Sécurité des objets connectés : attaquer pour mieux se défendre

Emilie Bout, Valeria Loscri

THE CONVERSATION

L'expertise universitaire, l'exigence journalistique

Sécurité des objets connectés : attaquer pour mieux se défendre

Auteurs

Émilie Bout
Doctorante, Inria

Valeria Loscri
Associate research scientist, Inria

6 juin 2021, 18:35 CEST

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 »).

À lire aussi : Rançongiciels, vos données en otage

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).

Dans quelles conditions les algorithmes sont-ils fiables ? Natilyn Hicks, Unspash, CC BY

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.

automobile Internet Internet des objets technologies intelligence artificielle (IA) informatique sécurité cybersécurité hacker cyber-attaques objets connectés