

Développement d'un pare-feu domestique

Pré-rapport de projet

Activité d'Apprentissage S-INFO-037

Rémy Decocq

Année Académique 2018-2019
Master en Sciences Informatiques, bloc 1
Faculté des Sciences, Université de Mons

Table des matières

1	Présentation de l'<i>internet des objets</i>	4
1.1	Généralités	4
1.2	Caractéristiques des équipements de l' <i>IoT</i>	4
1.2.1	Domaines d'application	4
1.2.2	L'environnement <i>smarthome</i>	5
1.2.3	Exemples d'équipements	6
1.2.4	Restrictions des équipements	7
2	Présentations des pare-feus	8
2.1	Généralités	8
2.2	Types de pare-feu	8
2.3	Ressources logicielles importantes	8
3	La protection dans l'<i>IoT</i>	9
3.1	Vulnérabilités liées à l' <i>IoT</i>	9
3.2	Possibilités d'amélioration	9
3.3	Solutions existantes	9
4	Les pare-feus et l'<i>IoT</i>	10
4.1	Différents types d'architecture	10
4.2	Les pare-feus domestiques	10
4.2.1	Caractéristiques d'un réseau domestique	10
4.2.2	Attaques possibles et conséquences	10
4.3	Application et implémentation	10
5	Mise en pratique : ébauche	11

Introduction

Depuis maintenant plusieurs années, la connectivité n’a cessé d’évoluer : en se limitant au domaine de l’Internet entre 2000 et 2015, une estimation de l’augmentation du pourcentage de la population mondiale l’utilisant avoisine 40% [2] [1]. Que ce soit dans le cadre d’infrastructures de type ”mainframe” ou dans le contexte des ordinateurs personnels, les technologies et équipements relatifs au réseau et aux communications sont devenus indispensables. En conséquence, corrélé au fait de pouvoir de plus en plus s’interconnecter et rejoindre des réseaux de natures variées, le nombre de menaces potentielles pour une machine ainsi connectée augmente grandement. Heureusement, parallèlement à cette évolution, les performances des machines classiques qui en sont équipées ont également suivi une progression en terme de performances. Cela a permis d’en renforcer la sécurité à plusieurs niveaux, et surtout d’intercepter efficacement les menaces étrangères liées à l’utilisation des réseaux. À l’heure actuelle, les OS utilisés classiquement sur des machines desktop fournissent un pare-feu simple (*Windows Defender*, un utilitaire fournit de base dans MAC OS X, *iptables/Netfilter* ou autre pour les distributions Linux). Ce dernier tournant en arrière plan de façon quasi invisible car il demande peu de ressources par rapport à ce qu’une machine actuelle peut offrir.

En parallèle avec la montée en puissance de ces machines de type desktop, serveurs, etc. s’est développée depuis à peu près les années 2000 la tendance de l’« Internet des Objets », ou encore plus communément abrégé IoT pour *Internet of Things*. Bien qu’assez large, cette dénomination regroupe beaucoup d’objets et de concepts, qu’ils soient virtuels ou non mais possédant un dénominateur commun : la capacité de communiquer en réseau avec d’autres équipements. Cela englobe par exemple la domotique, les outils et capteurs de mesures diverses, les imprimantes et scanners en réseau, etc. Tous ces éléments convergeraient idéalement vers une mise en réseau commune. Cela peut se faire par le réseau Internet, il n’est pas rare d’orienter ces connections vers un cloud permettant de traiter globalement et intelligemment la masse de données qu’il reçoit de ces équipements. Or, comme évoqué ci-dessus, plus on s’interconnecte et plus on s’ouvre à des attaquants potentiels, ce qui pose problème si rien n’est mis en place pour s’en protéger.

Ce travail aura pour objectif premièrement de faire un état de l’art des dispositifs de protection qui sont actuellement déployés dans l’IoT et plus particulièrement dans le cadre domestique. Il s’agit d’un monde beaucoup plus hétérogène et restreint en terme de ressources que celui des ordinateurs qu’on retrouve classiquement dans ce milieu, de fait il n’est pas toujours possible de réutiliser telles quelles toutes les technologies de protection y attendant. De plus, il faut prendre en considération les spécificités d’une habitation : au centre de tous ces équipements communiquant se trouve l’habitant, une personne n’étant pas forcément habilitée à manipuler et contrôler ces nouvelles technologies. Il sera également question d’établir une vision globale des différentes formes de pare-feus et sous quelles formes ceux-ci peuvent être implémentés dans les équipements d’une habitation classique. Deuxièmement, il sera question de mettre en pratique ces connaissances pour développer un système en lien avec ces nouvelles mesures de sécurité inhérentes à l’IoT. Celui-ci fera intervenir les connaissances acquises au préalable sur les pare-feus.

1 Présentation de l'*internet des objets*

1.1 Généralités

L'Internet des objets, qu'on désignera par *IoT* pour le terme plus répandu de *Internet Of Things*, représente un tout qui évolue maintenant en flèche depuis plusieurs années. Aucune définition formelle n'est acceptée globalement, mais plusieurs organismes ont tenté d'en établir une ébauche. Par exemple, l'ITU-T (ITU Telecommunication Standardization Sector) Y.2060 le définit comme tel :

“Global infrastructure for the society, enabling advanced services by inter-connecting (physical and virtual) things based on existing and evolving in-teroperable information and communication technologies.”

Derrière cette définition très générale, on peut distinguer plusieurs sous-groupes d'objets connectés distincts, aux applications tant variées que hétérogènes, dans des domaines et secteurs également très différents. C'est ce qui fait la force et en même temps la faiblesse de cet ensemble d'équipements et services qu'on regroupe derrière le terme *IoT* et que des efforts considérables sont déployés pour inter-connecter au maximum. C'est un domaine d'étude intéressant car il représente littéralement ce qu'on pourrait considérer comme le futur de notre environnement technologique. De fait, les équipements que l'on peut associer à une partie de l'IoT ont déjà fait leur apparition dans notre quotidien : en 2017 on comptait 8,4 milliards de machines en présentant les caractéristiques et les estimations pour l'année 2020 tendent vers 20,4 milliards d'objets connectés d'après la société d'analyse Gartner [5].

1.2 Caractéristiques des équipements de l'*IoT*

1.2.1 Domaines d'application

Les secteurs dans lesquels l'IoT s'est implanté ces dernières années sont nombreux et très variés : ils s'étendent de l'industrie au domaine des soins de santé en passant par la tendance des *Smart Home*. C'est ce dernier domaine qui est approfondi dans ce travail et qui sera le plus sous-entendu par la suite quand le terme *IoT* est utilisé. La Figure 1 présente une vision d'un schéma global des autres domaines qui gravitent autour du vaste monde de l'IoT.

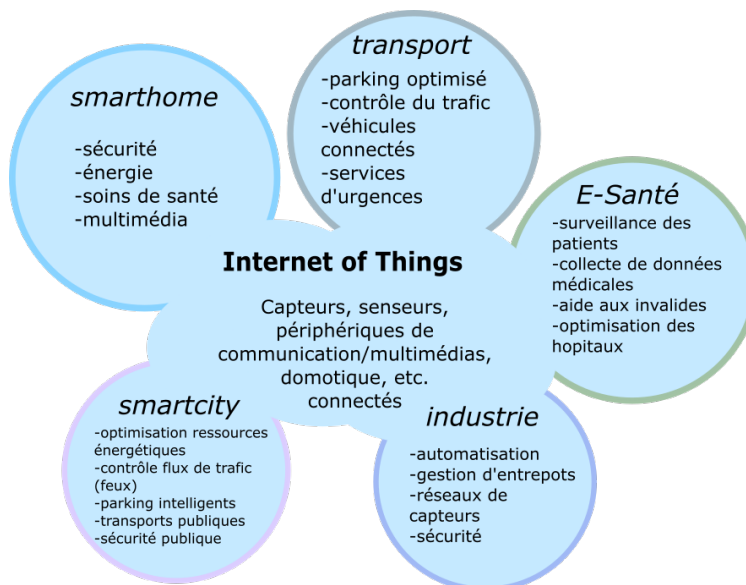


FIGURE 1 – Domaines d'application de l'IoT

1.2.2 L'environnement *smarthome*

Le terme émergeant *Smart Home* est une fois de plus très englobant et généra. Il n'en existe pas de définition formelle et communément acceptée. Basman M. Hasan et al. [4] en présentent plusieurs. Un résultat les unifiant pourrait être

« Une *smarthome* est un environnement lié au domicile particulier où plusieurs équipements ou sous-systèmes sont inter-connectés et où les informations qu'ils échangent sont collectées et utilisées afin de surveiller, réguler et automatiser l'écosystème du domicile ».

L'utilisateur en tant que personne physique y vivant est donc au centre de cette architecture, et y siège comme le principal intervenant. Puisque dans l'idée où toute cette technologie est déployée dans le but d'améliorer sa qualité de vie, c'est lui qui devra interagir avec. La notion d'intelligence est intrinsèquement liée avec celle de l'interconnexion de tous ces senseurs et actuateurs déployés dans l'environnement du domicile : il s'agit d'en récolter et regrouper toutes les données en un point central doté d'une capacité de traitement plus évoluée afin qu'il puisse en tirer une optimisation globale du domicile et la proposer sous une forme donnée à l'habitant.

Une certaine classification fonctionnelle peut être établie pour distinguer de façon plus concrète les différents équipements qui peuvent intervenir dans l'écosystème d'une *smarthome*. Elle est schématisée par la Figure 2, inspirée de [4]. Ce qui est désigné par *point d'interconnexion* peut dépendre de l'architecture réelle d'une *smarthome*. Dans la plupart des cas il s'agit d'une machine faisant office de collecteur pour toutes les données transitant dans le domicile et de gateway vers le reste de l'Internet, éventuellement le cloud associé au domicile.

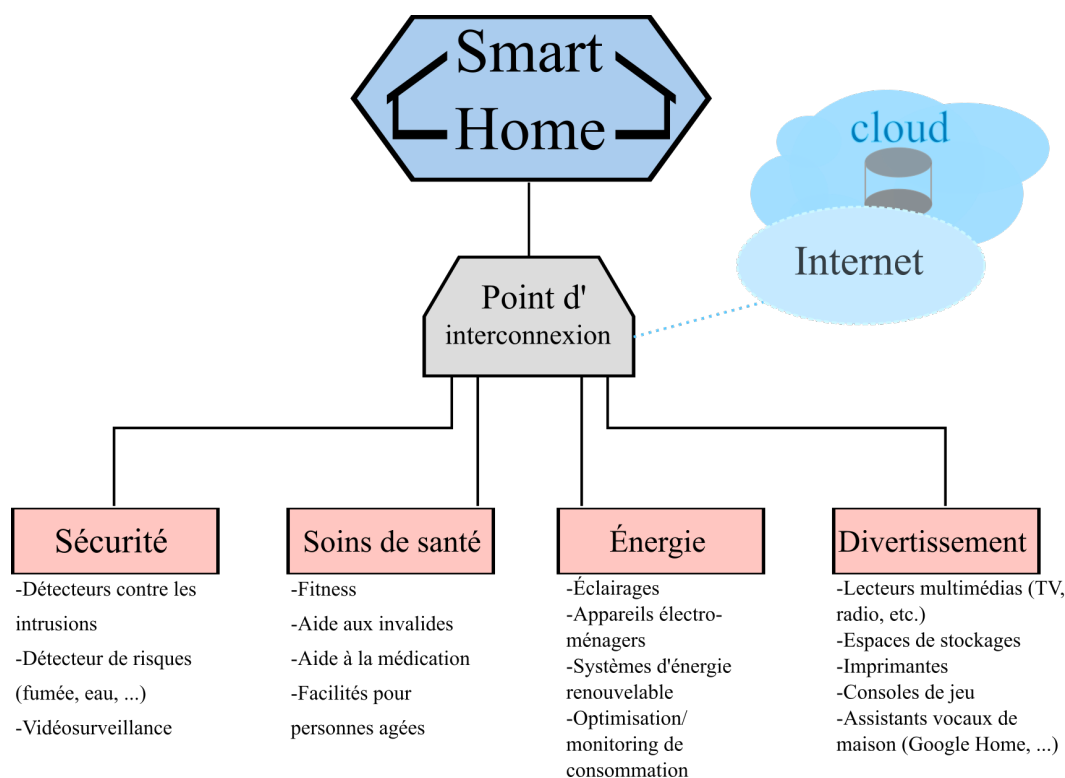


FIGURE 2 – Classification fonctionnelle des équipements *IoT* d'une *smarthome*

1.2.3 Exemples d'équipements

La perception de ce qu'est l'*IoT* par le grand public se résume énormément à l'environnement que constitue la *smarthome* [5]. Il s'agit d'une erreur d'incompréhension, on peut tenter de l'explicitier en analysant ce qui compose cette perception. La Figure 3 en donne une vision générale (tirée d'un sondage effectué aux États-Unis), qui va être étayée par les exemples concrets d'équipements la suivant.

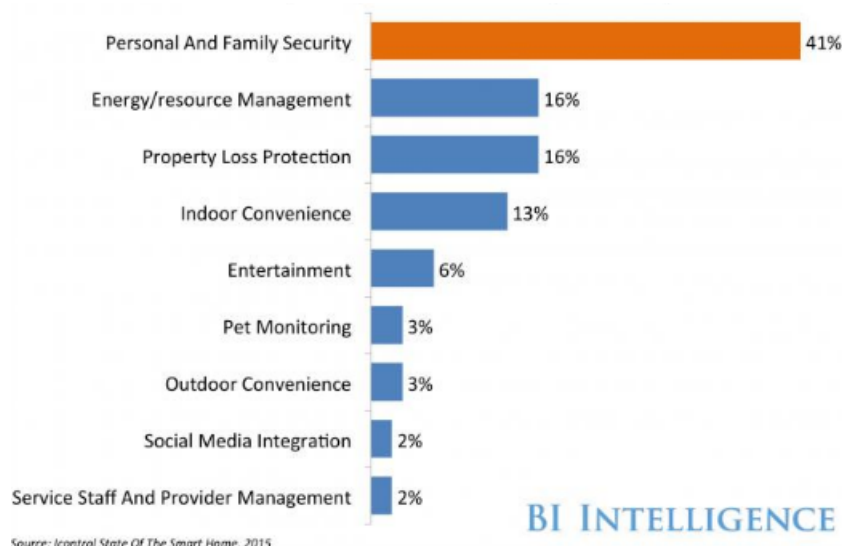


FIGURE 3 – Top des meilleurs apports des *smarthome* tel que perçu par les Américains

Appartenant à la classe sécurité

- Caméras de vidéosurveillance dites IP
- Systèmes de gestion d'alarme à distance
- Verrous de portes intelligents
- Simulateurs de présence et occupation du domicile

Appartenant à la classe soins de santé

- Surveillance des patients à leur domicile (contrôle des mesures médicales)
- Accessoires de fitness : montres, balances connectées et autres
- Outils divers d'aide aux personnes invalides (fauteuils, bracelets de secours, ...)

Appartenant à la classe des énergies

- Luminaires intelligents/automatisés contrôlables à distance
- Frigos, lave-vaisselles, etc.
- Thermostats connectés, compteurs et senseurs énergétiques

Appartenant à la classe du divertissement & multimédia

- Outils de communication : smartphones, babyphones, etc.
- SmartTV, consoles, casques connectés et lecteurs multimédia divers
- Imprimantes et scanners en réseau
- Assistants vocaux de maison comme le *google home*

1.2.4 Restrictions des équipements

Malgré le fait que l'ensemble des objets considérés comme appartenant à l'IoT soit très hétérogène, on peut distinguer plusieurs caractéristiques communes à beaucoup d'entre eux. Elles tendent généralement vers ce qui est vu comme une restriction par rapport à un ordinateur type classique (*desktop*). Ces éléments constituent les plus gros freins au développement de la sécurité sur de tels système [3]. Les conséquences de ces restrictions sont discutées plus en détail dans la section 3 de ce document.

Conçus pour satisfaire une unique fonction

Le meilleur exemple est celui des capteurs : un capteur a pour objectif de faire une mesure d'une grandeur physique (température, pression, etc.), d'en tirer une valeur numérique et de faire remonter via son interface avec le réseau cette information vers une unité centrale qui la traitera. Ce genre d'équipement est généralement minimaliste au possible et ne peut donc pas remplir d'autre tâche.

Requièrent une faible consommation énergétique

Les systèmes embarqués n'ont pas toujours accès à une source illimitée d'énergie, et auront donc une durée de vie limitée à celle de leur batterie. En conséquence, il est souhaitable d'économiser un maximum, ce qui peut se faire en réduisant les temps d'éveil de l'équipement et en optimisant le nombre d'opérations effectuées quand il tourne à plein régime. Dés lors, certains protocoles et algorithmes doivent être adaptés (relatifs aux communications réseaux mais aussi à la sécurité) [7].

Sont contraints en ressources CPU, mémoires et radios Ces contraintes sont aussi identiques à celles des systèmes embarqués classiques. En plus de celles-ci, on peut mettre en évidence le fait que les radios (quand il s'agit d'une interface sans fil) sont assez faibles et ne permettent pas des communications à haut débit. En résulte également que des techniques comme le saut de fréquence et les algorithmes de chiffrement de type asymétrique sont plus compliquées à mettre en œuvre [6].

Sont programmés à un bas niveau d'abstraction

Étant conçus pour ne remplir que des fonctions spécifiques, certains équipements ne sont pas programmables en utilisant des langages de haut niveau. Par conséquent, ce sont souvent des boîtes noires difficilement manipulables et statiques : les mises à jour et patch de sécurité ne sont pas déployables aisément par les constructeurs [7]. Les seules interactions que l'utilisateur peut avoir avec l'équipement sont celles prévues par l'interface de ce dernier s'il y en a une.

2 Présentations des pare-feus

2.1 Généralités

2.2 Types de pare-feu

2.3 Ressources logicielles importantes

3 La protection dans l'*IoT*

3.1 Vulnérabilités liées à l'*IoT*

3.2 Possibilités d'amélioration

3.3 Solutions existantes

4 Les pare-feus et l'*IoT*

4.1 Différents types d'architecture

4.2 Les pare-feus domestiques

4.2.1 Caractéristiques d'un réseau domestique

4.2.2 Attaques possibles et conséquences

4.3 Application et implémentation

5 Mise en pratique : ébauche

Conclusion

Références

- [1] Cable broadband technology gigabit evolution. Dernière lecture le 27/11/2018.
- [2] Internet growth statistics par internet world stats. <http://www.ti.com/lit/ml/swrb028/swrb028.pdf>. Dernière lecture le 26/11/2018.
- [3] Security in the Internet of Things. https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf, 2015.
- [4] Alhafidh Basman M.Hasan and William Allen. Design and simulation of a smart home managed by an intelligent self-adaptive system. *Int. Journal of Engineering Research and Application*, 2016.
- [5] Dan-Radu Berte. Defining the IoT. *De Gruyter*, 2018.
- [6] Engin Leloglu. A review of security concerns in Internet of Things. *Journal of Computer and Communications*, 2017.
- [7] Huichen Lin and Neil Bergmann. IoT privacy and security challenges for Smart Home environments. *Information (online MDPI journal)*, 2016.