Considérations architecturales pour la sécurité des appareils IoT au domicile
Date de publication: 16 avril 2021

Résumé
Les consommateurs ont besoin de moyens pour gérer les appareils IoT dans leurs réseaux domestiques. Nous allons plus précisément examiner plusieurs technologies émergentes, en commençant par la manière dont les appareils et les réseaux domestiques sont introduits via le protocole de provisionnement des appareils de l'Alliance Wi-Fi et le démarrage des infrastructures de clés sécurisées à distance de l'IETF. Une fois qu'un appareil est connecté, il doit être protégé. Nous traitons des mécanismes de profilage appris et déclarés tels que les descriptions d'utilisation du fabricant. Pour détecter et corriger les attaques, nous discutons des technologies de signature d'attaque. La clé de tout cela est la nécessité de tirer parti de la relation entre le consommateur et un intervenant comme un fournisseur de services ou de pare-feu, afin que les informations présentées au consommateur soient compréhensibles et exploitables. Ce document est destiné aux opérateurs Internet (FAI) qui spécifient les exigences pour ces périphérique CPE ; il fournit également des conseils pratiques sur les technologies actuelles qui peuvent être utilisées. Ce document est susceptible d'être mis à jour au fur et à mesure que les technologies évoluent.

Contenu

1 Introduction
D'ici 2025, il est estimé que 75 milliards de périphériques disposeront d'une connectivité réseau.[1] À mesure que de plus en plus de foyers utilisent l'Internet des objets (IoT), l'établissement d'approches sécurisées permettant une gestion simple de l'accès au réseau domestique par les consommateurs deviendra de plus en plus important. Les taux d'adoption de certaines fonctionnalités augmentent de façon exponentielle. Il a fallu quatre ans à Amazon pour atteindre 100 millions d'appareils compatibles Alexa, et seulement un an plus tard, 200 millions d'appareils ont été vendus.[2] De nombreux types d'appareils différents se connecteront bientôt à Internet et les normes pour répondre à leurs besoins commencent à arriver à maturation.
Ce document se concentre sur plusieurs aspects clés :

- Introduction sécurisée d'un périphérique sur le réseau
- S'assurer qu'il obtient l'accès dont il a besoin (et pas plus)
- Surveiller le comportement des périphériques et atténuer les menaces
- Quelques principes que les fabricants d'appareils devraient suivre pour garantir la sécurité et la confidentialité des utilisateurs

L'un de ces principes clés est que les utilisateurs ne devraient pas se voir poser des questions auxquelles ils ne connaîtraient probablement pas la réponse (voire qu'ils ne comprendraient même pas). Ainsi, l'architecture doit permettre à un tiers, qu'il s'agisse d'un fournisseur de services ou de pare-feu, de fournir à l'utilisateur l'expertise nécessaire pour limiter ces interactions.

Un autre de ces principes clés est de supposer que chaque appareil IoT présentera des vulnérabilités. Une approche en couches est donc nécessaire, où le fabricant de l'appareil et le fournisseur de services ou le fabricant de pare-feu travaillent ensemble pour protéger l'utilisateur.

Aspects importants que ce document ne couvre pas
Ce document se concentre sur la façon dont le réseau peut être utilisé pour protéger l'appareil. Nous ne couvrons pas ce que les fabricants d'appareils doivent faire pour protéger leurs produits et leurs consommateurs. Il existe un certain nombre de normes telles que NISTIR 8228, les recommandations de sécurité IoT de l'ENISA, et les bonnes pratiques de l'IOT Security Foundation qui couvrent ces aspects de manière très détaillée.

1.1 Hypothèses de confiance
La technologie décrite dans ce document fait plusieurs hypothèses de base sur la confiance. La première est que le consommateur fait confiance au matériel client à domicile (CPE pour *Customer Premises Equipment*) ou à un pare-feu placé devant le CPE. La deuxième hypothèse est qu'il existe une relation entre l'utilisateur et le fournisseur de ce CPE ou pare-feu qui peut être exploitée pour maintenir un inventaire des périphériques autorisés sur le réseau local. Cette relation peut se faire via une application ou un contrat.

1.2 Hypothèses de facilité de gestion
Une autre hypothèse est que la plupart des consommateurs ne disposent pas de la formation, de l'expérience ni même des informations nécessaires sur leurs appareils pour gérer leurs propres réseaux. Ils ont donc besoin de l'expertise des fournisseurs de services et des fournisseurs de pare-feu pour les aider. Pour que cela se produise, les capacités de gestion dont les fournisseurs ont besoin doivent être disponibles dans leur équipement. Ces fonctionnalités incluent la surveillance du trafic, les informations sur l'état des périphériques (y compris le nombre de paquets abandonnés et la raison de cet abandon), ainsi que les informations de réussite et d'échec d'authentification. Les interfaces pour collecter ces informations doivent exister, de même que les interfaces pour modifier la configuration.

2 Introduction sécurisée des appareils sur le réseau
L'intégration réseau d'un nouvel appareil offre la meilleure opportunité d'initier des processus qui peuvent aider à intégrer en toute sécurité cet appareil dans un foyer. Aujourd'hui, de nouveaux appareils IoT sont ajoutés au réseau d'un consommateur comme n'importe quel appareil « normal », tel qu'un PC, un smartphone ou une tablette. Les appareils IoT manquent souvent d'interfaces d'entrée ou de sortie que le consommateur pourrait utiliser pour entrer ou établir des informations d'identification à long terme. Un moyen automatisé d'établir les informations d'identification doit donc exister pour le périphérique.
Cette section se concentre sur l'intégration **sans fil**. Les futures itérations de ce document peuvent également aborder l'intégration filaire.

2.1 Mécanismes[3] d'intégration « hérités »
Dans le cas de nombreux d'appareils électroménagers, le processus d'intégration fonctionne comme suit :

1. Un bouton ou une commande sur l'appareil active le processus d'intégration.
2. L'appareil devient un point d'accès pour un SSID Wi-Fi spécifique. Celui-ci peut être non chiffré ou chiffré avec une clé partagée privée (PSK pour *Private Shared Key*) bien connue.
3. Le consommateur télécharge une application spécifique à l'appareil sur son téléphone. L'application prend le contrôle du Wi-Fi du téléphone[4], modifie le SSID bien connu ci-dessus, puis exécute une API spécifique à l'appareil.
4. L'application prend le contrôle de l'appareil et copie généralement le PSK du téléphone vers l'appareil.[5] L'appareil est maintenant en ligne.

Si le consommateur change de PSK, le processus d'intégration doit être répété pour tous les appareils connectés. Si un périphérique se comporte mal et est mis en quarantaine selon cette PSK, le consommateur peut constater qu'il ne peut gérer aucun autre périphérique disposant de la même PSK. Cette méthode nécessite également une application pour smartphone pour chaque marque d'appareil IoT. Enfin, si la sécurité d'un appareil est rompue, le réseau est accessible pour n'importe quel appareil utilisant cette clé. Ce modèle **n'est pas** recommandé à l'avenir.

2.2 Utilisation d'une PSK par appareil

Les segments de réseau L2 par appareil peuvent être réalisés en attribuant à chaque appareil une PSK unique au lieu d'utiliser une seule PSK pour tous les appareils du réseau local. Cela accomplit deux choses :

- Le routeur est certain qu'aucun autre appareil ne peut usurper l'identité de cet appareil, à condition que la clé de l'appareil soit restée sécurisée.
- Si l'appareil se comporte mal, le routeur peut isoler l'appareil sans affecter les autres.

La PSK moyenne aujourd'hui se compose d'une grande chaîne de lettres et de chiffres, ce qui rend la gestion des PSK par appareil intenable sans automatisation. La section suivante traite des moyens d'automatiser les PSK par appareil. Cela peut être mis en œuvre via le protocole DPP (*Device Provisioning Protocol*), à condition que l'application « configurateur » et le point d'accès puissent provisionner la PSK unique pour un appareil donné.

2.3 Protocole de provisionnement de périphérique

Le protocole DPP, également connu sous le nom de Wi-Fi Easy Connect[6], est une norme industrielle volontaire introduite par la Wi-Fi Alliance. Le DPP simplifie l'intégration de l'appareil en demandant au fabricant d'imprimer une paire de clés publique/privée dans l'appareil et de fournir la clé publique au consommateur, généralement via un code QR. Le consommateur peut alors prouver qu'il est en possession du dispositif en disposant de la clé publique correspondante, tandis que l'appareil peut prouver au propriétaire qu'il dispose de la clé privée associée. Ainsi, l'authentification mutuelle est établie et le périphérique peut être configuré avec les informations d'identification appropriées pour le réseau du propriétaire. Dans certains cas, l'appareil peut fournir des informations supplémentaires au réseau, comme une description d'utilisation du fabricant (URL MUD (décrite ci-dessous).
Pour les utilisateurs, le DPP semble très similaire aux méthodes de type d'appareil ou de marque. Cependant, le DPP utilise des trames publiques 802.11 plutôt que des trames IP sur un réseau privé. Alors que le DPP envisage des applications sur les téléphones approvisionnant directement les terminaux, en raison de problèmes de chipset dans les téléphones, il est plus probable qu'une application de gestion de routeur domestique pourra utiliser une API personnalisée pour communiquer les capacités de l'appareil directement ou indirectement via un connecteur cloud. au routeur.

Activité DPP menée par le routeur

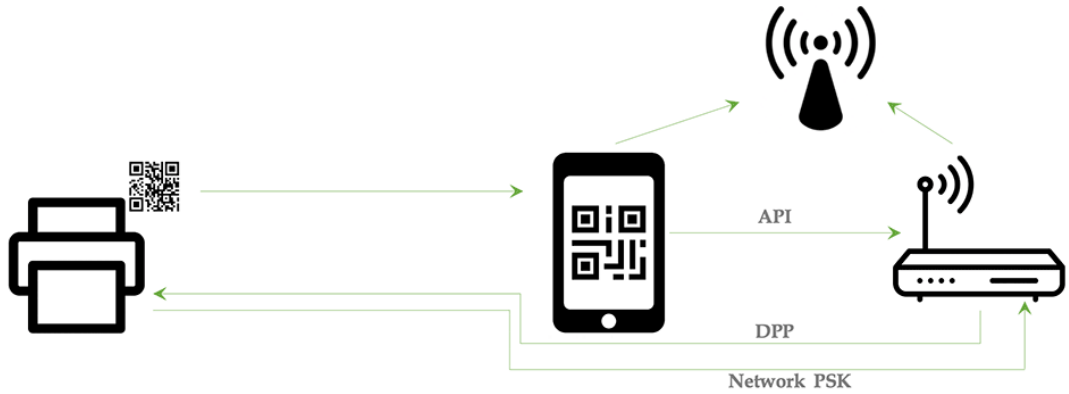

Figure 1 : Intégration de l'appareil via un DPP mené par un routeur

Dans un scénario (Figure 1), le téléphone mobile n'est utilisé que pour scanner le code QR fournissant la clé publique. Le téléphone utilise ensuite une API pour communiquer avec le routeur, et le routeur envoie les trames publiques 802.11 spécifiques à l'appareil, terminant la prise de contact par DPP. Le routeur est alors en mesure de fournir toute PSK qu'il juge appropriée. Dans ce modèle, seul le routeur doit prendre en charge les trames DPP. En outre, le routeur a établi un chemin de communication de confiance avec le point d'extrémité en cours d'intégration, sur lequel il peut échanger des informations de configuration ou d'état liées au réseau. Il est conseillé aux fournisseurs de routeurs de vérifier auprès de leurs fournisseurs PHY et de pilotes la compatibilité avec le DPP. L'exposition d'une API à un téléphone nécessite des considérations de sécurité importantes sur la manière dont la confiance entre ces deux appareils est établie.

Le consommateur peut parfois souhaiter changer les PSK par appareil. Dans ce cas, une certaine forme de coordination entre chaque périphérique d'extrémité existant et le routeur serait nécessaire. Cela peut impliquer la réinitialisation de l'appareil et/ou la réexécution du DPP. Ainsi, les dispositifs avec des PSK individuelles sont plus faciles à identifier et à contrôler. La révocation de la PSK correspondante d'un périphérique défectueux empêchera uniquement *ce* périphérique d'accéder au réseau.

2.4 Démarrage des infrastructures de clés sécurisées à distance (BRSKI)

Le « BRSKI » est une spécification de suivi des normes IETF[7] pour l'intégration sans contact des appareils. Il était à l'origine destiné à intégrer des appareils de commutation d'entreprise et de classe ISP dans des centres de données sans nécessiter un accès physique à l'équipement. Il est également destiné à être utilisé dans les applications IoT industrielles où il existe une sorte d'opérateur de réseau pour configurer et maintenir une autorité de certification privée (CA), un serveur d'inscription via Secure Transport (EST)[8] et une authentification, une autorisation et une responsabilisation (AAA).

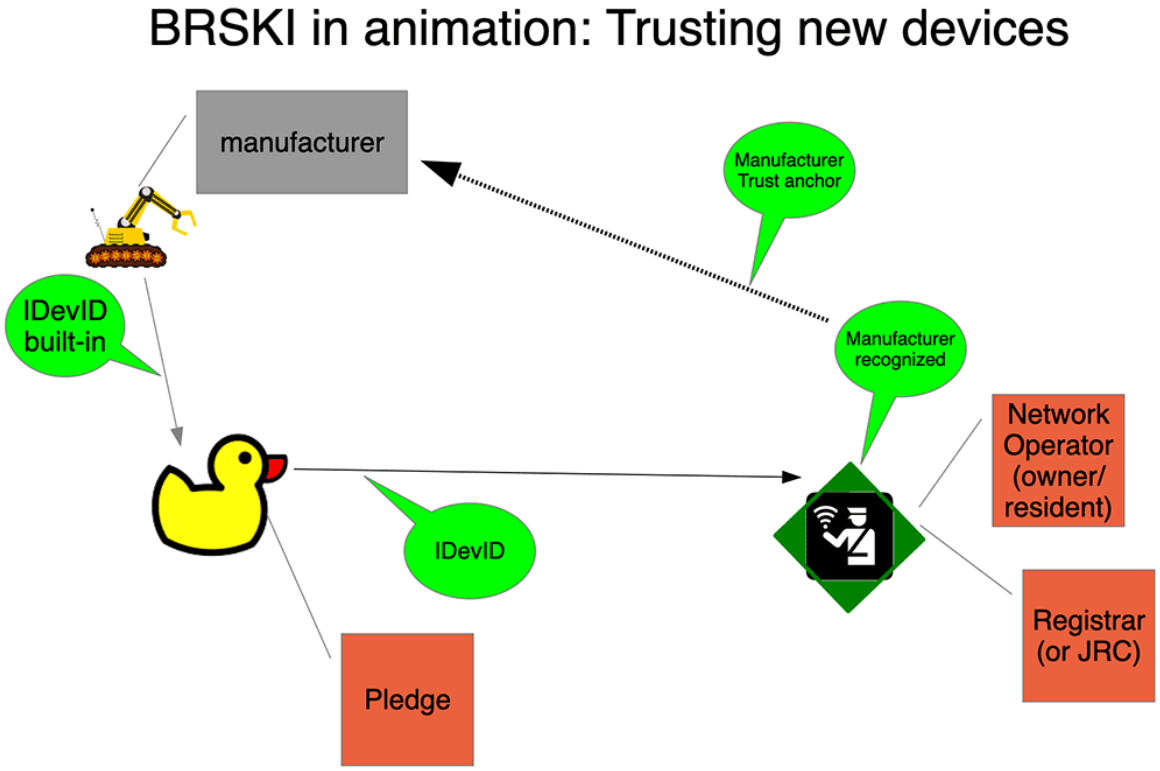

Figure 2 : Intégration de l'appareil via BRSKI

Le BRSKI utilise un certificat IEEE 802.1AR (IDevID) installé par le fabricant pour que le réseau valide l'identité de l'appareil. L'appareil utilise un voucher RFC 8366 pour valider que le réseau est un propriétaire approprié. Dans les réseaux gérés par des professionnels (FAI, entreprises et IoT industriel), l'opérateur de réseau sait quels types d'appareils ils ont achetés auprès de quels fabricants et peut même connaître l'ensemble des numéros de série à attendre. Ils peuvent ne pas savoir quel numéro de série ira où, ni l'ordre dans lequel les boîtes seront ouvertes. D'un autre point de vue, le fabricant sait, via l'automatisation de son processus de vente, à qui il a vendu des appareils. Cela peut présenter un défi avec les reventes où une inscription préalable peut être requise.

Les relations de vente envisagées par le modèle opérationnel BRSKI peuvent ne pas s'appliquer facilement à la maison. Pour que le BRSKI réussisse ici, le registre BRSKI doit trouver son chemin vers le routeur domestique du consommateur ou un autre appareil (tel que le stockage en réseau domestique (NAS)), afin de gérer les relations de propriété du consommateur. Cette fonctionnalité est similaire à celle fournie par le DPP. Cependant, elle inclut d'autres fonctionnalités qui peuvent paraître complexes, comme une autorité de certification privée. La fonctionnalité du registre BRSKI s'intègre parfaitement dans un conteneur sur le CPE existant[9] il est plus probable que le registre s'exécute dans un service basé sur le nuage.

Certificats (de naissance) installés par le fabricant
Le BRSKI exige explicitement que chaque appareil (appelé « engagement » jusqu'à ce qu'il soit inscrit) soit accompagné d'un certificat installé par le fabricant. Les applications d'intégration spécifiques au fabricant peuvent également nécessiter ce certificat si la communication entre l'application et l'appareil est basée sur TLS (par exemple HTTPS). Dans les deux cas, le certificat proviendra d'une autorité de certification (CA) privée gérée par le fabricant. Le BRSKI traite explicitement la transition de la confiance du fabricant vers l'environnement local, tandis que les méthodes spécifiques au fabricant incluent les ancres de confiance appropriées dans l'application elle-même.

3 Fournir un accès approprié à l'appareil
Lorsqu'un appareil passe par le processus d'intégration, son type/sa classe d'appareil doit être identifié et placé dans un segment de réseau approprié. Idéalement, cela devrait se produire avec l'approbation du consommateur. Le CPE ou un agent associé doit conserver une base de données des périphériques déjà intégrés (ou qui le seront).
Sur les dizaines de milliards d'appareils connectés, un seul appareil IoT n'aura généralement besoin d'accéder qu'à une poignée de points de terminaison. Deux défis président à la fourniture d'un accès correct :

1. Déterminer les points de terminaison que l'appareil peut contacter et le type de trafic qui peut s'exécuter entre l'appareil et ces points de terminaison.
2. Fournir les capacités pour limiter l'accès à ce sous-ensemble d'autres points de terminaison et services.

Deux approches permettent de relever le premier défi : un modèle appris et un modèle déclaré. Les deux modèles tentent de limiter l'accès au réseau d'un appareil afin de réduire sa surface de menace à diverses formes d'attaque par des appareils qui n'ont aucune activité avec lui.

Avec le modèle appris, le CPE peut apprendre en observant ce qu'est l'appareil. De telles approches de prise d'empreinte digitale impliquent l'observation des demandes et des réponses DHCP, des adresses MAC, des annonces de multidiffusion et des caractéristiques similaires pour établir ce que l'on pense que le périphérique est. Des techniques avancées telles que l'apprentissage automatique peuvent également examiner les flux de trafic, les options TLS utilisées pour communiquer et d'autres informations comportementales afin de prendre une décision.

Soit le CPE traitera lui-même toutes ces informations, soit il les enverra en amont pour une analyse plus approfondie.[10] Un certain nombre de normes de format d'information existent déjà, deux formats courants étant PCAP et IPFIX. Les mêmes informations peuvent également être utilisées pour analyser si un appareil reste dans le profil et ne fait que ce qu'il est censé faire.

Ce modèle appris présente un défi : soit le CPE doit effectuer des traitements importants, soit une copie des communications (au moins certaines) doit être envoyée en amont pour traitement. Il est donc gourmand en ressources, en fonction de la quantité d'informations utilisées pour identifier les exigences d'accès aux périphériques. En outre, les appareils peuvent mentir ou masquer les informations utilisées pour les empreintes digitales.
L'approche déclarée consiste pour l'appareil ou son fabricant à indiquer clairement ce qu'il est et le type d'accès dont il a besoin. C'est l'approche adoptée par les descriptions d'utilisation du fabricant (MUD pour *Manufacturer Usage Descriptions*) [RFC 8520]. Les MUD peuvent être utilisées pour fournir aux déploiements une liste d'accès généralisée qui peut être localisée sur un réseau spécifique. Elles peuvent également être utilisées pour partager d'autres informations sur un appareil, par exemple comment récupérer une nomenclature logicielle (SBOM). Les MUD peuvent spécifier les sites Internet auxquels l'appareil peut accéder (parfois appelé contrôle nord/sud) et quels appareils du foyer doivent être autorisés à communiquer entre eux (contrôle est/ouest).

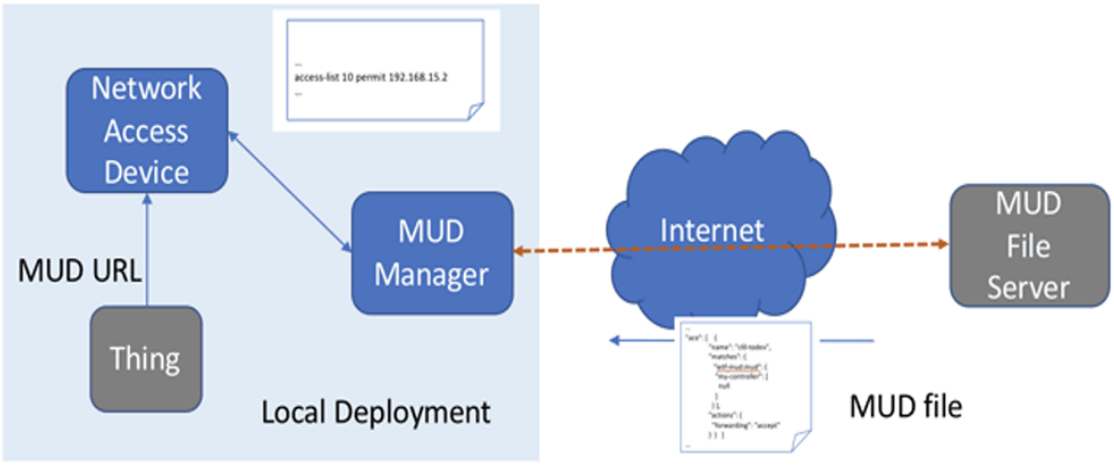

Figure 3 : Architecture générale des MUD

La figure 3 représente l'architecture générale des MUD. Dans un environnement grand public, soit le périphérique d'accès au réseau sert de gestionnaire MUD, soit, plus probablement, un service joue ce rôle. Cela peut être fourni par le fournisseur de services ou un fournisseur de pare-feu. La clé réside dans le fait qu'un chemin de contrôle est nécessaire entre le dispositif d'accès au réseau, tel que le CPE, et le gestionnaire MUD pour les besoins du CPE partageant les informations MUD et le gestionnaire MUD fournissant des règles d'accès que le CPE devrait mettre en œuvre. En outre, un canal de communication est nécessaire entre le gestionnaire MUD et le consommateur pour approbation, comme indiqué ci-dessous. Étant donné que les MUD constituent une approche déclarative, elles sont moins gourmandes en ressources en soi et peuvent faire davantage autorité. Cependant, elles nécessitent que le point de terminaison IoT annonce une URL (par exemple via DHCP ou Link Layer Description Protocol (IEEE 802.1ab)).
Une fois les exigences d'accès déterminées, elles doivent être déployées sur CPE. La plupart des équipements CPE ont des capacités de pare-feu de base pour limiter l'accès vers et depuis Internet. Seuls **certains** CPE ont la capacité de limiter l'accès entre les appareils de la maison. Cependant, ce type d'accès limité est essentiel, au cas où un appareil domestique en infecterait un autre.

4 Surveiller le comportement des appareils et atténuer les menaces
Une fois qu'un appareil est connecté à un réseau, il y a toujours la possibilité qu'une attaque réussisse contre lui. Si cela se produit, l'appareil lui-même peut commencer à se comporter comme un acteur malveillant. Il existe plusieurs approches générales pour détecter et atténuer ces cas :

- **Autoriser/Bloquer en fonction d'une liste noire** – Le trafic malveillant est détecté par sa destination Par exemple :
  - Comparer la destination de la couche 4 avec des listes de refus connues (« liste noire »)
  - Valider que la destination du trafic de la couche 4 correspond au profil MUD
  - Effectuer des recherches DNS inversées pour mapper la cible du réseau sur les listes noires de domaine
- **En fonction de la signature** – Le trafic malveillant est détecté par ses propriétés. Par exemple :
  - Détection lorsque les périphériques sur un réseau local lancent un trafic UDP usurpé
  - Inférence d'un profil basé sur l'empreinte digitale MAC
  - Effectuer DPI
  - Effectuer une analyse Netflow
  - Examen des certificats et des paramètres TLS
- **En fonction d'une anomalie** – Un trafic malveillant est détecté par un comportement anormal de l'appareil. Par exemple, l'apprentissage en profondeur ou toute autre intelligence artificielle qui résume le trafic « normal », combiné à des seuils qui marqueraient l'activité comme anormale.

4.1 Technologies existantes

Plusieurs efforts tentent de fournir certaines de ces fonctionnalités. En général, ceux-ci ont tendance à utiliser soit des approches d'autorisation/de liste noire, soit des approches basées sur des signatures, en utilisant des listes similaires aux outils antivirus. Étant donné que ces listes peuvent devenir assez volumineuses, cette analyse est généralement effectuée de manière centralisée, en envoyant un résumé du trafic à un serveur central, et elle repose sur un modèle de service d'abonnement.
Snort, Zeek et Suricata sont des exemples source libre de cette approche.[11] Plusieurs entreprises proposent également des « routeurs sécurisés », qui fournissent cette fonctionnalité, généralement accompagnée d'un modèle d'abonnement pour les règles, ou même d'un VPN complet pour l'analyse basée sur le nuage.
Le projet Turris[12] contient un pare-feu adaptatif distribué, où le trafic suspect est collecté et analysé de manière centralisée. Les règles de pare-feu supplémentaires qui en résultent sont distribuées à tous les routeurs connectés. Cela peut protéger les réseaux domestiques et, avec un déploiement suffisant, offrir également un moyen d'atténuer les attaques à grande échelle.
La détection basée sur les anomalies est toujours un domaine de recherche actif. Le projet SPIN[13] est une plateforme de recherche et développement sur la sécurisation des réseaux domestiques. Il contient un module expérimental qui compare le nombre de paquets et leur destination à une moyenne de l'appareil, le bloquant lorsque celui-ci dépasse un certain seuil.[14]

4.2 Rapports et atténuation

Une fois qu'une anomalie a été détectée, une fonction de support technique doit décider des mesures à prendre et des mécanismes appropriés afin de déterminer une atténuation (en bref, qui est notifié et quand, et ce qui doit être fait). Il est peu probable que le consommateur soit le premier point de contact, car une certaine expertise peut être nécessaire pour utiliser des options de résolution significatives. Les rapports doivent se dérouler en deux phases : premièrement, la fonction de support technique, généralement proposée par le fournisseur de pare-feu ou le FAI, peut évaluer le risque pour le consommateur et les autres ; deuxièmement, le fournisseur de pare-feu ou le fournisseur de services Internet doit alerter le consommateur.[15]
La plateforme de services aux utilisateurs (TR-369), est une norme de gestion du cycle de vie des appareils qui inclut la surveillance des appareils et la gestion des alertes. Légèrement plus limitée dans sa portée, la spécification de canal de signal DOTS (*Distributed Denial-of-Service Open Threat Signaling*, pour Signalisation distribuée des menaces ouvertes de déni de service) (RFC 8782) fournit également une méthode de demande d'actions d'atténuation à un routeur. Cela n'inclut pas les informations complètes sur la correction pour les consommateurs, mais cela pourrait être utilisé pour prendre des mesures d'atténuation immédiatement.

5 Interactions avec les utilisateurs

Comme mentionné ci-dessus, le nombre d'interactions utilisateur doit être réduit au minimum. Il existe trois options possibles pour communiquer avec un consommateur. L'une d'elles est via un portail sur le CPE. Dans ce cas, le consommateur doit se connecter directement au CPE sur le réseau local. Une autre approche est lorsque le CPE dispose d'une interface de contrôle dans un connecteur cloud, lui-même en contact avec le consommateur via une application. Une troisième approche consiste à faire en sorte que l'application se connecte directement au CPE. Ces approches ne s'excluent pas mutuellement. Alors que des normes telles que TR 369 et NETCONF fournissent certaines des capacités nécessaires, différents fabricants de CPE peuvent ou non utiliser ces protocoles.
Pour minimiser les interactions des utilisateurs, les développeurs doivent déterminer si l'utilisateur qui intègre un appareil est le consommateur ou le propriétaire, plutôt qu'un visiteur ou un membre de la famille. De cette manière, le consommateur peut savoir ce qui est intégré.

6 modèles de déploiement

Dans presque tous les cas décrits ci-dessus, il existe un appareil sur le réseau domestique auquel le consommateur (ou éventuellement le FAI) fait déjà confiance et qui joue un rôle dans la sécurité de l'appareil IoT. Nous donnons quelques exemples ci-dessous.

6.1 Appareils CPE fournis par les FAI

Dans ce cas, le fournisseur de services a inclus le CPE dans son service Internet. La plupart des composants nécessaires à l'intégration et à la protection des appareils IoT sont disponibles aujourd'hui via des distributions telles que le projet OpenWrt[16] et des associations industrielles telles que la Fondation prpl[17]. Certains FAI ont mis en service leur propre matériel de routeur ou l'ont acheté auprès d'un fournisseur qui peut fournir les bons packages et autorisations. D'autres FAI

achètent des solutions complètes auprès de fournisseurs. Beaucoup de ces fournisseurs ne sont que des codes d'expédition du projet OpenWrt et pourraient être convaincus d'inclure les composants respectifs aujourd'hui.

6.2 Routeurs secondaires achetés par les consommateurs

Pour de nombreux services Internet tels que le câble et la fibre jusqu'au domicile (FTTH), le routeur et le modem CPE sont souvent intégrés. Certains consommateurs trouvent que ces appareils CPE sont inadéquats. Soit les CPE ne disposent pas de certaines fonctionnalités telles qu'une portée Wi-Fi décente, soit les consommateurs ne font tout simplement pas confiance à leurs FAI. Certaines juridictions ont une obligation légale selon laquelle les consommateurs peuvent choisir d'utiliser leur propre CPE acheté individuellement, tandis que dans d'autres cas, des exigences optiques spécifiques pour le FTTH font qu'il est difficile ou impossible pour le consommateur de choisir son propre matériel. Les fournisseurs de CPE et de pare-feu doivent faire attention : si deux routeurs domestiques en cascade sont utilisés et que les deux offrent des services de sécurité, il est possible que leurs politiques soient en conflit ou prêtent à confusion.

7. Conclusion

L'Internet des objets requiert une perspective différente de la part des consommateurs, des fournisseurs de services et autres. Le rôle du prestataire de services dans la protection du consommateur et de la communauté au sens large contre les externalités introduites par des dispositifs qui ne sont pas sûrs (ou qui ne le resteront probablement pas) doit être soigneusement étudié. Nous avons proposé des méthodes qui permettent aux appareils de s'intégrer en toute sécurité de manière évolutive, qui tirent parti des relations existantes d'une manière qui les rend faciles à comprendre pour le consommateur. Cela nécessite un rôle étendu du CPE ou du fournisseur de pare-feu.

Références

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
- https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/white-paper-c11-743623.html
- https://www.itu.int/rec/T-REC-Y.4807-202001-I
- https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect
- Rapport sur la sécurité des appareils IoT https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur/Report+on+IoT+Device+Security.pdf

Ressources supplémentaires

- https://docs.oasis-open.org/cacao/security-playbooks/v1.0/csd01/security-playbooks-v1.0-csd01.pdf

Notes de bas de page

[1] https://www.softwaretestinghelp.com/iot-devices/
[2] https://www.cnet.com/news/amazon-sees-alexa-devices-more-than-double-in-just-one-year/
[3] Nous parlons d'« hérité », mais il s'agit d'un cas général aujourd'hui.
[4] Si cela ressemble à un problème de sécurité, c'est parce que c'en est un. Cependant, ne pas autoriser le contrôle automatique du Wi-Fi rend l'expérience utilisateur beaucoup plus complexe.
[5] Encore une fois, l'application finit par accéder à la liste des PSK du téléphone pour la plupart des réseaux !
[6] https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect/
[7] Draft-ietf-anima-bootstrap-keyinfra, en attente de références dans l'éditeur RFC Q. Consulter également https://www.sandelman.ca/SSW/ietf/brski-links pour davantage de matériau explicatif.
[8] Pritikin, et al, *Enrollment over Secure Transport (EST*), RFC 7030.
[9] Par exemple, consulter https://minerva.sandelman.ca/
[10] Une question ouverte est de savoir si le canal utilisé pour communiquer ces informations doit être normalisé.
[11] https://www.snort.org, http://zeek.org, https://suricata-ids.org
[12] https://turris.com/
[13] https://spin.sidnlabs.nl/

[14] Un autre exemple open source de « DPI » est ntopng, disponible à l'adresse ntop.org.
[15] La gouvernance est un domaine exploré par d'autres : Quelles parties sont responsables et doivent rendre compte des différents aspects du maintien de la sécurité du foyer et des appareils qui s'y trouvent ?
[16] https://openwrt.org/
[17] https://prplfoundation.org/

Date de publication: 16 avril 2021 — IoT