

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

Introduction

Depuis maintenant plusieurs décades, la connectique n'a cessé d'évoluer, que ce soit dans le cadre d'infrastructures de type "mainframe" ou dans le contexte des ordinateurs personnels. De fait, corrélé au fait de pouvoir de plus en plus s'interconnecter et rejoindre des réseaux de nature variée, le nombre de menaces potentielles pour une machine ainsi connectée augmente grandement. Heureusement, parallèlement à la connectique, les performances des machines classiques qui en sont équipée ont également suivi une bonne courbe de progression. C'est ce qui 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, n'importe qui a sur son PC au minimum un pare-feu basique fourni par l'OS de la machine, celui-ci tournant en arrière plan de façon quasi invisible car il demande peu de ressources par rapport ce qu'une machine actuelle peut offrir.

En parallèle avec l'émancipation de ces machines de type *desktop*, serveurs, etc. s'est développé depuis à peu près les années 2000 la tendance de l'"internet des objets", ou encore plus communément appelé *IoT* pour *Internet of Things*. Assez complexe à définir, cette dénomination regroupe beaucoup d'objets et de concepts, qu'ils soient virtuels ou non : cela englobe notamment la domotique, les outils de mesures diverses, etc. Tous ces éléments tendent vers une mise en réseau commune, souvent directement avec l'Internet. 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 globalement la sécurité dans ce *Web 3.0*. Effectivement, on approche un monde beaucoup plus hétérogène et restreint en terme de ressources que celui des ordinateurs modernes et classiques, de fait on ne peut pas réutiliser telles quelles toutes les technologies de protection y attendant. Deuxièmement, il sera question de mettre en pratique ces connaissances pour développer un système en lien avec ces nouvelles pratiques inhérentes à l'*IoT*.

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 très différents. C'est ce qui fait la force et en même temps la faiblesse de ce tout ce qu'on regroupe derrière le terme *IoT* et que des efforts considérables sont déployés pour interconnecter 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 [Defining_the_IoT].

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 *SmartHome*. C'est ce dernier domaine qui est approfondi dans ce travail et dont il sera le plus question 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*, ainsi que les utilisateurs qui en sont les exploitants.

Le terme émergeant *SmartHome* est une fois de plus très englobant et général, il n'en existe pas de définition formelle et validée de tous. [Design_simulation_smarthome] nous en présente 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.

1.2.2 Exemples d'équipements

1.2.3 Restrictions des équipements

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