les pratiques de sécurité appliquées des protocoles.

B. Modélisation du réseau

La modélisation du réseau IoT est une phase essentielle permettant d'obtenir une représentation intermédiaire dans laquelle il est possible d'avoir des informations sur les noeuds ou les liens entre les noeuds par requêtes dans le modèle. Cette représentation intermédiaire facilite la définition de la surface d'attaque et l'identification des menaces potentielles indépendamment du protocole utilisé. Ce modèle se construit par écoute passive du système IoT, en deux étapes : classification des objets et modélisation automatique.

Classification: Dans [3], les auteurs énumèrent les différentes manières d'identifier des objets, par caractéristiques spécifiques aux matériels ou décalages d'horloges. Ils proposent également leur propre modèle d'identification de type combinant la marque, le modèle et la version logicielle de chaque objet. Bien que ces informations soient utiles lors

d'un test d'intrusion, nous avons besoin d'une approche plus générique du type de l'objet. Dans [4], les auteurs proposent une classification des objets en fonction du trafic généré selon 3 types de *frames* : contrôle, gestion ou donnée. Cette classification est trop générique pour nos besoins et repose uniquement sur le type et la quantité de trafic généré sur un ensemble d'objets déjà connus, ce qui la rend inefficace lors de la découverte de nouveaux objets dans le réseau. Notre approche définit des modèles abstraits pour chaque type d'objet en les classifiant selon leur fonction comme par exemple des capteurs, des actionneurs, des antennes, etc. Les caractéristiques principales de chaque modèle abstrait sont le trafic généré, sa provenance, sa destination et la fréquence d'émission.

Modélisation: La modélisation intervient après la classification de l'intégralité des objets du réseau. Elle consiste à relier les différents objets selon le trafic observé. Représentée graphiquement, une telle modélisation simplifie la visualisation de la surface d'attaque et met en évidence les menaces potentielles présentes dans le réseau. La modélisation du réseau permet enfin l'élaboration des scénarios d'attaques.

V. Analyse de vulnérabilités

Cette étape consiste à tester le système, que soit ses composants, ses applications ou ses ressources, afin d'y découvrir des failles qu'un attaquant pourrait exploiter.

L'analyse du modèle résultant de l'étape précédente permet de définir la surface d'attaque et d'identifier les différentes menaces potentielles pesant sur le système. Par nature les objets connectés sont sensibles à une surface d'attaque très importante [4] et cette dernière couvre aussi bien les attaques physiques que logicielles. Aussi, Notre approche ne réside pas dans la recherche de nouvelles vulnérabilités, mais plutôt dans l'exploitation de celles déjà connues.

Les objets connectés ont des vulnérabilités qui utilisent les mêmes mécanismes que celles présentes dans l'IT, qu'elles soient physiques (*side channel attacks*), ou logicielles (*buffer overflows*). Nous décidons de nous concentrer uniquement sur les vulnérabilités spécifiques à l'IoT basées sur les protocoles et les communications entre objets.

Nous avons choisi de classifier les vulnérabilités en deux groupes : les attaques contre les protocoles et messages, et les attaques contre la topologie. Tout comme dans le test d'intrusion conventionnel, ces vulnérabilités peuvent impacter la C onfidentialité, l'I ntégrité et la D isponibilité.

Protocoles et messages: Le caractère sans fil des réseaux IoT facilite les attaques sur le protocole et les messages. Nous en distinguons deux types : les attaques passives qui visent à compromettre la confidentialité des messages et les attaques actives qui consistent à manipuler le trafic pour injecter, altérer ou supprimer des données [5], [6]. Les attaques passives se concentrent uniquement sur de l'analyse de trafic au préalable capturé de façon non invasive pour le système. Ainsi, le niveau de protection, et par inversement la facilité d'exploitation, repose uniquement sur la qualité du chiffrement utilisé. Les attaques actives, quant à elles, peuvent porter atteintes aux trois critères en fonction de l'attaque effectuée comme par exemple : *same-nonce* C, *replay* I, *malleability* I et *MiTM* CI. L'impact de ces attaques dépend du type et de la position des objets compromis.

Topologie: Nous séparons les moyens d'altérer la topologie et les conséquences de cette dernière, c'est-à-dire les attaques qu'il est possible de réaliser une fois la topologie maîtrisée. Ainsi, dans le premier cas, les attaques telles que *sinkhole*, *spoffing* et *sybil* permettent à un attaquant de d'altérer l'architecture du réseau en lui-même. L'objectif est de contrôler une sous partie du réseau via un objet compromis [7], [8], ce qui altère l'intégrité de l'architecture réseau. Dès lors que la topologie est maîtrisée, d'autres attaques sont alors possibles telles que : *blackhole* D, *selective forwarding* D, *eavesdropping* C ou bien injections I. L'impact de ces attaques dépend fortement de la portée de l'altération du réseau.

VI. Discussion et travaux futurs

Dans cet article, nous proposons une méthodologie de test d'intrusion des systèmes IoT issue de la démarche conventionnelle IT, ainsi que les moyens pratiques à implémenter afin de la mettre en oeuvre. Notre travail en cours se concentre sur la modélisation du réseau et de ses menaces. Pour aller plus loin dans notre démarche, nous souhaitons définir des corrélations entre les attaques présentées en section V et chacun des protocoles proposés dans la section IV-A. Nous visons également l'ajout de plusieurs étapes, telles que l'analyse et la reconnaissance de trafic chiffré, ainsi que l'exploitation des vulnérabilités trouvées.

4. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Références

[1] R. Hallman, J. Bryan, G. Palavicini, J. DiVita, and J. Romero-Mariona, "Ioddos - the internet of distributed denial of sevice attacks - A case study of the mirai malware and iot-based botnets," in *IoTBDS*, 2017.

[2] M. Bishop, "About penetration testing," *IEEE Security & Privacy*, vol. 5, no. 6, 2007.

[3] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "Iot sentinel : Automated device-type identification for security enforcement in iot," in *ICDCS*, 2017, pp. 2177–2184.

[4] S. Siby, R. R. Maiti, and N. O. Tippenhauer, "Iotscanner : Detecting and classifying privacy threats in iot neighborhoods," *CoRR*, vol. abs/1701.05007, 2017.

[5] J. Durech and M. Franekova, "Security attacks to zigbee technology and their practical realization," in *SAMI*, 2014, pp. 345–349.

[6] A. Reziouk, E. Laurent, and J.-C. Demay, "Practical security overview of ieee 802.15. 4," in *ICEMIS*, 2016, pp. 1–9.

[7] J. R. Douceur, "The sybil attack," in *IPTPS*, 2002, pp. 251–260.

[8] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the rpl-based internet of things," *IJDSN*, vol. 9, no. 8, 2013.