Détection d'Intrusion dans l'Internet des Objets : Problématiques de sécurité au sein des domiciles

Jonathan Roux

Détection d'Intrusion dans l'Internet des Objets : Problématiques de sécurité au sein des domiciles

Jonathan Roux
LAAS-CNRS, Université de Toulouse, CNRS, Toulouse, France
Email : jonathan.roux@laas.fr

***Abstract*—Afin de comprendre les enjeux liés à l'Internet des Objets, nous présentons un état de l'art des problématiques de sécurité de ce domaine, notamment au sein des domiciles. Celui-ci décrit les surfaces d'attaque de ces objets présents dans les domiciles ainsi que les moyens de protection existants. Finalement, cet état de l'art nous permet d'identifier les insuffisances de ces solutions et de commencer à analyser les potentielles améliorations notamment l'utilisation de méthodes de détection d'intrusion en opération et d'analyse comportementale via des mécanismes d'apprentissage.**

1. Introduction

L'Internet des Objets (IoT) prend depuis quelque temps une ampleur de plus en plus importante. Il concerne, avec des frontières plus ou moins floues, la mise en connectivité massive d'objets, tel que des capteurs, téléphones, ou plus généralement d'objets du quotidien auparavant déconnectés (serrure, climatiseur, etc.) [1]. Aujourd'hui encore peu présents dans nos domiciles, certaines sources indiquent que le parc de ces objets pourrait atteindre facilement les 24 milliards d'ici 2024 [2]. Si l'interêt repose généralement sur la mise en place de services avancés pour les différents utilisateurs, ces nouveaux objets fragilisent dangereusement la sécurité de nos domiciles, à la fois numériquement mais également physiquement.

En effet, à la différence de l'informatique traditionnellement présente dans nos maisons, l'Internet des Objets répond notamment à des besoins tels que l'ouverture des portes, des volets, la surveillance de la maison ou le contrôle des ampoules, et ce, pour des utilisateurs insuffisamment sensibilisés aux problématiques de sécurité. Deux autres problèmes de ce point de vue apparaissent en analysant le contexte économique de développement de ces objets. Tout d'abord les fabricants de ce type d'objet sont souvent des entreprises d'objets ménagers n'ayant que très peu, voire aucune expertise dans le domaine de la sécurité. Ensuite, ces derniers étant principalement achetés pour les fonctionnalités supplémentaires "pratiques" qu'apporte la connectivité face aux objets traditionnels, la sécurité est donc très souvent négligée au profit d'une facilité d'utilisation pour les particuliers. En outre, l'Internet des Objets, s'il diffère de l'informatique traditionnelle dans sa conception et son utilisation, possède également des caractéristiques propres qui rendent moins adaptés les mécanismes de protection existants. Tout d'abord, contrairement aux ordinateurs, un réseau local d'IoTs est extrêmement dynamique, de nouveaux objets apparaissant et disparaissant en fonction de potentiels visiteurs au sein du domicile. Le nombre conséquent d'objets connectés présents peut également être un problème, notamment pour la surcharge et l'hétérogénéité des échanges engendrés, qui rendent difficile la surveillance de ces derniers. En outre, en plus de la connectivité IP, ces communications sont souvent directement effectuées entre les objets, via des protocoles réseaux dit ad hoc, et non plus relayées par un élément central comme un routeur. Finalement, les caractéristiques de mobilité, de simplicité et de consommation des IoTs imposent des performances relativement réduites, rendant difficile la mise en place de mécanismes de sécurité intégrés aux objets eux-mêmes [4].

S'il est bien entendu nécessaire de former les fabricants aux bonnes pratiques de sécurité recommandées notamment par le NIST [3] et l'US Department of Homeland Security [6], il est significativement plus difficile de le faire pour les utilisateurs. En effet, contrairement aux IoTs dans le contexte industriel, où des garants de la sécurité (experts) sont présents, la majorité des particuliers a des connaissances relativement faibles en matière de sécurité, et privilégie un objet fonctionnel à un objet contraignant. Il serait donc intéressant de réfléchir à un moyen d'apporter du soutien aux utilisateurs en matière de sécurité en utilisant l'auto-configuration, c'est-à-dire en limitant les opérations de configuration de la part du particulier.

La section suivante présente un état de l'art des différentes vulnérabilités et attaques liées aux IoTs, ainsi que les mécanismes de défense existants dans le contexte des domiciles. La section 3 discute les limites des solutions existantes et présente les problématiques auxquelles la thèse cherchera des réponses.

2. Sécurité dans l'IoT

2.1. Classes et surfaces d'attaque

L'Internet des Objets possède des caractéristiques différentes de celles de l'informatique traditionnelle, notamment en termes d'hétérogénéité et d'évolution dynamique de l'environnement dans lequel ces objets sont déployés. De ce

fait, les solutions usuelles permettant de sécuriser les réseaux locaux ne suffisent plus, et il est important de comprendre les besoins de sécurité pouvant prendre en compte ces particularités. Cette compréhension passe donc par un état de l'art des attaques représentatives pouvant survenir dans les réseaux locaux des domiciles. Des classifications existent pour énumérer les vulnérabilités des objets de l'IoT [5]. A titre d'exemple, la classification de l'OWASP identifie les surfaces d'attaques principales, notamment : mémoire, réseau, interface web, etc.. La manière dont les objets ont été concus et deployés est responsable de la majeure partie des vulnérabilités.

Tout d'abord, nous identifions une première catégorie d'attaques liée à l'authentification / autorisation. Il s'agit principalement de vulnérabilités de conception ou de configuration telles que des mots de passe ou des jetons d'authentification faibles voire inexistants. Si on prend l'exemple des ampoules connectées Phillips Hue [7], actuellement très populaires, l'utilisateur doit s'authentifier auprès du serveur Phillips pour pouvoir contrôler la lumière. Cependant, le mot de passe est contraint à seulement 6 caractères alphanumériques, engendrant de possibles faiblesses du point de vue de l'authentification. Deuxièmement, pour contrôler les ampoules via l'utilisation d'un smartphone, un jeton d'authentification est généré puis fourni à l'appareil. Si l'idée est intéressante, l'implémentation est vulnérable, ce jeton étant simplement un hashé MD5 de l'adresse MAC de l'appareil qui n'est pas une information privée. Le botnet Mirai [8] est également un parfait exemple des attaques pouvant survenir suite à des vulnérabilités de ce type. En effet, l'infection reposait principalement sur des mots de passe faibles ou utilisés par défaut.

La seconde catégorie d'attaques identifiée repose également sur des mauvais choix de conception. Il s'agit principalement d'implémentations vulnérables des protocoles réseaux ou des standards cryptographiques. Fouladi et Ghanoun [9] ont par exemple trouvé une vulnérabilité dans l'implémentation du protocole Z-Wave réalisée pour des serrures connectées. Celle-ci permettait à un attaquant de réaliser un nouvel échange de clé, et ce même après que la serrure ait été appairée avec un contrôleur légitime, lui donnant alors le contrôle sur l'ouverture et la fermeture des portes.

La troisième catégorie provient principalement de la confiance apportée par les concepteurs/fabricants de ces objets envers les autres équipements du domicile. C'est notamment l'utilisation massive d'UPnP (Universal Plug and Play) [10] au sein des IoTs qui engendre ce type d'attaques. UPnP est un protocole qui possède deux caractéristiques dangereuses au sein d'un réseau local. Tout d'abord, il permet à un utilisateur d'ouvrir des ports sur l'équipement d'entrée du réseau, autorisant ainsi à des personnes de contrôler les objets depuis l'extérieur. Cette fonctionnalité permet notamment aux botnets de se connecter et d'infecter les IoTs via l'utilisation de Telnet ou de SSH. Une recherche via Shodan.io [11], un moteur de recherche permettant de localiser un grand nombre d'objets connectés à Internet, permet vite de comprendre l'étendue des objets accessibles. Ensuite, UPnP fait l'hypothèse que l'ensemble du réseau local est de confiance, et qu'il suffit donc d'être connecté au même point d'accès WiFi pour s'authentifier définitivement auprès de l'objet l'utilisant. C'est notamment ce que montre Nitesh Dhanjani [7] sur un babyphone Belkin WeMo.

Si l'ensemble de ces premières classes d'attaques est surtout lié à des faiblesses ou des erreurs au niveau de la conception de la part des fabricants, il existe également des attaques reposant sur la limitation des ressources de ces objets. En effet, la faible puissance des IoTs ne permet pas d'implémenter aisément tous les mécanismes de protection habituellement présents dans l'informatique traditionnelle. S. Pastrana et al. [12] ont notamment montré qu'il était possible d'exploiter un débordement de tampon présent dans l'implémentation du protocole Bluetooth des Arduino Yun, très utilisé dans le monde IoT. Ils développent ensuite un ver permettant de se propager. Si cette vulnérabilité n'est pas propre aux objets connectés, la faible puissance de ce composant empêche la mise en place de protection mémoire comme la randomisation de l'espace d'adressage (ASLR en anglais) ou la mise en place de canari [13]. En outre, Mike Ryan [14] a également découvert une vulnérabilité dans la spécification du protocole Bluetooth Low Energy (BLE). La procédure d'échange de clés utilisée par BLE est en effet vulnérable à des attaques par brute-force. Il est évident qu'aucune de ces malveillances n'est propre au monde de l'Internet des Objets. Cependant, si une majorité d'entre elles est due à une mauvaise conception de la sécurité et à un manque de formation des entreprises et des particuliers, les ressources limitées sont également un facteur important qu'il ne faut pas négliger.

2.2. Mécanismes de défense

Les caractéristiques particulières comme l'aspect dynamique et les modes de communication directs du monde de l'IoT imposent de revoir les mécanismes de défense traditionnellement présents dans nos domiciles. Par exemple, le réseau est soumis à beaucoup plus de changements au niveau des différents objets qui le composent, rendant difficile le système de liste noire (blacklisting) ou de règles de pare-feu (firewall). De plus, contrairement aux ordinateurs, où des logiciels tels que des anti-virus peuvent être intégrés, les objets connectés possédent des ressources limitées, empêchant ce type de mécanismes d'être mis en place. Dans ce contexte, la mise en place d'outils de détection d'intrusion s'avère nécessaire, notamment car ils permettent d'analyser non seulement les messages échangés, mais également le comportement des éléments sur le réseau. Cependant, les solutions existantes sont limitées car elles ne permettent pas de surveiller les échanges directs entre les objets, et d'identifier les comportements considérés comme suspects dans le domicile.

Ces problématiques données, un certain nombre de recherches ont commencé à être conduites afin d'adapter ces mécanismes aux attaques qui peuvent survenir dans un réseau d'objets connectés. Les outils étudiés peuvent être classés en deux catégories selon leur type d'action :

soit en prévention, soit en détection / surveillance via des observations en opération.

Un exemple correspondant à la première catégorie est le système IoT Sentinel développé par M. Miettinen & al. [15], permettant d'identifier dynamiquement les objets connectés présents et de sécuriser les communications. Il utilise notamment des mécanismes d'apprentissage pour classifier les différents objets, puis identifie leurs vulnérabilités en utilisant la base de vulnérabilités (CVE). Il segmente ensuite le réseau local en définissant des classes, proposées en fonction du risque de compromission des objets, imposant des restrictions de communication en interne mais également vers l'extérieur. Cependant, l'outil ne prend pas en considération les potentielles communications via les protocoles ad hoc, il est donc possible que des attaques puissent survenir par ce biais. De plus, les restrictions peuvent rendre les objets inutiles, puisqu'ils ne disposent plus des communications nécessaires à leur fonctionnement. Les IoTs vulnérables étant nombreux, ce type de mécanisme peut engendrer de fortes contraintes d'usage pour les utilisateurs. Finalement, même si le côté préventif est intéressant, notamment pour identifier les éléments du réseau et leurs potentielles failles, il se doit d'être à notre avis complété par une méthode de protection basée sur l'analyse des flux en opération entre les objets du domicile.

L'organisation Dyne.org définit "Dowse" [16], un outil capable d'identifier les différents objets connectés présents via leur communication IP et Ethernet. Celui-ci s'installe comme passerelle entre le point d'entrée et le reste du réseau local et analyse les échanges tout en agissant comme serveur DHCP. Il fournit notamment la possibilité de prévenir le propriétaire de l'arrivée de nouveaux objets, de *monitorer* les échanges, ainsi que l'anonymisation des communications. Cependant, l'outil n'est pour l'instant qu'un concept, et il ne répond pas non plus aux potentielles attaques directes utilisant les protocoles ad hoc.

Finalement, un outil du nom de SVELTE a été imaginé par S. Raza et al. [17]. Il s'agit d'un IDS permettant de surveiller les échanges utilisant les protocoles IPv6 et 6LoWPAN, qui sont déployés dans le monde de l'IoT, permettant notamment d'accéder à l'objet depuis n'importe où sur Internet. La particularité et l'intérêt de cet outil résident notamment dans son faible coût, permettant de l'inclure dans les différents objets.

Force est de constater qu'il existe actuellement très peu de solutions pour la détection d'intrusion adaptées aux contraintes inhérentes aux domiciles connectés. Des travaux sont donc nécessaires pour répondre à ce besoin.

3. Contributions futures de la thèse

Les perspectives de la thèse se situent principalement dans le contexte de la surveillance et de la détection des intrusions pouvant survenir au sein des réseaux locaux de nos domiciles. Nos travaux visent à définir et à déployer une solution plus complète que celles existantes. Tout d'abord, en utilisant les mécanismes de classification et d'identification des objets tels que présentés, mais également des techniques de surveillance et de détection en opération, en utilisant notamment le monitoring des différents protocoles de l'IoT. Une exigence forte est de rendre facilement utilisable cette solution à tout utilisateur, expert ou non, ce qui est nécessaire pour la démocratisation d'une solution de sécurité.

Dans le cadre de nos travaux, nous distinguons quatre classes d'attaques ciblant les domiciles connectés :

1) Attaque extérieure vers objets locaux : un attaquant extérieur effectue des attaques sur les objets connectés au sein du domicile.
2) Attaque locale : un attaquant ayant temporairement accès au réseau local corrompt un objet du domicile.
3) Attaque par rebond : un objet corrompu par un attaquant extérieur ou local est utilisé pour attaquer d'autres objets du domicile, sans que celui-ci n'ait quitté le réseau local.
4) Attaque lié à la mobilité : un attaquant extérieur corrompt un objet momentanément hors du réseau local. Celui-ci est ensuite utilisé pour attaquer d'autres objets du domicile via des attaques par rebond.

Si ces hypothèses sont également présentes dans l'informatique traditionnelle, l'aspect mobile et dynamique renforce cependant le second et le dernier scénario. De plus, les attaques peuvent être menées non seulement via un point d'entrée sur le réseau local (box, routeur, etc), mais également en utilisant les protocoles de communications ad hoc. Ainsi, pour détecter d'éventuelles attaques, il est important dans un premier temps de monitorer les échanges via l'identification des éléments présents dans le réseau. Si les principes d'identification sont bien explorés dans la littérature, notamment via l'analyse des échanges IP [15], les autres protocoles ad hoc courtes et moyennes portées, pourtant largement utilisés [18], ne sont pas monitorés. Il convient pour cette partie de déterminer les moyens permettant de les surveiller, de façon à développer des sondes qui seront utilisées pour la détection d'intrusion.

Ensuite, pour déterminer la manière de détecter efficacement des attaques, nous étudions les approches comportementales permettant de définir des modèles d'échanges légitimes au sein d'un domicile. Cette partie nécessite de répondre à plusieurs problèmes. Tout d'abord, si ces solutions sont aujourd'hui utilisées dans l'informatique traditionnelle, l'aspect dynamique des réseaux d'objets connectés rendent la définition du modèle des comportements et des échanges légitimes extrêmement délicate. De plus, les hypothèses d'attaques, et notamment la quatrième, imposent non seulement de détecter l'apparition de nouveaux objets et la surveillance de ceux existants, mais également de ceux étant sortis puis rentrés dans le réseau. Cette partie comportementale est essentielle pour obtenir une solution autonome, permettant ainsi l'utilisation par des non-experts, et évolutive, c'est-à-dire capable de détecter des comportements anormaux. Un travail complémentaire est donc nécessaire pour spécifier et définir un modèle de comportements. Des approches basées sur des techniques d'apprentissage utilisant des observations en opération nous semblent pertinentes dans ce contexte.

References

[1] Postscapes, IoT Home Guide, Postscapes.com [Consulté : 3-01-2017]. [Online] http://www.postscapes.com/internet-of-things-award/connected-home-products/

[2] J. Greenough. How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond. Business Insider. [Consulté : 06-12-2016]. [Online]. http://uk.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10

[3] Ron Ross, Michaël McEvilley, Janet Carrier Oren. Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. *National Institute of Standards and Technology*, Mai 2016.

[4] IETF. Terminology for Constrained-Node Networks (RFC 7228). *Internet Engineering Task Force (IETF)*, Mai 2014.

[5] OWASP. OWASP Internet of Things (IoT) Project. *Open Web Application Security Project (OWASP)*, Jan 2017.

[6] U.S. Department of Homeland Security. Strategic Principles for Securing the Internet of Things (IoT). *U.S. Department of Homeland Security*, 15 Nov 2016.

[7] Nitesh Dhanjani. Abusing the Internet of Things, Blackouts, Freakouts, and Stakeouts. *Edition O'Reilly*, Août 2015.

[8] J. Gamblin. Mirai source code. [Consulté : 10-12-2016]. [Online] https://github.com/jgamblin/Mirai-Source-Code/blob/master/ForumPost.md

[9] Behrang Fouladi, Sahand Ghanoun. Security Evaluation of the Z-Wave Wireless Protocol. *Sensepost*. 2013

[10] HD Moore. Security Flaws in Universal Plug and Play: Unplug, Don't Play. 29 Jan 2013.

[11] Shodan.io, Search Engine for Internet-connected devices. [Consulté : 15-11-2016]. [Online]. https://www.shodan.io/

[12] Sergio Pastrana, Jorge Rodriguez-Canseco, Alejandro Calleja. ArduWorm: A Functional Malware Targeting Arduino Devices. *COSEC Computer Security Lab*. 2016.

[13] Hagen Fritsch. Stack Smashing as of Today. *Black Hat Europe*. 17 Av 2009.

[14] Mike Ryan. Bluetooth: With Low Energy Comes Low Security. *7th USENIX Workshop on Offensive Technologies*. 13 Au 2013.

[15] Markus Miettinen, Ahmad-Reza Sadeghi, Samuel Marchal, N. Asokan, Ibbad Hafeez, Sasu Tarkoma. IoT SENTINEL : Automated Device-Type Identification for Security Enforcement in IoT. *Computing Research Repository.*. arXiv:1611.04880. 13 Dec 2016.

[16] Dyne.org. Dowse, the Privacy Hub for the Internet of Things. [Consulté : 24-11-2016]. [Online]. http://dowse.eu/

[17] Shahid Raza, Linus Wallgren, Thiemo Voigt. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks, Elsevier*. Nov 2013.

[18] ARCEP. Préparer la révolution de l'Internet des Objets. [Consulté : 14-12-2016]. [Online]. http://www.arcep.fr/iot/