Les objets connectés

Bastien Labouche
Julie Lopez

24 février 2018

Table des matières

0.1 Les objets connectés

0.1.1 Objets connectés ? Kesako ?

Si l'on se base sur la définition de l'Insa Rennes :

> un objet connecté est une chose, fabriquée par l'homme, dont l'usage est d'établir une liaison afin de pouvoir faire passer des informations diverses et variées à un autre objet ou à toute autre chose connectée.

Il s'agit là d'une définition très basique mais assez claire de ce qu'est un objet connecté, même si il n'y a pas vraiment de définition "officielle" de ce qu'est un objet connecté. Nous retiendrons donc que ce sont des objets pouvant "communiquer", et ce grâce à différentes technologies, par exemple :

— La montre connectée communiquant avec le téléphone grâce au bluetooth.
— La caméra IP communiquant via un câble ethernet avec la box.
— Le drone piloté avec le téléphone via du wifi.
— Le thermostat compatible wifi.
— ...

Au fur et à mesure de l'avancée de la technologie, une sorte de réseau entre les objets s'est développé, on l'appel "l'internet des objets" mais vous le connaissez sûrement sous le nom de IoT (Internet of Things)

0.1.2 Internet Of Things

Comme dit plus haut, l'Internet of Things est un réseau reliant entre eux les objets connectés de par le monde, il s'agit de leur version d'internet. Selon Wikipedia, il s'agit d'une extension d'internet qui serait considéré comme la troisième évolution de l'internet :

> L'Internet des objets, ou IdO (en anglais Internet of Things, ou IoT), est l'extension d'Internet à des choses et à des lieux du monde physique.
>
> Alors qu'Internet ne se prolonge habituellement pas au-delà du monde électronique, l'Internet des objets connectés représente les échanges d'informations et de données provenant de dispositifs du monde réel avec le réseau Internet.

L'Union internationale des télécommunications nous donne la définition suivante, décrivant l'internet des objets comme une :

> infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets(physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution

Quelques chiffres

- En 2016, 5.5 millions d'objets sont connectés chaque jour dans le monde
- Gartner inc. prévoit que 26 milliards d'objets seront installés d'ici 2020
- Un être humain serait en contact avec 1000 à 5000 objets au cours d'une journée normale
- Il ne faut que quelques minutes pour qu'un objet connecté vulnérable se fasse hacker après sa mise en ligne

0.2 Failles de sécurité

0.2.1 Problèmes de configuration

Comme vu plus haut dans la partie sur l'IoT des millions (et bientôt des milliards) d'objets sont interconnectés entre eux. Même si de nos jours la sécurité des données commence à entrer dans les mœurs, 30% des objets connectés de l'IoT ne sont toujours pas sécurisés. La sécurité est non-seulement négligée du côté des constructeurs, mais aussi du côté des utilisateurs, la plupart ne prenant pas la peine de changer les identifiants par défaut, lorsqu'il y en a. Une pratique pouvant facilement être vérifiable en faisant un tour sur Shodan. Il s'agit d'un genre de moteur de recherche pour objets connectés, ce site référence le résultat de balayages de ports massifs effectués sur le réseau internet. Cet outil est utilisé par des pirates et chercheurs en sécurité pour trouver des dispositifs mal sécurisés et en prendre le contrôle. Le créateur de Shodan a même repéré des failles de sécurité assez importantes comme la possibilité de se connecter au système informatique gérant un énorme barrage hydroélectrique en France.

0.2.2 Failles systèmes

En plus d'être mal configurés, les objets connectés embarquent avec eux de nombreuses failles. En effet, ils sont développés avec une idée de praticité, ils sont fait pour être facilement utilisables. Les concepteurs ne les conçoivent pas en pensant à les rendre sécurisés. En effet, l'internet des objets est semblable aux débuts de l'internet actuel :

— Pas de cryptage des données.
— Faible conscience des vulnérabilités et possibles attaques.
— ...

Même sur d'importants systèmes il peut y avoir des failles extrêmement grave, par exemple, le 17 avril 2015 un chercheur en sécurité nommé Chris Roberts s'est fait arrêter par le FBI car il a piraté en plein vol l'avion de ligne dans lequel il se trouvait. Se permettant en passant de modifier légèrement la trajectoire de l'avion (sans qu'il y ait de conséquences pour les passagers). Comment il a fait ? Il a ouvert le boîtier situé sous chaque siège et y a relié son ordinateur via un câble ethernet, obtenant ainsi un accès au système d'information de l'appareil.

0.3 Pourquoi c'est dangereux

0.3.1 BotNet

0.3.2 Souriez, vous êtes filmés

0.4 Conclusion