Internet des objets

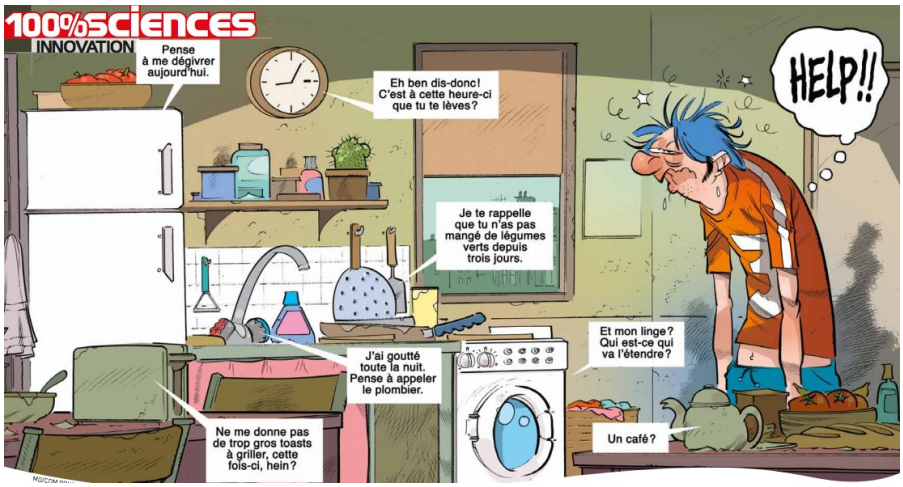
Source
Wikipédia
« Internet des objets »

L'**Internet des objets**, ou **IdO** (en anglais *Internet of Things*, ou *IoT*) est l'interconnexion entre Internet et des objets, des lieux et des environnements physiques. L'appellation désigne un nombre croissant d'objets connectés à Internet permettant ainsi une communication entre nos biens dits physiques et leurs existences numériques. Ces formes de connexions permettent de rassembler de nouvelles masses de données sur le réseau et donc, de nouvelles connaissances et formes de savoirs.

Considéré comme la troisième évolution de l'Internet, baptisé Web 3.0 qui fait suite à l'ère du Web social, l'Internet des objets revêt un caractère universel pour désigner des objets connectés aux usages variés, dans le domaine de la e-santé, de la domotique ou du *quantified self*.

L'Internet des objets est en partie responsable d'un accroissement exponentiel du volume de données généré sur le réseau, à l'origine du big data (ou mégadonnées en français).

Selon une équipe de l'ETH de Zurich, du fait des smartphones puis du nombre croissant d'objets connectés, en dix ans (2015-2025), 150 milliards d'objets devraient se connecter entre eux, avec l'Internet et avec plusieurs milliards de personnes. L'information issue de ces mégadonnées devra de plus en plus être filtrée par des algorithmes complexes, ce qui fait craindre une moindre protection des données personnelles, une information des personnes et de la société de moins en moins autodéterminée notamment en cas d'appropriation exclusive de filtres numériques par des entités (gouvernementales ou privées) qui pourraient alors manipuler les décisions. L'ETH plaide donc pour des systèmes d'information ouverts et transparents, fiables et contrôlés par l'utilisateur.



Source
VPN Zine
11 janvier 2016

1. La vie privée dans l'Internet des objets

L'Internet des objets, sans en avoir l'air, change radicalement notre relation avec la technologie et des données à caractère personnel que nous sommes au bord d'une explosion de données d'appareils

inter-connectés. Comme avec toutes les nouvelles technologies révolutionnaires, le déploiement des objets connectés apporte de nouveaux défis pour les entreprises, les organismes de réglementation, les consommateurs et en fait quiconque se soucie de l'utilisation responsable des données.

De profonds changements en cours

De nos jours, il n'est pas difficile d'imaginer un monde dans lequel notre voiture, sur le chemin du domicile, communique avec notre chauffage à la maison, garantissant ainsi que qu'il soit à température à notre arrivée. On peut également imaginer que notre réfrigérateur commande automatiquement les aliments dès qu'il commence à en manquer ou qu'il envoie des messages d'alertes en cas de givrage trop important. Les avancées technologiques nous plongent dans un monde nouveau, de dépendance complète à la technologie chargée de tout surveiller.

La maison connectée

La domotique, ou maison connectée, permet via des systèmes domotiques, de rendre la maison plus intelligente : on l'appelle aussi smarthome. Les objets concernés sont aussi divers que les ampoules, cadres, thermostats, sécurité, caméras, volets, serrures, réfrigérateurs, radiateurs, détecteurs de fumée, et aussi des plantes…

La santé ou e-santé

Ces objets connectés pour la santé aident, par exemple, les personnes à prendre leurs constantes comme le diabète, et permettent le maintien à domicile des personnes malades et dépendantes par l'aménagement du logement, par exemple en géolocalisent des personnes fragiles.

La smart city

À l'échelle d'une ville et non plus seulement d'une maison, l'IoT offre une mutualisation des énergies par bâtiments et quartiers, des voitures connectées et partagées dans un immeuble, du mobilier urbain et des institutions connectés pour fournir des services.

Le commerce et les loisirs

Les objets connectés relient le consommateur aux boutiques et aux sites d'e-commerce. Ils mesurent également les performances personnelles (*quantified self*). Les vêtements deviennent interactifs, les montres et bracelets connectés donnent des indications, les lunettes affichent des données, la réalité augmentée vous fait vivre une situation de fiction !

Les transports

De plus en plus utilisés par les communes, les objets servent à informer en temps réel d'une place qui se libère dans une rue, à piloter une voiture autonome, à recharger un forfait sur smartphone, et vont jusqu'à contrôler le trafic avec des drones.

Problématique de la vie privée

Cependant, alors que tant d'aspects de nos vies sont de plus en plus connectés, comment peut-on en profiter sans mettre en péril notre sécurité ou le respect de notre vie privée ? Cibles et acteurs passifs, les consommateurs peuvent raisonnablement craindre que le respect de leur vie privée soit fortement compromis. Déjà les exemples ne manquant pas. Par exemple, les personnes possédant une Smart TV Samsung ont été choquées d'apprendre que ses fonctionnalités de reconnaissance vocale impliquaient l'enregistrement et l'utilisation des conversations des utilisateurs, chez eux, par l'intermédiaire des micros incorporés dans cette télévision. Avec ce type de révélations, les utilisateurs ont l'impression de perdre le contrôle sur les informations et peut-être même perdre le contrôle de leurs objets.

Contrôler ce qui partagé

L'Internet des Objets ne peut gagner la confiance des utilisateurs qu'en faisant la transparence sur les données qui sont collectés, et des limites de partage qui sont définies. Les utilisateurs veulent clairement pouvoir contrôler le partage des données de de tout objet afin de contrôler la diffusion de ces données, entre autres avec leur famille et leurs amis, de manière pratique et ordonnée. Cela implique des accords de confidentialité justement respectés aussi bien dans leur limites que dans leur durée. Ainsi de manière toute aussi importante, la suppression des données doit être effectuée

intégralement lorsque les parties concernées en font la demande.

Définir des normes

La manière la plus raisonnable de protéger la vie privée consiste à utiliser des plateformes et des normes ouvertes et cohérentes. Il y a nécessité d'établir des standards validés permettant d'établir des connexions sécurisées entre les appareils, les services et les applications. Pour le moment, il y a peu de concertations. Chacun développe ses solutions dans son coin. Une fois que les utilisateurs auront des capacités sur le contrôle sur leurs informations, nous pourrons vraiment entrevoir la totalité du potentiel de tout ce que cette technologie a à offrir. Le succès d'internet repose sur l'adoption généralisée de protocoles de communication clairement définis comme TCP/IP, MAIL, FTP, SMTP, HTTP, HTTPS, VPN etc.). L'ensemble de ces protocoles représente un langage commun à tous les systèmes connectés mais en l'absence d'un tel langage commun, l'internet se réduirait à un assemblage hétéroclite de réseaux propriétaires et incompatible entre eux.

En l'absence de normes et de standards universels, le développement de l'internet des objets présente un grave risque de fragmentation. Sans définition de protocoles communs, ouverts et libres de droit sans licence, une guerre des compagnies multinationales semblable jadis à la lutte entre les défenseurs du DVD-ROM, du DVD-R et du Blu-ray, risquent de voir le jour. Et dans ce contexte, les considération sur le respect de la vie privée risquent de ne pas peser très lourd.

Problématique de la sécurité

Selon une enquête Hewlett-Packard et sa division Fortify, sur 10 appareils dotés d'une interface utilisateur, 6 présentaient des failles, comme par exemple une vulnérabilité aux attaques sur les éléments dynamiques ou encore authentification faible. 90 % des appareils recueillaient des données personnelles et 60 % d'entre eux possédaient une interface utilisateur non sécurisée. La nécessité de mettre à jour les firmware pour corriger les failles n'est pas assuré par les utilisateurs. Avec la hausse constante du nombre d'objets connectés, les préoccupations liées à la sécurité connaissent forcément une croissance exponentielle, d'autant qu'on en est qu'au début. On constate d'ailleurs que les rapports les plus alarmants sur le sujet se succèdent, sans aboutir à une réelle prise de conscience.

Sécuriser les objets domestiques

Étourdis par l'euphorie de toute cette stimulation, les développeurs et les industriels reportent beaucoup trop les questions de sécurité. Ils pensent tous ces objets en terme d'interactivité, d'innovation, de séduction des consommateurs, mais très peu en terme de sécurité ou de durabilité de cette sécurité. Si cette dernière est oubliée, des dispositifs sécurisés à l'achat deviendront exposés au piratage au fil du temps. Des hackers pourraient alors ouvrir à distance les portes d'une maison, prendre le contrôle d'un véhicule ou encore saboter de multiples appareils connectés…

Protéger les entreprises

Les entreprises aussi vont vite se retrouver confrontées à cet aspect de la sécurité. Elles doivent tout à la fois évaluer soigneusement les impacts en terme de sécurité de tous ces dispositifs et gérer les flux de cette myriade de dispositifs qu'elles vont installer sur leurs réseaux. D'autant que l'interaction entre les objets eux-mêmes créé des problèmes en cascade. Quelques problèmes de sécurité sur un téléphone mobile peuvent rapidement générer 50 à 60 vulnérabilités lorsque plusieurs objets connectés sont utilisés dans un foyer ou une entreprise connectés. Chaque objet connecté déployé en entreprise devient ainsi une porte à sécuriser. Le travail peut rapidement devenir herculéen.

Ce qui nous attend

On voit que dans ce vaste domaine de l'Internet des objets, tout reste à faire, mais que les premiers balbutiements ne sont pas très encourageants pour la sécurité et pour le respect de la vie privée. Seul un refus des consommateurs et des entreprises pour adopter ces objets posant trop de problèmes, pourrait rapidement infléchir cette politique de l'autruche de la part des constructeurs et développeurs. La définition de standard de sécurité, de règles de respect de la vie privée, d'éducation des consommateurs, sont les seuls sorties possibles de cette ornière vers laquelle glissent les sociétés high-tech qui développe cet Internet des objets, faute de motivation, faute de courage, faute de renoncer au profit le plus rapide, la plus facile.

Source
Psychomédia
6 décembre 2016

2. Des poupées connectées émettent des pubs ciblées aux enfants et permettent aux voisins et passants d'écouter

À l'approche de Noël, l'UFC-Que Choisir dénonce des lacunes concernant la sécurité et la protection des données personnelles de la poupée connectée Mon amie Cayla (voir ci-contre) et du robot connecté i-Que vendus en France. Ailleurs, la poupée Hello Barbie, notamment, présente les mêmes lacunes.

Ces jouets disposent d'un microphone intégré qui se connecte par Bluetooth à une application mobile, préalablement téléchargée par l'utilisateur sur son smartphone ou sa tablette. Le jouet peut comprendre ce que dit l'enfant et y répondre.

Les fabricants « ont fait le choix d'une connexion simple et rapide, aucun code d'accès ou procédure d'association entre ces jouets et les téléphones / tablettes n'est exigé avant la connexion au jouet, ce qui garantirait pourtant que seul le propriétaire puisse s'y connecter ».

« Un tiers situé à 20 mètres du jouet peut s'y connecter par Bluetooth et entendre ce que dit votre enfant à sa poupée ou à son robot, sans que vous en soyez averti. La connexion peut même se faire à travers une fenêtre ou un mur en béton et le nom du Bluetooth, « Cayla » et « i-Que », permet très simplement d'identifier les poupées. Plus grave encore… Un tiers peut prendre le contrôle des jouets, et, en plus d'entendre votre enfant, communiquer avec lui à travers la voix du jouet. »

« Les conditions contractuelles les autorisent, sans consentement express, à collecter les données vocales enregistrées par Cayla et i-Que, et ce, pour des raisons étrangères au strict fonctionnement du service. Ces données peuvent ensuite être transmises, notamment à des fins commerciales, à des tiers non identifiés. Les données sont aussi transférées hors de l'Union européenne, sans le consentement des parents : « aux États-Unis, ou vers les autres territoires concernés où les lois sur la protection de la vie privée ne sont peut-être pas aussi complètes que celles du pays où vous résidez et/ou dont vous êtes ressortissant » ! »

Les sociétés fabricantes n'hésitent pas à faire de la publicité ciblée à destination de vos enfants. Les conditions contractuelles supposent que le simple fait de visualiser une publicité ciblée, constitue de votre part, un accord express à recevoir de telles publicités ciblées. L'étude a ainsi révélé que Cayla et i-Que prononcent régulièrement des phrases préprogrammées, faisant la promotion de certains produits - notamment des produits Disney ou des références aux dessins animés de Nickelodeon.

Loin d'être des cas isolés, Cayla et i-Que reflètent un problème général de sécurité et de données personnelles des jouets connectés. En effet, l'étude commanditée par nos homologues norvégiens souligne que la poupée Hello Barbie (à gauche) est sujette aux mêmes griefs. »

« La protection des données personnelles des utilisateurs français est prévue par la loi *Informatique et Libertés* mais semble avoir été oubliée par les sociétés fabricantes. »

« L'UFC-Que Choisir appelle les parents à réfléchir à deux fois avant d'acheter la poupée Cayla et le robot i-Que ; rappelle qu'en cas de vente à distance, ils bénéficient d'un délai de rétractation de 14 jours. Pour ceux déjà équipés et qui souhaitent le conserver, l'association les invite à n'utiliser le jouet connecté qu'en leur présence, ou à défaut de l'éteindre. »

Elle saisit aussi la CNIL et la DGCCRF.

Source
presse-citron.net
Louise Millon
12 août 2019

3. Comment les enceintes connectées peuvent (facilement) devenir des armes

Un chercheur en sécurité a évoqué le fait que les enceintes connectées pouvaient devenir des armes utilisées par des personnes mal intentionnées pour diffuser des sons particulièrement nuisibles. Voici ce qu'il a indiqué à ce sujet.

Lors d'une conférence sur la sécurité qui s'est tenue ce dimanche à Las Vegas, un chercheur du nom de Matt Wixey a expliqué comment les enceintes connectées pouvaient se transformer en arme. Le responsable de la recherche en cybersécurité chez PWC UK a expliqué que celles-ci pouvaient facilement être exploitées pour diffuser des sons nuisibles.

Les enceintes connectées, de nouvelles armes potentielles qui peuvent être utilisées à grande échelle

Le chercheur a expliqué qu'il avait réalisé plusieurs expériences lui ayant permis de prendre le contrôle de certains appareils et de diffuser un son. Selon lui, il est donc assez aisé de « causer des dommages physiques, harceler des individus ou perturber les grandes organisations » avec des enceintes connectées ou d'autres appareils comme des casques sans fil. D'autre part, il aurait également été en mesure de générer « suffisamment de chaleur pour faire fondre les composants internes » d'un appareil intelligent.

Pour ce faire, il a d'abord recherché des réseaux WiFi et des connexions Bluetooth peu sécurisés. Il y a ensuite diffusé des malwares que son équipe et lui-même avaient préalablement conçus. Certaines des attaques ont été effectuées à distance, là où d'autres nécessitaient forcément un accès physique aux appareils.

Comme l'a expliqué Matt Wixey à Wired, il suppose que ce genre d'attaques a le potentiel de se multiplier dans les années à venir. Il évoque aussi les dangers potentiels en ajoutant : « Les attaques par des cyberarmes acoustiques pourraient potentiellement se faire à une échelle beaucoup plus grande en utilisant quelque chose comme les systèmes de sonorisation de zones commerciales ou dans les immeubles de bureaux ».

Pour rappel, une précédente enquête datée d'il y a environ un an pointait du doigt le fait que la technologie était de plus en plus utilisée dans des cas de violences faites aux femmes. Des témoignages évoquaient alors des changements sonores de la musique, des augmentations de température ou des modifications du code de la serrure de l'entrée.

Source
01net.com
Gilbert Kallenborn
15 août 2019

4. Armes acoustiques : nos enceintes connectées peuvent-elles nous faire du mal à notre insu ?

La multiplication de ces objets connectés crée un nouveau risque. Piratés, ils pourraient diffuser des infrasons et des ultrasons nocifs, pouvant provoquer nausées, maux de têtes et autres désagréments physiques chez les utilisateurs

L'ennemi le plus dangereux est toujours celui qu'on ne voit pas et qu'on entend pas. Et pour Matt Wixey, chercheur en sécurité chez PWC, les enceintes et les casques connectées pourraient bien rentrer dans cette définition. A l'occasion de la conférence DEF CON 27 à Las Vegas, l'expert s'est demandé s'il était possible, pour un pirate, d'infliger physiquement du mal à l'utilisateur d'un tel appareil sans même être détecté. Et selon lui, la réponse est oui.

Il suffirait, en effet, qu'une personne mal intentionnée arrive à pirater une enceinte ou un casque, et fasse émettre des signaux suffisamment forts à des fréquences inaudibles, dans la gamme des ultrasons (> 20 kHz) ou des infrasons (< 20 Hz). Des études scientifiques ont en effet montré que ce type de sons pouvaient affecter notre santé, en provoquant des acouphènes, de la nausée, des maux de tête, de la fatigue, de sauts d'humeur voire de la dépression. Or, certaines enceintes et certains casques disponibles dans le commerce sont parfaitement capables d'émettre ces sons à une puissance suffisante pour être nuisible.

Plusieurs appareils épinglés

Pour le prouver, le chercheur a sélectionné une petite dizaine d'appareils et les a manipulés pour en extraire des ondes ultrasoniques ou infrasoniques dans une chambre sourde (anéchoïque). Parmi eux figurent un PC portable, un smartphone, une enceinte Bluetooth, une enceinte intelligente et un casque. Mais aussi des appareils professionnels comme les cornes d'amplification ou les enceintes paramétriques.

Résultat : plusieurs appareils pouvaient effectivement générer des ultrasons ou des infrasons à des niveaux trop élevés au regard des recommandations scientifiques. L'enceinte intelligente et le casque étaient même capables de briller dans les deux domaines. « Ces appareils pourraient donc, en théorie, être piratés et transformés en armes acoustiques », explique Matt Wixey dans Wired. Alertés

par le chercheur, les fournisseurs épinglés ont apporté des correctifs pour éliminer ce risque.

Un tel scénario d'attaque peut sembler assez ésotérique. Mis à part le cas d'un voisin pirate et sadique, qui s'amuserait à créer ni vu ni connu des acouphènes chez un particulier ? Pourtant, ce risque existe et ne doit pas être négligé. D'ailleurs, depuis des années, les militaires explorent la voie des armes acoustiques.

D'après le chercheur en sécurité Ryan Littlefield, les premières recherches dans le domaine dateraient de la Première Guerre mondiale. Dans les années 60, l'acousticien français Vladimir Gavreau avait analysé les effets néfastes, voire fatals, des ondes acoustiques ultrabasses (7 Hz). Il aurait même développé en secret un canon acoustique pour l'armée française.

Les canons acoustiques ont déjà fait leurs preuves

Puis c'est au tour de l'armée américaine d'explorer le filon. En 1973, elle a expérimenté des attaques psychoacoustiques pour altérer la combativité des soldats vietnamiens. Des infrasons et ultrasons puissants étaient diffusés depuis un hélicoptère.

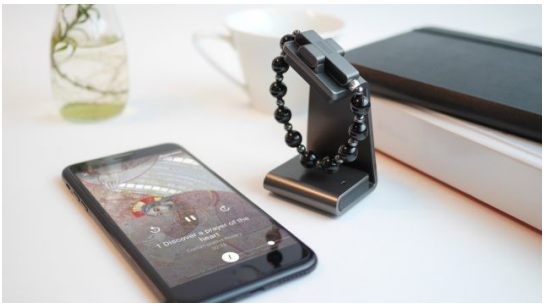
Plus récemment, l'armée américaine a fait l'acquisition, dans les années 2000, d'un canon acoustique capable de diffuser de manière ciblée des sons puissants à plus de 5 kilomètres. Des appareils similaires sont désormais utilisés un peu partout dans le monde par les forces de l'ordre dans le cadre de manifestations.

Bref, le risque acoustique n'est pas à prendre à la légère. Jusqu'à présent, l'usage des armes acoustiques a toujours été très circonscrit. Mais la multiplication des enceintes connectées dans les foyers ouvre un nouveau champ de possibilités qu'il faut désormais analyser.

Source
Les Numériques
Mathieu Chartier
22 octobre 2019

5. eRosary : le chapelet connecté du Vatican lancé avec une grosse faille de sécurité

Le Vatican a lancé urbi et orbi un chapelet connecté pour gérer ses prières à l'aide d'une application. Vendu 99 €, cet accessoire a connu des débuts un brin infernaux après la découverte d'une faille de sécurité (depuis exorcisée).



C'est en partenariat avec le constructeur taïwanais Acer que le Vatican a imaginé un chapelet connecté, commercialisé depuis quelques jours au prix de 99 € sous le pieux nom d'eRosary. Certifié IP67, équipé d'une batterie de 15 mAh, intégrant un module Bluetooth 5.0 et fonctionnant de pair avec une app Android ou iOS (Click to Pray), il promet jusqu'à quatre jours de dévotions sur une charge, fonctionne à l'aide d'un processeur intégré à sa croix et dispose d'un gyroscope.

Avec ce produit, le Vatican espère attirer les jeunes vers la prière, sachant que l'app Click to Pray a été lancée plus tôt cette année et permet d'être accompagné dans ses *pater*, *credo* et autres *miserere* via des contenus personnalisés et des guides audio. Il suffit d'effectuer un signe de croix avec le chapelet connecté en main pour lancer l'application sur son smartphone, puis de le secouer pour changer de prière. Rangé dans la poche ou le sac, l'eRosary se transforme en capteur d'activité, capable d'estimer le nombre de pas effectués et les calories brûlées dans sa dévote existence.

Les voies du Seigneur trop aisément pénétrables

Les développeurs y ont cependant perdu leur latin, cet objet connecté étant victime d'une importante faille de sécurité à son lancement, repérée par un expert français en sécurité informatique, Baptiste Robert (@fs0c131y sur Twitter). Il ne lui a fallu que 15 min pour venir à bout des protections de l'app du Vatican, avant de se rendre compte qu'il suffisait de connaître l'adresse email

d'un utilisateur pour prendre facilement le contrôle de son compte ainsi damné... et donc accéder à toutes ses données personnelles.

En effet, le code utilisé pour valider une connexion était présent dans la réponse envoyée à l'application. Or, celle-ci pouvait être interceptée. Il ne restait alors plus au diabolique hacker qu'à utiliser ce code et l'adresse email pour s'identifier sur l'app. Fort heureusement, le Vatican a été assez réactif et a rapidement corrigé cette faille de sécurité après avoir été alerté par Baptiste Robert. Béni soit-il...

Source
Clubic
Alexandre Boero
17 octobre 2019

6. Kaspersky a recensé 105 millions d'attaques contre des objets connectés au premier semestre

Le nombre d'attaques détectées sur les six premiers mois de l'année est environ neuf fois supérieur à celui enregistré au premier semestre 2018.

Les équipements IoT sont de plus en plus nombreux, et leur croissance s'accélère année après année. Le problème, c'est que les objets connectés sont historiquement moins bien protégés contre les cyberattaques. Ils représentent une proie idéale pour les hackers, comme en témoignent les dizaines de millions d'attaques détectées par les honeypots (des leurres qui appâtent les attaquants pour étudier leurs activités) de Kasperksy.

Mirai et Nyadrop, l'infernal duo de malwares

Le spécialiste de la cybersécurité a détecté 105 millions d'attaques contre des équipements de l'IoT au cours du premier semestre 2019, soit neuf fois plus d'assauts sur un an. Au premier semestre 2018, seules 12 millions d'attaques furent recensées, provenant de 69'000 adresses IP. Kaspersky affirme qu'au cours du premier semestre, les attaques sont provenues de 276'000 adresses IP différentes.

L'expansion des objets connectés incite naturellement les hackers à en tirer profit. Attaques DDoS, utilisation de l'objet comme proxy pour mener d'autres activités malveillantes... Souvent, les utilisateurs ne se rendent compte de rien.

Le roi des malwares, c'est le botnet Mirai, connu pour avoir infecté des centaines de milliers de caméras connectées et d'avoir lancé des attaques autour de 1 Tbit/s. Celui-ci serait responsable de 39 % des attaques sur l'IoT. Mirai exploite d'anciennes vulnérabilités, non corrigées ni résolues, pour prendre le contrôle.

La seconde technique la plus répandue, avec 38,57 % des attaques, est connue sous le nom de Nyadrop. Ce malware mène une attaque par force brute sur les mots de passe, et sert même de base pour le téléchargement de Mirai. Un duo infernal.

Un troisième botnet, Gafgyt, cible aussi les objets connectés avec 2,12 % des attaques. Il opère aussi par la force brute.

La Chine, source principale d'attaques des IoT

D'où viennent les infections ? Sur les 105 millions d'attaques recensées au premier semestre, les chercheurs notent que la Chine fut la source de 30 % d'entre elles, ce qui fait de l'empire du Milieu le principal foyer émetteur de cyberattaques de l'IoT. Le Brésil est également bien pourvu en hackers avec 19 %, devant l'Égypte (12 %).

Si le nombre d'attaques explose, leur provenance est aussi chamboulée. Il y a tout juste un an, ce n'est pas la Chine (alors 14 %) qui arrivait en tête, mais le Brésil, d'où partaient 28 % des infections. Le Japon complétait le podium (11 %).

Pour Dan Demeter, chercheur en sécurité chez Kaspersky, « nous assistons à une intensification des attaques contre l'IoT. (...) Nous pouvons dire que l'Internet des objets est un terrain fertile pour ceux utilisant des méthodes même les plus primitives, consistant par exemple à deviner les combinaisons de mot de passe et d'identifiant ». Et l'expert de rappeler que les combinaisons les plus répandues restent « support/support », puis « admin/admin » et « default/default ».

Mises à jour systématiques, changement des mots de passe et VPN sont considérés comme les ingrédients de base de la recette de protection.

Source
bfmtv.com
Elsa Trujillo
28 septembre 2020

7. Piratée, une machine à café connectée devient incontrôlable

Un chercheur en sécurité informatique est parvenu à pirater une machine à café connectée, de façon à simuler une attaque par rançongiciel.

Elle aura réclamé une rançon pour fonctionner à nouveau. Une machine à café connectée a fait les frais d'un piratage, orchestré par le chercheur en sécurité informatique Martin Hron, d'Avast.

Il aura tout de même fallu une semaine de travail, et de minutieux efforts pour démonter la machine, afin que Martin Hron parvienne à ses fins, relève le site spécialisé *Ars Technica*.

Une fois la machine sous contrôle, le chercheur en sécurité est parvenu non seulement à allumer le brûleur à distance mais aussi à faire couler de l'eau, à faire tourner le moulin à grains ou encore à afficher un message, clignotant et insistant, de demande de rançon. Devenue incontrôlable, la machine devait être débranchée en dernier recours pour se remettre à fonctionner normalement.

Une mise en garde

En sa démarche, Martin Hron voit un énième signal d'alarme à destination des concepteurs d'objets connectés. « Ce qui s'est produit (avec cette machine) pourrait très bien se produire pour d'autres objets connectés », avertit-il ainsi, comme bien d'autres chercheurs en sécurité avant lui.

La faille de sécurité se situait en l'occurrence au niveau de la liaison Wi-Fi, destinée à relier la machine à café à l'application de configuration installée sur smartphone, mais aussi au niveau du programme de mise à jour de l'appareil.

Pour Martin Hron, il s'agit de faire en sorte que les concepteurs d'objets connectés accordent une plus grande vigilance à la sécurisation de leurs produits, qu'il s'agisse des innovations tout récemment mises sur le marché ou des plus vieux modèles encore en circulation.

Anodins au premier abord, ces piratages peuvent en réalité rapporter gros à leurs auteurs. En 2016, une équipe de chercheurs était ainsi parvenue à pirater à distance le modèle d'ampoules connectées Philips Hue, relevait le *New York Times*. Ces simples objets connectés avaient pu être utilisés pour envoyer un logiciel malveillant à d'autres objets connectés au même réseau... et récupérer ainsi, potentiellement, un bien plus large éventail d'informations.

Source
The Conversation
Émilie Bout,
Valeria Loscri
6 juin 2021

8. Appareils connectés et cybersécurité : imaginer des attaques pour apprendre à se défendre

En 2015, deux chercheurs ont trouvé une vulnérabilité qui permettait de prendre le contrôle à distance d'une Jeep Cherokee, y compris son système de direction et de freinage. Cette découverte avait entraîné un retrait du marché de 1,4 million de véhicules.

En 2020, NCC Group a réalisé une analyse de sécurité approfondie sur onze modèles de sonnette sans fil, produits par des géants du numérique tels que Ring (filiale d'Amazon), Vivint et Remo. Ils ont montré que diverses vulnérabilités permettaient de s'insérer dans le réseau de votre maison ou de vous espionner. Cette enquête a donné lieu à un dépôt de plainte contre Amazon pour « protections insuffisantes » contre le piratage.

Le marché des appareils connectés n'a cessé de croître ces dernières années. À l'hôpital par

exemple, des thermomètres connectés surveillent la température des réfrigérateurs pour que les médicaments soient conservés dans des conditions convenables. Au quotidien, ampoules et balances connectées arrivent dans les logements, montres connectées à nos poignets, et aides aux manœuvres de stationnement dans nos véhicules.

Ces objets connectés constituent ensemble ce qu'on appelle l'« internet des objets » (soit « Internet of Things » ou « *IoT* », en anglais). Ils sont devenus une véritable aire de jeu pour les attaquants. Au moins 20 % des organisations ont subi une attaque en lien avec des dispositifs IoT entre 2015 et 2018 dans le monde. Par conséquent, sécuriser ces appareils, de plus en plus fréquents dans nos vies, est un enjeu primordial. Face à ces menaces, les entreprises et la recherche sont forcées d'adopter une stratégie basée sur l'attaque.

Quand l'attaque est la meilleure des défenses

Se mettre à la place d'un attaquant permet de mieux comprendre le fonctionnement des appareils IoT, en les détournant de leur fonctionnalité première. Ceci permet aussi d'anticiper les actions des attaquants et d'utiliser les mêmes outils et techniques, pour évaluer la sécurité des systèmes IoT et pour trouver de nouvelles vulnérabilités, des failles qui permettent de s'introduire dans le système.

Par exemple, une des failles les plus simples d'exploitation pour un cybercriminel est de trouver les identifiants de connexion par une attaque dite de « force brute » afin d'avoir accès a l'appareil. De plus, les utilisateurs ne modifient pas forcément les identifiants définis par défaut lors de la première utilisation. Il suffit alors pour un attaquant de retrouver les identifiants définis par le constructeur (la plupart du temps le même pour chaque type d'appareil) et de se connecter à un appareil afin d'avoir accès au réseau complet.

Cette faille a été utilisée lors de l'attaque Mirai Botnet en 2016. Les attaquants avaient identifié les objets IoT vulnérables qui utilisaient des identifiants et de mots de passe par défaut pour se connecter et installer un logiciel malveillant permettant d'effectuer des attaques à grande échelle. Plusieurs grandes entreprises responsables du trafic web, telles que OVH ou Dyn, en ont été victimes, ce qui a entraîné de nombreuses difficultés d'accès à Twitter ou Airbnb par exemple.

Cette faille a aussi permis a des attaquants de s'introduire dans le réseau d'un casino, afin d'avoir accès aux données des clients (identité, numéro de compte, etc.) par le biais d'un thermomètre déployé dans un aquarium.

Les failles liées aux spécificités des appareils connectés sont de plus en plus exploitées. Ces appareils fonctionnent sur batterie et sont pourvus de ressources mémoires limitées. Pour saturer le fonctionnement de ces éléments (batterie, mémoire), un attaquant peut envoyer de nombreuses requêtes à l'appareil et ainsi provoquer son arrêt – on parle alors d'attaque par « déni de service » (« DDoS »).

L'un des objectifs est d'identifier les « zones à risques » les plus évidentes dans le réseau d'objet connecté, afin de créer des solutions le plus rapidement possible… avant qu'une personne malveillante ne la trouve. On peut considérer cela comme un jeu où deux équipes s'affrontent pendant un temps imparti pour atteindre le même but : trouver la faille – certains la répareront, d'autres l'exploiteront.

Cette méthode a permis de découvrir plusieurs dysfonctionnements avant qu'ils n'engendrent des conséquences importantes, comme pour l'exemple du modèle de Jeep Cherokee cité plus haut. Cette méthode a aussi permis de rappeler plus de 500 000 pacemaker de la vente, suite à une découverte d'une faille pouvant entraîner la mort des patients par un groupe de chercheurs anglais.

Anticiper un portfolio d'attaques en développement constant

En adoptant le point de vue de l'attaquant, on peut aussi créer de nouvelles attaques qui dérivent des attaques existantes. De nouvelles attaques sont imaginées en continu, et les systèmes de sécurité doivent donc être testés continûment et mis à jour.

De plus, un nouveau type d'attaque se développe – elles utilisent des algorithmes d'apprentissage automatique, qui peuvent contourner plus facilement les systèmes de sécurité mis en place. En effet, en utilisant des algorithmes de machines learning, il est maintenant possible de créer des données semblables à celles circulant sur un réseau IoT et de les injecter dans ce dernier afin de falsifier des informations et de contourner le système de détection.

Ces algorithmes d'intelligence artificielle sont de plus en plus accessibles et faciles à implémenter, grâce à des outils libres et gratuits – ce qui va contribuer à rendre ce type d'attaque de plus en plus fréquent d'après Europol.

Les défis de sécurité des systèmes IoT

Avec un marché qui ne cesse de croître, les réseaux IoT deviennent de plus en plus nombreux et complexes. Cette croissance se fait de manière hétérogène, ce qui complique les travaux et les recherches en sécurité : chaque constructeur possède son propre matériel et logiciel. De nombreux protocoles peuvent être utilisés pour interconnecter les objets entre eux. Tous ces éléments sont à prendre en compte lors de l'établissement d'une solution de sécurité ou d'un nouveau système de détection d'attaque. Il n'existe pas encore pour le moment une solution applicable sur tous les appareils IoT permettant de faire face à toutes les attaques existantes et à venir.

De plus, ces appareils embarquent avec elle de nouvelles technologies comme l'intelligence artificielle. C'est par exemple le cas des enceintes Amazon Echo, qui intègrent des composants supportant l'apprentissage automatique permettant de répondre à des requêtes spécifiques (allumer une lumière, jouer une musique).

L'intelligence artificielle permet de résoudre de nombreux problèmes et de rendre les appareils IoT plus autonomes, mais elle ouvre aussi de nouveaux vecteurs d'attaques. Par exemple, les voitures autonomes sont capables de reconnaître, entre autres, les panneaux de signalisation routière. Cependant, une modification en apparence anodine pour l'homme peut mener à de terribles répercussions sur un algorithme de machine learning : le simple ajout d'un autocollant sur un panneau « STOP » peut par exemple mettre l'algorithme en échec. Celui-ci croit alors qu'il s'agit d'un panneau de limitation de vitesse, et ce avec une grande confiance en lui (97 %).

Il devient donc bien évidemment primordial d'inclure ces nouveaux champs de menace en compte dans l'élaboration des nouveaux moyens de sécurité.

Enfin, quand une solution de sécurité est trouvée, il peut être difficile de l'appliquer sur tous les appareils IoT déjà déployés. En effet, certains constructeurs, pour des raisons essentiellement financières et de temps, ne permettent pas de mettre à jour les dispositifs IoT, qui par rapport aux autres outils informatiques connectés sont par définition plus autonomes et moins développés.

Des risques, mais aussi des solutions

Apporter des solutions de sécurité pour l'ensemble des réseaux IoT existants est impossible de nos jours. Cependant, il est envisageable de les sécuriser en fonction de leur utilisation et de leur domaine. Par exemple, les solutions de sécurité apportées pour une utilisation de surveillance ne seront pas les mêmes que celles pour une exploitation dans un milieu hospitalier. En effet, de nombreuses données privées transitent au sein des hôpitaux, comme le numéro de sécurité sociale ou l'âge d'un patient, ce qui n'est pas le cas pour un système de surveillance. Dans ce dernier, les attaquants se focaliseront plus sur l'intégrité de l'appareil IoT (batterie, composants électroniques) qui pourrait empêcher son bon fonctionnement que sur les données qui sont véhiculées. Ainsi, repérer les failles en amont, en prenant la place d'un attaquant dans des milieux réels, permet de répondre à cette problématique.

Dans tous les cas, l'un des moyens de se protéger face à ces attaques est de faire attention à ce que nous connectons sur nos réseaux, et bien sûr de respecter les protections de base, par exemple en changeant régulièrement ses mots de passe.

Bien que de nombreuses solutions existent pour sécuriser les réseaux IoT, comme l'exigence d'identifiants de connexion d'un niveau de sécurité élevé pour les appareils ou le chiffrement des données qui y circulent, la sécurité de ces derniers reste faible. Il est essentiel d'adopter une stratégie fondée sur l'attaque afin de mieux comprendre les attaquants et les outils qu'ils utilisent. La sécurité reste encore un domaine en tension, et au vu du nombre d'attaques apparaissant chaque année, il est devenu urgent de former de nouvelles personnes sur ce sujet.

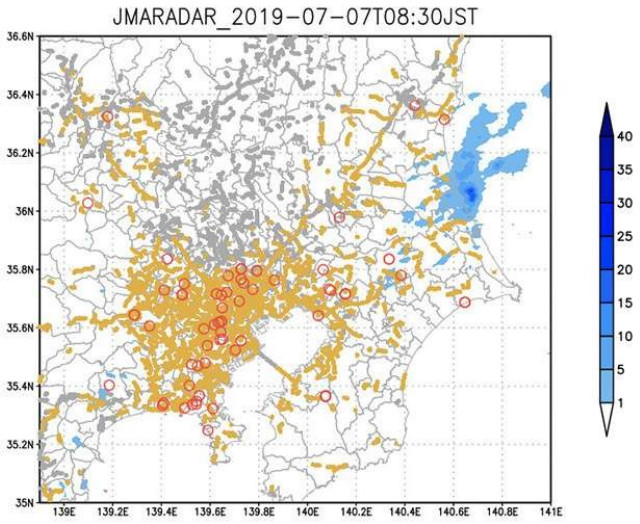
Source
Futura Tech
Céline Deluzarche
6 novembre 2019

9. Toyota veut améliorer les prévisions météo avec ses essuie-glaces connectés

Le taux d'accident par temps de pluie est quatre fois supérieur à celui des accidents survenant par journées ensoleillées. Or, si les radars météorologiques détectent parfaitement les grosses masses de précipitations, ils sont incapables de détecter les nuages de pluie situés dans la couche inférieure de la troposphère, à moins de 2 km d'altitude, et qui donnent les petites averses. Dans ce cas, quoi de mieux que les données remontant directement du terrain pour affiner les prévisions ?

C'est dans ce cadre que Toyota a annoncé le 1er novembre 2019 un partenariat avec l'entreprise

japonaise de services météo Weathernews, afin d'utiliser l'état de fonctionnement des essuie-glaces pour déterminer s'il pleut ou pas. Le constructeur automobile a commencé à déployer sur tous ses véhicules particuliers un DCM (*Data Communication Module*), un module permettant de partager les données de la voiture avec d'autres utilisateurs ou un opérateur central. L'usage des essuie-glaces permettra non seulement de détecter des nuages de pluie non décelables par les radars, mais aussi de préciser l'intensité de la pluie selon leur vitesse de fonctionnement.



Une carte météo fournie par Toyota : les zones oranges correspondent aux voitures dont les essuie-glaces fonctionnent, tandis que les cercles rouges désignent les zones de pluie détectées par les radars. © Toyota

Au-delà de la météo, les voitures connectées devraient aussi permettre de signaler les embouteillages, une chaussée en mauvais état, les plaques de verglas ou encore les accidents de la route.

Source
Futura
Thibault Caudron
12 mars 2022

10. Il était une fois le futur des objets connectés

Quel serait l'objet connecté le plus utile chez vous ? Une question qui peut laisser perplexe face au nombre exponentiel de nouvelles technologies et qui fait débat en ce moment sur la plateforme de co-idéation EDF Pulse & You. Futura s'est amusé à sourcer quelques-unes des meilleures idées pour imaginer le futur du bien-être à domicile. À votre imagination : action !

De plus en plus, les objets connectés s'invitent dedans-dehors. Sur la plateforme de co-idéation EDF Pulse & You, les idées fusent...

Dans la chambre

C'est l'ultime prise. Une toute dernière avant d'atteindre le sommet. J'étends le bras pour l'agripper quand soudain… C'est l'heure de l'éveil. Une musique d'ambiance tapisse mon réveil tandis que mes yeux s'ouvrent progressivement et en douceur grâce à la luminothérapie adaptée. Météo, trafic routier, rendez-vous de la journée, il me suffit d'un mot pour avoir toutes les informations utiles, tandis que les volets roulants se lèvent automatiquement pour s'ouvrir au jour naissant. La nuit a été particulièrement reposante sur ce grand matelas avec résistance séparée qui permet de réguler sa température en fonction du corps de chaque personne qu'il accueille. Après avoir vérifié la qualité de mon sommeil sur ma montre connectée, je me décide à poser un pied sur le sol terrestre.

Dans la salle de bains

Direction la douche pour bien commencer la journée. Car avec ce système d'écoulement d'eau automatique à la température appropriée en fonction de la météo et dont le débit est réglable à la voix, plus besoin de jongler entre le chaud et le froid ! Une fois propre, j'en profite pour passer par

ma balance connectée qui me livre toutes les informations nécessaires sur mon état de santé, poids, tension, température… L'armoire à pharmacie connectée m'alerte alors sur la prise de mon médicament et m'annonce qu'il va falloir renouveler l'ordonnance tout en intégrant la donnée dans ma *to do list* en ligne. Reste l'épreuve du miroir, heureusement en 3D qui me permet de me scruter sous tous les angles sans me faire un torticolis ! À chaque visage de la famille, il délivre des astuces beauté et des conseils en fonction de la météo, du grain de peau, du niveau de fatigue, de l'activité à venir...

Dans la cuisine

Le café programmé à distance depuis mon lit m'attend, tout chaud dans la cuisine. Le frigo connecté me conseille alors le petit déjeuner adapté à mon programme de la journée, me fait part de la météo, des données qu'a « balancées » la balance, et bien entendu de ce qu'il lui reste dans le ventre… D'ailleurs la liste des courses m'a été envoyée sur mon smartphone, pendant que je jette un œil sur la cuisson du pain dans le four que je peux consulter sans me déplacer grâce à la caméra intégrée. Pour les déchets, plus besoin de se prendre la tête, la poubelle m'indique les bons bacs en fonction des déchets que je lui propose d'avaler. Reste à préparer le lave-linge qui adapte son cycle en fonction du poids du linge, la couleur, ou les tissus. Je l'activerai à distance avec le *smart connect* pour tomber sur les heures creuses, comme le lave-vaisselle d'ailleurs.

Dans le salon

Arrivé dans le salon, je passe obligatoirement devant le téléviseur, qui devient un miroir une fois éteint. Pratique ! D'autant plus qu'il peut aussi servir de caméra de surveillance discrète, de visiophone pour voir qui est à la porte mais aussi pour afficher l'emploi du temps de la famille et donc ne pas oublier les rendez-vous. J'en profite d'ailleurs pour enregistrer un message d'encouragement à la petite dernière pour son interro du jour... En mode téléviseur d'ailleurs, l'appareil détecte les signes de fatigue, stoppe le film ou enregistre la fin comme un grand ! Bon, c'est pas tout ça, mais il est l'heure de partir en toute tranquillité grâce aux différents capteurs de la pièce qui régulent la ventilation de la maison en fonction du taux d'humidité, de la pollution de l'air, etc. Et puis, en cas de problème je serai alerté par smartphone de toute fuite ou plaque chauffante restée allumée. Mes ampoules pilotables à distance permettent en plus de simuler une présence lors de mes absences dans mon domicile. J'ai aussi installé dernièrement ce petit boîtier qui interrompt le courant sur les prises non utilisées. Économies garanties pour le portefeuille et pour la Planète !

À l'extérieur

Avant de partir, passage obligé par la boîte aux lettres, avec lecteur de QR Code qui commande l'ouverture en cas de colis, port USB pour les tracts en version numérique et lecteur optique pour lister les courriers du jour quand je ne suis pas à mon domicile. Des capteurs, il y en a aussi sur mon réseau de canalisations pour détecter la moindre fuite et agir avant le dégât des eaux ! Même la mangeoire pour les oiseaux est connectée pour leur distribuer des graines dès qu'ils s'y posent, mais aussi activer une caméra pour que je puisse les observer sans les effrayer. En attendant, j'arrive à ma voiture que j'ai dégivrée à distance pour être à l'heure pour mes covoitureurs. C'est parti, la journée commence bien !

Source
letemps.ch
Anouch Seydtaghia
7 août 2022

11. Méfiez-vous désormais de votre robot aspirateur Amazon…

Le géant de l'e-commerce a racheté le fabricant des aspirateurs Roomba. Une manière de récolter de nouvelles données sur ses utilisateurs.

Si j'étais propriétaire d'un aspirateur robot de la marque Roomba, je regarderais désormais cet appareil avec méfiance. La semaine passée, Amazon annonçait l'acquisition d'iRobot, société qui fabrique les Roomba, pour 1,7 milliard de dollars. Ces petites machines ont été lancées en 2002 par la société américaine et ont fait la preuve de leur efficacité pour aspirer de manière automatique tous les petits déchets qui se trouvent sur le sol. Désormais, Amazon pourrait donner de nouvelles missions à ces robots.

Les machines de Roomba savent faire beaucoup de choses elles-mêmes. Aspirer, nettoyer, s'orienter automatiquement dans un logement, revenir à leur station de base pour se recharger… Sans

mauvais jeu de mots, ce sont aussi des aspirateurs à données, puisqu'elles ont une connaissance intime de l'appartement de leur propriétaire. Les appareils sont dotés de caméras pour s'orienter efficacement. Les modèles les plus perfectionnés disposent d'une caméra équipée d'un système d'intelligence artificielle capable de détecter les objets qui se trouvent en face d'eux.

Mine d'or

En mettant la main sur les robots Roomba, Amazon va d'abord connaître avec détail le type de logement de ses utilisateurs, le nombre de pièces, la taille du salon ou encore de la salle de bains. Amazon pourra aussi commencer à savoir quels meubles se trouvent dans l'habitation, voire quels jouets se trouvent sur le sol. Une véritable mine d'or pour le géant de l'e-commerce.

La société iRobot avait déjà utilisé les Roomba pour mesurer la qualité des réseaux Wi-Fi dans les pièces. Il y a quelques années, son directeur avait évoqué l'idée de revendre les plans des appartements à Google ou à Amazon, avant de revenir en arrière. Désormais, Amazon a mis la main sur ces plans.

S'il y a de quoi être aussi méfiant par rapport à Amazon, c'est que son historique en matière d'objets connectés n'est pas bon. Prenons simplement ses sonnettes connectées Ring, dotées de caméras: elles envoient des données à la police, elles enregistrent les faits et gestes des utilisateurs et récoltent beaucoup trop de données sans aucun lien avec leur fonction première. Autour des aspirateurs, de devenirs de petits espions domestiques...