Recommandations sur la sécurité et la confidentialité de l'Internet des objets (IoT) RAPPORT DU GROUPE DE TRAVAIL TECHNIQUE SUR L'INTERNET BANDE LARGE (BROADBAND INTERNET TECHNICAL ADVISORY GROUP)

Un rapport d'accord uniforme

Délivré :

Novembre 2016

Droits d'auteur / Avis juridique

À propos du BITAG

Le Broadband Internet Technical Advisory Group (BITAG) est une organisation à but non lucratif, composée de plusieurs parties prenantes, dont l'objectif est de réunir des ingénieurs et des technologues au sein d'un groupe de travail technique (TWG) afin de développer un consensus sur les pratiques de gestion des réseaux à large bande et sur d'autres questions techniques connexes qui peuvent affecter l'expérience Internet des utilisateurs, notamment l'impact vers et depuis les applications, le contenu et les dispositifs qui utilisent l'Internet.

La mission du BITAG comprend : (a) l'éducation des décideurs politiques sur ces questions techniques ; (b) le traitement de questions techniques spécifiques dans le but de minimiser les différends politiques connexes ; et
(c) servir de caisse de résonance pour les nouvelles idées et les pratiques de gestion du réseau. Les fonctions spécifiques du TWG peuvent également inclure : (i) l'identification des "meilleures pratiques" des fournisseurs de large bande et d'autres entités ; (ii) l'interprétation et l'application des pratiques de "sphère de sécurité" ; (iii) la fourniture d'autres conseils techniques à l'industrie et au public ; et/ou (iv) l'émission d'avis consultatifs sur les questions techniques liées à la mission du TWG qui peuvent sous-tendre des différends concernant les pratiques de gestion des réseaux à large bande.

Le groupe de travail technique du GTAB et ses différents comités prennent leurs décisions par consensus, les niveaux d'accord correspondants étant représentés sur la couverture de chaque rapport. Chaque représentant du GTT s'efforce de parvenir à un consensus sur les recommandations que son organisation soutient, bien que, même au niveau d'accord le plus élevé, le consensus du GTAB n'exige pas que toutes les organisations membres du GTT soient d'accord avec chacune des phrases d'un document. Le président de chaque comité GTT détermine si un consensus a été atteint. En cas de désaccord au sein d'un comité quant à l'existence d'un consensus, le GTCV dispose d'un processus de vote permettant d'atteindre et d'indiquer plus formellement différents niveaux d'accord. Pour plus d'informations, veuillez consulter le manuel des groupes de travail techniques du GTCV, disponible sur le site Web du GTCV à l'adresse www.bitag.org.

Les rapports des GTT du GTC BITAG portent essentiellement sur des questions techniques, en particulier celles susceptibles d'être interprétées comme anticoncurrentielles, discriminatoires ou autrement motivées par des facteurs non techniques. Bien que les rapports puissent aborder un large éventail de questions liées à une pratique particulière de gestion de réseau, ils ne sont pas destinés à traiter ou à analyser de manière exhaustive les questions économiques, juridiques, réglementaires ou de politique publique que la pratique peut soulever. Le BITAG accueille volontiers les commentaires du public. N'hésitez pas à soumettre vos commentaires par écrit en envoyant un courriel à comments@bitag.org.

Résumé exécutif

Au cours des dernières années, bon nombre des nouveaux appareils connectés à Internet ne sont pas des ordinateurs personnels, mais plutôt une variété d'appareils intégrant une connectivité et des fonctions Internet. Cette catégorie d'appareils a été généralement décrite comme l'*Internet des objets* (IoT) et a entraîné de nouveaux risques pour la sécurité et la vie privée.

Le terme "IoT" a une portée potentiellement large. L'IoT peut faire référence à des déploiements dans les foyers, les entreprises, les installations de fabrication, les industries du transport et ailleurs. Ainsi, l'IdO peut se référer à bien plus que de simples dispositifs destinés aux consommateurs. Aux fins du présent rapport, nous utilisons le terme IdO pour désigner uniquement les appareils grand public et les systèmes logiciels locaux et distants qui leur sont associés, bien que certaines ou l'ensemble de nos recommandations puissent être applicables de manière plus large. Ce rapport s'intéresse aux scénarios dans lesquels les consommateurs installent, configurent et administrent des appareils qu'ils louent ou possèdent.

Le nombre et la diversité des dispositifs IoT grand public augmentent rapidement ; ces dispositifs offrent de nombreuses nouvelles applications aux utilisateurs finaux, et à l'avenir en offriront probablement encore plus. De nombreux dispositifs IoT sont soit déjà disponibles, soit en cours de développement pour un déploiement dans un avenir proche, notamment :

- des capteurs pour mieux comprendre les schémas de la vie quotidienne et surveiller la santé
- des moniteurs et des commandes pour les fonctions de la maison, des serrures aux systèmes de chauffage et d'eau.
- des dispositifs et des appareils qui anticipent les besoins d'un consommateur et peuvent prendre des mesures pour y répondre (par exemple, des dispositifs qui surveillent les stocks et réorganisent automatiquement les produits pour un consommateur).

Ces dispositifs interagissent généralement avec des logiciels fonctionnant ailleurs sur le réseau et fonctionnent souvent de manière autonome, sans nécessiter d'intervention humaine. En outre, lorsqu'ils sont couplés à l'analyse des données et à l'apprentissage automatique, les dispositifs IoT peuvent être en mesure de prendre des mesures plus proactives, de révéler des schémas de données intéressants et utiles, ou de faire des suggestions aux utilisateurs finaux susceptibles d'améliorer leur santé, leur environnement, leurs finances et d'autres aspects de leur vie.

Bien que les consommateurs soient confrontés à des menaces générales en matière de sécurité et de respect de la vie privée en raison de la présence de *tout* appareil connecté à l'internet, la nature de l'IdO grand public est unique en ce sens qu'elle peut impliquer des consommateurs non techniques ou non intéressés, ce qui complique la découverte et l'inventaire des appareils sur les réseaux domestiques des consommateurs, étant donné que le nombre et la variété des appareils prolifèrent, des effets sur le service d'accès à l'internet du consommateur et d'autres qui fonctionnent sur des liens de réseau partagés, et des effets sur d'autres services dans la mesure où, lorsque les dispositifs IoT sont compromis par des logiciels malveillants, ils peuvent devenir une plateforme pour le trafic de données indésirables - comme le spam et les attaques par déni de service - qui peuvent interférer avec la fourniture de ces autres services.

Plusieurs rapports récents ont montré que certains appareils ne respectent pas les meilleures pratiques rudimentaires en matière de sécurité et de confidentialité. Dans certains cas, des dispositifs ont été compromis et ont permis à des utilisateurs non autorisés d'effectuer une surveillance et un contrôle, d'obtenir un accès ou un contrôle, de provoquer des pannes de dispositifs ou de systèmes, et de déranger ou de harceler des utilisateurs autorisés ou des propriétaires de dispositifs.

Parmi les problèmes potentiels contribuant à l'absence de bonnes pratiques en matière de sécurité et de confidentialité, citons : le manque d'expérience de la chaîne d'approvisionnement IoT en matière de sécurité et de confidentialité, le manque d'incitations à développer et à déployer des mises à jour après la vente initiale, la difficulté d'effectuer des mises à jour logicielles sécurisées sur le réseau, les dispositifs dotés de ressources matérielles limitées ou restreintes (empêchant certaines mesures de sécurité de base ou "de bon sens"), les dispositifs dotés d'interfaces utilisateur limitées ou restreintes (qui, si elles sont présentes, peuvent n'avoir qu'une fonctionnalité minimale) et les dispositifs dotés de logiciels malveillants insérés au cours du processus de fabrication.

L'émergence de l'IdO offre des possibilités d'innovation importantes, des maisons intelligentes aux villes intelligentes. Dans de nombreux cas, des modifications simples des processus de développement, de distribution et de maintenance des appareils peuvent empêcher la distribution d'appareils IoT qui souffrent de problèmes importants de sécurité et de confidentialité. BITAG estime que le respect des lignes directrices décrites dans ce rapport peut améliorer considérablement la sécurité et la confidentialité des dispositifs IoT et minimiser les coûts associés aux dommages collatéraux qui affecteraient autrement les utilisateurs finaux et les FAI. En outre, à moins que le secteur des dispositifs IoT - le secteur de l'industrie qui fabrique et distribue ces dispositifs - n'améliore la sécurité et la confidentialité des dispositifs, la réaction des consommateurs pourrait entraver la croissance du marché de l'IoT et, en fin de compte, limiter les promesses de l'IoT.

Observations. À partir de l'analyse faite dans ce rapport et de l'expérience combinée de ses membres en matière de dispositifs de l'Internet des objets, le groupe de travail technique du BITAG formule les *observations* suivantes :

- **Vulnérabilités de sécurité :** Certains dispositifs IoT sont expédiés "d'usine" avec un logiciel qui est soit obsolète, soit le devient avec le temps. D'autres appareils IoT peuvent être livrés avec un logiciel plus récent, mais des vulnérabilités peuvent être découvertes à l'avenir. Les vulnérabilités découvertes tout au long de la durée de vie d'un dispositif peuvent rendre ce dernier moins sûr au fil du temps, à moins qu'il ne dispose d'un mécanisme de mise à jour ultérieure de son logiciel.

- **Communications non sécurisées :** De nombreuses fonctions de sécurité conçues pour des dispositifs informatiques plus polyvalents sont difficiles à mettre en œuvre sur les dispositifs IoT et un certain nombre de failles de sécurité ont été identifiées sur le terrain, notamment des communications non cryptées et des fuites de données provenant de dispositifs IoT.

    - **Communications non authentifiées :** Certains dispositifs IoT fournissent des mises à jour logicielles automatiques. Sans authentification et chiffrement, cependant, cette approche est insuffisante car le mécanisme de mise à jour pourrait être compromis ou désactivé. En outre, de nombreux dispositifs IoT n'utilisent pas l'authentification au cours de la communication.

    - **Communications non cryptées :** De nombreux dispositifs IoT envoient tout ou partie des données en clair, plutôt que sous une forme chiffrée. Les communications en clair peuvent être observées par d'autres appareils ou par un attaquant.

- **Absence d'authentification et d'autorisation mutuelles :** Un appareil qui permet à une partie inconnue ou non autorisée de modifier son code ou sa configuration, ou d'accéder à ses données, constitue une menace. L'appareil peut révéler que son propriétaire est présent ou absent, faciliter l'installation ou l'exploitation de logiciels malveillants, ou faire en sorte que sa fonction IoT principale soit fondamentalement compromise.
- **Manque d'isolation du réseau :** Ces appareils créent également de nouveaux risques et sont susceptibles de faire l'objet d'attaques *à l'intérieur de* la maison. Étant donné que de nombreux réseaux domestiques n'isolent pas, par défaut, les différentes parties du réseau les unes des autres, un appareil connecté au réseau peut être en mesure d'observer ou d'échanger du trafic avec d'autres appareils sur le même réseau domestique, ce qui permet à un appareil d'observer ou d'affecter le comportement d'appareils non liés.

- **Fuites de données :** Les dispositifs IoT peuvent provoquer des fuites de données privées des utilisateurs, à la fois depuis le cloud (où les données sont stockées) et entre les dispositifs IoT eux-mêmes.
  - **Fuites dans le nuage :** Les services hébergés dans le cloud pourraient subir une violation de données due à une attaque externe ou à une menace interne. En outre, si les utilisateurs s'appuient sur des méthodes d'authentification ou de cryptage faibles pour ces services hébergés dans le cloud, les données des utilisateurs peuvent également être compromises.
  - **Fuites depuis et entre les appareils :** Dans certains cas, les appareils situés sur le même réseau ou sur des réseaux voisins peuvent être en mesure d'observer les données d'autres appareils, comme le nom des personnes présentes dans un foyer, l'emplacement géographique précis d'un foyer, ou même les produits qu'un consommateur achète.

- **Susceptibilité à l'infection par des logiciels malveillants et autres abus : Les** logiciels malveillants et autres formes d'abus peuvent perturber le fonctionnement des dispositifs IoT, obtenir un accès non autorisé ou lancer des attaques.

- **Possibilité d'interruption de service :** La perte potentielle de disponibilité ou de connectivité diminue non seulement la fonctionnalité des dispositifs IoT, mais peut également dégrader la sécurité des dispositifs dans certains cas, notamment lorsqu'un dispositif IoT ne peut plus fonctionner sans cette connectivité (par exemple, un système d'alarme domestique se désactivant en cas de perte de connectivité).

- **Possibilité de persistance des problèmes de sécurité et de confidentialité des appareils : Les** problèmes de sécurité des dispositifs IoT sont susceptibles de persister car de nombreux dispositifs peuvent ne jamais recevoir de mise à jour logicielle, soit parce que le fabricant (ou une autre partie de la chaîne d'approvisionnement IoT, ou le fournisseur de services IoT) peut ne pas fournir de mises à jour, soit parce que les consommateurs peuvent ne pas appliquer les mises à jour déjà disponibles.
  - **De nombreux dispositifs IoT ne seront jamais corrigés :** Le déploiement de mises à jour logicielles qui corrigent les vulnérabilités de sécurité critiques est difficile en général. De nombreux vendeurs et fabricants de dispositifs ne disposent pas de systèmes ou de processus permettant de déployer des mises à jour logicielles sur des milliers de dispositifs, et le déploiement par réseau

Il est difficile d'apporter des mises à jour aux appareils qui fonctionnent dans les foyers des consommateurs, car les mises à jour peuvent parfois interrompre le service et ont parfois le potentiel de "briquer" l'appareil, si elles ne sont pas effectuées correctement. En outre, certains appareils peuvent même ne pas être en mesure d'effectuer des mises à jour logicielles.

- **Les mises à jour logicielles ne se limitent pas aux bogues :** Les mises à jour logicielles ne sont pas simplement destinées à corriger des bogues de sécurité ou de confidentialité. Elles peuvent également être destinées à introduire de nouvelles fonctions importantes ou à améliorer les performances et la sécurité.
- **Les consommateurs sont peu enclins à mettre à jour le logiciel des dispositifs IoT :** Peu d'utilisateurs finaux mettent systématiquement à jour le logiciel des appareils de leur propre chef ; il est préférable de supposer que la plupart des utilisateurs finaux ne prendront jamais d'initiative pour mettre à jour le logiciel.

- **Le remplacement du dispositif peut être une alternative aux mises à jour logicielles - pour les dispositifs peu coûteux ou "jetables" :** Dans certains cas, le remplacement complet d'un appareil peut être une alternative aux mises à jour logicielles. Certains dispositifs IoT peuvent être si peu coûteux que la mise à jour du logiciel peut être peu pratique ou non rentable.

Recommandations. Le groupe de travail technique du BITAG dispose également des éléments suivants *recommandations* :

- **Les dispositifs IoT devraient utiliser les meilleures pratiques logicielles actuelles :**
  - **Les dispositifs IoT devraient être livrés avec un logiciel raisonnablement à jour :** BITAG recommande que les dispositifs IoT soient livrés aux clients ou aux points de vente au détail avec un logiciel raisonnablement à jour qui ne contient pas de vulnérabilités graves et connues.
  - **Les dispositifs IoT doivent disposer d'un mécanisme de mise à jour logicielle automatisée et sécurisée :** Les bugs logiciels doivent être réduits au minimum, mais ils sont inévitables. Ainsi, il est essentiel qu'un dispositif IoT dispose d'un mécanisme de mises à jour logicielles automatiques et sécurisées. BITAG recommande aux fabricants de dispositifs IoT ou aux fournisseurs de services IoT de concevoir leurs dispositifs et systèmes en partant du principe que de nouveaux bogues et vulnérabilités seront découverts au fil du temps. Ils devraient concevoir des systèmes et des processus pour assurer la mise à jour automatique des logiciels des appareils IoT, sans exiger ou attendre un quelconque type d'action de la part de l'utilisateur, ni même d'opt-in de sa part.
  - **Les dispositifs IoT devraient utiliser une authentification forte par défaut :** BITAG recommande que les dispositifs IoT soient sécurisés par défaut (par exemple, protégés par un mot de passe) et n'utilisent pas de noms d'utilisateur et de mots de passe courants ou facilement devinables (par exemple, "admin", "password").
  - **Les configurations des dispositifs IoT doivent être testées et renforcées :** Certains dispositifs IoT permettent à un utilisateur de personnaliser le comportement de l'appareil. BITAG recommande aux fabricants de tester la sécurité de chaque appareil avec un éventail de configurations possibles, par opposition à la simple configuration par défaut.

- **Les dispositifs IoT devraient suivre les meilleures pratiques en matière de sécurité et de cryptographie :** BITAG recommande aux fabricants de dispositifs IoT de sécuriser les communications en utilisant la sécurité de la couche de transport (TLS) ou la cryptographie légère (LWC). Si les appareils s'appuient sur une infrastructure à clé publique (PKI), alors une entité autorisée doit être en mesure de révoquer les certificats lorsqu'ils sont compromis, et les fabricants doivent veiller à éviter les méthodes de cryptage, les protocoles et les tailles de clé présentant des faiblesses connues. Parmi les autres bonnes pratiques de cryptage, citons
    - Cryptage des communications de configuration (commande et contrôle) par défaut
    - Communications sécurisées vers et depuis les contrôleurs IoT
    - Cryptage du stockage local des données sensibles
    - Authentifier les communications, les modifications de logiciels et les demandes de données
    - Utilisez des informations d'identification uniques pour chaque appareil
    - Utilisez des informations d'identification qui peuvent être mises à jour
    - Fermer les ports inutiles et désactiver les services inutiles
    - Utilisez des bibliothèques qui sont activement entretenues et soutenues.

- **Les appareils IoT doivent communiquer de manière restrictive plutôt que permissive :** Dans la mesure du possible, les appareils ne doivent pas être joignables par défaut via des connexions entrantes. Les dispositifs IoT ne doivent pas s'appuyer uniquement sur le pare-feu du réseau pour restreindre la communication, car certaines communications entre dispositifs au sein de la maison peuvent ne pas traverser le pare-feu.

- **Les dispositifs IoT devraient continuer à fonctionner si la connectivité Internet est interrompue :** BITAG recommande qu'un dispositif IoT devrait être en mesure d'exécuter sa ou ses fonctions primaires (par exemple, un interrupteur d'éclairage ou un thermostat devrait continuer à fonctionner avec des commandes manuelles), même s'il n'est pas connecté à Internet, car la connectivité Internet peut être interrompue pour des causes allant d'une mauvaise configuration accidentelle à une attaque intentionnelle. Les dispositifs IoT qui ont des implications pour la sécurité des utilisateurs devraient continuer à fonctionner en mode déconnecté afin de protéger la sécurité des consommateurs.

- **Les appareils IoT devraient continuer à fonctionner si le back-end du cloud tombe en panne :** De nombreux services qui dépendent ou utilisent un back-end de cloud peuvent continuer à fonctionner, même dans un état dégradé ou partiellement fonctionnel, lorsque la connectivité au back-end de cloud est interrompue ou que le service lui-même tombe en panne.

- **Les dispositifs IoT doivent prendre en charge les meilleures pratiques d'adressage et de nommage :** De nombreux dispositifs IoT peuvent rester déployés pendant un certain nombre d'années après leur installation. La prise en charge des derniers protocoles d'adressage et de nommage permettra à ces appareils de rester fonctionnels pendant des années.
    - **IPv6 :** BITAG recommande que les dispositifs IoT prennent en charge la version la plus récente du protocole Internet, IPv6.

- **DNSSEC :** BITAG recommande que les dispositifs IoT prennent en charge l'utilisation ou la validation des extensions de sécurité DNS (DNSSEC) lorsque des noms de domaine sont utilisés.

- **Les dispositifs IoT devraient être livrés avec une politique de confidentialité facile à trouver et à comprendre :** BITAG recommande que les dispositifs IoT soient livrés avec une politique de confidentialité, mais cette politique doit être facile à trouver et à comprendre pour un utilisateur type.

- **Divulguer les droits de réduire à distance les fonctionnalités d'un dispositif IoT :** BITAG recommande que si la fonctionnalité d'un dispositif IoT peut être diminuée à distance par un tiers, comme par le fabricant ou le fournisseur de services IoT, cette possibilité doit être clairement indiquée à l'utilisateur au moment de l'achat.

- **L'industrie des dispositifs IoT devrait envisager un programme industriel de cybersécurité :** Le BITAG recommande que l'industrie des dispositifs IoT ou un groupe connexe d'électronique grand public envisage la création d'un programme soutenu par l'industrie, dans le cadre duquel une sorte de logo ou de mention "Secure IoT Device" pourrait figurer sur les emballages de vente au détail des dispositifs IoT. Un ensemble de meilleures pratiques soutenues par l'industrie semble être le moyen le plus pragmatique d'équilibrer l'innovation dans l'IdO avec les défis de sécurité associés à la nature fluide de la cybersécurité, et d'éviter la "mentalité de liste de contrôle" qui peut se produire avec les processus de certification.

- **La chaîne d'approvisionnement IoT devrait jouer son rôle dans la résolution des problèmes de sécurité et de confidentialité de l'IoT :** Les utilisateurs finaux des appareils IoT dépendent de la chaîne d'approvisionnement IoT, du fabricant au détaillant, pour protéger leur sécurité et leur vie privée, et certaines ou toutes les parties de cette chaîne d'approvisionnement IoT jouent un rôle essentiel tout au long du cycle de vie du produit. En plus des autres recommandations de cette section, BITAG recommande que la chaîne d'approvisionnement IoT prenne les mesures suivantes :

    - **Politique de confidentialité :** Les appareils doivent avoir une politique de confidentialité claire et compréhensible, en particulier lorsqu'un appareil est vendu en même temps qu'un service continu.

    - **Mécanisme de réinitialisation :** Les appareils devraient disposer d'un mécanisme de réinitialisation pour les appareils IoT qui efface toute la configuration à utiliser lorsqu'un consommateur retourne ou revend l'appareil. Les fabricants de dispositifs devraient également fournir un mécanisme permettant de supprimer ou de réinitialiser toutes les données que le dispositif respectif stocke dans le cloud.

    - **Système de signalement des bogues : Les** fabricants doivent fournir un système de rapport de bogues avec des mécanismes de soumission de bogues bien définis et une politique de réponse documentée.

    - **Chaîne d'approvisionnement en logiciels sécurisés :** Les fabricants doivent protéger la chaîne d'approvisionnement en logiciels sécurisés afin d'empêcher l'introduction de logiciels malveillants au cours du processus de fabrication ; les vendeurs et les fabricants doivent prendre les mesures appropriées pour sécuriser leur chaîne d'approvisionnement en logiciels.

- **Prise en charge de l'appareil IoT pendant toute sa durée de vie :** Les fabricants doivent prendre en charge un dispositif IoT tout au long de sa durée de vie, depuis sa conception jusqu'au moment où il est mis hors service, en faisant preuve de transparence sur la période pendant laquelle ils prévoient de fournir une assistance continue à un dispositif, et sur ce que le consommateur doit attendre de la fonction du dispositif à la fin de sa durée de vie.
- **Méthodes de contact claires :** Les fabricants doivent fournir des méthodes claires permettant aux consommateurs de déterminer qui ils peuvent contacter pour obtenir de l'aide et des méthodes pour contacter les consommateurs afin de diffuser des informations sur les vulnérabilités des logiciels ou d'autres problèmes.
- **Signaler la découverte et la correction des vulnérabilités :** Les fabricants doivent signaler la découverte et la correction des vulnérabilités logicielles qui menacent la sécurité ou la vie privée des consommateurs.
- **Processus clair de signalement des vulnérabilités : Les** fabricants doivent fournir un processus de signalement des vulnérabilités avec un formulaire de signalement des vulnérabilités bien défini, facile à trouver et sécurisé, ainsi qu'une politique de réponse documentée.

Table des matières

1 Introduction

Au cours des dernières années, bon nombre des nouveaux appareils connectés à l'Internet ne sont pas des ordinateurs personnels, mais plutôt une variété d'appareils intégrant une connectivité et des fonctions Internet. Parmi ces appareils, on peut citer les thermostats, les prises intelligentes et les caméras en réseau. Cette catégorie d'appareils est généralement décrite comme l'*Internet des objets* (IoT), et il est clair que cette nouvelle catégorie d'appareils connaîtra une forte croissance dans les années à venir, avec des estimations variables selon les sources, mais toutes prévoient plusieurs milliards de ces appareils d'ici 2020 [1].

Le nombre et la diversité des dispositifs IoT augmentent rapidement ; ces dispositifs offrent de nombreuses nouvelles applications aux utilisateurs finaux, et en offriront encore plus à l'avenir. De nombreuses solutions IoT sont soit déjà disponibles, soit en cours de développement pour un déploiement dans un avenir proche, notamment :

- des capteurs pour mieux comprendre les schémas de la vie quotidienne et surveiller la santé
- des moniteurs et des commandes pour les fonctions de la maison, des serrures aux systèmes de chauffage et d'eau.
- des dispositifs et des appareils qui anticipent les besoins d'un consommateur et peuvent prendre des mesures pour y répondre (par exemple, des dispositifs qui surveillent les stocks et réorganisent automatiquement les produits pour un consommateur).

En outre, lorsqu'ils sont couplés à l'analyse des données et à l'apprentissage automatique, les dispositifs IoT peuvent être en mesure de prendre des mesures plus proactives, d'exposer des modèles de données intéressants ou de faire des suggestions aux utilisateurs finaux susceptibles d'améliorer leur santé, leur environnement, leurs finances et d'autres aspects de leur vie.

L'émergence de l'IdO offre des possibilités d'innovation importantes, des maisons intelligentes aux villes intelligentes. Malheureusement, de nombreux dispositifs IoT ont été livrés avec de graves défauts de sécurité et de confidentialité [2] ; la section 3 examine en détail de nombreux exemples récents. Ces failles font courir de nombreux risques aux utilisateurs finaux qui achètent les dispositifs et peuvent affecter le service d'accès à l'internet de l'utilisateur des dispositifs et des autres utilisateurs dont le trafic passe par les mêmes liens internet partagés. Les failles créent également des problèmes de sécurité et d'atténuation plus larges pour les cibles des attaques, les fournisseurs d'accès à Internet (FAI), ainsi que d'autres fournisseurs de services - par exemple les services de moteurs de recherche, la messagerie électronique et les sites de jeux - et introduisent de manière importante de nouveaux coûts de support et d'atténuation (qui sont généralement répercutés sur les utilisateurs finaux) [3]. Des coûts supplémentaires peuvent également être imposés aux fabricants de dispositifs eux-mêmes, qui devront peut-être prendre des mesures pour atténuer ces problèmes.

Dans de nombreux cas, des modifications simples des processus de développement, de distribution et de maintenance des appareils peuvent empêcher la distribution d'appareils IoT qui souffrent de problèmes importants de sécurité et de confidentialité. BITAG estime que le respect des lignes directrices décrites dans ce rapport peut améliorer considérablement la sécurité et la confidentialité des dispositifs IoT et minimiser les coûts associés aux dommages collatéraux qui affecteraient autrement les utilisateurs finaux et les FAI. En outre, à moins que le secteur des dispositifs IoT - le secteur de l'industrie qui fabrique et distribue ces dispositifs - n'améliore la sécurité et la confidentialité des dispositifs, les réactions des consommateurs pourraient entraver la croissance du marché de l'IoT et, en fin de compte, limiter les promesses de l'IoT pour les utilisateurs finaux.

2 Qu'est-ce que l'Internet des objets ?

L'internet des objets (IoT) comprend des dispositifs qui fonctionnent comme des capteurs, des actionneurs, des contrôleurs et des enregistreurs d'activité. Ces dispositifs interagissent généralement avec un logiciel fonctionnant ailleurs sur le réseau, par exemple sur un téléphone mobile, un dispositif informatique universel (par exemple, un ordinateur portable), une machine sur l'Internet public (par exemple, dans le "nuage"), ou une combinaison de ces éléments. Les dispositifs IoT fonctionnent souvent de manière autonome, sans nécessiter d'intervention humaine.

Le terme "IoT" a une portée potentiellement large. L'IoT peut faire référence à des déploiements dans les foyers, les entreprises, les installations de fabrication, les industries du transport et ailleurs. Ainsi, l'IdO peut se référer à bien plus que de simples appareils destinés aux consommateurs.

Aux fins du présent rapport, le terme IdO est utilisé pour désigner uniquement les appareils destinés aux consommateurs et les systèmes logiciels1 locaux et distants qui leur sont associés, bien que certaines ou l'ensemble de nos recommandations puissent être applicables de manière plus large. Le présent rapport s'intéresse aux scénarios dans lesquels les consommateurs installent, configurent et administrent des dispositifs qu'ils louent ou possèdent.

2.1 Limites du champ d'application

Le rapport ne prend pas directement en compte les dispositifs destinés à des environnements industriels ou interentreprises, tels que les capteurs des réseaux d'hôtels ou d'aéroports, les villes intelligentes, l'automatisation industrielle, le contrôle des bâtiments commerciaux ou le contrôle des stocks de fabrication. Dans ces contextes, les clients disposent souvent des ressources et des incitations nécessaires pour spécifier et gérer les fonctions de sécurité et de confidentialité des produits qu'ils achètent. En outre, bon nombre de ces appareils utilisent des connexions sans fil commerciales qui ne permettent pas un accès complet à l'Internet. Ceci étant dit, certaines des questions abordées dans ce rapport peuvent également être présentes dans ces environnements.

Le champ d'application de ce rapport est également limité aux dispositifs IoT qui sont à l'origine ou à la fin d'un flux de données. Plus précisément, le rapport ne s'intéresse pas aux dispositifs qui traversent un trafic qui peut contenir des données à destination ou en provenance de dispositifs IoT, parmi d'autres trafics, comme une passerelle domestique, un point d'accès sans fil ou un routeur.

En outre, le rapport se concentre uniquement sur les dispositifs et les systèmes qui utilisent le protocole Internet (IP), qu'il s'agisse d'IPv4 ou d'IPv6 ou des deux. Divers dispositifs IoT utilisent d'autres mécanismes de transport, tels que Zigbee 1.0 [4], X10 [5], etc. Ces appareils ne peuvent pas être connectés à Internet autrement que par l'intermédiaire d'un dispositif qui effectue une conversion de protocole. Ils fonctionnent sur un réseau isolé. Toutefois, les présentes recommandations s'appliquent toujours au dispositif qui effectue la conversion de protocole (par exemple, le concentrateur ou la passerelle domotique).

Ce rapport se concentre sur les problèmes spécifiques aux dispositifs d'un réseau IP local qui peuvent communiquer sur Internet. Les problèmes de confidentialité et de sécurité qui surviennent sur des réseaux isolés qui n'ont pas de connexion à l'Internet public sont hors de portée de ce rapport.

2.2 Dispositifs IoT que les utilisateurs ont modifiés

Le logiciel de certains appareils peut être mis à jour ou remplacé par un logiciel autre que celui prévu par le fabricant, créant ainsi, à bien des égards, un nouveau produit. Par exemple, un utilisateur peut installer un logiciel libre sur un appareil, au lieu d'utiliser le logiciel fourni par le fabricant. Le produit qui en résulte peut être soumis aux considérations et recommandations du présent rapport, mais dans ce cas, le dispositif doit être considéré comme un produit distinct dont l'utilisateur est responsable.

[1] Lorsque BITAG utilise le terme "logiciel", il s'agit d'inclure le micrologiciel du dispositif, qui est une forme de logiciel, et tous les autres types de logiciels.

3 Pourquoi la sécurité et la confidentialité de l'IdO présentent un intérêt particulier

Les dispositifs IoT sont confrontés aux mêmes types de défis en matière de sécurité et de confidentialité que de nombreux dispositifs conventionnels destinés aux utilisateurs finaux. D'autre part, les dispositifs IoT n'offrent généralement ni contrôles clairs ni documentation pour informer un utilisateur des risques introduits lors du déploiement de ces dispositifs. En outre, des études ont montré que le fait de s'appuyer sur l'utilisateur final pour prendre des décisions en matière de sécurité et de confidentialité est susceptible d'échouer [6, 7, 8].

3.1 Consommateurs non techniques ou non intéressés.

Les utilisateurs finaux ne disposent pas de l'expertise technique nécessaire pour évaluer les implications en matière de confidentialité et de sécurité d'un dispositif IoT particulier, ou bien ils peuvent ne pas avoir envie de le faire [9]. En outre, le plus souvent, les dispositifs déployés ne disposent pas de mécanismes automatisés pour effectuer des mises à jour sécurisées ou appliquer la politique de sécurité [9,10].

3.2 La découverte et l'inventaire des appareils sont difficiles.

Les consommateurs ont déjà du mal à identifier et à dépanner les appareils qui sont actuellement connectés à leurs réseaux domestiques [11]. Les dispositifs IoT vont exacerber cette situation, car les consommateurs connectent une variété de plus en plus grande de dispositifs à leurs réseaux domestiques.
Au fil du temps, les utilisateurs perdront probablement la trace des appareils connectés à l'Internet, ce qui rendra leur sécurisation encore plus difficile. En outre, les FAI auront du mal à aider les consommateurs à identifier les sources des problèmes de sécurité. Bien que les FAI puissent être en mesure de déterminer qu'un dispositif du réseau domestique d'un client est compromis, ils peuvent être incapables d'identifier le dispositif spécifique compromis, en raison de technologies telles que la traduction d'adresse réseau (NAT) et d'autres technologies qui peuvent masquer l'identité des dispositifs individuels.

3.3 Effets sur le service d'accès à Internet.

Les dispositifs IoT compromis par des logiciels malveillants (voir les sections 4.5 et 5.3) peuvent affecter le service d'accès à Internet à la fois de l'utilisateur de ces dispositifs IoT et des autres utilisateurs dont le trafic passe par les mêmes liens Internet partagés. Ces appareils peuvent également présenter une menace pour l'utilisateur et les autres cibles du malware [12]. Ce logiciel malveillant peut être utilisé pour lancer des attaques DDoS [13],

envoyer des spams, attaquer d'autres dispositifs sur le réseau de l'utilisateur ou interférer de manière malveillante avec le service d'accès à Internet de l'utilisateur.

Ces problèmes augmentent les coûts supportés par le FAI, qui doit s'efforcer d'atténuer ces attaques, de fournir un service d'assistance aux utilisateurs qui ne parviennent pas à déterminer pourquoi leur service d'accès à Internet se comporte mal ou anormalement, voire de désactiver le service d'accès à Internet des utilisateurs dont les appareils se livrent à des activités réseau malveillantes. Ces problèmes augmentent également les coûts pour le consommateur en dégradant les performances et en créant un risque de perte d'identifiants. Enfin, ils imposent des coûts à la cible de toute attaque de ce type et aux fabricants de dispositifs IoT eux-mêmes (ou à d'autres parties de la chaîne d'approvisionnement IoT), qui peuvent être amenés à prendre des mesures pour atténuer ces problèmes

3.4 Effets sur les autres services.

Les appareils IoT compromis par des logiciels malveillants peuvent devenir une plateforme pour le trafic indésirable, comme le spam et les attaques par déni de service - y compris les attaques par réflexion et amplification, par lesquelles un attaquant envoie du trafic à un appareil avec l'adresse source usurpée d'une victime, ce qui amène l'appareil à envoyer de grandes quantités de trafic vers la victime) [14] - ce qui peut interférer avec la capacité d'un fournisseur de services à fournir un service [15]. Les dispositifs compromis peuvent également être utilisés pour écouter le trafic du réseau local ou comme "tremplin" pour attaquer d'autres dispositifs et services sur le réseau local du client, créant ainsi un risque de fuite de données. Les fournisseurs qui proposent des services tels que des moteurs de recherche, des courriers électroniques en ligne et des sites de jeux doivent investir des ressources pour atténuer ces attaques. Les victimes de ces attaques supporteront également des coûts financiers et de confidentialité. Les appareils IoT compromis peuvent aussi occasionnellement affecter le modèle économique d'un fournisseur de services. Le malware DNSChanger, qui permettait aux attaquants d'insérer leurs propres publicités dans les pages web des victimes, en est un exemple [16].

4 De nombreux appareils ne respectent pas les meilleures pratiques en matière de sécurité et de confidentialité

Les dispositifs IoT sont déjà devenus une plateforme d'abus et d'attaques. De nombreux technologues ont découvert divers risques pour la sécurité et la confidentialité associés aux dispositifs IoT disponibles aujourd'hui [17, 18, 19, 20, 21, 22, 23, 24]. Des dizaines de millions de dispositifs IdO supplémentaires seront probablement déployés au cours des prochaines années, ce qui pourrait constituer une vaste plate-forme pour lancer des attaques, à la fois sur d'autres dispositifs au domicile de l'utilisateur et sur l'Internet en général, et pour collecter subrepticement des informations privées sur des utilisateurs finaux ou des groupes d'utilisateurs spécifiques.
Outre les pertes que peuvent subir les consommateurs, les FAI peuvent subir une augmentation des appels à l'assistance technique et des attaques, ce qui augmente le coût des opérations qui est répercuté sur les consommateurs.

Plusieurs rapports récents ont étudié les caractéristiques de sécurité et de confidentialité des dispositifs IoT et ont constaté que certains dispositifs ne respectent pas les meilleures pratiques rudimentaires en matière de confidentialité et de sécurité [25, 26, 27, 28, 29, 30, 31]. Dans certains cas, les dispositifs ont été compromis [32].

Les problèmes potentiels contribuant à ce manque de bonnes pratiques en matière de confidentialité et de sécurité sont les suivants :

4.1 Manque d'incitations à développer et à déployer des mises à jour après la vente initiale.

Pour les appareils IoT grand public vendus par les canaux de vente au détail, les fournisseurs d'appareils peuvent être peu incités à fournir des mises à jour logicielles après la vente initiale. Si le revenu d'un appareil provient uniquement de la vente initiale, alors toute maintenance de l'appareil érode ce revenu initial, diminuant ainsi le bénéfice. Cette structure peut encourager l'obsolescence planifiée, où les fournisseurs donnent la priorité à la vente de nouveaux appareils plutôt qu'au soutien des appareils existants.

4.2 Difficulté des mises à jour sécurisées des logiciels via le réseau.

Les appareils IoT peuvent ne pas être conçus et configurés pour recevoir des mises à jour logicielles sécurisées sur le réseau, ce qui entraîne des processus de mise à jour fastidieux.

4.3 Dispositifs avec des ressources limitées

Les dispositifs IoT vendus dans un environnement de consommation à faible marge peuvent être conçus avec des ressources matérielles limitées. Par conséquent, certaines mesures de sécurité de base telles que le chiffrement, la vérification des signatures logicielles et le contrôle d'accès sécurisé ne sont pas réalisables. Ainsi, les conceptions qui limitent les capacités de traitement et de mémoire d'un appareil peuvent empêcher l'exécution d'un logiciel de sécurité basé sur l'hôte ou empêcher sa mise à niveau en toute sécurité. La section 5.1 aborde cette question de manière plus détaillée.

4.4 Dispositifs à interfaces limitées

De nombreux types de dispositifs IoT ont des interfaces utilisateur limitées ou inexistantes. Même lorsqu'un dispositif expose une interface utilisateur via un dispositif secondaire (par exemple, une application pour smartphone), sa fonctionnalité peut être minimale. Par conséquent, des tâches telles que la configuration d'un pare-feu local ou la désactivation de services distants peuvent être impossibles. Les dispositifs peuvent également ne pas avoir la capacité d'afficher des conditions d'erreur et des alertes significatives pour les utilisateurs qui peuvent utiliser les informations d'erreur pour mieux protéger un dispositif.

4.5 Appareils avec des logiciels malveillants insérés pendant la fabrication.

Les logiciels malveillants peuvent être insérés dans les appareils au moment de la fabrication ou de l'emballage par des employés du fabricant ou d'autres personnes ayant accès à l'environnement de fabrication ou d'emballage. Un dispositif compromis peut souvent sembler fonctionner normalement, auquel cas la violation de la sécurité ou de la vie privée peut persister jusqu'à ce que la compromission soit détectée. Les pare-feu et l'isolation du réseau ne peuvent pas se défendre contre les attaques lancées par ces dispositifs compromis sur d'autres dispositifs internes au réseau isolé. Pour des exemples connus de tels dispositifs compromis et une discussion supplémentaire sur les effets des logiciels malveillants, voir la section 5.3.

4.6 Manque d'expérience des fabricants en matière de sécurité et de confidentialité

De nombreux fabricants d'appareils IoT (et d'autres parties de la chaîne d'approvisionnement IoT) n'ont aucune expérience préalable de la conception, du développement ou de la maintenance des appareils connectés à Internet ou de la manipulation des données des consommateurs. Ces fabricants manquent de cycles de développement sécurisés, d'équipes de réponse aux incidents et d'expérience en matière de confidentialité et d'ingénierie de la sécurité en général.

4.7 Risques dus aux dispositifs vulnérables

Les exemples suivants illustrent la portée et l'étendue des problèmes possibles lorsque les dispositifs IoT deviennent vulnérables aux attaques contre la sécurité et la vie privée. Un utilisateur non autorisé peut être en mesure de :

- **Effectuer une surveillance et un contrôle non autorisés.**
    - savoir si une personne spécifique est à la maison, quelle pièce elle occupe et quand elle entre dans la maison
    - savoir quels autres appareils sont connectés au réseau domestique, et comment les utilisateurs interagissent avec eux
    - activer à distance un microphone ou une caméra sur un appareil pour écouter ou espionner quelqu'un [33].
    - découvrir si une porte ou un garage a été récemment ouvert et fermé afin de déterminer si quelqu'un est à la maison, pour aider à une effraction physique
    - installer un logiciel malveillant sur une caméra IoT pour accéder au flux vidéo de la caméra [34].

- **Obtenir un accès ou un contrôle non autorisé.**
    - éteindre un thermostat pendant les mois d'hiver pour provoquer l'éclatement des conduites d'eau et endommager une maison.
    - d'allumer ou d'éteindre des lumières, par exemple en éteignant l'éclairage du périmètre pour faciliter une effraction physique
    - déverrouiller des portes pour aider à une intrusion physique
    - suppression d'une alarme provenant d'un capteur de porte ou de fenêtre
    - réaffecter un appareil à un usage illicite (par exemple, comme mineur de bitcoins [35])

- **Provoquer des pannes de dispositifs ou de systèmes.**
    - activer des systèmes de climatisation résidentiels pour créer une surtension inattendue sur un réseau électrique dans le but de créer des conditions de brownout ou de blackout
    - subvertir les capteurs de collecte de données de santé pour modifier les données de santé telles que la pression artérielle, la glycémie ou les informations sur le poids qui peuvent être transmises à un service de surveillance de la santé ou à un dispositif médical (tel qu'une pompe à insuline)
    - émuler le logiciel de gestion de l'appareil de manière à ce qu'il semble fonctionner normalement, mais au lieu de cela, désactiver des fonctionnalités importantes ou apporter d'autres modifications de fonctionnement, ce qui entraîne des défaillances importantes de l'équipement ou des systèmes matériels [36] .

- empêcher un thermostat de contrôler le chauffage ou la climatisation d'un bâtiment, ce qui entraîne une chaleur ou un froid extrême.

- **Déranger ou harceler les utilisateurs.**
  - activer à distance un haut-parleur et se livrer à des menaces verbales ou à du harcèlement
  - activer les détecteurs de fumée ou autres détecteurs de sécurité

Tous ces scénarios créent de sérieux risques pour la sécurité et la vie privée des utilisateurs finaux et pour l'internet dans son ensemble. Certains risques pour la sécurité et la vie privée des utilisateurs finaux pourraient également permettre une nouvelle forme de harcèlement numérique. Dans des cas extrêmes, la subversion de la collecte de données sur la santé pourrait entraîner des blessures ou la mort. Dans le cas d'appareils largement déployés, les risques pour la sécurité peuvent être cumulés sur des centaines ou des milliers d'appareils pour créer des attaques distribuées sur les infrastructures critiques.

Les problèmes de sécurité et de respect de la vie privée liés aux dispositifs IoT pourraient, à terme, limiter la croissance future du secteur IoT. Un petit nombre d'incidents très médiatisés pourrait réduire la demande de dispositifs IoT ou limiter la croissance et le potentiel de l'IoT. Il est donc essentiel de résoudre ces problèmes pour soutenir la santé, le dynamisme et la croissance à long terme du marché de l'IdO.

5 Observations sur les questions de sécurité et de confidentialité de l'IdO

Il n'est pas réaliste d'attendre des fabricants qu'ils créent des produits logiciels exempts de bogues ; tous les logiciels ont des bogues, et produire des logiciels exempts de tels défauts reste un problème non résolu. Par conséquent, certains appareils IoT sortent de l'usine avec des logiciels qui sont ou deviennent obsolètes au fil du temps. Il ne s'agit pas d'expédier des logiciels bogués, ce qui est sans doute inévitable ; le problème est plutôt que les fabricants peuvent expédier des appareils avec des logiciels obsolètes qui contiennent de nombreuses vulnérabilités de sécurité importantes et documentées, dont certaines peuvent être immédiatement exploitables lorsque l'appareil est connecté à Internet pour la première fois [37].

D'autres dispositifs IoT peuvent être livrés avec un logiciel plus récent qui ne contient aucune vulnérabilité de sécurité majeure connue au moment de l'expédition. Même dans ces cas, des vulnérabilités peuvent être découvertes à l'avenir, ce qui peut rendre un appareil moins sûr au fil du temps, à moins qu'il ne dispose d'un mécanisme de mise à jour ultérieure de son logiciel. Malheureusement, de nombreux dispositifs IoT ne disposent pas de mécanismes de mise à jour logicielle sécurisés et automatisés permettant de corriger les vulnérabilités une fois que les dispositifs ont été expédiés et déployés. [2] Sans l'adoption généralisée de méthodes de mise à jour logicielle automatisée et sécurisée, le nombre de dispositifs IoT non sécurisés et compromis risque d'augmenter considérablement dans les années à venir.

Les dispositifs IoT qui sont livrés avec des problèmes de sécurité et de confidentialité ou qui les développent au fil du temps peuvent créer une nouvelle population de dispositifs qui peuvent être utilisés par des pirates malveillants, par exemple pour mener des attaques par réflexion et amplification [41]. Non seulement ces dispositifs présentent des risques pour leurs propriétaires, mais ils peuvent également être exploités pour abuser d'autres parties. La sécurité des dispositifs IoT intéresse donc non seulement les fabricants (et les autres parties de la chaîne d'approvisionnement IoT) et les clients des dispositifs IoT, mais aussi l'Internet au sens large.

Enfin, bien que ce rapport fournisse de nombreux exemples de dispositifs IoT qui présentent ou ont présenté des problèmes de sécurité ou de confidentialité, dans de nombreux cas, les exemples soulignés ici peuvent avoir été traités par les parties concernées avant la publication de ce rapport.

5.1 Communications réseau non sécurisées

Les dispositifs IoT en général peuvent être assez limités en ressources, n'ayant pas la puissance de calcul et la bande passante des dispositifs informatiques plus conventionnels tels que les téléphones mobiles, les ordinateurs portables et les ordinateurs de bureau, comme nous l'avons vu à la section 4. Par conséquent, de nombreuses fonctions de sécurité conçues pour des dispositifs informatiques plus polyvalents sont plus difficiles à mettre en œuvre sur les dispositifs IoT. Par exemple, le chiffrement à clé publique, qui sous-tend les communications sécurisées modernes basées sur Transport Layer Security (TLS) [42] et Datagram Transport Layer Security (DTLS) [43], peut être difficile à mettre en œuvre sur certains dispositifs IoT aux ressources limitées. Par exemple, les appareils Arduino et Raspberry Pi peuvent prendre plusieurs secondes pour effectuer une opération de chiffrement ou de déchiffrement asymétrique [44,45].

Au-delà des limites inhérentes aux dispositifs IoT et aux plateformes IoT sur lesquelles ils fonctionnent, un certain nombre de failles de sécurité ont été identifiées sur le terrain, notamment des communications non cryptées, des fuites de données des dispositifs IoT et des effets négatifs sur le réseau auquel le dispositif IoT est attaché [25,26,27,46,47].

Par exemple, certaines implémentations de serveurs TLS sont vulnérables aux attaques dites de " downgrade ", par lesquelles un attaquant peut forcer un serveur à utiliser une ancienne version du protocole TLS, qui peut présenter des problèmes de sécurité connus, tels que des vulnérabilités aux attaques de type man-in-the-middle. Dans ces scénarios, la communication entre un dispositif IoT et le service hébergé dans le cloud qui le prend en charge pourrait être compromise.

▪ Communications non authentifiées

Certains dispositifs IoT fournissent des mises à jour logicielles automatiques. Cependant, sans authentification ni chiffrement, cette approche est insuffisante, car le mécanisme de mise à jour pourrait être compromis ou désactivé [48]. Le mécanisme de mise à jour lui-même et tout trafic de commande et de contrôle associé doivent être authentifiés et chiffrés, et l'intégrité des communications entre le dispositif et les autres points d'extrémité doit être protégée. [3] Malheureusement, de nombreux dispositifs IoT n'utilisent pas l'authentification au cours de la communication. Par exemple, le hub Lightwave RF Smart a envoyé du trafic vers un serveur distant sur le réseau à chaque fois qu'il a redémarré et, par la suite, toutes les quinze minutes lors de la vérification des mises à jour logicielles [29]. Si la connexion n'est pas sécurisée, il n'est pas difficile pour un attaquant ayant accès au réseau de mener une attaque de type man-in-the-middle.

▪ Communications non cryptées

De nombreux appareils IoT envoient tout ou partie des données en clair, plutôt que sous une forme chiffrée. Cela signifie que les données peuvent "fuir" et être observées par d'autres appareils ou par un attaquant.

Par conséquent, certains dispositifs IoT laissent échapper des informations sur les utilisateurs (par exemple à un observateur du trafic réseau), ce qui peut permettre d'identifier le ou les dispositifs IoT utilisés, ainsi que de révéler l'activité et le comportement actuels des utilisateurs [17]. [4] Par exemple :

- Un cadre photo numérique transmet l'adresse électronique de l'utilisateur en clair lors de la synchronisation des photos, et l'activité actuelle de l'utilisateur est également affichée en clair [10].
- Une caméra web envoie des fichiers vidéo en clair [29].
- Un assistant personnel audio transporte les commandes audio de l'utilisateur, les relevés des capteurs et les adresses électroniques de l'utilisateur en clair [29].
- Un thermostat transporte des données météorologiques locales avec des informations précises sur la localisation de l'utilisateur en clair, et est clairement identifiable comme un thermostat d'une marque spécifique en fonction des ports utilisés. [5]
- Un hub de dispositif IoT a un profil de trafic en clair qui est si régulier et spécifique que le hub de dispositif peut être identifié simplement en prenant l'empreinte du modèle de trafic en clair [29].
- Certains stimulateurs cardiaques compatibles IoT utilisent des canaux de communication non cryptés [52].

L'envoi de trafic en clair n'est pas le modèle recommandé pour les nouveaux déploiements et crée des problèmes de fuite d'informations personnelles ou autres sur un réseau local ou sur Internet. À ce sujet, par exemple, l'Internet Architecture Board (IAB) a récemment déclaré : " L'IAB exhorte les concepteurs de protocoles à concevoir un fonctionnement confidentiel par défaut... Nous encourageons vivement les développeurs à inclure le chiffrement dans leurs implémentations et à les rendre chiffrées par défaut "[53].

- ***Absence d'authentification et d'autorisation mutuelles***

De nombreuses attaques proviennent de derrière un pare-feu, à la frontière d'un réseau, à la maison ou ailleurs. Par conséquent, les communications derrière un pare-feu ne doivent pas nécessairement être considérées comme dignes de confiance. Ainsi, un dispositif doit établir la confiance entre les dispositifs, indépendamment du fait qu'il se trouve sur un réseau local ou sur Internet ; il doit supposer que les autres dispositifs ne sont pas dignes de confiance par défaut et doivent être explicitement authentifiés et autorisés. Un appareil qui permet à une partie inconnue ou non autorisée de modifier son code ou sa configuration, ou d'accéder à ses données, constitue une menace ; l'appareil peut révéler que son propriétaire est présent ou absent, faciliter l'installation ou l'exploitation de logiciels malveillants, ou faire en sorte que sa fonction IoT principale soit fondamentalement compromise.

Heureusement, contrairement aux appareils informatiques polyvalents tels que les ordinateurs portables, qui peuvent communiquer avec de nombreuses destinations Internet, les appareils IoT communiquent souvent avec un petit nombre de destinations bien définies. Par exemple, un appareil peut communiquer régulièrement uniquement avec un serveur de contrôle ou de mise à jour qui a un nom DNS ou une adresse IP bien connus ; une communication importante avec d'autres destinations peut être source d'inquiétude.

- ***Manque d'isolation du réseau***

Outre les risques pour la sécurité et la vie privée que les dispositifs IoT introduisent en dehors du réseau domestique où le dispositif IoT lui-même est installé (voir section 4), ces dispositifs créent également de nouveaux risques et sont susceptibles d'être attaqués *à l'intérieur de* la maison. Étant donné que de nombreux réseaux domestiques n'isolent pas, par défaut, les différentes parties du réseau les unes des autres, un dispositif connecté au réseau peut être en mesure d'observer ou d'échanger du trafic avec d'autres dispositifs sur le même réseau domestique, ce qui permet à un dispositif d'observer ou d'affecter le comportement de dispositifs non liés.

Bien qu'il soit courant d'utiliser des pare-feu pour isoler les appareils d'un réseau les uns des autres, les pare-feu seuls ne peuvent pas toujours protéger les appareils contre les compromissions ou les fuites de données, ni contre les logiciels malveillants sur les appareils déjà présents sur le réseau domestique. Aujourd'hui, un réseau domestique typique n'offre que peu ou pas d'isolation entre les appareils. La section 6 traite plus en détail des pare-feu et des autres mécanismes d'isolation du réseau.

Ce manque d'isolement constitue une menace pour la sécurité et la confidentialité de tous les appareils du réseau, à la fois en raison des actions spécifiques du fabricant (ou des actions d'autres parties dans la chaîne d'approvisionnement de l'IdO) et en raison de la compromission de l'appareil [27,54,55]. Plus précisément, un attaquant peut être en mesure de collecter des renseignements ou des informations personnelles à partir d'autres appareils sur le même réseau. En général, chaque appareil d'un réseau domestique peut voir le trafic des autres appareils qui se trouvent sur le même réseau. Si les appareils transmettent le trafic en clair, un appareil peut être en mesure de découvrir les détails de l'activité d'un autre appareil. Des travaux récents ont montré que même la capacité d'observer des détails plus "grossiers", tels que les consultations DNS et les changements dans les volumes de trafic, peut révéler des informations sur l'activité des appareils et le comportement des utilisateurs [56]. Un attaquant qui compromet un dispositif peut donc être en mesure de déduire des informations importantes sur un utilisateur final, comme les heures d'entrée et de sortie de la maison via des capteurs de porte compromis ou des enregistrements audio et vidéo provenant de microphones et de caméras vidéo intégrés dans des dispositifs IoT. La conception de la sécurité de nombreux réseaux sans fil domestiques permet des attaques de type "stepping stone" [57], par lesquelles un attaquant peut compromettre un dispositif IoT vulnérable et utiliser cette compromission comme mécanisme pour accéder à d'autres dispositifs connectés depuis l'intérieur du réseau. En voici quelques exemples :

- Un produit smartwatch comprenait un serveur DNS fonctionnel que des attaquants externes pouvaient utiliser pour attaquer d'autres appareils sur le réseau auquel la smartwatch était connectée. Le même produit présentait une vulnérabilité qui permettait à des attaquants externes de visualiser le trafic du réseau local [27].

- Une ampoule intelligente pourrait être piégée pour envoyer des informations d'identification de réseau sans fil que des attaquants externes pourraient ensuite utiliser pour contrôler les lumières et visualiser le trafic du réseau local [54].

- Certains fabricants de dispositifs et fournisseurs de services Internet ont exposé des interfaces de gestion à distance non sécurisées de millions de dispositifs et d'équipements d'abonné (par exemple, des modems, des routeurs domestiques) qui partageaient tous la même clé privée connue, exposant ces dispositifs à des attaques man-in-the-middle passives et actives [55].

- Des vulnérabilités dans un certain modèle de téléphone VoIP permettraient à un attaquant de réseau local de fournir des mises à jour malveillantes du micrologiciel du téléphone [58].

- Un fabricant de caméras de sécurité Wi-Fi a conçu ses produits avec un logiciel de mise en réseau peer-to-peer qui "perce" plusieurs trous dans le pare-feu du réseau local et ne peut pas être facilement désactivé. Ce logiciel permettait aux attaquants non seulement de compromettre la caméra elle-même à partir d'une grande variété de points d'accès, mais aussi de lancer des attaques sur d'autres appareils du réseau local [31].

5.2 Fuites de données

L'installation de dispositifs IoT dans la maison crée un potentiel de fuite de données privées des utilisateurs, à la fois depuis le cloud (où les données sont stockées) et entre les dispositifs IoT eux-mêmes.

▪ Fuites dans le nuage

Une grande partie des données que les appareils IoT collectent sont actuellement stockées dans des services de cloud à l'extérieur du domicile ; ces services de cloud pourraient subir une violation des données en raison d'une attaque externe ou d'une menace interne.

En outre, si les utilisateurs utilisent des méthodes d'authentification ou de cryptage faibles pour ces services hébergés dans le nuage, les données des utilisateurs peuvent également être compromises.

En voici quelques exemples :

- Une application web associée à un ours en peluche (qui contient une petite caméra sur son nez) contenait une faille de sécurité qui exposait l'identité des enfants [59].
- La poupée envoyait des chats cryptés entre la poupée et les serveurs hébergés dans le nuage en utilisant une version de TLS qui était vulnérable à une attaque par déclassement, ce qui permettait d'écouter les enregistrements des enfants [60].
- Une violation des données chez un fabricant de jouets pour enfants a exposé les données personnelles de plus de six millions d'enfants [61].
- Des faiblesses dans la configuration du point d'accès Wi-Fi d'un véhicule automobile ont permis de suivre l'emplacement de nombreux véhicules sur des sites web qui récoltent les noms des points d'accès Wi-Fi et leur emplacement [62].
- Le système d'un constructeur automobile a envoyé des statistiques sur la consommation de carburant, des coordonnées géographiques précises, la vitesse, la direction et la destination en clair à un serveur central [63].

Il existe de nombreux autres exemples de violations de données à partir de ces dispositifs [25,28,30,32,64,65,66,67]. Les fuites de données à partir du cloud ne sont pas nouvelles ou spécifiques aux dispositifs IoT, mais la prévalence des vulnérabilités de fuite de données dans les services hébergés dans le cloud est particulièrement problématique pour les dispositifs IoT grand public, qui sont non seulement de plus en plus omniprésents mais collectent aussi de plus en plus de données personnelles et privées.

▪ Fuites depuis et entre les appareils

Les appareils IoT de différents fabricants, exécutant de nombreuses applications logicielles différentes, peuvent tous résider sur le même réseau local. Bien que les techniques de cryptage Wi-Fi standard puissent protéger la confidentialité des transmissions de données sur le réseau local, le cryptage seul ne garantit pas la confidentialité des utilisateurs.

Dans certains cas, les dispositifs du même réseau ou de réseaux voisins peuvent être en mesure d'observer les données d'autres dispositifs. Par exemple, un dispositif peut "fuir" des données vers des dispositifs ou des utilisateurs proches (soit sur le même réseau local, soit sur le réseau Wi-Fi, soit simplement à proximité). Même avec le cryptage Wi-Fi, un dispositif peut toujours observer la présence d'autres dispositifs sur le même réseau local, et les adresses matérielles des autres dispositifs - qui peuvent souvent révéler le type de dispositif - sont aussi généralement visibles en clair. Ce niveau de visibilité pourrait, par exemple, permettre au logiciel d'un cadre photo numérique de surveiller les interactions d'un utilisateur avec d'autres appareils sur le même réseau.

Les données qui fuient d'un appareil à l'autre peuvent inclure des informations telles que le nom des personnes présentes dans un foyer, la localisation géographique précise d'un foyer, ou même les produits achetés par un consommateur. Par exemple, une étude récente a découvert qu'un thermostat laissait échapper des informations géographiques précises de la maison [17]. Dans une autre étude récente, des chercheurs ont été en mesure de déterminer le code PIN d'un guichet automatique sur la base des données accélérométriques transmises par Bluetooth à partir d'un dispositif de suivi de la condition physique [68].

5.3 Susceptibilité à l'infection par des logiciels malveillants et autres abus

Les logiciels malveillants, qui sont des logiciels malveillants installés sur un appareil d'utilisateur qui perturbent généralement les opérations, obtiennent un accès non autorisé ou lancent des attaques, peuvent infecter les appareils IoT par divers mécanismes. De même, d'autres formes d'abus peuvent se produire. En voici quelques exemples :

- Le fabricant peut ne pas sécuriser correctement la chaîne d'approvisionnement en logiciels [69] et permettre ainsi l'installation de logiciels malveillants sur le logiciel initialement livré du dispositif IoT [34], comme indiqué à la section 4.5.
- Les appareils peuvent être livrés avec un logiciel obsolète qui contient des vulnérabilités connues. Lorsqu'un utilisateur connecte l'appareil au réseau, celui-ci devient immédiatement une cible pour les attaquants. Des études antérieures ont démontré que le "temps de survie" (c'est-à-dire le temps pendant lequel un appareil est connecté au réseau avant d'être infecté) peut dans certains cas être inférieur à dix minutes [70]. [6] Si un appareil est livré avec un logiciel obsolète et ne vérifie pas immédiatement les mises à jour logicielles, il risque d'être infecté immédiatement.
- Les mécanismes de mise à jour des logiciels peuvent ne pas inclure l'authentification des chargements de logiciels pour garantir que le logiciel provient d'une source fiable. Grâce à l'ingénierie sociale, l'utilisateur peut être influencé ou incité à charger un logiciel compromis sur un dispositif IoT.
- Le logiciel peut inclure des capacités de ligne de commande ou des interfaces de programmation d'applications (API) qui peuvent être exploitées (avec ou sans la participation de l'utilisateur) pour charger un logiciel malveillant sur un dispositif IoT.
- L'appareil a des ports inutiles laissés ouverts et non sécurisés, tels que telnet. Ces ports inutiles ont été utilisés pour compromettre un appareil, par exemple en demandant à l'appareil d'accéder à une destination afin de télécharger un logiciel malveillant [71,72,73]. Les ports inutiles peuvent également être utilisés dans des attaques par amplification.
- L'appareil utilise une authentification par défaut faible, comme des noms d'utilisateur et des mots de passe communs ou faciles à deviner (par exemple, "admin", "password") [74]. En outre, l'authentification pour l'accès à distance peut ne pas avoir été sécurisée, ce qui permet à des personnes qui ne sont pas physiquement présentes dans la maison de se connecter à l'appareil et d'y installer des logiciels malveillants [13,75,76,77,78].

5.4 Possibilité d'interruption de service

Un aspect important de la sécurité des dispositifs IoT est la disponibilité des services face aux pannes et aux attaques des dispositifs. La perte potentielle de disponibilité ou de connectivité diminue non seulement la fonctionnalité des dispositifs IoT, mais peut également dégrader la sécurité des dispositifs dans certains cas, par exemple lorsqu'un dispositif IoT ne peut plus fonctionner sans cette connectivité (par exemple, un système d'alarme domestique se désactivant si la connectivité est perdue). Un dispositif IoT peut subir une interruption de service de plusieurs manières.

- **Perte de support d'une application hébergée dans le nuage.** Si l'appareil dépend de la communication avec un service en nuage, il peut ne pas fonctionner lorsqu'il perd la connectivité avec le service en nuage. Cette déconnexion peut se produire pour diverses raisons, notamment l'interruption de la connectivité Internet, des bogues dans le service logiciel en nuage, la faillite d'un vendeur ou d'un fabricant, ou la décision d'un consommateur d'interrompre un abonnement à un service.
- **Perte de connectivité au réseau. La** connectivité au sein d'un réseau domestique peut être interrompue, par exemple en raison d'un câble d'alimentation débranché, d'interférences radio avec le Wi-Fi ou d'un pare-feu décidant de restreindre l'accès.

- **Dommage de l'appareil. Un** appareil peut être physiquement endommagé, ou son logiciel peut être corrompu ou inopérant (parfois appelé "bricking").

Un appareil "bricolé", c'est-à-dire endommagé physiquement ou logiquement, peut être irrécupérable, tandis qu'un appareil qui dépend de la communication avec un service hébergé dans le nuage peut redevenir opérationnel lorsque la communication est rétablie.
Les pannes de certains services peuvent endommager les biens et mettre les utilisateurs en danger. Par exemple, un bug logiciel dans un thermostat IoT a entraîné le non-fonctionnement des systèmes de chauffage domestique et (par conséquent) le gel des tuyaux dans les maisons [51]. Le mauvais fonctionnement des systèmes de chauffage et de refroidissement peut entraîner des décès. Lorsque les dispositifs IoT sont responsables de tout, de la santé personnelle à la sécurité de la maison, les enjeux pour la sécurité des utilisateurs sont élevés.

5.5 Les problèmes de sécurité et de confidentialité des dispositifs risquent de persister

La présente section explique brièvement pourquoi les problèmes de sécurité décrits dans la section précédente sont susceptibles de persister. On pourrait s'attendre à ce qu'un grand nombre de ces appareils IoT ne reçoivent jamais de mise à jour logicielle, soit parce que le fabricant (ou une autre partie de la chaîne d'approvisionnement IoT, ou le fournisseur de services IoT) ne fournit pas de mises à jour, soit parce que les consommateurs n'appliquent pas les mises à jour déjà disponibles. Il existe de nombreux exemples de cela avec des types d'appareils similaires [79,80,81,82].

▪ De nombreux appareils IoT ne seront jamais réparés

Le déploiement de mises à jour logicielles qui corrigent les vulnérabilités de sécurité critiques est difficile en général, mais les dispositifs IoT posent des défis uniques. Tout d'abord, de nombreux vendeurs et fabricants de dispositifs ne disposent pas de systèmes ou de processus permettant de déployer des mises à jour logicielles sur des milliers de dispositifs (ou plus). Deuxièmement, il est difficile de déployer des mises à jour via le réseau sur des appareils qui fonctionnent dans les foyers des consommateurs, car les mises à jour peuvent parfois interrompre le service et avoir le potentiel de "briquer" l'appareil, si elles ne sont pas effectuées correctement. En outre, certains appareils peuvent même ne pas être en mesure d'effectuer des mises à jour logicielles [83].

Trois approches de mise à jour logicielle ont vu le jour dans le secteur de l'électronique grand public. Deux d'entre elles reposent sur l'intervention de l'utilisateur (un défaut fondamental), tandis que la troisième est automatique et ne requiert aucune action de la part de l'utilisateur. L'efficacité de chacune d'entre elles varie dans la pratique. Ces approches sont les suivantes :

- **Mises à jour logicielles initiées par l'utilisateur.** Cette approche exige que l'administrateur local de l'appareil lance manuellement la vérification et l'installation de toute mise à jour logicielle de l'appareil. On trouve un exemple de ce modèle sur le marché des passerelles domestiques ou des routeurs. Pour certains de ces appareils, l'utilisateur doit télécharger une nouvelle image logicielle sur le site Web du fabricant, puis accéder à une page Web d'administration locale de l'appareil, trouver l'interface de mise à jour logicielle et télécharger un fichier. Ce processus prend non seulement beaucoup de temps, mais il peut être décourageant pour les utilisateurs non techniques ou occasionnels pour lesquels un appareil peut encore fonctionner "suffisamment bien".

- **Vérifications automatisées des mises à jour logicielles, avec l'approbation de l'utilisateur.** Ces dispositifs vérifient périodiquement la présence de nouvelles mises à jour logicielles. Lorsqu'une mise à jour est disponible, l'appareil présente à l'utilisateur une invite qui lui demande la permission de procéder à la mise à jour. Les téléviseurs intelligents et les consoles de jeux utilisent souvent cette approche. Dans ces scénarios, l'application d'une mise à jour logicielle particulière peut prendre plusieurs minutes, voire plus, c'est pourquoi l'utilisateur a la possibilité de différer l'installation.

- **Mises à jour logicielles entièrement automatisées.** Certains appareils vérifient périodiquement si un nouveau logiciel est disponible ; s'il l'est, ils le téléchargent et l'installent sans intervention de l'utilisateur [84,85]. Dans certains cas, l'appareil peut appliquer la mise à jour à un moment particulier de la journée, par exemple tard dans la nuit ou lorsqu'il n'y a pas eu d'activité relative à l'appareil pendant un certain temps, afin de minimiser les perturbations pour l'utilisateur.

Malheureusement, les mises à jour logicielles automatisées peuvent également poser des problèmes à certains utilisateurs qui ont des plafonds de données (le cas échéant), et lorsque les mises à jour elles-mêmes introduisent de nouveaux bogues [51].

Les approches courantes pour les mises à jour logicielles sont soit initiées par l'utilisateur, soit approuvées par l'utilisateur, qui ont toutes deux tendance à conduire à des taux de mise à jour relativement faibles [86]. Par conséquent, des millions de passerelles domestiques appartenant au client et entretenues par lui (COAM) ne recevront probablement jamais de mise à jour logicielle. Par exemple, certains modèles de passerelles domestiques NetGear ont été livrés avec un bogue logiciel qui a provoqué l'inondation aléatoire des serveurs DNS des FAI avec des milliers de requêtes DNS par seconde, soit plusieurs millions par jour, ou un déluge de requêtes NTP vers les serveurs NTP [87,88,89,90]. Bien que ce bogue logiciel spécifique ait été signalé depuis de nombreuses années, les opérateurs de réseau continuent néanmoins à observer ces dispositifs exécutant des logiciels plus anciens et se comportant mal sur le réseau, effectuant par inadvertance des attaques DDoS en raison de bogues logiciels.

- **Les mises à jour logicielles ne se limitent pas aux bogues**

Il convient également de garder à l'esprit que les mises à jour logicielles ne sont pas simplement destinées à corriger des bogues de sécurité ou de confidentialité. Elles peuvent également être destinées à introduire de nouvelles fonctions importantes. En outre, elles peuvent être plus généralement liées aux performances et à la sécurité, comme la prise en charge ou la correction de bogues liés à l'adressage IPv6, à la validation des extensions de sécurité DNS (DNSSEC) et au contrôle des tampons TCP (par exemple, "buffer bloat") ou à la gestion active des files d'attente (AQM).

- **Les consommateurs sont peu enclins à mettre à jour le logiciel des dispositifs IoT**

Peu d'utilisateurs finaux mettent systématiquement à jour le logiciel de leur propre chef, à moins que l'interface utilisateur graphique (IUG) de l'appareil ne le leur rappelle constamment et de manière ostensible (c'est-à-dire une fenêtre contextuelle régulière sur un PC, un compteur dans une boutique d'applications mobiles, une icône d'application rebondissante, etc. D'autres travaux récents suggèrent que les utilisateurs renoncent à appliquer les mises à jour logicielles sur les appareils fixes et mobiles pour diverses raisons, allant de la perturbation de leur cycle de travail aux coûts des données associés aux mises à jour logicielles [86].

Bien qu'aucune étude approfondie sur le comportement des utilisateurs en matière de mise à jour logicielle n'ait été entreprise pour les appareils IoT, la situation est probablement pire que pour les appareils conventionnels, ou non IoT. En plus du comportement déjà risqué des utilisateurs en matière de mises à jour logicielles, de nombreux appareils IoT ne disposent pas d'une interface graphique ou d'un autre indicateur de la disponibilité ou de la nécessité d'un nouveau logiciel. De plus, la prolifération des appareils, tant en nombre qu'en diversité, fait du suivi des mises à jour logicielles une tâche difficile pour le consommateur Internet typique.

Ainsi, pour les appareils IoT, il est préférable de supposer que la plupart des utilisateurs finaux ne prendront jamais d'initiative pour mettre à jour le logiciel de l'appareil.

5.6 Le remplacement du dispositif peut être une alternative aux mises à jour logicielles

Dans certains cas, le remplacement complet d'un appareil peut être une alternative aux mises à jour logicielles. Certains dispositifs IoT peuvent être si peu coûteux que la mise à jour du logiciel peut être peu pratique ou non rentable. Par exemple, un adaptateur de charge qui coûte 0,99 $ peut avoir une fonction IoT limitée. À ce coût unitaire, la mise à jour d'un appareil peut ne pas être économique ; il peut être plus logique de recycler l'appareil et d'en acheter un autre. Toutefois, cette approche nécessite les éléments suivants pour offrir une alternative sécurisée aux mises à jour logicielles :

- Un moyen d'identifier quand une ou plusieurs vulnérabilités accumulées dans un appareil l'ont compromis au point qu'il doit être remplacé.
- Un moyen de désactiver la communication avec le dispositif une fois qu'il a été déterminé qu'il est vulnérable. Parmi les exemples de méthodes possibles, citons la désactivation à distance de l'appareil du réseau ou le blocage de l'accès à l'appareil depuis une passerelle domestique.
- Un moyen d'informer les utilisateurs que la communication avec l'appareil a été désactivée.

Même dans ces cas, bien sûr, les utilisateurs peuvent être réticents à cesser d'utiliser un dispositif tant qu'il continue à

fonctionner en partie. Cependant, tant que la capacité de communication du dispositif a été désactivée, son utilisation continue ne devrait pas présenter de faille de sécurité.

6 Un rôle possible pour la technologie des réseaux domestiques

La sécurisation par défaut des appareils par les fabricants constitue une étape importante pour améliorer la sécurité et la confidentialité de l'IoT, mais elle est loin d'être suffisante. Même les appareils IoT qui ne sont pas infectés par des logiciels malveillants peuvent toujours écouter le trafic d'autres réseaux domestiques (par exemple, via des logiciels installés par le fabricant ou des logiciels tiers), compromettant ainsi la vie privée des utilisateurs. Une maison est souvent considérée comme un environnement isolé ou doté d'un pare-feu, et de multiples dispositifs IoT non liés auront généralement un accès illimité derrière ce pare-feu. En outre, comme mentionné aux sections 3.4 et 5.1, un seul dispositif non sécurisé ou compromis dans le réseau domestique peut conduire à des attaques de type "stepping-stone", de sorte que la "défense en profondeur" [91] est essentielle.

Des études et des rapports récents ont suggéré qu'à l'avenir, un appareil de réseau domestique pourrait jouer un certain rôle dans le contrôle et la gestion du trafic que les dispositifs IoT échangent entre eux et avec le reste d'Internet [92]. Les capacités possibles d'un tel appareil réseau comprennent :

- Découverte et inventaire automatiques des appareils domestiques connectés à Internet [93].
- Mécanismes permettant de présenter à l'utilisateur des informations claires sur (1) les données que l'appareil envoie au reste de l'Internet et (2) les autres appareils de la maison avec lesquels l'appareil communique, comme cela a été fait dans le passé pour les smartphones et les navigateurs [94,95].
- Des mécanismes qui fournissent à l'utilisateur des moyens simples d'empêcher ou de désactiver la communication d'un seul appareil avec d'autres appareils IoT sur le réseau domestique, ou avec des serveurs de stockage dans le cloud, *sans altérer la fonctionnalité primaire de l'appareil.* Une étude récente a pu y parvenir avec deux exemples de dispositifs IoT, une ampoule Philips Hue et un thermostat Nest [92].

La technologie de réseau visant à améliorer la sécurité et la confidentialité pourrait finalement prendre l'une des nombreuses formes suivantes. Une passerelle de réseau domestique, qu'elle soit séparée (par exemple, un concentrateur IoT ou un routeur domestique séparé) ou intégrée à l'équipement fourni par le FAI, pourrait effectuer des mesures au sein du réseau qui aident les utilisateurs à comprendre les flux de données complexes à la fois entre les dispositifs IoT dans la maison et entre ces dispositifs et les sites et services tiers à l'extérieur de la maison. En ce sens, la technologie de réseau dans la maison qui surveille le trafic des appareils peut finalement aider à améliorer la *transparence du* comportement de ces appareils IoT.

Il existe un certain conflit entre la surveillance et la gestion du trafic IoT par un hub et la sécurité de bout en bout du trafic lui-même. Il convient de noter que même si le trafic réseau vers et depuis ces dispositifs est crypté de bout en bout, certaines caractéristiques, telles que les autres dispositifs et emplacements avec lesquels un dispositif particulier communique, seront toujours évidentes à partir de ce trafic. Une normalisation permettant une classification et une protection coopératives du trafic avec un tel concentrateur IoT permettrait au dispositif d'être une partie reconnue et authentifiée de l'écosystème, fournissant à cette gestion un contrôle à grain fin disponible pour l'initiateur du trafic sur une base d'opt-in.

En plus d'aider simplement à visualiser ces flux de trafic, une telle passerelle pourrait appliquer des paramètres *par défaut raisonnables* pour améliorer la sécurité et la confidentialité des appareils IoT connectés. Par exemple, des recherches récentes suggèrent qu'un pare-feu de réseau domestique peut empêcher certains appareils d'exfiltrer des journaux et d'autres informations vers des fournisseurs de nuages tiers sans paralyser la fonctionnalité de l'appareil lui-même [92]. Une question ouverte consiste à identifier des paramètres de pare-feu par défaut raisonnables qui pourraient être installés sur une telle passerelle pour améliorer la sécurité et la confidentialité. Étant donné qu'un tel pare-feu pour réseau domestique pourrait donner lieu à une "course à l'armement" en matière de protection de la vie privée (on pourrait par exemple imaginer qu'un fabricant d'appareils ne fournisse pas de mises à jour de sécurité à un utilisateur qui bloque les capacités de suivi de l'appareil), un aspect de la certification des appareils pour les fabricants et les vendeurs pourrait finalement consister à s'assurer que les consommateurs conservent un *choix* éclairé quant à la manière dont ces appareils communiquent entre eux et avec les sites et services tiers.

Enfin, l'interaction entre les dispositifs IoT peut nécessiter une médiation plus complexe. Par exemple, si un utilisateur ne souhaite généralement pas que certains dispositifs communiquent ou interagissent entre eux, il peut y avoir des cas d'utilisation spécifiques qui permettent la communication ou l'interaction entre les dispositifs pour des tâches spécifiques. Prenons l'exemple d'un scénario dans lequel un utilisateur souhaiterait faire varier automatiquement l'intensité des lumières lorsqu'il regarde un film à la maison. Dans ce cas, l'application pourrait impliquer une communication médiatisée entre un dispositif de diffusion en continu (par exemple, un Roku ou une Apple TV) et les prises et interrupteurs intelligents (par exemple, un interrupteur WeMo de Belkin). D'autre part, en général, un utilisateur peut ne pas vouloir que ces dispositifs interagissent, ou même qu'ils observent le trafic de chacun. Ainsi, la passerelle réseau, associée à l'interface utilisateur appropriée, peut finalement offrir de meilleures possibilités pour ce type d'interaction médiatisée complexe.

Des rapports récents suggèrent que nombre de ces objectifs sont probablement à portée de main. Par exemple, des chercheurs ont utilisé un pare-feu de réseau domestique pour empêcher un thermostat Nest d'envoyer ses journaux d'état au nuage, sans nuire à l'appareil lui-même [92]. Toutefois, comme il est peu probable que l'utilisateur type configure des règles de pare-feu, ces fonctions de pare-feu doivent être plus faciles à utiliser et, si possible, automatisées, avant d'être considérées comme pratiques.

7 Recommandations

Cette section du rapport présente les recommandations du groupe de travail technique (TWG) du BITAG. Bien que les sections précédentes de ce rapport aient abordé le potentiel de solutions à plus long terme, tournées vers l'avenir (par exemple, le rôle de la technologie des réseaux domestiques pour atténuer l'insécurité des appareils), cette section se concentre sur les recommandations que le GTCBT estime pouvoir mettre en œuvre à court terme en utilisant la technologie existante.

7.1 Les dispositifs IoT doivent utiliser les meilleures pratiques logicielles actuelles

- **Les appareils IoT doivent être livrés avec des logiciels raisonnablement récents**

  BITAG recommande que les appareils IoT soient expédiés aux clients ou aux points de vente au détail avec un logiciel raisonnablement à jour qui ne contient pas de vulnérabilités graves et connues. Toutefois, les bogues logiciels sont en quelque sorte une "réalité" et il n'est pas rare que de nouvelles vulnérabilités soient découvertes pendant que les appareils sont en rayon. Il est donc essentiel qu'un dispositif IoT dispose d'un mécanisme permettant aux appareils de recevoir des mises à jour logicielles automatiques et sécurisées (voir point suivant).

- **Les dispositifs IoT doivent disposer d'un mécanisme de mise à jour logicielle automatisée et sécurisée**

  Les bogues logiciels doivent être réduits au minimum, mais, comme indiqué ci-dessus, ils sont inévitables. Il est donc essentiel qu'un dispositif IoT dispose d'un mécanisme de mise à jour logicielle automatique et sécurisée, comme indiqué à la section 5.5.

  BITAG recommande que les fabricants d'appareils IoT ou les fournisseurs de services IoT conçoivent donc leurs appareils et systèmes en partant du principe que de nouveaux bogues et vulnérabilités seront découverts au fil du temps. Ils devraient concevoir des systèmes et des processus pour assurer la mise à jour automatique des logiciels des appareils IoT, sans exiger ou attendre un quelconque type d'action de la part de l'utilisateur, ni même d'opt-in de sa part.

  Bien que ces mises à jour doivent être automatiques et obligatoires pour les utilisateurs finaux, si, pour une raison quelconque, le système de mise à jour doit permettre de choisir entre l'option "opt-out" et l'option "opt-in", alors, sur la base d'études sur l'interaction homme-machine, un tel système devrait être "opt-out" de sorte que les mises à jour se produisent automatiquement par défaut et sans aucune intervention de l'utilisateur, approbation de l'utilisateur ou autre action de l'utilisateur final. La possibilité pour un utilisateur de configurer la nature des mises à jour logicielles peut être importante pour certains utilisateurs finaux, comme ceux qui utilisent des appareils dans des environnements où les ressources sont limitées (par exemple, connexions par satellite ou autres endroits où les coûts des données sont élevés).

  Dans certains cas, les dispositifs de réseau domestique pourraient interagir avec les consommateurs pour émettre des alertes périodiques afin de faciliter la prise de décision en connaissance de cause (par exemple, en posant à l'utilisateur des questions qu'il peut comprendre sur la manière dont il souhaite que les dispositifs interagissent). L'intégration de ce type de fonction exige un soin extrême dans la conception, afin de garantir que ces alertes à l'utilisateur sont significatives et que le volume des mises à jour n'est pas écrasant. Ce type de fonctionnalité peut être compliqué à mettre en œuvre de manière fiable.

- **Les appareils IoT devraient utiliser une authentification forte par défaut**

  BITAG recommande que les dispositifs IoT soient sécurisés par défaut (par exemple, protégés par un mot de passe) et n'utilisent pas de noms d'utilisateur et de mots de passe courants ou facilement devinables (par exemple, "admin", "password"). Enfin, l'authentification pour l'accès à distance doit être sécurisée, car elle permet potentiellement à d'autres personnes qui ne sont pas physiquement présentes dans la maison de surveiller et de contrôler des aspects au sein de la maison (par exemple, modifier les commandes de climatisation, surveiller l'activité des utilisateurs).
  Les informations d'authentification doivent être uniques pour chaque appareil.

  Les méthodes d'authentification par défaut qui répondent à ces critères sont les suivantes :

(1) l'expédition de chaque appareil avec un mot de passe fixe par défaut, mais en demandant à l'utilisateur de le changer dans le cadre du processus d'installation (c'est-à-dire avant que l'appareil ne fonctionne) ; et (2) l'expédition de chaque appareil avec un mot de passe unique pour chaque unité et l'impression du mot de passe sur une étiquette qui est apposée sur l'appareil.

- **Les configurations des dispositifs IoT doivent être testées et renforcées.**

  Certains appareils IoT permettent à un utilisateur de personnaliser le comportement de l'appareil. BITAG recommande aux fabricants de tester la sécurité de chaque appareil avec une gamme de configurations possibles, par opposition à la simple configuration par défaut. L'interface d'un appareil devrait empêcher - ou du moins décourager activement - les utilisateurs de configurer l'appareil d'une manière qui le rendrait moins sûr.

7.2 Les dispositifs IoT doivent respecter les meilleures pratiques en matière de sécurité et de cryptographie

BITAG recommande aux fabricants de dispositifs IoT de sécuriser les communications en utilisant la sécurité de la couche de transport (TLS) ou la cryptographie légère (LWC) [96,97,98]. Certains appareils peuvent effectuer un chiffrement à clé symétrique en temps quasi réel. En outre, la cryptographie légère (LWC) offre des options supplémentaires pour sécuriser le trafic à destination et en provenance de dispositifs aux ressources limitées. Si les dispositifs s'appuient sur une infrastructure à clé publique (PKI), une entité autorisée doit pouvoir révoquer les certificats lorsqu'ils sont compromis, comme le font les navigateurs Web et les systèmes d'exploitation des PC [99,100,101,102,103,104,105]. Les services en nuage peuvent renforcer l'intégrité des certificats émis par les autorités de certification en participant, par exemple, au programme Certificate Transparency [106]. Enfin, les fabricants doivent veiller à éviter les méthodes de cryptage, les protocoles et les tailles de clé présentant des faiblesses connues.

Les fournisseurs qui s'appuient sur une prise en charge hébergée dans le cloud pour les dispositifs IoT doivent configurer leurs serveurs pour suivre les meilleures pratiques, notamment en configurant l'implémentation TLS pour n'accepter que les dernières versions du protocole TLS.

- **Cryptage des communications de configuration (commande et contrôle) par défaut**

  Comme expliqué à la section 5.1, l'utilisation d'une communication non authentifiée ou en clair pour la gestion d'un dispositif présente un risque de sécurité important. BITAG recommande que toutes les communications pour la gestion des appareils se fassent par un canal authentifié et sécurisé.

- **Communications sécurisées vers et depuis les contrôleurs IoT**

  Si les dispositifs IoT utilisent un contrôleur centralisé pour faciliter la communication par Internet avec un service en nuage, BITAG recommande que ce canal de communication soit sécurisé dans les deux sens.

- **Cryptage du stockage local des données sensibles**

  BITAG recommande que toutes les données sensibles ou confidentielles (par exemple, la clé privée, la clé pré-partagée, les informations sur l'utilisateur ou l'installation) résident dans un stockage crypté.

- **Authentifier les communications, les modifications de logiciels et les demandes de données**

  BITAG recommande que les dispositifs IoT authentifient les points d'extrémité avec lesquels ils communiquent. L'authentification de la communication implique de vérifier l'identité du point d'extrémité, ce qui implique également de vérifier que le certificat utilisé par le point d'extrémité est signé par une autorité de certification à laquelle le dispositif fait confiance et qui n'a pas été révoquée.

- **Utilisez des informations d'identification uniques pour chaque appareil**

  BITAG recommande que chaque dispositif ait des informations d'identification uniques. Si un dispositif utilise la cryptographie à clé publique (par exemple, pour signer des messages, échanger une clé de session ou s'authentifier), chaque dispositif doit avoir un certificat unique et vérifiable. Si un dispositif utilise la cryptographie à clé symétrique, les paires de points d'extrémité ne devraient

jamais partager la clé symétrique avec d'autres parties.

- **Utilisez des informations d'identification qui peuvent être mises à jour**

  Le BITAG recommande aux fabricants de dispositifs de prendre en charge un mécanisme sécurisé permettant de mettre à jour les informations d'identification utilisées par un dispositif. Toutefois, la mise en œuvre de cette recommandation de manière sécurisée nécessite une attention particulière, car une mise en œuvre incorrecte peut elle-même introduire un nouveau vecteur d'attaque.

- **Fermer les ports inutiles et désactiver les services inutiles**

  Le BITAG recommande aux fabricants de dispositifs de fermer les ports inutiles, tels que telnet, car les ports inutiles peuvent être non sécurisés ou peuvent être compromis d'une autre manière [107]. Les dispositifs doivent fermer ou désactiver les interfaces et fonctions administratives qui ne sont pas utilisées. Ils ne doivent pas non plus être livrés avec des pilotes qu'ils n'utilisent pas.

- **Utilisez des bibliothèques qui sont activement entretenues et soutenues.**

  Bon nombre des recommandations formulées dans ce rapport exigent la mise en œuvre de canaux de communication sécurisés. Cependant, les implémentations maison des protocoles cryptographiques et des canaux de communication sécurisés peuvent elles-mêmes introduire des vulnérabilités. Le BITAG recommande aux fabricants de dispositifs, lorsqu'ils mettent en œuvre les recommandations de ce rapport, d'utiliser, dans la mesure du possible, des bibliothèques et des cadres qui bénéficient d'un soutien et d'une maintenance actifs.

7.3 Les dispositifs IoT doivent communiquer de manière restrictive plutôt que permissive.

BITAG recommande que les appareils IoT ne communiquent qu'avec des points d'extrémité de confiance. Lorsque cela est possible, les appareils ne doivent pas être joignables par défaut via des connexions entrantes. Les appareils IoT ne doivent pas s'appuyer uniquement sur le pare-feu du réseau pour restreindre la communication, car certaines communications entre appareils au sein de la maison ne traversent pas nécessairement le pare-feu.

Il convient de noter qu'une recommandation du BITAG visant à restreindre la *configuration* des communications des dispositifs IoT ne doit pas se faire au détriment d'un écosystème ouvert. Un utilisateur doit pouvoir configurer les communications entre des dispositifs IoT arbitraires, et les dispositifs qui se font confiance doivent être autorisés à communiquer. Les communications sécurisées peuvent amorcer des listes de confiance restreintes qui reflètent l'ensemble des dispositifs avec lesquels un dispositif donné s'attend à communiquer. Ces communications inter-appareils ne devraient être autorisées que par des mécanismes de confiance et des canaux de communication sécurisés.

7.4 Les dispositifs IoT devraient continuer à fonctionner si la connectivité Internet est interrompue

Le BITAG recommande qu'un dispositif IoT soit capable d'exécuter sa ou ses fonctions principales (par exemple, un interrupteur d'éclairage ou un thermostat doit continuer à fonctionner avec des commandes manuelles), même s'il n'est pas connecté à Internet. En effet, la connectivité Internet peut être interrompue pour des causes allant d'une mauvaise configuration accidentelle à une attaque intentionnelle (par exemple, une attaque par déni de service) ; la fonction du dispositif doit être robuste face à ces types de perturbations de la connectivité.

Les dispositifs IoT qui ont des implications pour la sécurité des utilisateurs devraient continuer à fonctionner en mode déconnecté pour protéger la sécurité des consommateurs. Dans ces cas, le dispositif ou le système dorsal devrait informer l'utilisateur de la panne.

Dans la mesure du possible, les fabricants d'appareils doivent faire en sorte que les utilisateurs puissent facilement désactiver ou bloquer (par exemple, à l'aide d'un pare-feu) divers trafics réseau sans entraver la fonction principale de l'appareil.

7.5 Les appareils IoT doivent continuer à fonctionner en cas de défaillance du back-end du cloud.

De nombreux services qui dépendent ou utilisent un back-end en nuage peuvent continuer à fonctionner, même dans un état

dégradé ou partiellement fonctionnel, lorsque la connectivité au back-end en nuage est interrompue ou que le service lui-même tombe en panne. Par exemple, un thermostat dont les réglages peuvent être modifiés via un service en nuage devrait, dans le pire des cas, continuer à fonctionner en utilisant les derniers réglages connus ou les réglages par défaut. Une caméra de sécurité domestique hébergée dans le nuage doit être accessible depuis l'intérieur de la maison, même en cas de défaillance de la connectivité Internet.

7.6 Les dispositifs IoT doivent prendre en charge les meilleures pratiques d'adressage et de nommage

De nombreux dispositifs IoT peuvent rester déployés pendant de nombreuses années après leur installation. Par conséquent, les périphériques IoT doivent prendre en charge les meilleures pratiques relativement récentes, bien qu'actuelles, pour l'adressage IP et l'utilisation du système de noms de domaine (DNS). La prise en charge des derniers protocoles d'adressage et de nommage garantira que ces appareils resteront fonctionnels pendant des années, qu'ils seront performants et qu'ils pourront prendre en charge d'importantes fonctionnalités de sécurité basées sur le DNS.

- **IPv6**

  BITAG recommande que les appareils IoT prennent en charge la version la plus récente du protocole Internet, IPv6.

- **DNSSEC**

  BITAG recommande que les dispositifs IoT prennent en charge l'utilisation ou la validation des extensions de sécurité DNS (DNSSEC) lorsque des noms de domaine sont utilisés. Par exemple, si un dispositif IoT communique avec un service en nuage en utilisant le domaine exemple.com, le fournisseur de nuage doit pouvoir signer le domaine et le dispositif IoT doit pouvoir valider cette signature (ou s'assurer que son résolveur DNS en amont l'a fait et l'a indiqué dans une réponse DNS).

7.7 Les dispositifs IoT devraient être livrés avec une politique de confidentialité facile à trouver et à comprendre.

BITAG recommande que les dispositifs IoT soient livrés avec une politique de confidentialité, mais cette politique doit être facile à trouver et à comprendre pour un utilisateur type.

7.8 Dévoiler les droits permettant de réduire à distance les fonctionnalités des dispositifs IoT

BITAG recommande que si la fonctionnalité d'un dispositif IoT peut être diminuée à distance par un tiers, comme par le fabricant ou le fournisseur de services IoT, cette possibilité doit être clairement indiquée à l'utilisateur au moment de l'achat.

7.9 L'industrie des dispositifs IoT devrait envisager un programme industriel de cybersécurité

BITAG recommande à l'industrie des dispositifs IoT ou à un groupe connexe d'électronique grand public d'envisager la création d'un programme soutenu par l'industrie, dans le cadre duquel une sorte de logo ou de mention "Secure IoT Device" pourrait figurer sur les emballages de vente au détail des dispositifs IoT. Un tel programme pourrait être analogue à la manière dont la Wi-Fi Alliance ou d'autres groupes valident la conformité des appareils à diverses normes et/ou meilleures pratiques.

Un ensemble de meilleures pratiques soutenues par l'industrie semble être le moyen le plus pragmatique d'équilibrer l'innovation dans l'IdO et les défis de sécurité associés à la nature fluide de la cybersécurité, et d'éviter la mentalité de liste de contrôle qui peut se produire avec les processus de certification.

7.10 La chaîne d'approvisionnement de l'IdO doit jouer son rôle dans la résolution des problèmes de sécurité et de confidentialité de l'IdO.

Dans la chaîne d'approvisionnement actuelle de l'usine au détail, il est souvent difficile de définir les rôles que chaque partie joue au fil du temps. C'est pourquoi elles sont définies ici simplement comme la "chaîne d'approvisionnement IoT". Les utilisateurs finaux des dispositifs IoT et d'autres personnes dépendent de la chaîne logistique IoT pour protéger leur sécurité et leur vie privée, et certaines ou toutes les parties de cette chaîne logistique IoT jouent un rôle essentiel tout au long du cycle de vie du produit. En plus des autres recommandations de cette section, BITAG recommande que la chaîne d'approvisionnement IoT prenne les mesures suivantes :

- Les appareils doivent être dotés d'une **politique de confidentialité** claire et compréhensible, en particulier lorsqu'un appareil est vendu en même temps qu'un service continu.

- Les appareils devraient disposer d'un **mécanisme de réinitialisation** pour les appareils IoT qui efface toute la configuration à utiliser lorsqu'un consommateur retourne ou revend l'appareil. Les fabricants de dispositifs devraient également fournir un mécanisme permettant de supprimer ou de réinitialiser toutes les données que le dispositif respectif stocke dans le cloud.

- Les fabricants doivent fournir un **système de signalement des bogues** avec des mécanismes de soumission des bogues bien définis et une politique de réponse documentée.

- Les fabricants doivent protéger la **chaîne d'approvisionnement en logiciels sécurisés** afin d'éviter l'introduction de logiciels malveillants au cours du processus de fabrication ; les vendeurs et les fabricants doivent prendre les mesures appropriées pour sécuriser leur chaîne d'approvisionnement en logiciels.

- Les fabricants doivent **assurer le soutien d'un dispositif IoT tout au long de sa durée de vie**, depuis sa conception jusqu'à sa mise hors service, en faisant preuve de transparence sur la période pendant laquelle ils prévoient d'assurer le soutien continu d'un dispositif et sur ce que le consommateur doit attendre du fonctionnement du dispositif à la fin de sa durée de vie.

- **Les** fabricants doivent fournir des **méthodes claires permettant aux consommateurs de déterminer qui ils peuvent contacter pour obtenir de l'aide** et des **méthodes permettant de contacter les consommateurs** pour diffuser des informations sur les vulnérabilités des logiciels ou d'autres problèmes.

- Les fabricants doivent **signaler la découverte et la correction des vulnérabilités logicielles** qui représentent des menaces pour la sécurité ou la vie privée des consommateurs.

- Les fabricants doivent fournir un **processus de signalement des vulnérabilités** avec un formulaire de signalement des vulnérabilités bien défini, facile à trouver et sécurisé, ainsi qu'une politique de réponse documentée. Les fabricants devraient envisager de se conformer à la norme ISO 30111 [108], une norme pour le traitement des rapports de vulnérabilité.

8 Autres groupes s'intéressant à cette question

Bien que le BITAG ait un point de vue unique sur cette question, il convient de noter que plusieurs autres groupes se concentrent également sur divers aspects de cette question. Ces groupes sont les suivants

- Alliance pour le protocole Internet pour les objets intelligents (IPSO) [109].
- Institut des ingénieurs électriciens et électroniciens (IEEE) [110]
- Instituts nationaux des normes et de la technologie (NIST) [111]
- Groupe de travail sur l'ingénierie Internet [112]
    - LWIG (Light-Weight Implementation Guidance) [113] (en anglais)
    - 6Lo (IPv6 sur les réseaux de nœuds soumis à des contraintes de ressources) [114].
    - 6TiSCH (IPv6 sur le mode TSCH de l'IEEE 802.15.4e) [115].
    - ROLL (Routing Over Low power and Lossy networks) [116] (Routage sur les réseaux à faible puissance et à pertes)
    - CoRE (Constrained RESTful Environments) [117] (en anglais)
    - DICE (DTLS in Constrained Environments) [118] (en anglais)
    - ACE (Authentification et autorisation pour les environnements contraints) [119].
    - COSE (CBOR Object Signing and Encryption) [120] (en anglais)

    - 6lowpan IPv6 sur WPAN à faible puissance (fermé) [121] (en anglais)
- GSMA : La vie connectée [122]
- IRTF : Internet Research Task Force [123] (en anglais)
    - T2TRG : Thing-to-Thing Research Group (Groupe de recherche sur les relations entre les choses) [124]
- W3C : Worldwide Web Consortium [125]
    - WoT : Groupe d'intérêt sur le Web des objets [126]
- Commission fédérale du commerce (FTC) des États-Unis [127,128,129].
- Département du commerce des États-Unis, Administration nationale des télécommunications et de l'information (NTIA) [130, 131].
- Forum sur la gouvernance de l'Internet (FGI) [132]
- Online Trust Alliance [133]
- Comité technique mixte 1 de l'Organisation internationale de normalisation (ISO/CEI JTC1) [134] : A créé deux groupes de travail spéciaux sur la gestion et l'Internet des objets ; l'un est administré par l'ANSI.
    - Commission électrotechnique internationale [135] : Bien que la CEI ne se limite pas uniquement aux dispositifs IoT (et travaille sur toutes les technologies électriques/électroniques), elle a réalisé plusieurs documents de recherche sur l'IoT qui peuvent contenir des normes.
- InterNational Committee for Information Technology Standards (INCITS) [136] : Accrédité par l'ANSI, pour "servir de groupe consultatif technique américain central pour un effort mondial".
- Groupe de travail multipartite TRUSTe sur la protection de la vie privée dans l'IdO [137] : Vise à élaborer des normes techniques pour aider les entreprises à développer les solutions nécessaires à la protection de la vie privée des consommateurs dans l'IoT.
- Institut des ingénieurs en électricité et en électronique (IEEE) P2413 [138] : Un projet de l'IEEE concernant une norme pour un cadre architectural pour l'IoT.
- Wireless IoT Forum [139] : "N'est pas un organisme de normalisation, mais vise à fournir des exigences... aux organismes de normalisation lorsqu'il y a un manque de normes (par exemple, la connectivité sans fil à longue portée), et à favoriser le consensus lorsqu'il y a des normes concurrentes (par exemple, la découverte des appareils domestiques)."
    - Groupe "Applications" : groupe de travail qui examine les API standard.
    - Groupe Connectivité : groupe de travail évaluant l'accès radio.
    - Groupe réglementaire : groupe de travail chargé d'harmoniser les réglementations mondiales en matière d'exemption de licence et la disponibilité du spectre sous licence.
- Open Connectivity Foundation (anciennement appelée Open Interconnect Consortium) [140] : Organisation créée par Intel, Cisco et Samsung pour créer une spécification interopérable ouverte pour l'IdO. A également acquis le Forum UPnP.
- Object Management Group (OMG) [141] : Consortium international de normes technologiques à but non lucratif, effectuant un travail important sur l'IdO industriel.
    - Consortium de l'Internet industriel [142] : "... est le consortium international à but non lucratif et à adhésion ouverte... qui définit le cadre architectural et l'orientation de l'Internet industriel." Travaille à l'accélération de l'adoption des technologies WAN sans fil dédiées au marché de l'IoT. Fondé par CISCO, il comprend Accenture, Arkessa, BT Telensa et WSN.
- oneM2M [143] : Élaboration de spécifications techniques répondant au besoin d'une couche de service M2M commune pouvant être intégrée à divers matériels et logiciels.
- Société internationale d'automatisation (ISA) [144] : "Association professionnelle à but non lucratif qui établit des normes pour ceux qui appliquent l'ingénierie et la technologie pour améliorer la

gestion, la sécurité et la cybersécurité des systèmes modernes d'automatisation et de contrôle." A effectué quelques recherches sur l'IdO, mais rien n'indique l'existence d'un groupe de travail.

- OASIS [145] : "Consortium à but non lucratif qui conduit le développement, la convergence et l'adoption de normes ouvertes pour la société de l'information mondiale."
    - OASIS Advanced Message Queuing Protocol (AMQP) TC : Définition d'un protocole Internet omniprésent, sécurisé, fiable et ouvert pour la gestion de la messagerie d'entreprise.
    - OASIS Message Queuing Telemetry Transport (MQTT) TC : Fournit un protocole de transport de messagerie fiable, léger, de type publication/abonnement, adapté à la communication dans des contextes M2M/IoT où une petite empreinte de code est requise et/ou la bande passante du réseau est limitée.
    - OASIS Open Building Information Exchange (oBIX) TC : Permettre aux systèmes de contrôle mécanique et électrique des bâtiments de communiquer avec les applications d'entreprise.
- Hypercat [146] : Un consortium et une norme conduisant à un IoT sécurisé et interopérable pour l'industrie et les villes.
- Alliance AllSeen [147] : A créé AllJoyn, qui est un "écosystème ouvert et collaboratif".
- Thread Group [148] : A créé le protocole Thread, qui est un protocole de mise en réseau libre de droits pour l'Internet des objets. Offre une certification des produits.

9 Références

1] James Manika et al., L'Internet des objets : Mapping the Value Beyond the Hype, McKinsey Global Institute, juin 2015, http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the- physical-world.

[2] Brian Krebs, "IoT Reality : Smart devices, Dumb defaults ", Krebs on Security, Blog, 8 février 2016, http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/.

[3] Kalev Leetaru, " How the Internet of Things will Turn your Living Room into The Future Cyber Battleground ", 6 nov. 2015, Forbes.com, http://www.forbes.com/sites/kalevleetaru/2015/11/06/how-the-internet-of-things-will-turn-your-living-room-into-the- future-cyber-battleground/ (dernière visite le 18 nov. 2016).

[4] IEEE Standards Association, IEEE 802.15 : Wireless Personal Area Networks (PANs), https://standards.ieee.org/about/get/802/802.15.html (dernière visite le 18 novembre 2016).

[5] X10, https://www.x10.com/ (dernière visite le 18 novembre 2016).

[6] Hewlett Packard, Étude de recherche sur l'Internet des objets : rapport 2015, HP Enterprise, 2015, *disponible à l'adresse suivante* . https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[7] John Pescatore, Securing the Internet of Things Survey, Sans Institute Analyst Survey, janvier 2014, *disponible à l'adresse suivante* . https://www.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785.

[8] Charlie Osborne, " Internet of Things devices lack fundamental security, study finds ", 8 avril 2015, ZDNet, http://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds/ (dernière visite le 18 novembre 2016).

[9] Ka-Ping Yee, "Aligning security and usability". IEEE Security & Privacy 2.5 (2004) : 48-55, *disponible sur* http://zesty.ca/pubs/yee-sid- ieeesp2004.pdf.

[10] Veracode, L'Internet des objets : Security Research Study, Whitepaper, 2014, *disponible à l'adresse suivante* . https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

[11] Rebecca E. Grinter, et al, "The work to make a home network work". *ECSCW 2005*. Springer Netherlands, 2005, *disponible à l'adresse* http://www.cc.gatech.edu/~beki/c27.pdf.

[12] Yin Min Pa Pa, et al. "IoTPOT : Analysing the Rise of IoT Compromises". (2015), *disponible à l'adresse* https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

[13] Symantec, " IoT devices being increasingly used for DDoS attacks ", Symantec Security Response, 22 septembre 2016, *disponible sur :* http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks.

[14] Steve Rogerson, " IoT blamed for denial of service attacks ", IoT MTM Council, 29 avril 2015, *disponible sur* . http://www.iotm2mcouncil.org/serviceattacks.

[15] Energin Janina, " Distributed denial-of-service (DDoS attack) knocked the file-sharing site Pirate Bay offline ", 17 mai 2012, ceoworld.biz, http://ceoworld.biz/ceo/2012/05/17/distributed-denial-of-service-ddos-attack-knocked-the-file-sharing-site-pirate-bay- offline.

[16] Angela Moscaritolo, "FBI arrests six in click-fraud cyber scam that netted $14M", SC Magazine, 9 novembre 2011, http://www.scmagazine.com/fbi-arrests-six-in-click-fraud-cyber-scam-that-netted-14m/article/216399/.

[17] Sarthak Grover et Nick Feamster, The Internet of Unpatched Things, PrivacyCon 2016, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf.

[18] Bruce Schneier, "The Internet of Things Is Wildly Insecure - And Often Unpatchable", Wired, 6 janvier 2014, https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html.

[19] Bruce Schneier, " Surveillance et Internet des objets ", Blog, 21 mai 2013, https://www.schneier.com/blog/archives/2013/05/the_eyes_and_ea.html.

[20] Matt Loeb, " Internet of Things Security Issues Require a Rethink on Risk Management ", Wall Street Journal, 14 octobre 2015, http://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/.

[21] Arik Hesseldahl, " A Hacker's-Eye View of the Internet of Things ", Recode.net, 7 avril 2015, http://recode.net/2015/04/07/a- hackers-eye-view-of-the-internet-of-things/.

[22] Arik Hesseldahl, " L'Internet des objets est le nouveau terrain de jeu des hackers ", Recode.net, 29 juillet 2014, http://recode.net/2014/07/29/the-internet-of-things-is-the-hackers-new-playground/.

[23] Julie Knudson, " Security Challenges of the Internet of Things : L'absence de protocoles normalisés et les nouveaux flux de trafic de l'IoT compliquent les efforts de sécurité des administrateurs ", Enterprise Networking Planet, 13 mai 2015, http://www.enterprisenetworkingplanet.com/netsecur/security-challenges-of-the-internet-of-things.html.

[24] Reddit, Liste de discussion sur la vie privée, " J'ai acheté et retourné un ensemble de caméras de sécurité domestiques connectées en WiFi, j'ai oublié de supprimer mon compte et je peux maintenant surveiller le nouveau propriétaire ", https://www.reddit.com/r/privacy/comments/4ortwb/i_bought_and_returned_a_set_of_wifi_connected/ (dernière visite le 18 novembre 2016).

[25] Christina Cardoza, "Des pneus Princeton pour savoir si vos appareils IoT sont sûrs", SD Times, 22 janvier 2016, *disponible à l'adresse suivante* .
http://sdtimes.com/princeton-tries-to-find-out-are-your-iot-devices-safe/.

[26] Christian Dancke Tuen, "Security in Internet of Things Systems", thèse de maîtrise, Université norvégienne des sciences et de la technologie, département de télématique, juin 2015, *disponible sur* https://brage.bibsys.no/xmlui/bitstream/handle/11250/2352738/12892_FULLTEXT.pdf?sequence=1&isAllowed=y.

[27] Hewlett Packard, Étude sur la sécurité de l'Internet des objets : Smartwatches, IoT Research Series 2014,
http://go.saas.hpe.com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_Series_Smartwatches.pdf.

[28] Kim Zetter, " Hospital Networks are Leaking Data, Leaving Critical Devices Vulnerable ", 25 juin 2014,
https://www.wired.com/2014/06/hospital-networks-leaking-data/.

[29] Mario Ballano Barcena et Candid Wueest, Insecurity in the Internet of Things, 12 mars 2015, Symantec,
https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf.

[30] Katie Natopoulos, "Somebody's watching : how a simple exploit lets strangers tap into private security cameras", 3 février 2012, The Verge,
http://www.theverge.com/2012/2/3/2767453/trendnet-ip-camera-exploit-4chan.

[31] Brian Krebs, "This is Why People Fear the Internet of Things", 8 février 2016, Krebs on Security,
https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/.

[32] Brady Dale, " Huit échecs de sécurité de l'Internet des objets : Changez les mots de passe de vos routeurs lorsque vous les installez, pour l'amour du ciel ", Observer, 16 juillet 2015, http://observer.com/2015/07/eight-internet-of-things-security-fails/.

[33] Michael Winter, "Calif. youth admits Miss Teen USA 'sextortion' plot", USA Today, 12 novembre 2013,
http://www.usatoday.com/story/news/nation/2013/11/12/miss-teen-usa-sextortion-guilty-plea/3510461/.

[34] Kevin Townsend, " Malware Found in IoT Cameras Sold by Amazon ", Security Week, 11 avril 2016,
http://www.securityweek.com/malware-found-iot-cameras-sold-amazon.

[35] Johannes Ullrich, "Coin Mining DVRs : A compromise from start to finish", Internet Storm Center, SANS ISC InfoSec Forums,
https://isc.sans.edu/forums/diary/Coin+Mining+DVRs+A+compromise+from+start+to+finish/18071/.

[36] Kim Zetter, " An Unprecedented Look at STUXNET, the World's First Digital Weapon ", WIRED, 3 nov. 2014,
https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[37] Swati Khandelwal, " IoT Botnet - 25 000 caméras CCTV Hacked to launch DDoS Attack ", The Hacker News, 28 juin 2016,
http://thehackernews.com/2016/06/cctv-camera-hacking.html.

[38] Dahua, Déclaration sur la cybersécurité, communiqué de presse, 1er octobre 2016, *disponible à l'adresse suivante* .
http://www.dahuasecurity.com/en/us/single.php?nid=274.

[39] Dahua, page principale de Dahua Support Wiki, http://www.dahuawiki.com/Main_Page (dernière visite le 18 novembre 2016).

[40] Dahua, Comment créer un système de sécurité plus sûr, http://www.dahuasecurity.com/en/us/best-practices.php (dernière visite le 18 novembre 2016).

[41] Broadband Internet Technical Advisory Group (BITAG), SNMP Reflected Amplification DDoS Attack Mitigation, août 2012, http://bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf.

[42] T. Dierks & E. Rescorla, "The Transport Layer Security (TLS) Protocol 1.2", RFC 5246, Aug. 2008, https://tools.ietf.org/html/rfc5246.

[43] E. Rescorla & N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, Jan. 2012,
https://tools.ietf.org/html/rfc6347.

[44] Aaron Ardiri, "Est-il possible de sécuriser les microcontrôleurs utilisés dans le cadre de l'IoT ?", EVO Things, Blogs/Tutoriels, 27 août 2014,
https://evothings.com/is-it-possible-to-secure-micro-controllers-used-within-iot/ ;

[45] Reinhard Seiler, Blog, Truecrypt benchmark for Raspberry Pi, 20 juillet 2012, http://blog.rseiler.at/2012/07/truecrypt-benchmark- for-raspberry-pi.html.

[46] Darlene Storm, " MEDJACK : les pirates détournent les dispositifs médicaux pour créer des portes dérobées dans les réseaux hospitaliers ", Computerworld, 8 juin 2015, http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create- backdoors-in-hospital-networks.html.

[47] Kim Zetter, " How Thieves Can Hack and Disable Your Home Alarm System ", WIRED, 23 juillet 2014,
https://www.wired.com/2014/07/hacking-home-alarms/.

[48] Marek Majkowski, " Say Cheese : a snapshot of the massive DDoS attacks coming from IoT cameras ", 11 octobre 2018, Cloudflare Blog, https://blog.cloudflare.com/say-cheese-a-snapshot-of-the-massive-ddos-attacks-coming-from-iot-cameras/ (dernière visite le 18 novembre 2016).

[49] Nest, " Historique des mises à jour logicielles du thermostat d'apprentissage Nest ", Nest Support, https://nest.com/support/article/Nest-Learning-Thermostat-software-update-history (dernière visite le 18 novembre 2016).

[50] Nest, " How do I update the software on my Nest Learning Thermostat ", Nest Support, https://nest.com/support/article/How-do-I- update-the-software-on-my-Nest-Learning-Thermostat (dernière visite le 18 novembre 2016).

[51] Nick Bilton, " Le thermostat Nest laisse les utilisateurs dans le froid ", 13 janvier 2016, NYTimes, *disponible sur* .
http://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html.

[52] Catalin Cimpanu, " Security Researcher with Implanted Pacemaker Sounds the Alarm on IoT Medical Devices ", Softpedia, 5 janvier 2016,
http://news.softpedia.com/news/security-researcher-with-implanted-pacemaker-sounds-the-alarm-on-iot-medical-devices- 498448.shtml.

[53] Russ Housley, Les mots du président de l'IAB : Déclaration de l'IAB sur la confidentialité de l'Internet, IETF Journal mars 2015,
https://www.internetsociety.org/publications/ietf-journal-march-2015/words-iab-chair-12.

[54] Jane Wakefield, " Smart LED light bulbs leak wi-fi passwords ", BBC News, 8 juillet 2014, http://www.bbc.com/news/technology- 28208905.

[55] SEC Consult, "House of Keys : Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide ", Blog, 25 nov. 2015, http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html (dernière visite le 18 nov. 2016).

[56] Erik C. Davis, "Clustering and Outlier Detection : Methods and Applications in Smart Home Networks", Undergraduate Dissertation, Operations Research and Financial Engineering. Université de Princeton. Juin 2016 .

[57] Yin Zhang & Vern Paxson, "Detecting Stepping Stones", USENIX *Security Symposium,* août 2000, https://www.cs.utexas.edu/~yzhang/papers/stepping-sec00.pdf.

[58] Robert Vamosi, "Covert Hacking of IoT Trivial Say Researchers", Mocana, 28 février 2014, https://www.mocana.com/blog/2014/02/28/covert-hacking-iot-trivial-say-researchers.

[59] Lorenzo Franceschi-Bicchierai, " Internet-Connected Fisher Price Teddy Bear Left Kids' Identities Exposed ", Motherboard, 2 février 2016, http://motherboard.vice.com/read/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed.

[60] Lorenzo Franceschi-Bicchierai, " Bugs in 'Hello Barbie' Could Have Let Hackers Spy on Children's Chats ", Motherboard, 4 déc. 2015, http://motherboard.vice.com/read/bugs-in-hello-barbie-could-have-let-hackers-spy-on-kids-chats.

[61] Lorenzo Franceschi-Bicchierai, "Hacked Toymaker VTech Admits Breach Actually Hit 6.3 Million Children," Motherboard, Dec. 1, 2015, http://motherboard.vice.com/read/hacked-toymaker-vtech-admits-breach-actually-hit-63-million-children.

[62] BBC, " Mitsubishi Outlander hybrid car alarm 'hacked' ", BBC News : Technology, 6 juin 2016, http://www.bbc.com/news/technology-36444586.

[63] Darlene Storm, "Nissan Leaf secretly leaks driver location, speed to websites", ComputerWorld, 14 juin 2011, http://www.computerworld.com/article/2470123/endpoint-security/nissan-leaf-secretly-leaks-driver-location--speed-to- websites.html.

[64] Leo Kelion, " Nissan Leaf electric cars vulnerability disclosed ", BBC News : Technology, 24 février 2016, http://www.bbc.com/news/technology-35642749.

[65] Colin Neagle, " Smart refrigerator hack exposes credentials ", NetworkWorld, 26 août 2015, http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[66] Newswise, " Georgia Tech Warns of Threats to Cloud Data Storage, Mobile Devices in Latest 'Emerging Cyber Threats' Report ", communiqué de presse, 6 nov. 2013, http://www.newswise.com/articles/georgia-tech-warns-of-threats-to-cloud-data-storage-mobile-devices-in- latest-emerging-cyber-threats-report.

[67] Institute for Information Security & Privacy, Georgia Institute of Technology, Emerging Cyber Threats Report 2016, 2016, *disponible à l'adresse* http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf.

[68] Phys.Org, " Your smartwatch is giving away your ATM PIN ", 6 juillet 2016, http://phys.org/news/2016-07-smartwatch-atm-pin.html (dernière visite le 7 octobre 2016).

[69] Robert J. Ellison et al, "Evaluating and Mitigating Software Supply Chain Security Risks", Software Engineering Institute, Note technique, mai 2010, *disponible sur* http://www.sei.cmu.edu/reports/10tn016.pdf.

[70] Internet Storm Center, Survival Time : Summary, https://isc.sans.edu//survivaltime.html (dernière visite le 18 novembre 2016).

[71] Brian Krebs, " KrebsOnSecurity Hit with Record DDoS ", KrebsOnSecurity, 21 septembre 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (dernière visite le 3 octobre 2016).

[72] Flashpoint, "Attack of Things !", Blog Post, 17 septembre 2016, https://www.flashpoint-intel.com/attack-of-things/ (dernière visite le 18 novembre 2016).

[73] Drew Fitzgerald, " Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks ", Wall Street Journal, 30 sept. 2016, http://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428 (dernière visite le 3 oct. 2016).

[74] Federal Trade Commission, " ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk ", communiqué de presse, 23 février 2016, *disponible sur* https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges- insecure-home-routers-cloud-services-put.

[75] Network World, " KrebsOnSecurity moves to Project Shield for protection against DDoS attack censorship ", Ms. Smith Blog, 25 sept. 2016, http://www.networkworld.com/article/3123806/security/krebsonsecurity-moves-to-project-shield-for-protection-against-ddos- attack-censorship.html (dernière visite le 3 oct. 2016).

[76] Brian Krebs, " The Democratization of Censorship ", KrebsOnSecurity, 16 septembre 2016, https://krebsonsecurity.com/2016/09/the- democratization-of-censorship/ (dernière visite le 3 octobre 2016).

[77] Tim Greene, " Largest DDoS attack ever delivered by botnet of hijacked IoT devices ", Network World, 23 septembre 2016, http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html (dernière visite le 3 octobre 2016).

[78] Dan Goodin, " Record-breaking DDoS reportedly delivered by >145k hacked cameras ", ArsTechnica, 28 sept. 2016, http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/ (dernière visite le 3 oct. 2016).

[79] David Plonka & Elisa Boschi, L'Internet des anciens et des non gérés, 2016, *disponible sur* . https://down.dsg.cs.tcd.ie/iotsu/subs/IoTSU_2016_paper_25.pdf.

[80] David Plonka, Measurement and Analysis for the Internet of Things, 18 juillet 2016, *disponible à l'adresse suivante* . https://www.ietf.org/proceedings/96/slides/slides-96-maprg-8.pdf.

[81] Lucian Constantin, " Attackers hijack CCTV cameras to launch DDoS attacks ", Computerworld, 22 oct. 2015, http://www.computerworld.com/article/2996079/internet-of-things/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html.

[82] Kashmir Hill, "This guy's light bulb performed a DoS attack on his entire smart house", Fusion.net, 3 mars 2015, http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/.

[83] Tom Spring, " Insecurity : Pinpointing the Problems ", ThreatPost, 21 juillet 2016, https://threatpost.com/iot-insecurity-pinpointing- the-problems/119389/.

[84] DirectTV, Guide de l'utilisateur : Genie et récepteurs DVR HD antérieurs, pg. 107, http://www.directv.com/learn/pdf/System_Manuals/DIRECTV/DIRECTV_HDDVR_HR20-44.pdf.

[85] Roku, " Comment mettre à jour le logiciel de mon lecteur Roku ? ", https://support.roku.com/hc/en-us/articles/208755668-How-can-I- update-the-software-on-my-Roku-player- (dernière visite le 18 novembre 2016).

[86] Arunesh Mathur, et al. "They Keep Coming Back Like Zombies' : Improving Software Updating Interfaces", *USENIX Symposium on Usable Security and Privacy,* 2016, *disponible à l'adresse* https://www.usenix.org/system/files/conference/soups2016/soups2016-paper- mathur.pdf.

[87] David Plonka, Flawed Routers Flood University of Wisconsin Internet Time Server, 19 juillet 2006, http://pages.cs.wisc.edu/~plonka/netgear-sntp/.

[88] Comcast, " Some NetGear Routers Causing Flood of DNS Queries ", Comcast DNS News, 20 mai 2013, http://dns.xfinity.com/index.php/entry/some-netgear-routers-causing-flood-of-dns-queries.

[89] NetGear Community Discussion List, "Thousands of DNS Requests Per Second !?", 2 mars 2012, https://community.netgear.com/t5/General-WiFi-Routers/Thousands-of-DNS-Requests-Per-Second/td-p/414710.

[90] Benoit Panizzon, DDOS Attack by Netgear Products caused by CNAME instead of A record ?, [SWINOG] Discussion List, 27 juin 2013, http://lists.swinog.ch/public/swinog/2013-June/005863.html.

[91] National Security Agency, Defense in Depth, Whitepaper, 2010, *disponible sur* https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf.

[92] Vijay Sivaraman et al. " Network-Level Security and Privacy Control for Smart-Home IoT Devices ", *IEEE Wireless and Mobile Computing, Networking, and Communications.* 2015, https://www.researchgate.net/publication/281275810_Network- Level_Security_and_Privacy_Control_for_Smart-Home_IoT_Devices.

[93] Konstantinos Grivas & Stelios Zerefos, Inventaires domestiques augmentés, Conférence européenne sur l'intelligence ambiante, 2015.

[94] William Enck, et al. "TaintDroid : An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," In Proc. of the USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 2010, *available at* http://appanalysis.org/tdroid10.pdf.

[95] Disconnect, Disconnect Privacy Tool, https://disconnect.me/ (dernière visite le 18 novembre 2016).

[96] Masanobu Katagi et Shiho Moriai, Lightweight Cryptography for the Internet of Things, 2011, https://www.iab.org/wp- content/IAB-uploads/2011/03/Kaftan.pdf.

[97] GitHub, " SSL and TLS Deployment Best Practices ", SSL Labs Wiki, https://github.com/ssllabs/research/wiki/SSL-and-TLS- Deployment-Best-Practices (dernière visite le 3 octobre 2016).

[98] Mozilla, " Security/Server Side TLS ", Mozilla Wiki, https://wiki.mozilla.org/Security/Server_Side_TLS (dernière visite le 18 novembre 2016).

[99] Dan Auerbach, " 2011 In Review : Ever-Clearer Vulnerabilities in Certificate Authority System ", Electronic Frontier Foundation, 27 décembre 2011, https://www.eff.org/deeplinks/2011/12/2011-review-ever-clearer-vulnerabilities-certificate-authority-system.

[100] Wikipedia, Liste des révocations, https://en.wikipedia.org/wiki/Revocation_list (dernière visite le 18 novembre 2016).

[101] Dennis Fisher, " Final Report on Diginator Hack Shows Total Compromise of CA Servers ", ThreatPost, 31 oct. 2012, https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/.

[102] Eric Mill, " Certificate Authorities are actually a Tremendous Problem ", Blog Post, 21 juin 2013, https://konklone.com/post/certificate-authorities-are-actually-a-tremendous-problem (dernière visite le 18 novembre 2016).

[103] Chester Wisniewski, " Another certificate authority issues dangerous certificates, Naked Security ", 3 nov. 2011, https://nakedsecurity.sophos.com/2011/11/03/another-certificate-authority-issues-dangerous-certficates/ (dernière visite le 18 nov. 2016).

[104] Glenn Fleishman, "The Huge Web Security Loophole That Most People Don't Know About, And How It's Being Fixed", FastCompany, *disponible sur* http://www.fastcompany.com/3042030/tech-forecast/the-huge-web-security-loophole-that-most-people-dont-know- about-and-how-its-be.

[105] Steve Roosa, " The Flawed Legal Architecture of the Certificate Authority Trust Model ", Freedom to Tinker, 15 déc. 2010, https://freedom-to-tinker.com/blog/sroosa/flawed-legal-architecture-certificate-authority-trust-model/ (dernière visite le 18 nov. 2016).

[106] Google, Certificate Transparency Project, What is Certificate Transparency, https://www.certificate-transparency.org/what-is-ct (dernière visite le 18 novembre 2016).

[107] Level 3 Threat Research Labs, "Attack of Things !", Level 3 Blog, http://blog.level3.com/security/attack-of-things/ (dernière visite le 18 novembre 2016).

[108] Organisation internationale de normalisation, ISO/IEC 30111:2013 : Technologies de l'information - Techniques de sécurité - Processus de traitement des vulnérabilités, 2013, *disponible sur* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231.

[109] IPSO Alliance, http://www.ipso-alliance.org (dernière visite le 18 novembre 2016).

[110] Institute of Electrical and Electronics Engineers (IEEE), https://www.ieee.org (dernière visite le 18 novembre 2016).

[111] Département du commerce des États-Unis, Institut national des normes et de la technologie, http://nist.gov (dernière visite le 18 novembre 2016).

[112] Internet Engineering Task Force (IETF), http://www.ietf.org (dernière visite le 18 novembre 2016).

[113] Internet Engineering Task Force (IETF), Light-Weight Implementation Guideance (lwig) https://datatracker.ietf.org/wg/lwig/ (dernière visite le 18 novembre 2016).

[114] Internet Engineering Task Force (IETF), IPv6 Over Networks of Resource-Constrained Nodes (6lo), https://datatracker.ietf.org/wg/6lo/ (dernière visite le 18 novembre 2016).

[115] Internet Engineering Task Force (IETF), IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch), https://datatracker.ietf.org/wg/6tisch/ (dernière visite le 18 novembre 2016).

[116] Internet Engineering Task Force (IETF), Routing over Low power and Lossy networks (roll), https://datatracker.ietf.org/wg/roll/ (dernière visite le 18 novembre 2016).

[117] Internet Engineering Task Force (IETF), Constrained RESTful environments (core), https://datatracker.ietf.org/wg/core/ (dernière visite le 18 novembre 2016).

[118] Internet Engineering Task Force (IETF), DTLS in Constrained Environments (dés), https://datatracker.ietf.org/wg/dice (dernière visite le 18 novembre 2016).

[119] Internet Engineering Task Force (IETF), Authentification et autorisation pour les environnements contraints (ace), https://datatracker.ietf.org/wg/ace/(dernière visite le 18 novembre 2016).

[120] Internet Engineering Task Force (IETF), CBOR Object Signing and Encryption (cose) https://datatracker.ietf.org/wg/cose/ (dernière visite le 18 novembre 2016).

[121] Internet Engineering Task Force (IETF), IPv6 over Low power WPAN (6lowpan), https://datatracker.ietf.org/wg/6lowpan (dernière visite le 18 novembre 2016).

[122] Groupe Speciale Mobile Association (GSMA), GSMA IoT Security Guidelines, http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/ (dernière visite le 18 novembre 2016).

[123] Internet Research Task Force, http://irtf.org (dernière visite le 18 novembre 2016).

[124] Internet Research Task Force, Thing-to-Thing Research Group, https://irtf.org/t2trg (dernière visite le 18 novembre 2016).

[125] World Wide Web Consortium (W3C), http://www.w3c.org (dernière visite le 18 novembre 2016).

[126] World Wide Web Consortium (W3C), groupe d'intérêt sur le Web des objets, https://www.w3.org/WoT/IG/ (dernière visite le 18 novembre 2016).

[127] Federal Trade Commission, Bureau of Consumer Protection et Office of Policy Planning, In The Matter of The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancemenet of the Internet of Things, Docket No. 160331306-6306-01, Comments of Staff, https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection- office-policy-planning-national-telecommunications/160603ntiacomment.pdf.

[128] Commission fédérale du commerce, Internet of Things : Privacy & Security in a Connected World, Staff Report, janvier 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled- internet-things-privacy/150127iotrpt.pdf.

[129] Dennis Fisher, FTC Warns of Security and Privacy Risks in IoT Devices, 3 juin 2016, https://www.onthewire.io/ftc-warns-of- security-and-privacy-risks-in-iot-devices/ (dernière visite le 18 novembre 2016).

[130] National Telecommunications & Information Administration, Internet of Things, https://www.ntia.doc.gov/category/internet- things (dernière visite le 18 novembre 2016).

[131] L'administration nationale des télécommunications et de l'information, le ministère américain du commerce, recherche Comment on Potential Policy Issues Related to Internet of Things, Communiqué de presse, 5 avril 2016, https://www.ntia.doc.gov/press- release/2016/us-department-commerce-seeks-comment-potential-policy-issues-related-internet-thi.

[132] Forum sur la gouvernance de l'Internet, Coalition dynamique sur l'Internet des objets, https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/827-dciot-2015-output-document- 1/file.

[133] Online Trust Alliance, Internet of Things, 19 septembre 2016, https://otalliance.org/initiatives/internet-things (dernière visite le 18 novembre 2016).

[134] Organisation internationale de normalisation (ISO), Comité technique mixte ISO/CEI sur les technologies de l'information, http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?c ommid=45020 (dernière visite le 18 novembre 2016).

[135] Commission électrotechnique internationale (CEI), http://www.iec.ch/ (dernière visite le 18 novembre 2016).

[136] Comité international pour les normes de technologie de l'information, http://www.incits.org/ (dernière visite le 18 novembre 2016).

[137] TRUSTe, Privacy Risk Summit 2016, 8 juin 2016, http://www.truste.com/events/privacy-risk/.

[138] Institute of Electronic and Electrical Engineers (IEEE), P2413 - Standard for an Architectural Framework for the Internet of Things (IoT), https://standards.ieee.org/develop/project/2413.html (dernière visite le 18 novembre 2016).

[139] Wireless IoT Forum, http://www.wireless-iot.org/ (dernière visite le 18 novembre 2016).

[140] Open Connectivity Foundation, https://openconnectivity.org/ (dernière visite le 18 novembre 2016).

[141] Object Management Group, http://www.omg.org/ (dernière visite le 18 novembre 2016).

[142] Industrial Internet Consortium, http://www.iiconsortium.org/ (dernière visite le 18 novembre 2016).

[143] oneM2M, http://www.onem2m.org/ (dernière visite le 18 novembre 2016).

[144] Bill Lydon, "Internet of Things : Industrial automation industry exploring and implementing IoT", InTech Magazine, mars-avril 2014, *disponible à l'adresse* https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/mar-apr/cover-story-internet-of-things/.

[145] OASIS, OASIS Committee Categories:IoT/M2M, https://www.oasis-open.org/committees/tc_cat.php?cat=iot (dernière visite le 18 novembre 2016).

[146] HYPERCAT, http://www.hypercat.io/ (dernière visite le 18 novembre 2016).

[147] AllSeen Alliance, https://allseenalliance.org/ (dernière visite le 18 novembre 2016).

[148] Thread, http://threadgroup.org/ (dernière visite le 18 novembre 2016).

10 Contributeurs et réviseurs de documents

- Fred Baker, *CISCO*
- Steven Bauer, *MIT*
- Richard Bennett
- Don Bowman, *Sandvine*
- William Check, *NCTA*
- kc claffy, *UCSD/CAIDA*
- David Clark, *MIT*
- Shaun Cooley, *CISCO*
- Amogh Dhamdhere, *UCSD/CAIDA*
- Nick Feamster, *Université de Princeton*
- Francis Ferguson, *niveau 3*
- Joseph Lorenzo Hall, *Centre pour la démocratie et la technologie*
- Ken Ko, *ADTRAN*
- Jason Livingood, *Comcast*
- Patrick McManus, *Mozilla*
- Chris Morrow, *Google*
- Donald Smith, *CenturyLink*
- Barbara Stark, *AT&T*
- Darshak Thakore, *CableLabs*
- Matthew Tooley, *NCTA*
- Jason Weil, *Charter Communications*
- Greg White, *CableLabs*
- Todd Whitenack, *Cellcom*

David Winner, *Charter Communication*