Internet des Objets grand public : l'économie de la sécurité

Sam Wood, Mark McFadden

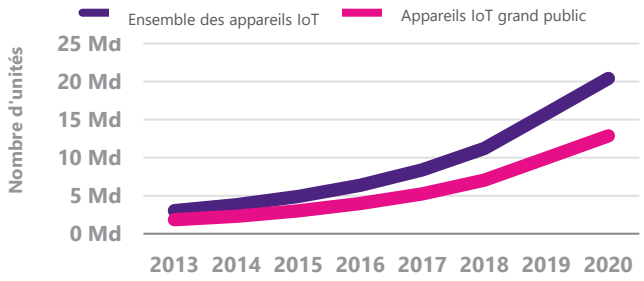
Postes de télévision et thermostats intelligents, électroménager connecté… Les applications de l'Internet des Objets se répandent dans les foyers. Pourtant, ces appareils connectés comportent souvent de sérieuses failles de sécurité qui les rendent vulnérables face aux cybermenaces. Si ces lacunes s'expliquent en partie par des raisons techniques, la véritable cause du problème est d'ordre économique, avec pour principaux facteurs une asymétrie d'informations ainsi que la présence d'incitations contradictoires et d'une variété d'externalités et de biais comportementaux. Le présent document, qui s'appuie sur un rapport récent réalisé pour l'association Internet Society, analyse ces facteurs économiques et propose des mesures de remédiation. Nous espérons ainsi améliorer la sécurité à la fois des appareils et de l'Internet en général.

Introduction

L'Internet des Objets (*Internet of Things*, IoT) constitue un vaste réseau d'appareils capables de se connecter à Internet. Cette connectivité améliore grandement leur utilité : elle permet par exemple un contrôle et une surveillance à distance, davantage de commodité pour l'utilisateur ou encore une meilleure efficacité énergétique.

En conséquence, le nombre d'appareils connectés à l'IoT connaît une croissance rapide. Selon les estimations de Gartner, il aurait ainsi dépassé 10 milliards[i] en 2018 (sans inclure les smartphones). Leur chiffre exact peut varier, mais indique toujours un ordre de grandeur impressionnant.

Figure 1 : Parc existant d'appareils IoT



Source : Gartner

Environ deux tiers de ces appareils sont des applications « IoT grand public » destinées à un usage domestique ou personnel, de type : télévisions intelligentes, électroménager connecté, éclairage intelligent, automatisation domotique, sécurité résidentielle, technologie prêt-à-porter (*wearables*), équipements de santé personnelle, etc.

Risques de sécurité sur le marché de l'IoT

Toutefois, la sécurité de ces appareils grand public fait souvent défaut. Une étude des dispositifs les plus courants a en effet conclu que 70 % d'entre eux montraient une sévère vulnérabilité aux cybermenaces.[ii] Dans une autre étude, 20 appareils IoT grand public ont été testés selon quatre axes de sécurité : tous ont révélé des faiblesses dans au moins l'un de ces axes.[iii]

Les recherches indiquent également que ces risques s'accentuent à mesure que le marché se développe. Symantec a ainsi noté une augmentation de 600 % des attaques informatiques visant les appareils IoT entre 2016 et 2017,[iv] alors qu'environ 4 000 nouveaux produits connectés vulnérables sont mis en service chaque jour.[v]

L'exploitation des failles de sécurité de ces appareils pose un risque très concret pour la sûreté et la vie privée de leurs propriétaires. Par exemple, la sécurité des modèles munis de microphones ou de caméras peut être compromise pour permettre l'enregistrement et la diffusion publique de conversations et d'images privées.[vi] Des systèmes de verrouillage intelligents peuvent aussi être ciblés pour permettre à des intrus de pénétrer dans une propriété sans effraction. S'ils ne sont pas protégés efficacement, les équipements de santé personnels connectés pourraient même être altérés de sorte de modifier les dosages des traitements. En 2015, des chercheurs ont ainsi déclaré qu'ils avaient réussi à pirater des pompes à insuline.[vii]

Outre les risques qu'ils posent aux utilisateurs, les appareils dont la sécurité a été compromise peuvent servir de point d'entrée pour attaquer une cible tierce. Ils sont en effet susceptibles de rejoindre un « botnet » : un réseau regroupant des milliers, voire millions, d'appareils connectés à Internet placés sous le contrôle d'un hacker. Ces réseaux peuvent être utilisés pour envoyer des spams, dérober des authentifiants, répandre des logiciels malveillants, alimenter la fraude publicitaire en ligne, miner de la cryptomonnaie ou commettre une attaque par déni de service (DDoS).

Le botnet Mirai représente un célèbre exemple d'attaque à grande échelle par le biais d'appareils IoT. Lancé sur le fournisseur de serveurs de noms de domaines (DNS) Dyn, il a mis des dizaines de sites hors ligne pendant toute une journée. Amazon, Spotify et Twitter comptaient notamment parmi les victimes. Au pic de son activité, Mirai est parvenu à infecter plus de 600 000 appareils IoT.[viii] L'éventualité d'un recours à un botnet similaire pour attaquer des infrastructures nationales critiques est une source d'inquiétude considérable.

Pourquoi les appareils IoT grand public sont-ils si vulnérables ?

Le faible niveau de sécurité de ces appareils s'explique au premier abord par différents facteurs techniques, tels que :

- **Faiblesse des authentifiants par défaut.** De nombreux appareils sont commercialisés avec des identifiants et des mots de passe faciles à deviner (« admin » et « mot de passe » par exemple).
- **Manque de protection du logiciel et du réseau.** Les communications entre l'appareil, l'application utilisateur et le réseau Internet en général ne sont pas toujours chiffrées. Sur certains modèles, des ports réseau peuvent même être laissés ouverts par défaut, les laissant exposés à des cyberattaques répandues.
- **Capacités limitées des jeux de composants.** Les jeux de composants et les mémoires de taille limitée et de moindre qualité sont plafonnés en termes de puissance de chiffrement.
- **Peu de mises à jour logicielles.** De nombreux fabricants ne proposent pas de mises à jour immédiates ou régulières pour les logiciels de ces appareils. Plus inquiétant, certains produits ne sont même pas conçus pour en recevoir.
- **Absence de mécanisme de mise à jour sécurisé.** Il a été démontré qu'un grand nombre de fonctions de mise à jour d'appareils IoT grand public peuvent être exploitées, par exemple par leur absence de chiffrement, pour permettre aux hackers de charger des versions modifiées ou malveillantes des logiciels embarqués.

Les facteurs économiques sous-jacents

Ces facteurs techniques nous offrent une première réponse, mais ne suffisent pas à eux-seuls à expliquer les failles de sécurité de la majorité des appareils IoT grand public. Si ces lacunes peuvent avoir de graves conséquences, pourquoi sont-elles si répandues ? Pourquoi les consommateurs continuent-ils à les acheter ? Et pourquoi les fabricants n'investissent-ils pas dans l'amélioration de la sécurité de leurs produits pour gagner un avantage sur le marché ?

L'identification de facteurs économiques, plutôt que techniques, nous permet de répondre à ces questions : asymétrie d'informations, incitations contradictoires et externalités entrent en jeu. Nous proposons ci-dessous une étude détaillée de chacun de ces éléments.

À la croisée de l'économie et de la psychologie, des recherches en économie comportementale apportent en outre un nouvel éclairage, révélant que des biais cognitifs pourraient influer sur les décisions individuelles. En effet, les utilisateurs auraient tendance à sous-estimer les risques posés en termes de sécurité informatique et à croire qu'une cyberattaque ne pourrait pas leur arriver.

Asymétrie d'informations

En 1970, l'économiste George Akerlof a utilisé l'exemple du marché de l'automobile d'occasion pour illustrer le concept d'asymétrie d'informations.[ix] Le point saillant de son analyse consistait à dire que les acheteurs sont réticents à payer un supplément pour une qualité qu'ils ne peuvent pas mesurer. En conséquence, les vendeurs ne sont pas incités à fournir des produits de haute qualité.

> Bien souvent, les consommateurs n'ont aucun moyen d'évaluer facilement le niveau de sécurité offert par un appareil connecté avant son achat.

Bien souvent, les consommateurs n'ont aucun moyen d'évaluer facilement le niveau de sécurité offert par un appareil connecté avant son achat. En effet, peu d'informations leur sont généralement données sur les mesures de protection incluses (telles que la fréquence et la durée de vie des mises à jour) en amont de l'acquisition.

Les renseignements éventuellement communiqués s'apparentent parfois à du jargon technique incompréhensible pour de nombreux consommateurs. Sans parler du fait que la puissance de chiffrement vantée par les appareils ou services IoT grand public peut en réalité se révéler pas si sécurisée que ça[x].

Ces conditions font obstacle à une évaluation concrète du niveau de sécurité précisément offert par un appareil une fois connecté et en service.

Cela signifie que les consommateurs ne seront pas disposés à payer le plein prix pour un appareil IoT « sécurisé » tant qu'ils n'auront pas la possibilité de vérifier cette information, et donc qu'il n'existe pas de forte incitation pour les fabricants à proposer des modèles mieux protégés.

Incitations contradictoires

Le ciblage d'un appareil IoT grand public implique toute une série de désagréments pour son propriétaire, qui devra potentiellement faire face à l'usurpation de son identité, à des actes frauduleux, à des dommages sur ses biens ou à des atteintes à sa sécurité personnelle. Or, puisque ces coûts sont tous assumés par les propriétaires, les fabricants ne sont pas fortement encouragés à améliorer la sécurité de leurs produits.

On observe donc une contradiction entre ces deux acteurs : celui qui recherche un compromis entre sécurité et efficacité n'est pas celui qui est pénalisé par les attaques.

Au contraire, les fabricants y gagnent, puisqu'ils peuvent ainsi réduire les coûts, ajouter des fonctionnalités et commercialiser leurs produits plus rapidement. En effet, les étapes de test et d'implémentation de mesures de sécurité, en générant des frais supplémentaires et en retardant la sortie des produits, impactent négativement leurs bénéfices. Une sécurité plus stricte pourrait aussi entraver la fonctionnalité de l'appareil et ainsi réduire sa valeur aux yeux des consommateurs.

Si certaines sociétés accordent davantage d'importance à la sécurité afin de protéger leur image, le marché compte une multitude de produits en marque blanche ou issus de marques peu connues qui ont probablement moins à perdre en termes de réputation.

Externalités

Les conséquences d'une faille de sécurité sur un appareil, un service ou un système IoT n'affectent pas uniquement l'utilisateur, mais aussi tout l'écosystème internet lié. Comme évoqué précédemment, lorsqu'un appareil rejoint un botnet, il peut être utilisé pour lancer des attaques DDoS, envoyer des spams, propager des logiciels malveillants ou héberger des escroqueries par hameçonnage.

Dans bien des cas, la cible de ces attaques n'est pas le propriétaire de l'appareil lui-même, ce qui signifie que les coûts importants qu'elles occasionnent ne sont assumés ni par le fabricant *ni* par le propriétaire, mais par la victime en bout de chaîne (et par extension, par la société en général).

Il s'agit là d'« externalités négatives ». Les externalités négatives sont problématiques dans la mesure où ni le fournisseur, ni le consommateur du produit IoT n'intègre dans ses prises de décisions toutes les répercussions que peuvent avoir ces failles de sécurité.

Mentionnons cependant qu'il existe aussi des externalités *positives* liées aux appareils IoT grand public. Outre leurs avantages pour les utilisateurs, ces produits ont des effets bénéfiques pour la société. Par exemple, les appareils intelligents contribuent à réduire notre consommation globale grâce à leur efficacité énergétique.

Malgré tout, le manque de cyberprotection et les récents problèmes de sécurité liés à l'IoT pourraient dissuader de potentiels acquéreurs : une enquête menée auprès de 2 000 personnes révèle ainsi qu'un consommateur sur cinq n'aurait pas acheté d'appareil ménager intelligent pour cette raison. De quoi gâcher les externalités positives mentionnées plus haut.

Quelles solutions ?

Sous l'effet de ces facteurs économiques, les fabricants sont susceptibles de ne pas suffisamment investir dans la sécurité de leurs produits. Des mesures devront être prises pour compenser ces facteurs et ainsi améliorer le niveau de protection des appareils et services IoT grand public.

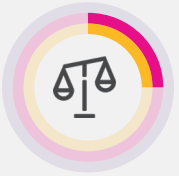
Pour être efficaces, ces solutions nécessiteront vraisemblablement l'implication des pouvoirs publics et du secteur. Elles devront aussi trouver un compromis entre amélioration de la sécurité et création d'un environnement propice à l'innovation et à l'évolution du marché, sans pour autant nuire à l'adoption des technologies.

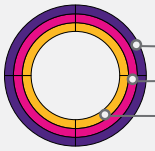
Nous proposons ci-dessous une liste de mesures potentielles visant à atténuer les facteurs économiques identifiés. Ces actions sont résumées dans le tableau suivant (voir Figure 2), hiérarchisé en fonction de notre estimation de leur coût et de leur difficulté de mise en place.

La Figure 2 indique également l'efficacité de chaque mesure en termes d'atténuation (ou de compensation) de chacun des trois facteurs économiques responsables du manque de sécurité de l'IoT grand public : asymétrie d'informations, incitations contradictoires et externalités.

Enfin, notre rapport associé contient une étude plus détaillée des solutions potentielles et propose un ensemble de mécanismes plus généraux visant à améliorer la sécurité de l'IoT grand public.[xi]

Figure 2 : Mesures potentielles et efficacité sur les facteurs économiques responsables du manque de sécurité de l'IoT grand public

Mesure potentielle	Efficacité sur les facteurs économiques
1. Initiatives de sensibilisation aux problèmes de sécurité de l'IoT ; information des consommateurs par les pouvoir publics et le secteur	
2. Spécification par les gouvernements d'un ensemble de critères de sécurité pour leurs propres procédures d'achat	
3. Incitation par le secteur et les pouvoirs publics à la divulgation responsable des vulnérabilités logicielles de l'IoT grand public	
4. Développement par le secteur d'un label de confiance garant d'appareils IoT grand public sécurisés	
5. Définition par les pouvoirs publics d'un ensemble de principes de sécurité pour les appareils IoT grand public (par ex. : prise en charge de mises à jour)	
6. Démarches actives par les pouvoirs publics visant à poursuivre les fabricants ou les fournisseurs de services coupables d'affirmations trompeuses en matière de sécurité	
7. En l'absence d'amélioration concrète de la sécurité de l'IoT grand public malgré ces mesures, intervention des autorités de réglementation pour imposer des exigences de sécurité minimum	



Les mesures 1 à 6 visent à améliorer la sécurité de l'IoT grand public sans intervention majeure du gouvernement. Cependant, si les initiatives des acteurs du secteur ne mènent pas à des améliorations concrètes de la sécurité des appareils, les pouvoirs publics doivent être disposés à imposer des exigences spécifiques pour l'IoT grand public, avec ou sans certification (mesure 7).

La mesure 7 constitue ainsi une extension logique de la mesure 5, à la différence près qu'elle comporte un niveau de spécification technique plus exigeant quant aux obligations de sécurité définies, par exemple : une puissance de chiffrement minimale ou des critères plus précis pour les authentifiants par défaut (par ex. : la longueur du mot de passe).

Toutefois, si ces exigences de sécurité minimum devraient suffire à réduire le risque de cyberattaques, elles pourraient aussi considérablement augmenter le coût de fabrication des appareils. Il deviendrait alors plus onéreux de fournir des mises à jour logicielles régulières, ou de procéder à des tests rigoureux de la sécurité des produits avant leur commercialisation.

Cette hausse des coûts pourrait aussi entraîner une augmentation des prix et par-là même, réduire l'adoption des appareils connectés (diminuant ainsi les bénéfices qu'ils pourraient apporter aux utilisateurs et à la société), et / ou favoriser l'apparition d'un « marché noir » de modèles non conformes. Bref, certaines exigences de sécurité minimum pourraient engendrer plus de « coûts » (en termes de bénéfices perdus) que d'avantages. Étant donné que l'évaluation exacte de ces conséquences, positives comme négatives, s'avèrerait probablement très complexe, nous ne recommandons une mise en place de la mesure 7 qu'en dernier recours, dans l'éventualité où les autres initiatives s'avéreraient inefficaces.

Conclusion

La sécurité informatique de nombreux appareils IoT grand public est insuffisante, faisant d'eux des proies faciles face aux cyberattaques. Les coûts qui en découlent affectent non seulement les propriétaires de ces produits, mais aussi des tiers et d'autres utilisateurs d'Internet.

À la racine de ces problèmes, nous avons identifié des facteurs économiques plutôt que techniques. Tant que ces facteurs économiques sous-jacents ne seront pas traités, des appareils mal protégés continueront d'être produits, vendus et achetés.

Il est important de reconnaître les implications mondiales des failles de sécurité de l'IoT grand public : car même si un pays prend des mesures visant à protéger son marché intérieur, il n'est pas à l'abri des menaces provenant d'autres territoires moins réglementés.

La croissance globale du parc IoT va intensifier les risques et les problèmes transnationaux de sécurité et de confidentialité et à terme, probablement constituer un défi de taille pour les cadres de coopération légale actuels. Il est donc primordial d'encourager les diverses parties prenantes à participer à des initiatives collectives, aux niveaux transnational, régional et mondial, en vue d'améliorer la sécurité de l'IoT grand public.

Les auteurs remercient l'association Internet Society pour sa contribution aux recherches présentées au sein du présent rapport ainsi que pour ses services de révision.

À propos de Plum

À la pointe du marché, Plum est une société de conseil indépendante spécialisée dans les télécommunications, les médias, les technologies et autres secteurs connexes. Nous nous appuyons sur notre maîtrise de l'industrie, notre expérience en conseil et nos analyses rigoureuses pour étudier les défis et les opportunités dans les domaines de la réglementation, du spectre radio, de l'économie, du commerce et de la technologie.

Pour plus d'informations, veuillez nous contacter sur :

www.plumconsulting.co.uk

+44 20 7047 1919
+33 (0)6 23 33 83 97

[i] Cf. https://www.gartner.com/en/newsroom/press-releases/2017-02-07- gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31- percent-from-2016(communiqué de presse de Gartner du 2 juillet 2017 (en anglais) : « Huit milliards d'objets connectés seront en service en 2017, soit 31 % de plus qu'en 2016. »)

[ii] Hewlett Packard (2015), Internet of Things Research Study (Recherche sur l'Internet des Objets), http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050

[iii] F. Loi, et al (2017), Systematically Evaluating Security and Privacy for Consumer IoT Devices (« L'évaluation systématique de la sécurité et de la confidentialité des appareils IoT grand public »), compte-rendu de l'atelier 2017 sur la sécurité et la confidentialité de l'Internet des Objets, IoTS&P '17 pp.1-6, 2017

[iv] Symantec (2018), Internet Security Threat Report – Volume 23 (mars 2018) (Rapport sur les menaces à la sécurité sur Internet – Volume 23), https://www.symantec.com/content/dam/symantec/docs/reports/istr-23- 2018-en.pdf

[v] James Scott et Drew Spaniel (2016), Rise of the Machines : The DYN Attack was just a Practice Run (« Le soulèvement des machines : l'attaque DYN n'était qu'un échauffement »), CreateSpace, ISBN-13 : 978-1540894571

[vi] Ceci s'est notamment produit en 2017 sur des jouets connectés. Cf. http://www.bbc.co.uk/news/technology-39115001

[vii] FTC (2015), Internet of Things – Privacy & Security in a Connected World (« L'Internet des Objets : vie privée et sécurité dans un monde connecté »), Rapport FTC, https://www.ftc.gov/system/files/documents/reports/federal-trade- commission-staff-report-november-2013-workshop-entitled-internet- things-privacy/150127iotrpt.pdf [FTC (2015)]

[viii] https://www.usenix.org/system/files/conference/usenixsecurity17/sec17- antonakakis.pdf

[ix] George A. Akerlof (1970), The Market for "Lemons": Quality Uncertainty and the Market Mechanism (« Le Marché des « tacots » : incertitude sur la qualité et mécanisme de marché »), The Quarterly Journal of Economics, Vol. 84, No 3. (août 1970), pp. 488-500.

[x] Les produits certifiés ZigBee en sont un exemple. Cf. Philipp Morgner et Zinaida Benenson (2018), Exploring Security Economics in IoT Standardization Efforts (« L'économie de la sécurité dans les initiatives de normalisation de l'IoT »), atelier sur la sécurité et les normes de l'IoT décentralisé (DISS) 2018 18 février 2018, San Diego, CA, États-Unis, https://dx.doi.org/10.14722/diss.2018.23009

[xi] Plum Consulting (2019), The economics of the security of consumer-grade IoT products and services (« L'économie de la sécurité des produits et services IoT grand public ») https://plumconsulting.co.uk/the-economics-of-the- security-of-consumer-grade-iot-products-and-services/