UTEC Melun – 1ère année de Manager en Ingénierie Informatique

Parcours Cybersécurité des Systèmes d'information

Domotique « Do It Yourself »

Créer sa domotique personnelle : opportunités et défis sécuritaires

Présenté et soutenu par Nicolas Morais, Florian Henaff, Benjamin Pacheco et Guillaume Sanchez

Promotion 2026

Sommaire

Résumé :

Grâce aux avancés technologiques, les habitats intelligent se sont vu transformer en se retrouvant de simple projet de laboratoire à un système accessible quotidiennement au grand public. La transition ne s'est pas faite sans obstacle ou sans questionnement sur certains aspects comme la souveraineté des données, la vie privée ou la sécurité. Le marché se retrouve lui saturé par un nombre de solution commerciales qui sont déjà prête à l'emploi et qui sont fermé. Les produits dits de grande consommation, créé une certaine dépendance envers les serveurs cloud des créateurs, ce qui rend l'utilisateur dépendant des pannes de services ou des changements politique des fournisseurs. Pour faire face à ce modèle, la domotique DIY est une alternative qui a su s'imposer comme un choix pour ce qui souhaite privilégier la confidentialité de leur vie privée. C'est une approche qui permet d'avoir un contrôle sur l'environnement domestique et sur les données qui seront générées par chaque interaction du système. L'un des outils utilisés et un nano-ordinateur qui s'est démocratiser par son rapport qualité-prix et qui à donner un élan sur l'accès à l'informatique embarquée. Cette nouvelle liberté est accompagnée d'un certain besoin de technicité et une responsabilisation des utilisateurs comparer aux autres solutions commerciales dites « clés en main » qui avait la sécurité à gérer de leur côté. Le rôle d'un concepteur de système domotique de type DIY devient multiple, il est autant un administrateur système qu'un expert en cybersécurité pour la domotique.

Le choix du matériel est un pilier important car, c'est sur lui que reposera la robustesse de l'infrastructure. Le Raspberry Pi est une référence grâce à sa communauté et aussi sa faible consommation électrique. Cependant, son usage intensif a mis en avant les limites physiques de la solution comme la fragilité de la mémoire des cartes micro SD liée aux écritures répétées. Des alternatives peuvent permettre de palier à cette faiblesse par des caractéristiques techniques supérieurs mais aussi en incluant un stockage plus rapide et robuste, on peut parler de Orange Pi ou l'Odroid. Il peut y avoir sur certaines de ces solutions des questionnements sur des risques cybersécurités car ils peuvent être moins documentés. On peut parler de dans certains cas de portes dérobés, appelés Backdoors) sur le matériel ou des potentiels vulnérabilités sur les pilotes. Pour des utilisateurs ayant des besoins liés à de l'analyse d'image par IA ou de la gestion de flux vidéo, le passage vers un mini-PC sous un environnement de virtualisation peut être intéressant. C'est une approche qui permet d'isoler la logique de service, ce qui peut être un compromis sur un serveur de fichier qui n'entrainera pas une prise de contrôle du système. Les autres points de réflexion sont sur la redondance matériel et sur la gestion de l'alimentation car ce sont ces points qui peuvent garantir la continuité de service en cas de coupure électrique.

Un système domotique est bien plus qu'une unité centrale, c'est un système qui s'étend à travers un réseau de capteurs et d'actionneurs. Les capteurs servent à mesurer les données de l'environnement que ce soit la température ou l'humidité ou bien les états de sécurité. L'un des défis reste la disponibilité de ces capteurs car ils dépendent autant des protocoles sans fil que les alimentations. On peut prendre l'exemple d'un capteur de fenêtre qui fonctionnerait avec une pile, lorsque la pile est vide alors la fenêtre devient un angle mort dans le système de sécurité. Les actionneurs sont présents pour transformer une commande ou demande en action

physique, on peut parler ici d'un micromodule de volets roulant. Ces éléments sont vulnérables aux attaques de proximité. Une étude de cas a démontré qu'une ampoule connectée qui serait mal conçu, peut être utiliser comme point d'entrée pour l'extraction de données comme des clés de chiffrement Z-WAVE ou Zigbee. Le pirate peut écouter le réseau ou faire une injection de commande sans même être dans le domicile. La sécurisation des terminaux vient d'un choix sur les marques utiliser mais aussi de la mise à jour régulière des micrologiciels, l'opération peut être complexe sur des appareils à basse consommation.

La communication entre les différents appareils du système domotique est constitués de différents protocoles qui doivent être définit au préalable pour lier confort et sécurite. Le Wi-Fi est simple à déployer mais peut arriver rapidement à saturer les routeurs et présente une surface d'attaque conséquente si le réseau n'est pas configuré correctement par segmentation.

Le Zigbee et le Z-Wave sont pertinent car ils sont utilisables sur des fréquences différentes de celle du Wi-Fi et offrent ainsi une meilleure résilience et une consommation réduite. La structure du réseau est aussi différente car elle suit une structure réseau dites maillés. Ils restent, cependant, vulnérables au brouillage radio (Jamming). Un attaquant peut saturer les fréquences pour empêcher une alerte d'intrusion d'atteindre l'unité centrale.

Pour les fonctions dites critiques, la liaison filaire peut être une solution car elle offre une immunité aux perturbations électromagnétique et une fiabilité supérieure. Les industriels tentent de résoudre cela par une fragmentation avec le standard Matter, solution soutenue par les géants de la technologie. Matter mets en avant, l'interopérabilité universelle et un renforcement de la sécurité nativement par le chiffrement de bout en bout et à cela s'ajoute l'authentification des appareils. L'utilisation de ces standards est un moyen de réduire la complexité technique tout en élevant la protection globale des installations.

Pour les logiciels, des plateformes tels que Home Assistant ou Jeedom ont su se mettre en avant comme des leaders du système domotique. Leur atout provient du traitement local, c'est-à-dire que les données ne quittent le réseau que si l'utilisateur autorise l'exportation de ces données. L'idée est de protégé les données contre de potentiels exploitation commerciales basés sur les habitudes de vie des personnes utilisant des écosystème domotiques. Cependant la sécurité dépendra de l'utilisateur. Les vulnérabilités sont hélas inévitables, certaines failles peuvent être exploiter pour passer outre l'authentification ou faire exécuter des codes malveillants à distance, on peut parler ici de failles de types « Zero Day ». L'IA intégré aux systèmes et fonctionnel en local, ouvre de nouvelles possibilités pour faire face à des tentatives d'intrusion comme la détection d'anomalies. L'avantage de l'IA, vient du fait que cette technologie peut apprendre des schémas répétitifs d'action ou commande lié à l'environnement domotique et ainsi avertir l'utilisateur en cas de problème externe par exemple, la communication d'un appareil connecté avec un serveur inconnu. Un point qui reste sensible est la gestion des accès extérieur par le biais de tunnel sécurisé ou VPN pour éviter d'exposer les interfaces d'administrations.

Les actualités sur la domotique mettent en avant les dangers d'un système domotique mal sécurisé. Des réseaux d'objets connectés qui sont compromis, sont appelés botnets et sont utilisés pour lancer des attaques DDOS. Des incidents ont montré des attaquants qui prennent le contrôle des caméras intérieures ou de robot aspirateur qui sont équipés de micros ou caméra. La menace ne se limite pas aux appareils mais aussi à des véhicules connectés qui partagent les mêmes types de vulnérabilités. Les failles logicielles permettent à des chercheurs de potentiellement déverrouiller et démarrer à distance des véhicules. Certains scénarios démontrent que la sécurité doit être intégrée dés la conception de l'architecture. La segmentation du réseau est une stratégie qui permet d'isoler les objets connectés sur un réseau qui sera séparer et qui empêchera un capteur compromis d'avoir accès à l'ordinateur personnel qui pourrait contenir des données sensibles et privées.

La domotique DIY permet d'offrir une opportunité sans précédent et ainsi de se réapproprier sa propre technologie domestique. Elle exige cependant, une certaine rigueur et discipline. Les recommandations d'organisme comme l'ANSSI peuvent fournir une feuille de route, comme le fait de changer systématiquement les identifiants par défaut, désactiver des services inutilisés, chiffrer les communications et permettre de maintenir un écosystème sain. L'avenir de la domotique passera par une forme d'hybridation entre la facilité des usages de standards modernes et robustes et la robustesse de systèmes locaux ouvertes. Les utilisateurs doivent rester acteurs de la sécurité en ayant une conscience concrète sur le fait que l'ajout d'un appareil ouvre une porte supplémentaire vers nos vies privées. Le fait de faire une veille technologique est une méthode qui permet aux professionnels de se tenir aux courants des avancés mais aussi aux citoyens pour être apte à vivre avec un système domotique. Il s'agit ici d'un moyen d'acquérir un confort tout en ayant une domotique sécurisée car, une faille numérique peut entraîner des conséquences physiques.

Abstract Anglais

In 2026, there are more connected peripherals than ever before, this includes computers, smartphones, entertainment devices and much more. In these devices we can also find IoT devices which can be cameras, NVRs, smart bells, smart locks, and much more smart appliances.

In this document you will find multiple angles on how smart appliances can be unsecure and how to protect your home from intrusions.

First, we will elaborate on the hardware which is the core of the machine, its characteristics will determine whether it is a device capable of handling several processes and the Input and Output Panel will determine its compatibility with other peripherals.

The very popular Raspberry Pi, known for its performances, its size and its cost-efficiency. This ARM chip is capable of running multiple programs but has physical constraints. It uses micro-SD cards as storage and is vulnerable to data corruption, and its GPIO connectors are not protected against voltage surges.

The alternative options to Raspberry Pi include Orange Pi, Odroid and more. These cards eliminate the Micro-SD cards for more reliable NVMe ports or integrated eMMC memory. They have more processing power but present other risks such as hardware trojans and counterfeit.

Micro controllers like the ESP32 are very affordable and perfect for running simple tasks, they have both Bluetooth and Wi-Fi capabilities as well. Mini PCs are great for running hypervisors and can prevent propagation of malware in case of an attack on the network.

The infrastructure of IoT is based on sensors which can then trigger actions, the integration of such devices is a challenge because of physical and networking constraints.

Battery-powered devices can become defective without warning, devices located outdoors are exposed to sabotage, theft and data extraction and jamming. These can lead to Wi-Fi password theft for example.

Protocol	**Characteristics**	**Pros & Cons**
Wi-Fi	Uses the already existing network for centralized management.	Simple and scalable, vulnerable to hacking and dependent on the existing network. Can be energy-consuming

Bluetooth (BLE/Mesh)	Uses receptors coupled with profiles.	Low power communication (BLE), Limited range, can be upgraded with a hub.
Z-Wave	Bidirectional proprietary protocol, uses 868.4 MHz frequency in Europe	Stable, traverses through obstacles well, meshed network, encrypted communications, high cost
Zigbee	Protocol IEEE 802.15.4 using 2,4 GHz frequency	Low power, can manage up to 65 000 devices, risks of saturating the 2,4 GHz Frequency band

There are new standards arising to eliminate the need for proprietary hubs:

- Matter, a new norm usable in local networking
- Thread, a new meshed networking protocol using IPv6

We will also elaborate on multiple software used in domotics applications, the topic of home-automation is getting wider spread among tech enthusiasts and they need a software that can fully utilize the power of the hardware they bought, some hardware already comes with proprietary software but the open-source alternatives are generally better as they are built by the community for the community's needs.

Home assistant is the best-known and most used OS right now, it is Open-Source software opting for on-premises functionality. No cloud-based technologies and assuring data confidentiality.

Domoticz or OpenHAB are both light Open-Source software and are highly customizable for advanced users or prosumers.

Jeedom is the French alternative using specific plugins

We can also look at different protocols such as MQTT which is a asynchronous mailing protocol using a server where clients sign-up to lists and publish to these lists called "topics".

DIY domotics has been introduced very early and some consumers weren't aware of the risks of having devices connected to the internet and resulted in some of the biggest cyberattacks in history.

The infamous Mirai Botnet is one the biggest botnet in the world and consists largely of different IoT devices, there has been reported cases of "swatting" which is a fake report to the police of illegal activity or hostage situations in homes. These attacks lead to the specialized authorities to be mobilized only to discover that there is no threat on site.

Everything in a connected home can be compromised, From Nest cameras to smart toilets, everything can be used against the consumer and contains data to be stolen, even smart watches can be tracked by activity tracking applications like Strava, which recently leaked the position of the nuclear aircraft carrier Charles-De-Gaulle while in operation.

These devices can also malfunction due to internet outages, a malfunction in AWS servers induced some connected mattresses to overheat which can cause harm to the customer. Some KIA vehicles were tracked only by using the license plate number. Unfortunately, some malfunctions can have dire consequences, some diabetes sensors that were defective induced the death of 7 people.

Fortunately, some governmental agencies are starting to make guides and labels to accompany the customers and regulate the making of IoT devices. This is helping consumers by making sure their devices are secured properly and will not compromise the network they occupy. It can also help customers make better decisions for choosing hardware and software depending on their needs and their preferences.

The European Telecommunications Standards Institute made a guide referenced EN 303 645 to accompany the users that have little to no knowledge of IT and aid them in setting up their devices and their data.

The ANSSI has also made a guide which is much completer and more usable in multiple contexts. They tackle different subjects such as networking, cryptography, software and hardware.

They also specify which of their recommendations are primordial and which are applicable only to very sensitive contexts

Some Cybersecurity labels exist or are in the making like the U.S Cyber Trust Mark but IoT devices still aren’t labeled by the authorities yet but the will to have a governmental agency to help customers identifying secured products is getting stronger.

Introduction

L'habitat intelligent a longtemps été une vision futuriste de notre quotidien. Aujourd'hui, il fait pleinement parti de nos vies. Beaucoup de solutions commerciales sont proposées aux particuliers, mais elles sont souvent fermées et dépendantes du cloud. Heureusement, il existe également une solution alternative, la domotique personnelle, autrement appelé le « Do It Yourself » (DIY). L'un des produit phare de cette solution est le Raspberry Pi, un nano-ordinateur qui permet de réaliser sa propre centrale domotique, tout en étant abordable. Cette solution permet le contrôle total sur son environnement et ses données.

Le Raspberry Pi est le produit le plus utilisé pour dans les installations DIY, mais il est loin d'être seul sur le marché. Aujourd'hui, on retrouve divers nano-ordinateurs et des microcontrôleurs plus adapter à certains besoins spécifiques qui embarque par exemple des capteurs de température, des actionneurs, des caméras ou encore des relais. Cela rend le choix de l'équipement à utiliser plus complexe et amène une réelle réflexion sur le besoin que les utilisateurs en ont.

Avec cette technologie, on peut se demander qui sont les personnes qui l'utilise aujourd'hui ? Est-ce qu'il s'agit uniquement de passionnés d'informatique ou cette solution intéresse et est à la portée également du grand publique ? N'importe qui peut réaliser chez soit sa domotique sans passer par des solutions commerciales ? Le DIY est un marché de niche ou bien peut-il concurrencer les géants de la tech ?

Créer sa propre infrastructure soulève un sujet critique, la cybersécurité. La domotique commerciale gère la sécurité de l'utilisateur, mais la domotique DIY elle laisse l'entière responsabilité à son créateur. On peut se demander, est ce que le Raspberry Pi est sécurisé ? Comment les utilisateurs parviennent à protéger leurs données et résister aux intrusions potentiel ? La communication entre les multiples périphérique peut-elle être à la fois performant, privé et inviolable ?

La domotique est applicable dans différents domaines mais s'inscrit surtout de plus en plus dans notre quotidien avec la gestion des lumières par exemple et des différents équipements qu'utilises les personnes. Il y a aussi une dimension économique lié à l'usage de la domotique. La gestion des équipements et des logiciels permettant aux personnes d'avoir un contrôle sur leurs consommations. On peut donc se demander s'il est plus pertinent d'investir dans du matériel de domotique dans une habitation ancienne ou de faire en sorte de construire un lieu lié directement à un système de domotique intégrer directement avec des spécificités selon le propriétaire.

Cela pourrait aller de la gestion simple d'équipement jusqu'à la mise en place d'une IA interactive qui s'adapterait au besoin des propriétaires. Il peut aussi y avoir une dimension sécuritaire sur les équipements types caméras ou même ouverture de porte sécuriser par commande vocal ou digital.

On peut se demander si la domotique peut être utiliser pour toutes les fonctionnalités du quotidien et que cela sera suffisamment sécuriser ou qu'il faudrait selon certains cas privilégiés les méthodes plus traditionnels.

La Couche Physique : Le matériel et ses vulnérabilités

Dans ce chapitre, on va parcourir l'aspect matériel lié à la domotique. Le choix du matériel est un des facteurs les plus important d'une installation. La comparaison entre les solutions est capitale pour gérer au mieux ses besoins et le prix qu'on est prêt à mettre pour une installation optimale et sécurisé.

Dans un premier temps, nous allons parler des différentes options de matériel disponible sur le marché dont LA référence de la domotique, le Raspberry Pi, mais également ses concurrents et leurs différentes caractéristiques. Dans un second temps, nous allons parler des périphériques que l'on peut utiliser dans un installation Do It Yourself (DIY). Enfin en troisième point nous allons voir les interfaces et la communication physique entre les et les périphériques.

Les différentes options de matériel

La star de la domotique DIY, le Raspberry Pi

On ne peut pas parler de domotique, sans parler du Raspberry Pi ? Il est la référence du marché de la domotique. Il s'agit d'une famille d'ordinateur à carte unique (Single Board Computers ou SBC) développé en Angleterre par la Fondation Raspberry Pi. Les premiers modèles sont sortie dans les années 2012 et 4 ans plus tard, on comptait déjà plus de 10 millions d'exemplaire vendu. La force du Raspberry Pi qui a séduit grand nombre d'utilisateur sont sa taille réduite et sa faible consommation en énergie.

Ce qui la différencie d'un microcontrôleur classique comme de l'Arduino, c'est qu'ils embarquent une architecture complète. Un microcontrôleur classique lui est conçu pour exécuter un seul programme à la fois. Cela limite grandement son usage. Le Raspberry Pi étant un ordinateur à part entière, il a un processeur basé sur l'architecture ARM (un CPU), de la mémoire vive (RAM) un port Ethernet, des ports USB, un port HDMI et des broches GPIO (General Purpose Input/Output). Cette configuration lui permet donc d'exécuter plusieurs programmes en même temps et donc d'être un équipement parfait pour être le cerveau d'une installation domotique avec plusieurs matérielle dépendent et indépendant entre eux.

On le sait maintenant, le Raspberry Pi est une option très alléchante pour réaliser une infrastructure de domotique, mais il faut prendre en compte certain aspect qui peuvent jouer sur le bon fonctionnement et la sécurité d'une installation. En effet, il a été conçu pour être accessible facilement, donc avec un cout limité. Cela engendre une limitation physique qui peut apporter certaines limites et certains problèmes à son utilisation.
Le Raspberry Pi utilise comme stockage une carte micro SD, le système d'exploitation et les données repose donc sur une technologie qui ne dispose pas de la commande de contrôle "TRIM" utilisé par les disques durs SSD pour limiter l'usure du disque, ce qui peut engendrer des problèmes de corruption du système et donc la perte de toute son installation.
Un autre problème à prendre en compte, les connecteurs GPIO qui permette de connecter le Raspberry Pi à d'autres circuits électroniques n'a aucune protection contre les surteintions. En effet, le Raspberry Pi est basé sur une logique de fonctionnement sur 3,3 volts, si par accident on connecte un équipement basé lui sur du 5 volts (ce qui peut être fréquent), cela entrainera la destruction permanente de la carte.

Tous matériels on leur avantage et leur inconvénient, un utilisateur bien informé de ces différents problèmes et limites n'aura aucun mal à les gérer et à utiliser correctement et avec précaution un Raspberry Pi.

Ce qui fait la force du Raspberry Pi, c'est son prix. Il existe plusieurs modèles et l'une de leur politique phare est de conserver l'entrée de gamme de chaque model a un prix tout à fait abordable. Chaque version d'un model part sur la même structure, ce qui les différencie entre elles, c'est la capacité de la RAM. Par exemple, la version d'entrée de gamme du model Raspberry Pi 5 est à 45 $ pour une 1GO de RAM. Plus on grimpe dans la capacité mémoire, plus il est cher donc 65 $ pour 2GO, 100$ pour 4GO, 175$ pour 8Go et 305$ pour 16GO (Prix officiel MSRP US).
Pour une domotique DIY légère avec des règles simples, les versions d'entrée de gamme du Raspberry Pi avec 1GO de RAM suffise largement, On peut par exemple trouver la version 1GO du model Raspberry Pi 4 pour 35$ ce qui est imbattable sur le marché pour un micro-ordinateur. Avec la monté du prix de la RAM ses derniers mois, la Fondation Raspberry Pi pour garder une politique d'équipement abordable pour tous, a même sortie une nouvelle version du Raspberry Pi 4 avec 3GO de RAM pour environ 83$.

Les alternatives d'ordinateur à carte unique

Comme tout produit phare, Raspberry Pi ne fait pas exception à la règle et a vu naitre une multitude de concurrent offrant des alternatives qui résout les limitations du Raspberry Pi. Parmi les plus célèbres dans l'univers de la domotique DIY, on retrouve le Orange Pi, Odroid et Radxa avec sa gamme Rock Pi. Ce sont tous les trois des ordinateurs à carte unique (Single Board Computers) et sont plus adapté à certaines tâches que le Raspberry Pi.

Le plus gros souci du Raspberry Pi, c'est son système de stockage basé sur une carte SD. L'avantage de ces alternatives est qu'ils ont embarqué dans leur « Single Board Computers » nativement un port M.2 permettant de connecter des disques SSD NVMe. Pour les modèles qui n'ont pas de port disponible, il embarque souvent un module de mémoire eMMC soudés directement sur la carte. Ces deux solutions écartent complètement le système de carte SD proposé par le Raspberry Pi et les différents problèmes de défaillance qu'il représente. Cela permet aux systèmes domotique qui fonctionne en continu d'être plus fiable et garantie leur longévité.
Ces cartes utilisent également un autre type de processeur, les Rockchip. Ces processeurs qui offrent de meilleures performances et réalise de meilleur calcule brut. Cela permet de pouvoir réaliser des tâches dans les domotiques DIY que le Raspberry Pi a du mal à faire comme un système de cameras de sécurité qui n'utilise pas une solution cloud mais interne.

Sur le papier, ces solutions on l'air réellement mieux, mais elles ont également des défauts qui ne sont pas négligeable et souvent ignoré des amateurs de domotique DIY. À la différence du Raspberry Pi qui maintient un certain niveau de transparence et qui a une communauté qui maintient une surveillance permanente des écosystèmes logiciel, les SBC (Single Board Computers) concurrents sont produit par des entreprise sans nom ou qui ont des processus d'assemblage qui ne sont pas transparent. L'ENISA (L'Agence de l'Union européenne pour la cybersécurité) elle-même a souligné ces problèmes et prévient sur le fait que la non-

traçabilité des composants matériels représente une vulnérabilité critique.
Des problèmes ont déjà été constaté comme des backdoor (porte dérobé) qui permette à une personne mal vaillante de rentrer dans le système installé, mis en place dans des « Hardware Trojans » (un cheval de trois matériels). Cela représente un danger réel pour l'utilisateur et pour ses données.
L'utilisation de leurs processeurs spécifiques, nécessitent souvent l'utilisation de pilotes matériels fermés ce qui engendre un problème de transparence et de sécurité. Les fabricants de matérielles utilisé sur les SBC peuvent très bien ajouter des backdoor intentionnelles et indétectable ou laisser passer une faille critique sans que l'entreprise qui assembles les composant ne le sache ou puissent le savoir.
Certain assembleurs pour économiser, utilisent des puces recyclées ou des contrefaçons rendant la fiabilité des cartes électroniques particulièrement dangereuses et multipliant le facteur risque d'une panne matérielle ou pire les dommages sur d'autre équipement de l'infrastructure domotique.

En termes de prix, les 3 concurrents principaux du Raspberry Pi offrent un large éventail de possibilité. Orange Pi par exemple, avec leur model son Orange Pi 5 et 5 plus, sont extrêmement puissant. Au niveau des prix, On peut retrouver Orange Pi 5 à 108$ le Orange Pi 5 plus à 141,99$ et le Orange Pi 5 Max a 125$ (Prix officiel MSRP US). C'est une alternative robuste et extrêmement intéressante. Parmi les concurrents sérieux, on peut également parler de la marque sud-coréenne Hardkernel avec les Odroid. On retrouve leur Odroid-M1S avec 4 GO de RAM à 49$ et leur Odroid-M1 avec 8 GO de RAM 90$ (Prix officiel MSRP US). Enfin la marque Radxa propose le Rock 5B avec 8 GO de RAM à149$ (Prix officiel MSRP US). Sur le papier, ces prix on l'aire intéressant, mais avec la montée des prix de la RAM, leurs prix ont considérablement augmenté, en rajoutant les problèmes cités auparavant, le choix de ces solutions n'est peut-être pas la meilleure des options. Tout dépend de son besoin et de ses attentes.

La nouvelle vision, les Microcontrôleurs et Mini-PC

Nous nous sommes concentrés depuis le depuis de cette partie, sur les infrastructures domotique basé sur les ordinateurs à carte unique. Mais il y a d'autre solution possible. Des solutions ultra légères, ou au contraire beaucoup plus complexe et robuste. Ces solutions permettent de pouvoir juger selon un besoin précis, qu'elle matérielle est réellement nécessaire pour une infrastructure domotique DIY.

Lors de la présentation de la famille du Raspberry Pi, il a été évoqué les microcontrôleurs. Cette technologie permet de réaliser des tâches simples qui ne nécessite pas de système d'exploitation. Le plus connu est la puce ESP32, conçue par l'entreprise Espressif Systems. Pourquoi utiliser un monstre de puissance pour allumer une simple lumière si c'est la seule chose que l'on veut mettre en place. Les microcontrôleurs sont la solution parfaite pour ça. L'ESP32 embarque nativement des puces Wi-Fi et Bluetooth et des connectique GPIO pour connecter ses équipements.
On peut trouver des puces ESP32 pour environs 8$ (Prix officiel MSRP US).

L’ESP32 peut très bien être indépendant et servir à une tâche unique, mais il peut également être associer dans une infrastructure encore plus grande, servir de périphérique dans une infrastructure contrôlé par des ordinateur fiable qui embarque l'architecture standard x86 utilisé par Intel et AMD.

Les mini-PC sont l’une des meilleures solutions à ce jours pour réaliser une infrastructure domotique DIY. Une multitude de maque propose ce genre d’équipement. Lenovo avec ses Tiny, peu gourmand en consommation (20-25 W au repos) ou Dell avec ses gammes QCM et FCM ou encore HP avec sa gamme EliteDesk. Etant donné que ce sont des ordinateurs à part entière, ils ont des composant plus ou moins modulable et donc, les prix sont plus ou moins cher. On peut en trouver avec des composant convenable pour environs 200 euro, tout comme on peut payer le dernier cri a plus de 1000 euro. Le tout est de savoir à quoi va-t-il servir. Pour un simple environnement domotique, les moins chère ferons l’affaire.

L’avantage du mini-PC est que l’on peut le transformer en hyperviseur de type 1 et donc faire de la virtualisation. Cela permet de réaliser un système domotique isolé dans une machine virtuelle et donc d’en faire plusieurs distinct selon le besoin. Par exemple réaliser tout un system de vidéo surveillance interne, mais à part de tout le système de gestion des lumières ou des volets électriques. L’utilité de cette séparation est de limiter les attaques à un environnement fermé qui ne peut pas accéder à un autre environnement. Bien sécuriser, c’est le meilleur moyen de limiter les mouvements latéraux sur le réseau physique. Autre aspect que le mini-PC transformé en hyperviseur de type 1, c’est la possibilité de réaliser des sauvegardes régulières afin de garantir la redondance de ses données et des captures (snapshot) de son infrastructure pour pouvoir le redéployer rapidement en cas de problèmes ou d’une mauvaise mise à jour. L’avantage, c’est que l’on peut également réaliser à côté un HomeLab à partir de ce même PC, donc avoir par exemple un serveur multimédia ou un bloqueur de publicité. Avec un mini-Pc les possibilités de création pour du Do It Yourself est quasiment infini.

Les Périphériques : Capteurs et Actionneurs

Nous avons vu jusqu’à présent, les possibles « cerveau » d’une infrastructure domotique DIY, nous allons maintenant parler des membres d’une infrastructure. Un environnement domotique peu utiliser une multitude de petit appareille pour fonctionner, tout dépend de nos besoins. On distingue deux grandes familles de périphérique, les capteurs et les Actionneurs.

Dans un premier temps, nous allons nous attarder sur les capteurs, a quoi servent t’ils, comment fonctionnent t’ils et qu’elle autonomie ont t’ils. Dans un second temps, nous allons parler des actionneurs, que peuvent-ils faire et qu’elle risque existe-t-il. Enfin nous allons voir quelle vulnérabilité existe t’il sur ses équipements physiques.

Les Capteurs

La principale fonction d’un capteur, c’est d’acquérir des données afin qu’elles soient exploitables par toute l’infrastructure domotique. Il existe une multitude de capteur différent que l’on peut, pour simplifier, séparer en deux grandes familles différentes, les capteurs d'état et les capteurs environnementaux.

Parmi les capteurs d'états (ou d'intrusion) on retrouve plusieurs types de capteurs. Les capteurs magnétiques que l'on place sur les portes et sur les fenêtres, il permet de savoir si une porte ou une fenêtre est ouverte et de savoir laquelle. On a également les capteurs de présence, avec des détecteurs de mouvement infrarouge passif de type PIR qui utilise la technologie infrarouge pour mémoriser l'image infrarouge d'une zone et qui détectera si cette image est changée par un mouvement. Toujours dans la détection de mouvement, nous avons le simple capteur de mouvement qui réagira si l'on agite quelque chose devant. Pour de la surveillance, tous ces capteurs peuvent être jumeler avec une caméra de surveillance qui s'activera en cas de mouvement anormal ou de l'ouverture d'une porte ou d'une fenêtre.

L'autre grande famille des capteurs, les capteurs environnementaux sont basés sur des mesurent de variables ambiantes. Il en existe une multitude. Les capteurs de température qui, selon le degré d'une pièce, peut activer ou désactiver le chauffage. Les capteurs hygrométriques afin de mesure l'humidité présente dans l'aire. Les capteurs de luminosité LDR qui réagis selon l'intensité lumineuse qu'il détecte. Les détecteurs de monoxyde de carbone pour le renouvellement de l'aire et les détections des fuites de gaz. Les détecteurs de fumée qui peuvent déclencher une alarme incendie et même prévenir les pompiers afin qu'ils puissent intervenir au plus vite.

L'une des contrainte de la domotique, c'est qu'il faut faire fonctionner tous ces équipements et donc les placer dans des endroits précis d'un environnement pour pouvoir continuer à les alimenter. Le problème, c'est que souvent, les endroits où on en le plus besoin sont également les endroits où il n'y a pas d'alimentation électrique, donc ils reposent souvent sur de batteries ou des piles. Par exemple dans le battent d'une fenêtre, ou sur un plafond, ou encore dans un jardin, compliquer de faire passer des câbles d'alimentation jusqu'à ces endroits. Cela représente également un autre problème, d'ordre sécuritaire, la perte de la disponibilité des données qui est l'un des 3 piliers de la CIA, Confidentialité, Intégrité, Disponibilité. Un capteur fonctionnant sur batterie qui ne peut alerter son utilisateur qu'il n'a presque plus d'énergie, représente « un point de défaillance silencieux ». Dans le cas des capteurs d'état, un système domotique mal configurer et sans redondance pourrait par exemple bloquer l'accès à un bâtiment créant une un scénario que l'on nomme « fail-open » représentant une faille majeure de sécurité.

Un utilisateur bien informé et préventif pourra palier à ce genre de problème en mettant en place un protocole stricte et rigoureux. Privilégier les bons emplacements pour les appareille utilisant la Wi-Fi car c'est un protocole lourd qui doit avoir une connexion continue avec un routeur, donc ne pas utiliser une simple pile bouton qui se viderait en quelque semaine mais privilégier un branchement sur le réseau électrique directement. Il faut adapter son matériel au besoin, en général, les appareille de qualité privilégie les puces radio basées sur le standard IEEE 802.15.4. Cette technologie est conçue pour se mettre en veille, ou dormir la majorité du temps, et d'émettre un signal uniquement en cas de changement d'état comme l'ouverture d'une porte par exemple. C'est ce qu'on appelle un protocole maillé (Mesh). Ce type d'approche permet en général de pouvoir faire fonctionner un équipement pendant 2 ou 3 ans en toute autonomie avec

une simple pile. Avec un planning de changement de pile bien rodé, c'est le meilleur moyen d'avoir une infrastructure DIY sur et autonome.

Les Actionneurs

Nous avons vu les capteurs, voyons à présent l'autre élément essentiel d'une infrastructure domotique, les interrupteurs. Au-delà d'un simple bouton ON / OFF, leurs rôles d'intercepter une action physique pour la traduire en instruction l'environnement logiciel du réseau domotique.

Aujourd'hui, un actionneur dans la domotique ne s'arrête pas à ouvrir ou fermer un circuit avec un simple bouton. On peut mettre en place des microcontrôleurs lié à des appareille, afin de pouvoir déclencher des actions précise selon des données reçu. Par exemple, un capteur de luminosité LDR qui selon les rayons lumineux peut envoyer un signal à des semi-conducteurs comme des triacs ou des transistors MOSFET afin de pouvoir contrôler la monter et la descente des volets roulant d'une maison.
Aujourd'hui, on retrouve beaucoup de technologie encastrable directement dans les murs d'une maison. Des petit boité ou équipement qui embarque des microcontrôleurs tel qu'un ESP32. Une prise électrique intelligente par exemple, elle est installable comme une prise électrique classique, mais embarque un capteur et un actionneur, le capteur lui va pouvoir mesurer la chute d'une tension électrique pour pouvoir calculer en temps réel la consommation, et pourra être entièrement programmable pour par exemple démarrer une machine à laver à un horaire précis, ou une cafetière en déclenchant sans lancement à distance.

L'un des buts des ingénieurs qui travaillent sur ces équipements, c'est la mise en place des équipements récent dans des maison déjà existante. Dans le cas d'une maison en construction, l'intégration des équipements sont directement mis sur les plans de construction c'est plus simple. Mais dissimuler un équipement dans de l'existant c'est déjà plus compliqué. Il y a deux problèmes à ce défi. La taille des équipements, et la dissipation thermique.
Beaucoup d'équipement domotique rentre parfaitement dans les boités électrique standard (4-5 cm), facilitant de plus en plus leur installation directement sur le réseau électrique et d'autres sont prévu pour être installé derrière une prise électrique mural. C'est un véritable défi, les ingénieurs ont dû intégrer dans un circuit imprimé de la taille d'une pièce de monnaie, des technologies comme un convertisseur énergétique qui passe l'énergie d'une maison donc 230 volts, en 3,3 volts qui est le standard de ces équipements, ou encore le moyen de communication comme un microcontrôleur muni d'une antenne Wi-Fi, Zigbee ou Z-Wave afin de pouvoir communiquer avec les autres équipements. Mais également des sécurités comme des varistances ou des fusibles, afin d'éviter des arcs électriques ou des pics de tension pouvant provoquer la détérioration de l'équipement ou pire, un incendie.
Autre point compliqué comme nous l'avons vu, c'est la dissipation thermique. Tous ces équipements ont un défaut en commun, il chauffe. Ils sont souvent donc enfermés dans des endroits clôt, sans circulation d'aire donc les composant chauffe. L'une des solutions trouvées est de réaliser des composants multicouches pour qu'ils puissent servir de radiateur passif afin de pouvoir dissiper au mieux la chaleur.

Les actionneurs sont un point crucial d'un environnement domotique, les dissimuler comme nous l'avons vu, est un véritable défi matériel et il est autant compliquer d'un point de vue physique qu'électronique.

Les vulnérabilités physiques : Sabotage et extraction matérielle

Qui dit équipement physique, dit également risque de sabotage physique. Le cœur d'une infrastructure domotique DIY est naturellement au sein d'une maison, il est très rarement exposé directement depuis l'extérieur, à la différence des capteurs et actionneurs qui eux sont très souvent exposé. On peut en trouver partout où il peut y avoir une utilité par exemple une façade extérieure, un jardin ou bien même une boîte aux lettres, ce sont autant de zones complètement non sécurisées. Les attaquants et saboteurs peuvent exploiter cela et endommager les équipement ou pire s'emparer des clés de connexion ou des données présent dans un appareil.

Un saboteur n'a pas besoin de compétences spécifique en informatique pour neutraliser un équipement. Par exemple, il a été observer des attaques sur les capteurs de mouvement infrarouge passif PIR qui servent souvent pour prévenir d'une intrusion, que des personnes malveillantes utilisait des objets en verre ou avec une certaine couverture thermique pour masquer une intrusion physique. Grace à se procéder, ils peuvent se déplacer librement devant les capteurs bloqués sans être inquiété.

Une autre forme de sabotage, consiste tout simplement à détruire un équipement pour éviter qu'ils donnent l'alerte, arracher une alarme d'un mur. Pour remédier à ça, certains équipements sont dotés de petit capteur de sabotage, si l'équipement est déplacé ou retiré du mur, une alerte se déclenché immédiatement.

Certain équipement, souvent de mauvaise facture, laisse la possibilité de se connecter au terminal d'un microcontrôleur avec les privilèges maximum pour pouvoir débuguer se dernier. Les attaquants avec des connaissance en informatique qui peuvent avoir accès à certains périphériques d'une infrastructure domotique peuvent donc tout à fait se connecter sans mot de passe et obtenir la possibilité de pénétrer le réseau.

L'une des failles les plus connu et peut être l'une des plus exploité est le vol d'une ampoule connecter. Une personne mal attentionnée peut tout à fait l'exploiter pour soutirer le nom d'un réseau Wi-Fi et son mot de passe ou la clé de réseau du maillage Zigbee ou Z-Wave. Sur des objet connecté low-cost, ces données sont souvent laissées en claire donc elles sont complètement exploitables pour un attaquant qui peut tenter de se connecter au Wi-Fi et attaquer le cœur du réseau domotique.

Les Interfaces et la Communication Physique

Pour sécuriser son environnement de manière optimal, il faut que les objets connectés soient directement connectés en local, sans passer par internet. C'est crucial dans une infrastructure DIY, cela permet de garder le contrôle. Nous avons vu jusque-là les différents équipements nécessaire et possible pour construire une architecture domotique Do It Yourself, nous allons maintenant comment ils communiquent entre eux. Dans un premier temps, nous allons parler

des contrôleurs de protocoles et les vulnérabilités qui lui sont lié. Dans un second temps, nous allons voir les failles que les connexions dites directes ou filaire peuvent représenter.

Les contrôleurs de protocoles (Dongles USB) et la vulnérabilité radio

Dans la majorité des cas, la communication entre les périphériques et le hub central s'effectuer par onde radio, avec ce que l'on appel des dongles USB. C'est petit capteur, repère une fréquence émise et il sait selon la fréquence, de quel objet il s'agit.

Dans ces petites clés USB, on retrouve un microcontrôleur qui peut avoir généralement de 2 types d'antennes :

- Les antennes gravées, souvent sur les clés d'entrée de gamme, directement gravé sur le circuit imprimé. Sa porter est très limité et très perturbable par les obstacles.
- Les antennes externes, qui comme leur nom l'indique son des éléments externes a l'objet, souvent des antennes à viser sur le périphérique. Beaucoup plus performant qu'une simple antenne gravée.

L'un des gros problèmes avec ce type de connectique, c'est qu'un attaquant peut également intercepter un signal et le reproduire si le signal n'est pas chiffré. Une sonnette de maison connecté par exemple est facilement interceptable et peut être aussi facilement reproduit.

Un autre type d'attaque physique connu est le brouillage que l'on nomme « Jamming ». Cela consiste, à l'aide d'un brouilleur, de perturber les onde radio émis afin de saturer le dongles USB et d'empêcher, par exemple les capteurs d'une alarme de se déclencher et de signaler un problème. C'est ce qu'on appelle un déni de service (DoS).

Une infrastructure DIY bien construit privilégiera donc pour un système de surveillance plus souvent une connexion filaire.

Les connexions filaires directes et les failles électriques

L'autre manière de connecter un périphérique a son réseau domotique, c'est de passer par des connexions filaires avec notamment les broche GPIO, très utilisé par les Single Board Computers. Ce sont des câbles directement branché à la carte mère qui évite d'utiliser du réseau sans fil ou de l'onde radio.
Les broches GPIO présente cependant certaine vulnérabilité. Comme nous l'avons vu auparavant, des broches permette à une personne de pouvoir se connecter directement à la carte mère et donc de prendre le contrôle physique de l'objet. Également, une défaillance ou un court-circuit peut détruire instantanément et irrémédiablement l'objet.

Parmi les méthodes de connexion filaire, on peut également retrouver les connexions en Ethernet avec RJ45. Plus fiable que les broches GPIO, une connexion Ethernet peut même suffire à l'alimentation d'une caméra de vidéosurveillance par exemple, c'est ce qu'on appelle « Power over Ethernet ». Cela évite de devoir tire un câble électrique en plus d'un câble RJ45 pour un seul équipement.
Le soucis avec la connexion en RJ45, c'est qu'une personne mal veillant, peut tout à fait arracher un équipement, récupérer le câble et se connecter directement au réseau de l'habitation.

Pour contrer cette vulnérabilité matérielle, une installation domotique DIY doit segmenter son réseau par appareille pour éviter une propagation dans le réseau.

Dans cette partie, nous avons vu quel matériel était possible d'utiliser comme cœur d'une infrastructure domotique DIY, quels type objets pouvait y être connectés et par quel moyen physique ils pouvaient tous communiquer ensemble. Nous avons également survolé leur limite et leur problème de sécurité potentiel. Voyons maintenant comment tout cela fonctionne.

Les "Langages" (les Protocoles de communication)

On parle ici de la frontière entre le matériel et le logiciel. On cherche à comprendre comment la communication entre les différents appareils se font en internes.

Le protocole domotique est un langage de communication qui permet aux appareils connectés d'échanger des informations ou des données entre eux. Il permet l'interopérabilité entre les différents types d'appareils connectés au sein du système de domotique.

Protocole ouvert ou fermé

Les protocoles peuvent être ouvert ou ferme.

- *Un protocole ouvert* est basé sur des spécifications publiques et partagés. Ils sont accessibles à tous les fabricants ou développeurs. Les spécifications techniques sont documentées et utilisables par différentes entreprises pour créer des dispositifs qui seront compatibles.

- Alors qu'un *protocole fermé ou propriétaire* est exclusivement gérer et développer par une entreprise ou un fabricant. Les informations techniques ne sont pas publiques, cela limite les accès à ce protocole et implique donc que seuls les appareils produits par la même entreprise ou les partenaires peuvent les utiliser.

Le choix du type de protocole dépend des besoins, en termes de simplicité ou optimisation, mais aussi de flexibilité ou de choix de matériels.

La Portée du protocole

Il faut aussi prendre en compte la portée du protocole qui correspond à la distance maximale de communication d'un appareil avec un autre.

- *Les protocoles à courte portée* sont utilisables pour des communications à faible distance. Ils sont utilisés pour relier des appareils dans une même pièce ou dans un environnement avec peu d'obstacles.

- *Les protocoles à longues portées* sont utilisés pour faire communiquer des appareils à longue distance comme pour des applications extérieures ou des lieux vastes comme des bâtiments commerciaux ou de vaste propriété.

Protocole bidirectionnel ou unidirectionnel

Un protocole peut aussi être soit bidirectionnel soit unidirectionnel.

Dans le cas d'un protocole de communication unidirectionnelle, les données circulent dans une seule direction. C'est-à-dire, d'un émetteur vers un récepteur. Un appareil envoie une information, mais ne recevra pas de retour. Alors qu'un protocole dit bidirectionnelle permet une transmission dans les deux sens. L'émetteur envoie une commande ou information à

l'appareil et le récepteur envoi une confirmation ou des informations sur l'état de l'appareil. L'idée est d'avoir un accusé de réception de ce qu'a reçu l'appareil dans le système domotique.

Les Catégories de Protocoles

On distingue deux grandes catégories de protocoles domotiques :

- *Les protocoles radios* qui ne nécessitent pas de câblage physique entre les appareils. Ils fonctionnent comme le Bluetooth, par émission d'ondes électromagnétiques. Cela permet de faire évoluer l'installation à la demande, sans limite et sans effectuer de travaux. L'objectif est de rendre accessibles à tout le monde ce type de langages.
- *Les protocoles filaires* nécessitent de câbler les équipements connectés entre eux afin qu'ils puissent dialoguer. Ils sont idéalement installés pendant la phase de construction d'un logement en étant directement intégrés dans les plans. Cela offre une installation domotique plus durable et robuste, mais n'offre pas la même flexibilité que les protocoles radios.

Les standards actuels

De nos jours, on ne sait quel protocole serait le plus approprié. Pourtant certains standards se sont imposés. Ils ont chacun leurs forces et leurs faiblesses.

Le Wi-FI

Le Wi-Fi est un protocole de communication qui semble naturellement être la solution idéale, car nous avons déjà un réseau en place. Il permet d'avoir une gestion centralisée des différents éléments étant branchés dans l'environnement. Cela nécessite peu de travaux et permet d'avoir une évolution constante, car on peut ajouter ou retirer des appareils comme on le souhaite, et cela, sans avoir à modifier les câblages existants.

Pour que cela soit mis en place, il faut une box domotique qui constituera le cœur du système. Les capteurs collecteront des données et les transmettront à la box. Les actionneurs recevront les commandes pour actionner les différents appareils et l'interface permettra à l'utilisateur de piloter à distance, et même de mettre en place des réglages programmer ou de vérifier les différents états des appareils.

Ce fonctionnement permet de centraliser les échanges et de faciliter la gestion. Elle peut être évolutive avec l'ajout des nouveaux appareils. Les avantages du Wi-Fi sont la simplicité de la mise en place, la gestion centralisée par la box et une application ainsi que les possibilités d'évolution avec des modules compatibles.

Les limites sont la dépendance au réseau internet et à la qualité du signal qui peut créer des dysfonctionnements s'il y a saturation du réseau. La sécurité des données est aussi à mettre en

avant, car, de nos jours, il est indispensable de protéger l'accès à la box en utilisant des mots de passe robustes et de maintenir les équipements à jours. Il y a des risques de piratages.

L'autre point faible est la consommation d'énergie qui peut être excessives, car tous les équipements doivent être alimenté constamment. Le système est donc énergivore.

Le Bluetooth

Le Bluetooth est un outil puissant dans la domotique, car il englobe un ensemble de technologie et souvent utiliser en complément des autres protocoles de communication.

Un récepteur Bluetooth est un dispositif électronique qui permet de recevoir et d'interpréter les signaux Bluetooth émis par des appareils. Le rôle principal est de capter les données transmises et par la suite de les convertir en informations et de les transmettre de nouveaux au système central.

Il existe différents types de récepteur qui sont utilisables selon les besoins et le système central mis en place (Dongles, Modules Bluetooth intégrés aux Hubs domotiques, Passerelles Bluetooth dédiées).

Il y a aussi des protocoles divers :

- Le Bluetooth Classic est de moins en moins utilisé, car il demande une consommation énergétique élevée et la complexité du protocole le rend moins adapté aux besoins de la domotique.
- Le Bluetooth Low Energy est le protocole qui est le plus utilisé pour la domotique. Les avantages liés à ce protocole sont la faible consommation d'énergie, la communication rapide et fiable.
- Le Bluetooth Mesh est un moyen de créer des réseaux maillés de dispositif Bluetooth ce qui offre une couverture étendue et fiable. Les dispositifs servent de relais en amplifiant le signal et éliminant les zones-mortes

La mise en place de profils Bluetooth est aussi à prendre en compte, car ils définissent le type de communication qu'auront les appareils entre eux. Il y a différents profils :

- Le Health Device Profile : ce profil est utilisé pour des appareils de santé. Il permet de transmettre des données médicales.
- Le Generic Attribute Profile (GATT) est un profil qui est utilisé pour la communication entre les appareils BLE et le contrôleur associé. Cela permet d'échanger des données avec une grande flexibilité et une large compatibilité. Le GATT est grandement utilisé par les capteurs domotiques.

Les avantages sont une faible consommation avec le BLE, mais énergivore, car les équipements doivent être sous tension. Et il est intégré à de nombreux appareils.

Les inconvénients sont qu'il a une portée limitée, il nécessite des installations en amont comme un Hub domotique, la compatibilité du Hub avec le Bluetooth et l'installation des logiciel et des dépendances nécessaires comme des drivers.

Z-Wave

Z-Wave est un protocole de communication sans fil, il est de faible puissance et moyenne portée. Sa fréquence est de 868,4 MHz en Europe et 908 MHz aux Etats-Unis et il permet d'échanger de façon fiable et sécurisée. Il utilise une communication bidirectionnelle fiable. La fréquence utilisée par le Z-Wave lui permet de traverser plus efficacement les obstacles physiques et réduit ainsi les zones mortes tout en améliorant la couverture globale du réseau.

L'architecture réseau maillé est le cœur du fonctionnement Z-Wave, car chacun des appareils alimentés sur secteur devient un relais de communication vers les autres. Cela permet d'éliminer des points de défaillance, par exemple si l'un des appareils devient indisponible. Automatiquement, le réseau se configurera de nouveau pour trouver un chemin de communication alternatif. On peut y voir une garantie de la continuité de service.

Il peut accueillir plus de 200 équipements (232 appareils gérés) par un contrôleur ce qui est suffisant dans le cadre de la domotique. Cependant, la technologie Long Range s'étend, elle a plus de 4 000 nœuds dans le réseau. Les appareils qui sont sur batterie fonctionneront en mode économie d'énergie, ils seront éveillés que lorsqu'ils devront transmettre des informations aux autres appareils.

La communication Bidirectionnelle assure la fiabilité des commandes transmises. En cas de non-réception, le contrôleur renverra la demande via un chemin alternatif. L'accusé de réception permet d'avoir des informations sur les états des différents appareils en temps réel.

Pour ce qui est de la sécurité, le Framework S2 élève le niveau de protection en utilisant le chiffrement des communications est en AES-128 que ce soit pour les commandes ou les données. Le chiffrement est unique pour chaque réseau et il est généré dynamiquement lorsque l'on intègre un appareil. Une certification Z-Wave Alliance est une certification qui garantit que tous les appareils Z-Wave fonctionneront ensemble et indépendamment du fabricant. Si le Logo de certification Z-Wave est présent, cela met en avant la compatibilité du produit avec le système mis en place.

Les avantages de Z-Wave sont la fréquence qui permet de garantir une communication stable sur des environnements qui seront saturés d'appareils sans fil, la certification obligatoire qui garantit l'interopérabilité, la portée par nœuds qui réduit le nombre de répéteurs.

Les inconvénients sont :

- Le coût, car les fabricants devront payer une licence et soumettre leurs produits en tests pour obtenir la certification Z-Wave. Le prix d'un module Z-wave sera plus chère qu'un module Wi-Fi par exemple. Cela vient du fait que le protocole soit un protocole propriétaire.
- Le débit de données sera faible ce qui empêche l'envoi de données ou de flux gourmands.
- Le zonage fréquentiel, si vous êtes en Europe, il faudra une fréquence de 868 Mhz alors que pour les Etats-Unis, on sera sur une fréquence de 908 MHz, il faut donc vérifier à prendre un module européen si le système est en Europe.

Zigbee

Il s'agit d'un protocole à courte portée permettant la communication d'équipements ayant de petits émetteurs radios. Il désigne une technologie pour la communication sans fil de type WPAN (Wireless Personal Area Network). On l'appelle aussi IEEE 802.15.4

C'est une technologie à part qui vient compléter les appareils de communications standards comme le WLAN ou Wi-Fi. Cette technologie est adaptée pour être directement intégrée sur des appareils électroniques, car elle consomme peu et a un bas prix. Elle est fonctionnelle à une fréquence de 2,4 GHz ce qui permet d'obtenir des débits intéressants (250 kb/s) avec une portée maximale de 100 m.

Un réseau Zigbee se démarque par les différentes configurations topologiques qu'elle peut prendre. Elle peut être en étoile avec un coordinateur qui se charge de l'ensemble des routages, les autres nœuds servent de terminaux. Le point négatif est que le bon fonctionnement ne dépend que d'un seul nœud.

La topologie maillée (Mesh) et arbre fonctionnent avec un coordinateur, mais différents routeurs ce qui permet une redondance en cas de défaillance sur le routeur qui servait de route principale sur le traitement de la commande allant du coordinateur vers le terminal ou plutôt de l'émetteur de la commande vers le récepteur.

La force du protocole vient aussi des éléments de sécurité :

- La mise en place d'un compteur de trame. Cela sert à éviter les attaques par rejeu qui consiste à capturer une trame valide pour l'envoyer plus tard. Si le compteur est inférieur ou égale, le message est rejeté, mais s'il est supérieur, alors le message est accepté et le récepteur mets à jour la table de suivi des compteurs des appareils environnent.
- Le centre de confiance centralisé est un nœud du réseau Zigbee qui sert à centraliser la gestion de la sécurité du réseau. Il sert à authentifier les nouveaux appareils sur le réseau ainsi que l'accès ou non à ce même réseau. Il distribue aussi les clés de sécurités.
- Liste d'accès contrôlé : c'est une liste qui permet au centre de confiance de mettre en place des règles d'accès au réseau Zigbee pour les nouveaux arrivants. Cela peut être utilisé pour identifier les appareils autorisés ou bien une Black list des appareils.
- Une clé de chiffrement sur AES-128 bits est commune à tous les appareils du réseau et elle est transmise lorsque qu'un appareil est intégré. Elle sert à chiffrer les informations réseau dans les messages envoyés.

Avec le temps, Zigbee permet la décentralisation de la sécurité du réseau (Zigbee3.0). Lors de l'ajout d'un appareil sur le réseau, les routeurs ont la charge d'authentifier les nouveaux et de distribuer les clés de sécurité et il n'y a donc plus de nœud central.

Les avantages sont une faible consommation d'énergie, la capacité autoréparante de son réseau, son interopérabilité et donc la flexibilité du produit qui peut être utilisé avec des appareils divers. Il a une longue portée et peut avoir sur son réseau à grand nombre d'appareils (65 000).

Dans la version Zigbee 4.0, il y a trois axes majeurs qui ressortent :

- Une meilleure sécurité : la mise en place des Dynamic Link Key, cela permet de mieux contrôler qui entre, comment et avec quel niveau de confiance sur le réseau.
- L'amélioration de la résilience du réseau permet une synchronisation des compteurs de trames pour limiter les attaques de rejeu.
- Permettre le changement du contrôleur principal d'un réseau sans devoir tout reconfigurer.
- Un appairage simplifié par le biais du BLE
- Ouverture des fréquences sub-GHz : il s'agit de proposer la prise en charge des fréquences que Z-Wave propose déjà, cela permettrait de gagner en portée, mais aussi d'une meilleure couverture et de diminuer les zones mortes.

L'idée est de conserver ce qui fait de Zigbee un protocole très fiable et flexible tout en améliorant les points faibles ou limitants comme la portée, la fiabilité dans des environnements surcharger sur la fréquence en 2,4 Ghz et améliorer le déploiement à grande échelle quand on voit le nombre d'appareils que peut avoir le réseau Zigbee.

Les nouveaux standards unificateurs

L'un des points faibles de Zigbee et Z-Wave est l'utilisation d'un hub ou d'une box domotique. Cela peut être complexe à mettre en œuvre, car avec ces protocoles, plusieurs hubs différents peuvent être nécessaires pour que les appareils puissent communiquer entre eux. Cette complexité peut être une opportunité d'amélioration pour unifier tout le système et simplifier la mise en place.

Pour cela, la solution Matter existe. Il fonctionne autant en utilisant le Wi-Fi, le BLE et le protocole domotique Zigbee ou Z-Wave. Tous associé à la technologie de communication Thread.

Nous allons voir par la suite, le fonctionnement de Matter en tant qu'unificateur et Thread, le protocole domotique.

Matter, l'unificateur

Matter est une norme ouverte qui cherche à mettre en commun toutes les marques et à proposer un nouveau standard. L'idée est de simplifier l'expérience utilisateur grâce à ce logiciel. Les grands noms de la domotique comme Apple Homekit, Google Home, Samsung SmartThings et Amazon Alexa ont déjà adhéré à cette nouvelle norme.

Matter est une plateforme qui comporte les spécifications techniques des nouveaux appareils ce qui facilite l'interopérabilité. L'idée est de brancher et de faire marcher directement l'appareil tout en étant sécurisé. Matter est conçu pour fonctionner en local avec Ethernet et avec deux réseaux sans fil en complément le Wi-Fi et le Thread. L'utilisateur final contrôle la gestion des appareils et de la communication entre eux.

Les équipements certifié Matter peuvent s'intégrer à n'importe quel écosystème grâce à un seul protocole.

La nouvelle norme de la domotique provient de la Connectivity Standards Alliance qui est une organisation regroupant les entreprises qui produisent et créer des produits pour la domotique.

Matter se veut être une source ouverte et transparente pour le public qui peut consulter les informations à disposition dans un dépôt GitHub. A partir de cela, l'idée est de faire en sorte que les utilisateurs bénéficient au plus vite des améliorations et d'avoir un visuel continue sur l'évolution du logiciel.

Thread, le protocole IPV6

Thread est un protocole réseau basé sur l'IPV6, utilisé pour les appareils connectés à basse consommation dans un réseau maillé sans fil. Il est conforme à la norme IEE 802.15.4-2006, il est appelé aussi réseau personnel sans fil ou WPAN. Ce protocole est indépendant des autres protocoles vus précédemment.

Le protocole Thread a des caractéristiques intéressantes pour répondre aux attentes des utilisateurs de Matter.

Il est simple en ce qui concerne l'installation, la mise en service et le fonctionnement. Il est sécurisé et fiable, car les appareils dans ce réseau auto réparer, seront authentifiés et les communications seront chiffrés. Son efficacité se tient par l'utilisation d'appareils basses consommation sur batterie qui leur permet une longévité plus conséquente.

Avec ce protocole, l'objectif est de permettre une évolution du système en intégrant des appareils qui sont certifiés par le groupe Connectivity Standards Alliance.

L'objectif est d'unifier et de simplifier l'utilisation de la domotique pour tout type d'utilisateur en utilisant un protocole unique et un unificateur unique qui permettrons ensemble un système domotique fiable, sécurisée, évolutive et qui permet d'avoir une économie d'énergie autant sur le court ou long terme. De plus, le groupe ayant mis en place ces deux nouveaux standards offre la possibilité aux personnes extérieures de les aider à améliorer de façon continue ce système en répondant à leurs besoins.

Le système Nerveux (le Software et les OS)

Dans la domotique, les logiciels et OS sont perçus comme le système nerveux d'un organisme. Il s'agit de transformer une intelligence brute en automatisation qui est cohérente.

On attend de cette partie la collection de données, la mise en place des règles et l'exécution des commandes.

Comme pour les appareils ou protocoles de communication, une multitude de possibilités existent avec chacun des fonctionnements propres.

Comparaison des OS Domotiques

Home Assistant

Le Home assistant est une plateforme open source qui permet de commander les appareils connectés et intégrer au même système. Le système est flexible et permet de faire en sorte que différents appareils puissent cohabiter. Le point fort de ce système est qu'il fonctionne sans cloud, ce qui garantit une confidentialité et une sécurité accrue pour les utilisateurs.

Home Assistant utilise une architecture modulaire, c'est-à-dire que le système travail soit avec les appareils de façon indépendante ou selon des scénarios prédéfinis comme l'extinction des lumières la nuit à une certaine heure et lancer la vérification de la fermeture des portes.

Il y a aussi la vérification de l'état des appareils à l'instant T et ainsi de mettre en avant les potentiels dysfonctionnements.

L'objectif est d'assurer un automatisme complet selon les besoins de l'utilisateur tout en lui offrant une expérience simple et confortable d'utilisation quotidienne.

Les avantages sont la fluidité, la réactivité et permettent d'avoir une meilleure gestion énergétique. La gestion se fait via une interface web qui permet de gérer les appareils.

Le projet étant en open source, cela offre des possibilités d'amélioration continue grâce à son dépôt Git, mais aussi l'incitation aux personnes d'améliorer leur propre environnement.

Les autres avantages sont que Home Assistant peut être mis sous la forme d'un container Docker ou être intégré à un environnement virtuel Python.

Dans le cas général, Home Assistant est intégré à un Rasperry PI ou à un ordinateur mono carte, une mémoire d'environ 32 Go, un chargeur capable de fournir 2,5 A et si besoin un câble Ethernet. Il existe une image disponible et utilisable qui propose l'installation du logiciel et du système d'exploitation.

Dans les années à venir, Home assistant souhaite intégrer de nouveaux appareils comme les lunettes intelligentes ou les assistant vocaux. Il est aussi intégré dans d'autres plateformes domotiques. Il y a aussi l'intégration de l'IA avec les appareils cité avant.

Jeedom

Ce logiciel est le concurrent principal de Home Assistant. Il est aussi Open source et s'installe sur tout type de plateforme linux. Il repose sur une architecture PHP. Son point fort vient de sa large proposition de plugin. Il est utilisé localement tout comme Home Assistant.

Contrairement à Home Assistant, Jeedom fonctionne sur un principe de fonction spécifique. Il est créé par deux Français et la communauté accumulée avec le temps propose de nombreux tutoriels. Son objectif est de piloter des modules de différentes technologies tout en suivant les normes comme Z-Wave.

Il y a 4 modes d'installation, chacun adapter à l'utilisateur. Cela peut être une image prête ou un script Debian, une machine virtuel Linux ou bien une box officielle. Cela dépendra du budget de la personne. Il faudra aussi prendre en compte un prix sur certains services ou plugins.

Les avantages sont la compatibilité avec les différents protocoles et la gestion peut être faite par une interface unique et locale ou par l'application. Il peut être intégré à différents matériels allant de la box Jeedom déjà prête, en passant par un mini Pc ou bien l'utilisation d'un Rasperry PI.

La différence entre Jeedom et Home Assistant se fait sur la philosophie du système. Home Assistant cherche à donner un contrôle total à l'utilisateur via une interface alors que Jeedom offrira cela avec la mise en place de plugin.

Domoticz et OpenHAB

Domoticz est un logiciel open source gratuit, il est utilisable sur différentes plateformes. Il permet de contrôler les appareils via les protocoles vue auparavant. Il utilise un langage C++. Il est considéré comme léger et consomme très peu de ressource. Un dépôt Git est disponible pour les utilisateurs que ce soit pour l'aide à l'installation ou des questions diverses.

OpenHab est un système domotique open source qui offre une large possibilité de fonctionnalité pour contrôler et automatiser les appareils et prend aussi en charge des protocoles variés. Ce système utilise un fonctionnement modulaire et la personnalisation. Il est utilisé par des personnes ayant déjà une expérience avancée de la domotique et qui souhaites passer du temps à personnaliser les configurations des appareils. Il utilise un langage Java.

Les utilisateurs peuvent aller sur le site officiel pour avoir accès à de nombreuses informations que ce soit pour les débutants ou les personnes expertes. Allant de la simple installation aux actualités.

Le protocole MQTT

Le protocole Message Queuing Telemetry Transport (MQTT) est un protocole de messagerie qui permet à des appareils de communiquer entre eux de façon asynchrone avec de faibles bandes passantes.

Il est composé de trois parties. La structure du protocole est composée du Broker qui est le serveur distant. Tous les objets et les services se connectent à lui en tant que client. Il sert à transmettre les messages entre les différents clients.

Le logiciel Mosquitto agit comme un centre de tri des messages publiés et à transmettre aux différents souscripteurs.

Ces clients peuvent envoyer les messages en tant que publicateurs ou recevoir des messages en tant que souscripteur. Les messages qui sont publiés sont appelés topic.

Dans le MQTT, les clients peuvent s'identifier via un id client. L'avantage, c'est que si l'id est vide le broker en crée un aléatoirement.

Les topics servent à transmettre des messages aux personnes abonnés aux différents sujets. Les souscripteurs recevront donc des copies publiées avec les sujets correspondants aux topics. Le client peut aussi demander au broker de conserver le message, on appelle cela le retained message. Ainsi, les futurs abonnements peuvent correspondre au sujet et le nouveau message sera conservé à la place de l'ancien.

Gestion des données et Archivages

Les données dans la domotique fonctionnent selon un cycle de vie. Ce cycle fonctionne selon quatre étapes.

Il y a tout d'abord l'acquisition des données par les capteurs de notre système de domotique. Elles vont être des données brutes comme des valeurs analogique ou des états binaire. Le fait que l'appareil soit allumé par exemple.

Par la suite, les données passeront par la phase de traitement. La box domotique traite l'information localement pour déclencher une action ou une commande.

Il y a le stockage temporaire qui correspond à l'utilisation de la base de données acquises pour faire du monitoring en temps réel. Ceci permet d'avoir des informations à l'instant T et de proposer des tableaux de bord sur les états de chaque appareil.

Pour finir, l'archivage, les données vont être compresser et déplacer vers un stockage qui servira pour l'analyse historique.

Pour la partie donnée, les DIY utilisent principalement SQLite qui est un système de gestion de base de données qui exécute les commandes SQL. SQLite consomme très peu de ressources, il ne nécessite pas de configuration et dispose d'une portabilité et il est très fiable. Son rôle au sein du système est d'être la mémoire sur un court ou moyen terme.

Dans le cas de Home Assistant, L'utilisation de SQLAlchemy permet d'utiliser différents types de solutions de base de données comme SQLite ou MySQL

Pour cela, il y a différents types de stockage :

- La sauvegarde locale qui peut être faite à l'aider d'un appareil de stockage pouvant être par exemple un disque dur qui est certes peu coûteux, mais représente des risques de perte. On peut donc penser à mettre en place un NAS qui reste une sauvegarde locale et qui peut être utilisé pour la sécurité des données. Il permet une redondance en cas de défaillance des disques. Par l'utilisation d'un NAS pour la sauvegarde, on minimise au mieux les risques de corruption ou de perte de données. L'autre avantage est de permettre de proposer des services au sein de note système domotique comme être un serveur multimédia ou bien un lieu de stockage pour les documents sensibles ou privés.
- La sauvegarde Cloud est une alternative qui permet de soulager notre système domotique qui peut être surchargé par les nombreux appareils. Le point fort de ce type de sauvegarde est son externalisation que ce soit pour les ressources ou les données. Cela offre une solution sécurisée et fiable en évitant une mise en place complexe ou

coûteuse. Dans le cas de Home Assistant, en plus d'un espace de stockage, il y a des services comme la gestion de la synthèse vocale ou une configuration de Google Home ou Alexa simplifier. Cela offre aussi un service d'accès externe sécurisé au système domotique mis en place.

L'IA Locale

L'IA prenant de plus en plus de place dans notre monde, la domotique peut y voir aussi des avantages et ainsi évoluer en incorporant l'IA. L'IA sert à traiter localement les données plus rapidement et d'améliorer l'expérience de l'utilisateur. L'idée est d'être indépendant du Cloud pour les actions répétitives ou de couramment utiliser.

Un exemple d'évolution avec l'IA est le SwitchBot AI Hub. Il permet d'offrir bien plus qu'un contrôle sur les appareils, mais une polyvalence centralisée de notre système domotique. Par la collaboration avec OpenClaw, les utilisateurs peuvent contrôler les différents appareils appartenant au système. L'un des autres avantages provient du fait que les notifications ne seront pas juste gérées, mais filtrer, interpréter et permettra de fournir des messages plus personnalisés à l'utilisateur.

Le Switchbot est compatible avec un certain nombre d'appareils et de protocoles de communication. Les objectifs sont d'offrir une nouvelle expérience à l'utilisateur en donnant des instructions avec un langage humain et avoir en résultat des processus automatisés qui peuvent paraître répétitif ou avoir des informations personnalisées selon des scénarios. La dimension locale permet d'assurer une confidentialité et que la rapidité d'exécution offre un confort adéquat.

Les différents incidents survenus au fil des années sur la domotique personnelle :

Dans cette section, nous allons donc exposer et discuter des divers incidents qui ont eu lieu au cours des années passées avec les objets domotiques connectés dans la maison. Afin de faire cela, nous avons effectué une veille afin de suivre les différents incidents survenus, mais nous avons aussi effectué diverses recherches pour recenser ces cas. Pour commencer, nous allons donc parler par ordre chronologique des incidents qui sont survenus.

Le premier incident dont on va parler est l'incident historique de 2014 La première cyberattaque qui a été documentée officiellement, ce fut une attaque qui a eu lieu entre le 23 décembre 2013 et le 6 janvier 2014 et qui a utilisé 100 000 appareils connectés différents. Pour cette attaque, tous ces appareils ont été transformés en un réseau de botnets (zombies) géants nommés « thingsbot ». A l'aide de ce réseau, il y a eu 750 000 spams qui ont été envoyés, cela ayant servi à des campagnes de pubs frauduleuses. Pour ce qui est des appareils utilisés, il y a eu de tout type d'appareils à partir du moment où ils possédaient une adresse IP, donc une connexion internet. On a donc eu des routeurs, des télévisions connectées, au moins 1 réfrigérateur et des appareils de la vie quotidienne en tout genre. Cette attaque a été découverte par le groupe Proofpoint qui sont des spécialistes de la sécurité

Le second incident que l'on va aborder sera au sujet du " botnet Mirai ", un logiciel malveillant qui a pour objectif de se servir de toutes les failles de sécurité que possèdent les appareils connectés que l'on peut trouver partout dans nos habitations. On appelle cela les " appareils IDO". IDO étant l'abréviation d'internet des objets, d'où le fait qu'on parlait des objets que l'on peut trouver dans nos habitations, mais l'on peut aussi trouver dedans les objets en rapport avec la santé et le bien-être tels que les implants de surveillance cardiaque, les capteurs de suivi du diabète que l'on abordera dans un incident prochain, et donc d'autres appareils de soins médicaux connectés en général. On y trouvera aussi la catégorie des industries et des villes intelligentes ce qu'on y trouvera dedans ce sera tous les différents capteurs environnementaux, pour la pluie et d'autres objets urbains connectés. Et on trouvera une dernière catégorie sur l'agriculture et le commerce, donc on y trouvera par exemple les capteurs agricoles qui aident à l'optimisation des rendements et à la gestion de l'eau sur les cultures, et ensuite on peut y trouver les appareils qui aident pour le suivi des chaînes d'approvisionnement. Maintenant que l'on a défini ce qu'est un appareil IDO, on va pouvoir revenir à notre incident. Donc le botnet Mirai qui a causé une grosse attaque en 2016, en effet le fonctionnement de ce logiciel est d'infecter tous les appareils intelligents dans le but de les transformer, comme dans le premier incident, en un réseau de bots zombies qui seront donc contrôlés à distance. Ils seront ainsi nommés botnet. Ce qui s'est produit en septembre 2016 fut donc une attaque DDoS à l'encontre du blog sur la sécurité de Brian Krebs. Ce fut une attaque record pour l'époque puisqu'elle a atteint près de 620Gb par seconde. Lors de l'attaque, il y avait aussi 380 000 IDO d'infectés

utilisés pour cette attaque DDoS. Ensuite, en fin septembre début octobre, une attaque contre OVH, le grand site d'hébergement français, qui a atteint une charge d'au moins 1.1Tb par seconde, ce qui brisa un nouveau record. Cette attaque ayant atteint un pic de près de 1.5Tb par seconde, ce qui est énorme et jamais atteint auparavant. Il y a eu aussi une attaque contre Dyn qui est un acteur majeur sur le marché pour la vente et l'hébergement de DNS. Cette attaque a atteint une charge de 1.2Tb par seconde, ce qui a causé la perte de l'accès à de nombreux sites dont Amazon, Twitter, Netflix ou bien même GitHub. Cette attaque a affecté de nombreuses personnes. Par la suite, les auteurs du botnet Mirai ont tenté de mettre le code source sur internet afin de réduire les risques de chances de se faire repérer et trouver, mais ils furent quand même trouvés. Ce qui a été découvert à leur sujet est qu'ils se nomment Paras Jha et Josiah White, âgés de 21 ans au moment des faits, ont cofondé l'entreprise Protraf Solutions : les services proposés par cette entreprise étaient, par exemple, de l'atténuation d'attaques DDoS à leur encontre. Ce fut l'une de leurs méthodes principales pour gagner de l'argent puisqu'ils vendaient leurs services à toutes les entreprises, même celles qui se faisaient attaquer par le botnet, cela leur permettant de donner plus de crédit à leur entreprise pour inciter à signer des contrats avec eux.

Le troisième incident que l'on va aborder sera au sujet d'une famille qui possède de nombreux objets connectés chez eux. Ils possèdent un thermostat connecté, des lumières connectées à l'entrée de la maison, une serrure connectée pour la porte, ainsi que des caméras pour surveiller chez eux. Cette famille étant très inquiète pour la sécurité de leur maison, ils ont fait appel à l'entreprise Marketplace qui a engagé des white hat, donc des hackeurs, qui ont pour but d'aider les gens avec leur piratage et maîtrise de l'informatique. Dans le but de vérifier l'intégrité des objets connectés et de leur maison pour ne pas être facilement attaquables ou piratables, malheureusement pour eux, il n'a suffi que de 3 personnes dans un van devant chez eux et d'un mail de phishing pour pouvoir déverrouiller la serrure de la porte d'entrée de la maison. En effet, les hackeurs ont pris moins de 2h pour cracker le wifi de la maison pour y avoir accès. Par la suite, ils se sont aperçus que le thermostat connecté avait le même mot de passe que le wifi, donc ils ont aussi pu en prendre le contrôle. Ils pouvaient alors le couper ou le pousser à haute puissance sans difficulté. Ce qu'ils ont fait en parallèle fut d'envoyer un faux mail à la mère de famille en se faisant passer pour l'application qu'elle utilise pour déverrouiller la serrure et activer les lumières. À l'aide du mail, ils l'ont donc redirigée vers le faux site de l'application Wink afin qu'elle y rentre ses identifiants de connexion. Lorsque cela fut fait, ils avaient alors accès à son compte et donc à la serrure de la porte d'entrée. Ils ont alors eu juste à se connecter et déverrouiller la porte, et alors ils pouvaient faire ce qu'ils voulaient dans la maison. Puisque le mot de passe pour Wink était aussi utilisé pour d'autres applications tels que celle des caméras, ils pouvaient alors voire tout ce qu'ils voulaient souhaitaient dans la maison, ou même couper les caméras, Cela ayant aussi permis aux hackeurs d'envoyer des messages vocaux à l'Amazon Echo du couple afin de faire des commandes Amazon avec la carte de crédit du mari. Heureusement pour le couple, ce furent des gens employés pour tester la sécurité de leur logement. Cela n'a donc entraîné aucune répercussion négative pour eux, mais ils ont donc pris conscience de la faiblesse de ce type d'objets s'ils sont mal sécurisés.

Le quatrième incident dont on va parler sera le cas d'une attaque qui a eu lieu en janvier 2019 sur la caméra de la maison d'une famille. Ce qu'il s'est produit fut qu'un hackeur a pris le contrôle de la caméra du domicile de la famille. Cette caméra fonctionnait de sorte à ce qu'on puisse entendre le son par la caméra et qu'on puisse aussi, à l'inverse, faire sortir du son par la caméra à travers le micro intégré. Le pirate a ainsi profité de cela pour faire sortir une alerte à la bombe nucléaire qui arrivait vers les États-Unis en provenance de la Corée du Nord. Cela ayant donc créé la panique chez la famille avec leur enfant en bas âge, ils ont pu par la suite se rendre compte qu'ils étaient les victimes d'une attaque par un pirate envers eux. L'entreprise Nest, responsable de la distribution et de la vente de ces caméras, a alors fait un communiqué afin que toutes les personnes possédant leurs caméras aillent activer la double authentification sur leurs caméras afin d'éviter ce type d'intrusion. Pour commettre cette attaque, les hackeurs se sont servis des identifiants qui avaient déjà fuité par le passé sur internet à travers d'autres failles. Google, étant l'entreprise possédant Nest, a donc communiqué qu'il n'y avait eu aucune intrusion dans la base de données. Cet incident se termina alors par un communiqué de Nest conseillant aux utilisateurs de changer le mot de passe de leurs comptes pour les caméras pour réduire encore plus les risques d'attaques.

Le cinquième incident dont on discutera sera de multiples petits incidents survenus en septembre 2019, en effet une famille possédant un appareil Nest qui leur servait, comme dans le cas précédent, à gérer la température des thermostats ainsi que les caméras. Ce qu'il s'est produit, c'est que la mère de famille, en rentrant chez elle, a trouvé le thermostat à 90°F. En pensant à un bug ou une erreur avec le thermostat, elle a eu comme réflexe de le réinitialiser, mais lorsque cela fut fait, une voix bizarre sortant de la caméra de la cuisine a commencé à lui parler, à elle et à son mari, tout en jouant une musique vulgaire très forte. Son réflexe fut alors de débrancher la caméra et de la tourner vers le plafond. Par la suite, elle appela son fournisseur internet afin de changer les identifiants de leur wifi puisqu'il suspectait un piratage de leur réseau ayant permis à l'attaquant de prendre le contrôle de leur appareil Nest. Plus tôt dans l'année, une autre famille possédant des caméras de la marque Nest a subi une attaque du style. En effet, d'un coup la caméra s'est mise à parler à leur fils de 7 mois. Il y eut alors des injures qui furent hurlé et la température du thermostat ayant lui aussi été montée jusqu'à 90°F. Après que les propriétaires ont eu débranché la caméra, ils ont contacté Nest qui leur a dit d'activer la double authentification sur leurs appareils pour se connecter afin d'ajouter plus de sécurité et éviter ce type d'attaque par le futur

Le sixième incident qui va être abordé sera au sujet de différentes petites attaques qui ont eu lieu en Amérique en novembre 2020. Nelson, l'un des conspirateurs des attaques, avec d'autres personnes, se sont amusés à pirater les comptes Yahoo de nombreux habitants du Wisconsin. A l'aide des identifiants et mots de passe qu'ils ont récupérés de ces comptes, ils ont ensuite déterminé qui furent les personnes qui possédaient des comptes Ring pour gérer les caméras de sécurité sur leurs sonnettes qui ont été vendues par l'entreprise Ring LLC . Lorsqu'ils sont parvenus à déterminer cela, dans un premier temps ce qu'ils ont fait fut d'identifier leurs victimes et de récupérer des informations supplémentaires sur leurs victimes. Quand ils avaient suffisamment d'informations sur leurs cibles, ils décidèrent ensuite d'appeler la police en

passant de faux appels d'urgence auprès de la police ou d'alerter la police sur des dangers urgents qui se produisaient au domicile de leurs victimes. Cela causait donc que les policiers se rendaient en urgence au domicile des victimes, c'est alors que les policiers se rendaient compte de l'arnaque et les attaquants en profitaient alors pour provoquer les policiers ainsi que les habitants de la maison à travers la caméra de la sonnette. Cela se produisit dans de nombreux incidents, ce n'était pas un cas isolé. Par la suite, ils ont refait un coup du même style. Ils ont récupéré les informations et les accès à la caméra des victimes, et alors ils appelèrent la police en se faisant pour l'enfant de la famille qui signalait que ses parents buvaient énormément et s'amusaient à tirer dans la maison à l'aide d'armes à feu. Dans la maison, il avait alors pu compter 7 tirs de balles et signalait que les parents étaient en possession de multiples armes à feu à leur domicile. La police se rendit alors d'urgence dans la maison en étant armée, et ils ont alors vidé le domicile de la famille en menaçant les habitants avec des armes. Et pour finir, lorsque la police est arrivée au domicile, Nelson a pris l'accès à la caméra de la sonnette afin de menacer et de provoquer les policiers venus sur place pour gérer l'incident. Dans un autre cas du style, Nelson récupéra à nouveau l'accès à la caméra du domicile d'habitants en passant par leurs comptes Yahoo. À ce moment-là, ils ont appelé la police avec un faux appel, encore une fois, afin de prétendre qu'il était dans le domicile des habitants. Un dernier incident qui fut avoué auprès du tribunal par le comparse de Nelson fut un appel auprès de la police après avoir piraté la caméra du domicile d'un couple afin de se faire passer pour le mari de la femme et qu'il viendrait de la tuer, qu'il détenait un otage et qu'il avait mis en place de nombreux explosifs dans la maison. Ce qu'il faisait ensuite était de faire une diffusion en direct sur les réseaux sociaux de l'intervention de la police avant de poster sur les réseaux qu'il était le responsable de cet incident de swatting et qu'il a trouvé ça amusant.

Le septième incident dont on va parler sera au sujet des caméras de sécurité Xiaomi qui permettaient de recevoir des images vidéo du domicile de voisins ou d'autres personnes possédant ces caméras. Ce qu'il s'est produit est que, comme les caméras avaient accès aux Google Nest du domicile et au Google Assistant lorsque des personnes tentaient d'afficher le retour de la caméra sur leur Google Nest, des images provenant d'autres domiciles ressortaient. Certaines images de personnes en train de dormir ou même d'un bébé qui dort ont pu être affichées, cela posant un vrai problème de sécurité et de confidentialité pour les usagers. Cela causa à Google de très vite réagir vis-à-vis de cet incident et ils ont fait en sorte de désactiver la possibilité de lier les caméras Xiaomi au Google Nest et leurs autres appareils. Cela fut réglé par la suite par le fournisseur Xiaomi, expliquant que c'était un cas qui apparaissait dans de rares conditions lorsque l'on tentait de lier la caméra à un écran lié au Google Nest. Avec une mauvaise connexion, cela pouvait causer cet incident. Après une correction, le problème fut alors réglé.

Le huitième incident que l'on va traiter sera au sujet de la faiblesse des firmwares (micrologiciels) des IDO. Un chercheur chez Avast a souhaité vérifier sa théorie comme quoi les firmwares sont les nouvelles faiblesses des appareils connectés. Il pensait qu'un routeur peu sécurisé ou une exposition sur internet n'étaient pas les seules menaces auxquelles les IDO vont devoir faire face. Ainsi, il a réussi à contaminer une machine à café en passant par le signal

local du wifi de celle-ci. Lorsqu'ils ont pu infecter le firmware, ils ont ensuite pu faire en sorte que la machine à café bipe en boucle et par la suite ils y ont mis un ransomware afin de bloquer l'accès au propriétaire. Cela permettant ainsi de démontrer sa théorie que les firmwares peuvent aussi être une menace pour la sécurité des objets connectés.

Le neuvième incident dont on va parler sera au sujet de capteurs de diabète ayant dysfonctionné. En effet, ce qu'il s'est produit est que les capteurs FreeStyle Libre 3 et FreeStyle Libre 3 Plus, 2 types d'appareils que l'entreprise pharmaceutique Abbott vendait, ont fait l'affaire de rappel le 3 novembre 2025. La raison de ce rappel fut que les capteurs fournissaient des mesures mauvaises avec des taux de glycémie plus bas que ce qu'il y avait réellement. Au jour du rappel, il y a eu plus de signalements avec rien qu'aux États-Unis un rappel d'environ 3 millions de capteurs défectueux. Ces capteurs défectueux ont donc causé 736 incidents graves pour les personnes ainsi que 7 décès à la suite des dysfonctionnements. L'entreprise s'est exprimée à ce sujet, indiquant que ce problème provenait d'une seule ligne de production défectueuse. Cela indique donc un risque assez important vis-à-vis des usagers de ce type de produit, puisque leurs vies en dépendent en grande partie. Lorsque des dysfonctionnements de ce type surviennent, cela cause de gros problèmes et débat.

Pour ce qui est du dixième incident que l'on va analyser, ce sera au sujet de toilettes connectées. En effet, la société Kohler a mis en vente sur le marché une nouvelle caméra qu'il faut fixer au bord de la cuvette dans le but d'analyser les différentes images captées dans la cuvette pour faire un retour à l'utilisateur sur le bien-être digestif, s'il s'hydrate suffisamment ou s'il y a des anomalies présentes dans les déjections des utilisateurs. Ces informations sont censées ensuite être transmises vers l'application, qui est accessible seulement lorsqu'un abonnement est payé mensuellement pour y accéder. Le problème de cet incident survient dans le discours de l'entreprise, en effet l'entreprise a assuré que les données seraient chiffrées de bout en bout et que du coup seul l'utilisateur et le serveur ne pourraient accéder à ces données, Mais un expert en cybersécurité a permis de démontrer que ces données sont certes bien chiffrées, mais que les données sont totalement déchiffrables par le système de l'entreprise. Cela causant que l'entreprise peut se servir de ces données pour entraîner leur intelligence artificielle, malgré le fait que l'entreprise ait certifié que les données sont anonymisées et qu'il est possible de refuser l'utilisation de ces données. Cela engendre donc des discussions sur l'utilisation d'objets connectés chez nous et la sécurité de nos données.

Le onzième incident que l’on va traiter est sur un incident survenu en janvier 2026. Cet incident parle d’appareils connectés où l’accès à distance et la gestion depuis l’application n’était plus possible des suites d’une panne des serveurs. Ce qu’il s’est donc produit le 3 janvier 2026 fut donc une panne des serveurs de Netatmo, cela a donc causé que les appareils n’étaient plus contrôlables à distance heureusement pour les usagers les appareils pouvaient toujours être gérer manuellement, ce qui réduit la gêne pour les usagers, mais ce n’était pas le premier incident qui survenait sur les serveurs de Netatmo en effet précédemment le 27 septembre, le 29 octobre et le 5 novembre 2025 les serveurs eurent des pannes similaires malgré que la situation se soit rétablie au bout de quelques heures cela reste une grande gêne pour les

personnes surtout dans une période de froid tel que Janvier ne pas pouvoir gérer son thermostat si l'on est au travail par exemple peut causer des dépenses inutiles pour les gens. Cela va donc poser de nombreuses questions et ressortir le débat au sujet de la dépendance aux objets connectés chez nous.

Le douzième incident qui sera abordé sera au sujet d'un aspirateur robot de l'entreprise DJI. Comme on le sait, le robot aspirateur, pour fonctionner, va donc cartographier le domicile, le lieu et stocker tout cela dans une base de données. Ce qu'il s'est passé par la suite est qu'un jeune homme souhaitait contrôler son robot DJI Romo à l'aide d'une manette de PS5. Jusqu'ici, rien de problématique, le robot était bien protégé avec l'application officielle. Il dut alors développer sa propre application pour tenter de contrôler le robot avec sa manette, mais une fois qu'il est parvenu à se connecter aux serveurs de DJI, il se rendit compte que l'accès qu'il avait obtenu n'était pas seulement sur son robot mais sur des milliers d'autres robot. Il avait donc accès à la cartographie du domicile des autres robots, des informations sur l'état du robot, ainsi que des flux caméra et audio. En fonction des cas, cela était donc très problématique, puisque cela voulait dire que n'importe qui aurait pu faire en sorte d'accéder à ces informations s'ils avaient fouillé un petit peu comme ce jeune homme. L'entreprise a alors reconnu qu'il y avait un problème en termes de permission côté serveur et non un manque de chiffrement des données, ils ont alors publié une mise à jour corrective pour régler ce problème au plus vite afin d'empêcher qu'un cas similaire ne se produise. Cela va donc poser des questions sur le danger et la sécurité de nos données. Si des failles sur ce type de robot venaient à être trouvées par des pirates, n'importe qui pourrait obtenir de nombreuses informations sur le domicile d'usagers, cela créant une grande menace.

Pour ce qui est du treizième incident que l'on va traiter, il parlera de la découverte de failles majeures dans les nouveaux dispositifs de sécurité dans les produits domotiques de Shelly, cela exposant des millions de foyers d'européens à des attaques envers leurs systèmes censés les protéger. Ce qu'il s'est produit le 11 février 2026, c'est que des chercheurs en cybersécurité ont affirmé avoir découvert une faille majeure dans les produits de l'entreprise Shelly. Ces produits étant actuellement utilisés dans plus de 5.2 millions de foyers dans toute l'Europe, cela est une menace certaine pour les gens. Ce qui a été découvert est un défaut de conception qui crée donc une porte dérobée dans le système de sécurité, en effet les appareils Shelly Gen 4 maintiennent un point d'accès sans fil ouvert en permanence. De base, il est fait pour la configuration initiale, mais même après qu'il a été configuré, le réseau reste encore fonctionnel. Cela cause que n'importe qui peut se connecter à ce réseau et peut avoir accès à la porte d'entrée, du garage et même à n'importe quels appareils connectés dans le foyer, qu'ils soient de la marque Shelly ou non. Ce qui fait qu'il suffit qu'un seul appareil soit compromis, et on peut accéder à absolument tout le réseau et les appareils connectés du domicile. Au moment où l'article et le signalement ont été envoyés auprès du fournisseur du logiciel, il n'y avait eu aucun patch de sécurité de sorti et les utilisateurs devaient donc eux-mêmes désactiver ce réseau sur leurs appareils pour éviter des risques de sécurité.

Le quatorzième incident dont on va discuter est un incident survenu en octobre 2025 cela faisant suite à la panne des serveurs de Amazon les serveurs AWS (Amazon Web Services) ces serveurs servant ainsi d'hébergement pour de nombres sites et logiciels. Pour en revenir à notre cas ce qu'il s'est produit est que des milliers utilisateurs possédant des lits connectés de la marque Eight Sleep ont subis de nombreux problèmes de par la panne de ces serveurs, étant donné que les serveurs sont tombés en panne de nombreux lits se sont mis à dysfonctionner puisque les serveurs ne répondaient plus. Résultat des choses des matelas se retrouvant bloqués d'autres matelas ayant des housses chauffantes connectées se sont mises à chauffer à pleine puissance faisant que cela devenait impossible de dormir dessus. Cette panne sur les serveurs AWS n'a pas seulement impacté les lits Eight Sleep mais aussi de nombreuses autres applications dépendant de ces serveurs. Par la suite le PDG de la marque a annoncé qu'un patch avait été déployé sur leurs appareils faisant en sorte que les lits possédaient désormais un mode hors ligne qui pouvait être gérer par bluetooth afin de reprendre le contrôle si ce genre d'incidents venaient à se reproduire.

Le quinzième incident que l'on va traiter sera au sujet de robots aspirateurs qui se sont fait pirater et qui ont causé de nombreux problèmes. Ce qu'il s'est produit en janvier 2025 est que des robots aspirateurs de la marque Ecovacs ont subi des attaques et des piratages. Cela ayant causé qu'un premier robot s'est mis à bouger tout seul et à faire des bruits bizarres dans le domicile familial d'une famille dans le Minnesota, le père de famille a eu comme réflexe de vérifier ce qu'il se passait avec l'application pour gérer le robot. C'est là qu'il s'est aperçu que quelqu'un contrôlait à distance le robot. Il a alors décidé de changer le mot de passe du robot en pensant que c'était un simple bug avec le robot, il reposa alors le robot et partit faire autre chose. C'est alors qu'au bout de quelques minutes que le robot s'est remis à bouger et à débiter des propos racistes injurieux à l'aide des haut-parleurs du robot. Le propriétaire décida alors d'éteindre le robot et de le ranger dans le garage. Heureusement pour eux, l'attaquant s'est dévoilé rapidement car il aurait simplement pu ne pas se dévoiler et espionner la maison et la famille, témoignait le père de famille. Ce ne fut pas le seul cas de piratage de robot aspirateur Ecovacs, en effet un robot en Californie s'est mis à poursuivre le chien d'une famille tout autour de la maison en disant encore une fois des propos injurieux et racistes, et un troisième cas fut signalé où encore une fois un robot s'est mis à insulter ses propriétaires. Pour ce qui est du cas Ecovacs, des premières vulnérabilités sur les robots furent découvertes en août 2024 par des chercheurs en sécurité signalant à l'entreprise qu'il était aisé de pirater le robot pour y prendre accès, mais aussi de pirater l'application mobile, constatant alors qu'il était possible d'obtenir le flux vidéo du robot ainsi qu'un accès aux haut-parleurs, comme on a pu le voir dans les 3 cas précédents. La raison de ces faiblesses est la sécurisation de l'application. En effet, pour accéder au robot, il faut taper un code PIN, mais il est stocké en local sur l'application, faisant qu'il est simple de contourner ce code, soit si le réseau wifi auquel ils sont connectés n'est pas sécurisé. Les chercheurs ont aussi découvert qu'il était facile d'obtenir un accès root au robot, c'est-à-dire un accès administrateur avec toutes les permissions sur le robot. Ils ont aussi découvert qu'on pouvait envoyer du code malveillant à travers le Bluetooth vers le robot. Cela aurait pu être évité à l'aide d'un code de chiffrement sur le robot, mais comme Ecovacs utilise une clé statique pour tous les robots, cela constitue une faille de sécurité massive pour les appareils de la

marque. À l'aide de toutes ces informations, il est aisé de prendre le contrôle de tous les robots vulnérables à ce type d'attaque. Mais ça ne s'arrête pas à là puisque ce type de robot tourne sous Linux, il est aisé de pouvoir prendre le contrôle de plein de robots pour créer de plus grosses attaques.

Le seizième dont on va parler sera au sujet des puces ESP32, l'un des composants principaux de plus d'un milliard d'appareils connectés. Ce qu'il s'est passé est que des chercheurs en cybersécurité ont découvert une faille de sécurité critique sur ces puces, cela causant la vulnérabilité de milliards d'appareils de domotique. Les puces ESP32 développées par Espressif Systems, une grande compagnie d'informatique, servent en tant que microcontrôleurs Wifi et Bluetooth et sont équipées dans de nombreux appareils connectés différents tels que, par exemple, les enceintes connectées, les caméras de surveillance, des systèmes d'alarme et bien d'autres appareils du quotidien que l'on peut retrouver chez nous. Cette faille a donc été présentée en mars 2025 à la conférence RootedCON 2025, ce que fait cette vulnérabilité est qu'elle permet à un pirate d'exécuter du code malveillant à distance, cela pouvant causer de nombreuses autres menaces pour le système. Les chercheurs ont ainsi fait une démonstration sur scène démontrant, à l'aide d'un pilote Bluetooth, qu'il y avait des commandes cachées dans le firmware Bluetooth de la puce, ce faisant qu'ils ont pu trouver 29 commandes non documentées permettant, par exemple, de manipuler la mémoire des appareils, d'usurper l'adresse MAC d'un appareil, faisant qu'il était possible de se faire passer pour quelqu'un d'autres aisément ou bien même encore de l'injection de code malveillant par le Bluetooth. Cela causant donc plusieurs risques principaux :

- Le premier étant la prise de contrôle à distance d'appareils, ils pourraient alors soit servir d'outils d'espionnage ou bien simplement de rebond pour accéder au reste du réseau du domicile et donc aux autres appareils
- Le second est le vol de données sensibles et personnelles. En effet, certains appareils tels que les caméras vont stocker les images qu'elles ont filmées, mais aussi les robots aspirateurs qui vont stocker la cartographie du domicile
- Le troisième est que les appareils vont potentiellement finir par rejoindre le fameux réseau de botnet où les appareils ne seront que des zombies qui serviront à faire des attaques massives sur d'autres appareils sans que l'on ne se rende compte de cela.

Le dix-septième incident dont on va parler est un incident 13 mars 2026 survenu lors d’une opération militaire au moyen orient avec le porte avion Charles-de-Gaulle. En effet un militaire qui faisait simplement une course à pied a vu cette course enregistrée sur l’application Strava une application de course à pied enregistrant les parcours de l’utilisateurs et en y indiquant la position géographique et donc les déplacements fais. Cela ne devrait pas poser de problèmes de base, le problème étant que le profil du militaire ayant effectué cette course était en public causant que du coup lorsque la course fut enregistrée elle était accessible et visible de tous sur internet permettant ainsi à tout le monde de voir la position exacte du porte avion ainsi que le trajet effectué durant cette course. Cette information étant critique étant donné le fait que la seule information communiquée de base fût que le porte avion se trouvait en mer méditerranée pour cette opération mais la position exacte devant restée confidentielle cela pouvait causer un

incident de sécurité pour le porte avion militairement parlant. Cela peut causer aussi d'autres problèmes supplémentaires en effet étant donné que le militaire a partagé ces informations sur son profil public cela indiquait donc aussi l'identité de la personne permettant ainsi de traquer toutes les informations personnelles pour potentiellement servir de moyen de pression par la suite. Cet incident n'était pas le premier à survenir avec Strava, en effet en janvier 2025 des membres de l'équipage d'un sous-marin nucléaire avaient par mégarde publié sur Strava le calendrier des patrouilles à venir. Mais aussi en 2024 où des gardes du corps d'Emmanuel Macron, Joe Biden et Vladimir Poutine qui ont partagé des informations confidentielles.

Le dix-huitième incident que l'on va analyser sera au sujet de 2 failles survenues sur des home assistant. Ces failles furent publiées en mars 2026. Ce qu'il se passait est que si l'on possédait un home assistant chez nous avec l'application et qu'il était configuré avec le mode de réseau hôte, cela causait des points de terminaison non sécurisés, ce qui faisait par la suite que si le home assistant était lié à l'interface de pont de docker interne qui allait vers le réseau local. Cela causait qu'il n'y avait pas de restriction à l'accès sur l'application, donc on pouvait s'y connecter sans avoir besoin d'identifiants. La seconde faille publiée en mars 2026 est un incident qui rendait le home assistant vulnérable à de l'injection XSS (Cross-Site Scripting), cela affectant les systèmes dont la version se trouve entre février 2025 et janvier 2026. La
faille ne se situe pas directement sur le système du home assistant, mais sur une fonctionnalité, celle de l'intégration de données externes sur le home assistant. Et pour être précis, c'est le capteur mesurant le temps de charge d'un téléphone qui est importé par l'application Android Auto. C'est cette partie-là du système qui est vulnérable à de l'injection XSS. Le risque de cette faille est que de nombreuses personnes apprécient remonter des statistiques sur leur système, mais parfois cela peut causer des failles de sécurité très importantes pouvant permettre l'injection de code malveillant sur le système domotique et donc sur tout notre réseau local.

Le dix-neuvième incident dont on va parler sera au sujet d'un virus qui se trouvait sur de nombreuses box Android TV. Ce qu'il se passait est que les box avaient un virus préinstallé en usine directement, qui est un virus persistant et très sophistiqué qui était directement intégré dans le firmware. Ces boitiers étaient des T95 vendus sur Amazon et AliExpress donc accessibles très facilement par le grand public, ce qui se passait donc est que dès l'instant où le produit était branché en réseau dans le domicile de la personne, la box allait télécharger des modules supplémentaires en se connectant à un serveur externe. Lorsque cela était fait, la box allait alors intégrer le réseau de botnet afin d'effectuer des attaques DDoS en se servant de l'IP de la victime, ou alors effectuer de la collecte de données ou de la fraude publicitaire. Cela fut découvert à l'aide d'un script qui permet de nullifier le payload et stopper la communication avec les serveurs externes. Ce que les utilisateurs pouvaient aussi faire était de faire une réinitialisation d'usine de la box, puis par la suite il faudra exécuter le script.

Le vingtième incident qui sera traité sera au sujet d'un incident survenu sur le portail web de Kia en novembre 2024. En effet, cette faille permettait à n'importe qui de pirater des voitures de la marque et de suivre à la trace n'importe qui, pour cela il suffisait à l'attaquant d'être en possession du numéro du châssis du véhicule ou même plus simplement de la plaque d'immatriculation. Ce qui a aussi été constaté est que les véhicules, étant connectés à internet, collectent les données personnelles des conducteurs, ces données étant ensuite envoyées au constructeur des véhicules qu'ils revendaient par la suite aux assurances. Pour en revenir à l'incident, la raison de la faille est qu'à l'aide de l'API du site, l'attaquant pouvait très facilement s'identifier en tant que concessionnaire automobile, cela leur permettant d'accéder à toutes les informations sur les propriétaires et le véhicule, des informations que même les concessionnaires ne sont plus censés avoir accès après avoir vendu le véhicule. Ce que les chercheurs ont effectué par la suite, c'est une application permettant de contrôler le véhicule à distance très facilement. Il suffisait simplement de rentrer la plaque d'immatriculation du véhicule dans le champ de texte, cela permettant de récupérer le numéro d'identification du véhicule et ensuite de l'ajouter sur le profil des chercheurs. Lorsque cela était fait, il pouvait ensuite, à l'aide d'un simple bouton, avoir accès à de nombreuses fonctions du véhicule telles qu'obtenir les coordonnées du véhicule, verrouiller les portes ou pire encore arrêter ou démarrer le moteur. Même si cela ne suffisait pas à contrôler totalement le véhicule pour qu'il se déplace, cela reste très inquiétant puisqu'il était possible de localiser le véhicule puis de voler les objets précieux encore dedans. Ces informations furent publiées après qu'elles eurent eu été signalées auprès du constructeur et que la faille fut réglée mais cela prouve la dangerosité d'avoir trop d'informatiques dans ce type de système sans que la sécurité soit assurée au maximum

Les guides et bonnes pratiques à disposition des utilisateurs

Nous avons pu voir dans les parties précédentes les différents supports physiques de la domotique et les différents logiciels mis à disposition des clients. Les domaines que recouvrent la domotique sont très variés et certains objets connectés peuvent influer directement physiquement le logement du client comme l'accès au logement ou la consommation d'électricité.

Ces éléments critiques peuvent être impactés par un manque de disponibilité, ce qui crée une impossibilité d'utiliser les appareils connectés du logement. Cela peut être acceptable sur une courte période mais peut avoir un impact grave sur une période prolongée. Malgré tous les avantages apportés par la domotique, le risque numérique est considérablement accru si le client utilise des technologies non sécurisées et rendues disponibles sur internet, le client expose son réseau personnel et tous les équipements de son domicile. Un individu mal intentionné peut attaquer les vulnérabilités d'anciens appareils ou de technologies vieillissantes afin d'exploiter les IoT et perturber le système d'informations du client.
L'exemple le plus connu est le Botnet Mirai utilisant majoritairement des IoT exposés sur internet et comportant des vulnérabilités dû à un produit en fin de vie (EoL) ou un appareil non patché ou avec un mot de passe faible. Ce Botnet à servi lors de l'attaque de Dyn, un fournisseur DNS basé aux États-Unis. Cette attaque à crée une panne mondiale de plusieurs services comme Twitter, Netflix, GitHub, Spotify, PayPal et bien d'autres.
Cet exemple montre qu'aujourd'hui il n'est plus acceptable de garder des appareils vulnérables exposés sur internet ou si possible installer les mises à jour de sécurité ou remplacer les appareils en fin de vie. Le consommateur moyen est maintenant un peu plus au fait des enjeux de cybersécurité qu'il y a quelques années, et commence à s'inquiéter à la confiance accordée à certains constructeurs ou au niveau de sécurité de certains produits.
Avec toutes ces nouvelles menaces et les nouvelles inquiétudes des clients, on peut légitimement se poser la question ; Est-il possible de sécuriser sa domotique en étant un utilisateur moyen, sans réelle connaissance avancées ?
Le marché des IoT commence à voir apparaître plusieurs documents et papiers scientifiques pour établir un cadre structuré. Pour cette section, nous avons utilisé plusieurs sources et guides de différentes organisations gouvernementales :
ANSSI : Guide – Recommandations relatives à la sécurité des objets connectés
ETSI : EN 303 645 – Cyber Security for Consumer Internet Of Things : Baseline Requirements
ENISA : Baseline Security Recommendations for IoT
Nous parlerons aussi des labels et certifications des produits au niveau de la cybersécurité et de la différence entre le produit certifié et les produits communautaires Open-Source.
Premièrement, nous allons parler des documents et des cadres récemment écrits et portés à connaissance du public, cette liste ne sera pas développée dans l'ordre chronologique de publication mais plutôt dans un ordre de complexité technique.
Les deux premiers documents sont l'EN 303 645 (anciennement TS 103 645) par l'ETSI, l'Institut européen des normes de télécommunications, ce document est un guide de bonnes pratiques pour les appareils IoT vendus aux consommateurs. Contrairement aux normes ISO et

d’autres guides plus complexes, ce document a été écrit dans le but de guider les utilisateurs dans l’utilisations de leurs objets intelligents du quotidien.
Voici le tableau des différents points abordés dans le document et leur utilité au niveau de la protection du système d’information du consommateur.

Conseil	Détail	Protection Contre
Interdire des mots de passe par défaut	Mot de passe fort et unique	Botnets
Gérer les vulnérabilités divulguées par le fabricant	Canaux de signalement, mises à jour	Botnets et Scripts d’exploitation (Metasploit)
Gérer les mises à jour de l’appareil	Mises à jour, durée du support logiciel, impossibilité de revenir à une version moins sécurisée	Scripts d’exploitation, Obsolescence
Sécuriser les paramètres de sécurité	Impossibilité de modifier un paramètre sans autorisation	Scripts d’exploitation
Utiliser des moyens de communications sécurisés	Utilisation des moyens de cryptographie appropriés	Ecoute du réseau
Minimiser la surface d’attaque	Désactiver les fonctions inutilisées, les ports non utilisés	Scan du réseau
Assurer l’intégrité logicielle	Installer les mises à jour depuis le canal officiel ou vérifié	Cheval de Troie / Trojan
S’assurer que les données personnelles sont chiffrées	Si transmission sur le réseau	Ecoute du réseau
Rendre son système résiliant	Prévoir la possibilité d’une coupure d’électricité ou de réseau	Indisponibilité
Examiner les données de télémétrie	Vérifier si les données sont correctes et lisibles	Incidents de sécurité informatique
Rendre la suppression des données utilisateur simple	La suppression doit être rendue accessible	Litiges RGPD
Rendre l’installation et la maintenance de l’appareil simple	Manuels d’utilisation, tutoriels, guides, bonnes pratiques	Erreur humaine

Valider les données d'entrée	Les données d'entrée devraient être transmises par API	Injections et attaques OOB

On se rend très vite compte que dans ce document on parle principalement de conseils de base pour le consommateur lambda avec aucune connaissance en informatique. Il s'agit d'un document très basique permettant de mettre en œuvre une sécurité minimale vis-à-vis des mises à jour, de limiter son empreinte digitale en évitant d'y inscrire ses données personnelles et de sécuriser l'appareil en configurant un mot de passe robuste. Ce document permet aussi d'informer le consommateur des obligations du constructeur comme l'obligation de permettre de renseigner un mot de passe difficile à obtenir mais avec une possibilité de le réinitialiser pour l'utilisateur en cas d'oubli.
Dans un second plan on peut aussi voir que le document s'intéresse aux plus chevronnés et parle d'un transfert de données par API. C'est un des seuls points abordés pour les utilisateurs plus avancés, le reste du document reste assez simple dans sa vision et propose des conseils simples à mettre en place.
Le document revient aussi sur les bonnes pratiques vis-à-vis du RGPD et informe le consommateur sur les obligations que doivent suivre les entreprises pour la collecte de leurs données personnelles.
Malgré des conseils en apparence basiques, ces-derniers permettent en théorie, pour des réseaux domestiques, permettre d'atteindre un niveau de sécurité informatique élevé.
On peut conclure que l'ETSI a élaboré un document simple pour les consommateurs ayant envie d'avoir une maison connectée plutôt sécurisée, mais ce n'est pas suffisant selon d'autres agences gouvernementales.
Nous allons maintenant parler du second document les Recommandations relatives à la sécurité des (systèmes d')objets connectés de l'ANSSI
Comme il est écrit ce document s'adresse aux particuliers comme aux professionnels
Cette fois le document fait la distinction entre les recommandations avec 4 niveaux :

Niveau	Notation	Détail
Recommandation à considérer en premier lieu	R*	Cette recommandation est d'une difficulté de mise en œuvre minime au regard des garanties qu'elle offre.
Recommandation à considérer en second lieu	R**	Cette recommandation est d'une difficulté de mise en œuvre intermédiaire au regard des garanties qu'elle offre.
Recommandation adaptée à un besoin de sécurité élevé	R***	Cette recommandation est d'une difficulté de mise en œuvre élevée, et doit être

		suivie lorsque les recommandations de mise en œuvre plus aisée ne permettent pas d'atteindre un niveau de risque résiduel acceptable.
Recommandation générale	R	L'effort requis pour mettre en œuvre cette recommandation, ou la protection qu'elle offre, ne peuvent être estimés indépendamment du contexte.

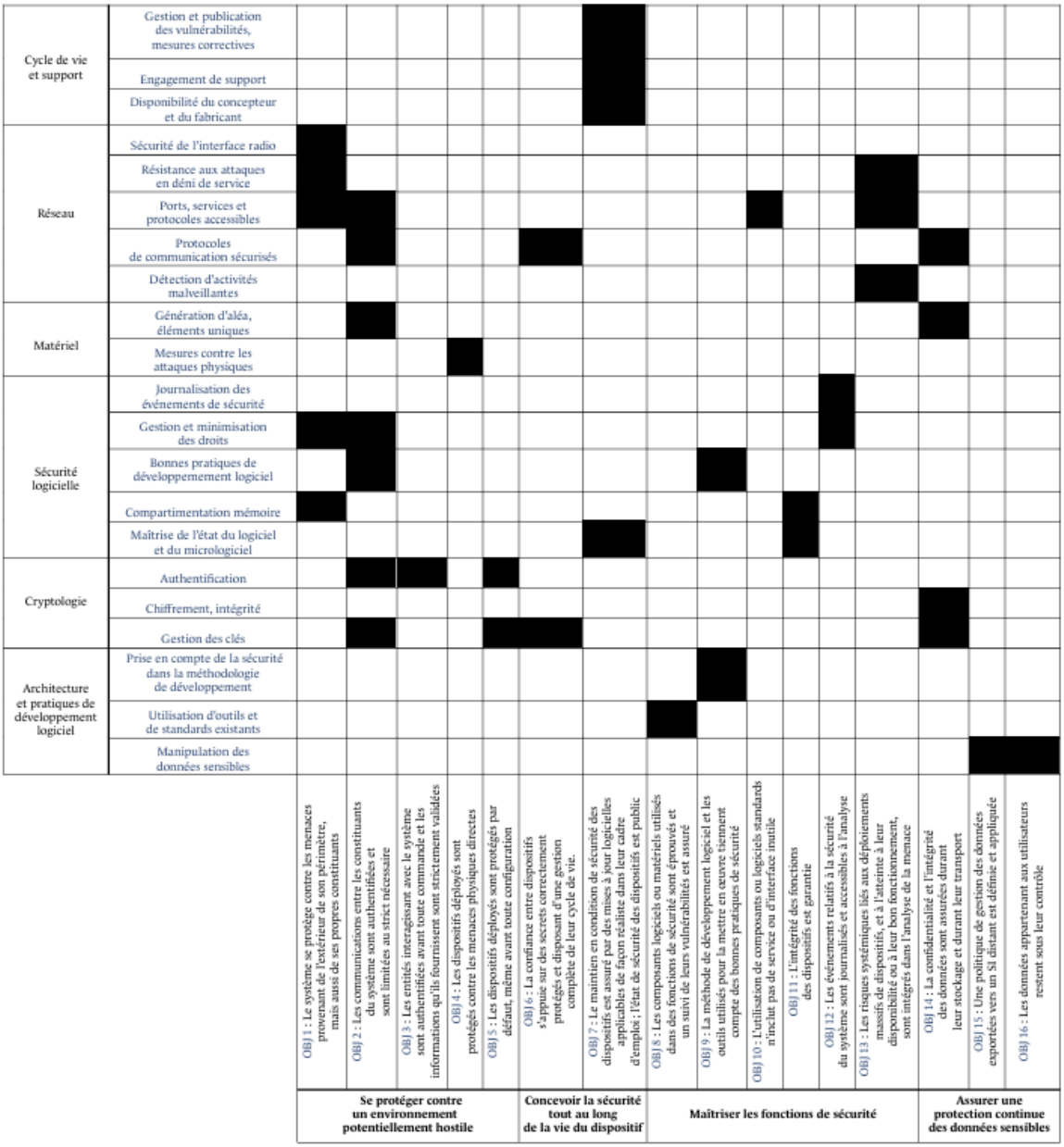
On peut tout de suite distinguer les véritables recommandations cles et les recommandations plutôt facultatives ou non applicables dans certains contextes, ce qui facilite la prise en main du document et de la priorisation des recommandations à appliquer.
L'ANSSI énonce alors les objectifs de ce document, voici les différents objectifs de sécurité que l'ANSSI traite dans ce docuement :

Numéro	Objectif	Détail
1	Menaces internes et externes	Le système se protège contre les menaces provenant de l'extérieur de son périmètre, mais aussi de ses propres constituants.
2	Communications	Les communications entre les constituants du système sont authentifiées et sont limitées au strict nécessaire.
3	Utilisateurs et commandes	Les entités interagissant avec le système sont authentifiées avant toute commande et les informations qu'ils fournissent sont strictement validées.
4	Menaces physiques	Les dispositifs déployés sont protégés contre les menaces physiques directes.

5	Sécurité par défaut	Les dispositifs déployés sont protégés par défaut, avant même toute configuration.
6	Initialisation et propagation de la confiance	La confiance entre dispositifs s'appuie sur des secrets correctement protégés et disposant d'une gestion complète de leur cycle de vie.
7	Maintien en condition de sécurité	Le maintien en condition de sécurité des dispositifs est assuré par des mises à jour logicielles applicables de façon réaliste dans leur cadre d'emploi ; l'état de sécurité des dispositifs est public
8	Composants éprouvés	Les composants logiciels ou matériels utilisés dans des fonctions de sécurité sont éprouvés et un suivi de leurs vulnérabilités est assuré
9	Méthode de développement	La méthode de développement logiciel et les outils utilisés pour la mettre en œuvre tiennent compte des bonnes pratiques de sécurité
10	Minimisation	L'utilisation de composants ou logiciels standards n'inclut pas de service ou d'interface inutile
11	Maîtrise de l'état des dispositifs	L'intégrité des fonctions des dispositifs est garantie
12	Journalisation	Les événements relatifs à la sécurité du système sont journalisés et accessibles à l'analyse

13	Prise en compte des risques systémiques	Les risques systémiques liés aux déploiements massifs de dispositifs, et à l'atteinte à leur disponibilité ou à leur bon fonctionnement, sont intégrés dans l'analyse de la menace.
14	Protection des données	La confidentialité et l'intégrité des données sont assurées durant leur stockage et durant leur transport
15	Interface avec des systèmes tiers	Une politique de gestion des données exportées vers un SI distant est définie et appliquée
16	Données utilisateurs	Les données appartenant aux utilisateurs restent sous leur contrôle

Sur ces 16 objectifs, l'ANSSI a ainsi construit une matrice sur laquelle se baser pour assurer la sécurité informatique de ses IOT et quelle branche technique correspond à un objectif de sécurité.
On peut ainsi clairement différencier quels concepts techniques sont directement liés aux objectifs de sécurité que l'ANSSI veut respecter. Sur cette analyse nous nous concentrerons uniquement sur les recommandations R* ou les « Recommandation à considérer en premier lieu »



L'ANSSI ensuite procède à l'énumération des recommandations techniques et liste les recommandations techniques à suivre selon les domaines techniques. C'est un document très complet qui permet aux entreprises de sécuriser leur infrastructure IoT, même pour les environnements très sécurisés.

Dans un premier temps l'ANSSI conseille fortement de surveiller la collecte, la protection, le transport vers une infrastructure distante de données sensibles. Il faut aussi éviter tout programme non nécessaire a l'utilisation du produit et les commandes doivent être protégées et authentifiées.

Ici on voit que l'ANSSI s'adresse autant au consommateur qu'au constructeur ce sont des conseils qui sont dirigés vers les deux partis. On remarque bien même que certains de ces conseils peuvent s'appliquer aux consommateurs comme aux constructeurs, par exemple dans le fait de limiter la collecte d'informations sensibles.

L'ANSSI développe ensuite l'utilisation de standards et d'outils existants pour permettre une sécurité par le design plutôt qu'une fausse sécurité basée sur l'obfuscation. Elle conseille d'utiliser des standards de cryptographie et de communication en réseau dont les tenants en sécurité sont bien compris et documentés. Les bibliothèques tierces utilisées doivent être suivies pour toute mise à jour de sécurité et toute vulnérabilité publiée. De plus, des tests fonctionnels et unitaires doivent être conduits pour assurer la qualité d'une mise à jour.
Encore une fois, les conseils donnés sont adressés aux deux camps, l'utilisateur comme le constructeur devraient s'adapter aux outils existants pour permettre une fortification des équipements et finalement du système d'informations.
En matière de cryptographie, l'ANSSI préconise l'utilisation de clés privées et secrètes et doivent être unique par dispositif et par fonction. La clé doit respecter une durée de vie donnée en fonction de la sévérité d'une compromission.
Ici, on peut voir que les conseils donnés sont très justes dans un environnement d'entreprise, mais il commence à devenir complique de gérer toutes les clés générées par ses appareils dans une maison connectée, on peut apercevoir quelques limitations pour un utilisateur de domotique DIY, mais le guide reste adaptable, on peut par exemple créer une clé par appareil, mais peut-être pas par fonction, au risque d'avoir trop de clés et de ne plus pouvoir suivre leur déploiement et durées de vie.
L'authentification est le sujet le plus sensible du moment, l'ANSSI préconise évidemment d'utiliser des mots de passe forts et uniques et tout dispositif doit disposer d'un portail d'authentification sécurisé. L'appareil doit pouvoir limiter le nombre de tentatives si plusieurs échecs venaient à se produire, et les protocoles de stockage d'empreinte doivent être unique à chaque identifiant et chaque appareil.
L'ANSSI rappelle les conseils d'ordre général pour les mots de passe mais prodigue aussi des conseils aux constructeurs pour le stockage des empreintes de mot de passe avec un mécanisme de dérivation à sens unique avec sel.
Le document aborde ensuite la question de la sécurité logicielle, tout d'abord en minimisant la surface d'attaque en ne gardant que les fonctionnalités nécessaires. Les mises à jour de micrologiciel doivent être possibles, elles doivent être authentifiées et avoir un numéro de version. Le système mis a jour doit disposer d'un mécanisme anti-rollback ou d' anti-downgrade pour éviter une rétrogradation du logiciel pour exploiter une version vulnérable. Le système de mise a jour doit pouvoir vérifier l'authenticité d'une mise a jour et le matériel comme le logiciel doivent avoir des numéros de version déterminable facilement.
Effectivement, les mises à jour sont importantes, mais de plus en plus de logiciels sont compromis par une mise à jour publiée comme légitime et finalement contient un code malveillant. Il est d'autant plus important quand cela concerne des appareils sensibles comme la gestion de la consommation d'électricité au sein d'un domicile.

Le prochain point est l'utilisation des bonnes pratiques de développement, ce point concerne majoritairement les constructeurs, cependant l'arrivée des ESP32 dans les maisons permet aussi de dire qu'une partie des consommateurs développent des codes et microcodes pour ces microcontrôleurs. D'autant que certains sont compatibles avec des technologies de réseau comme Zigbee. L'ANSSI recommande d'avoir des outils de développements à jour et de durcir

le code grâce aux différents outils mis a disposition dans les environnements de développement, les avertissements doivent être activés et corrigés avant leur déploiement.
L'ANSSI rappelle ensuite que le compte utilisateur d'un appareil doit avoir des droits minimisés et leur permettre d'effectuer des actions en fonction de leur niveau d'authentification. C'est un contrôle d'accès par les rôles, le niveau d'accès doit refléter le rôle de l'utilisateur.
La sécurité matérielle est abordée dans le document, selon l'Agence les fonctionnalités de deboguage et reprogrammation doivent être rendues inaccessibles, ou a minima rendues difficiles d'accès. Cela concerne principalement les constructeurs tout comme le point suivant concernant la génération d'aléa ou d'éléments uniques pour des objectifs cryptographiques.
Le prochain sujet abordé est le réseau, l'ANSSI détaille son analyse en conseillant de ne pas traiter les requêtes d'origine inconnue et de minimiser les services exposés. Elle précise aussi que le protocole UDP ne doit pas être utilisé sous peine de s'exposer a des attaques de déni de service. La protection des données en transport est recommandée par un protocole assurant la confidentialité ou l'intégrité. Pour les appareils radio, il est recommandé de devoir lier une action sensible à une action de l'utilisateur. De plus, les canaux radios et les identifiants utilises doivent minimiser le risque de traçage.
En effet, l'ANSSI insiste bien sur les réseaux et demande bien plus que le document de l'ETSI, il convient d'avoir les connaissances nécessaires pour pouvoir appliquer les recommandations, mais ce ne sont des recommandations jugées importantes voire vitales pour la sécurité des appareils connectes et par extension du système d'informations.
Nous entrons ensuite dans le cycle de vie et le support de l'appareil, selon l'Agence Française il doit y avoir un point de contact pour permettre de signaler un dysfonctionnement ou une faille de sécurité et tout signalement doit faire l'objet d'une réponse indiquant le délai de prise en compte et les modalités de prise en charge. Le support doit avoir une durée en rapport avec la durée de vie attendue du produit et une politique de gestion des vulnérabilités doit être mise en place.

Le document de l'ENISA ne stipule que quelques conseils pour les consommateurs c'est de développer et cultiver la culture de la cybersécurité dans le domaine de l'internet des objets pour pousser les constructeurs à rendre leurs produits sécurisés et informer d'autres consommateurs pour que tout le monde soit protégé le mieux possible.

Les labels concernant la cybersécurité des objets connectés commencent à émerger, il existe aujourd'hui un label américain, tous deux spécialisés et un label Français plus générique qui permet de labeliser un produit ou un logiciel conçu en France.

Conclusion

L'habitat intelligent n'est plus une simple promesse futuriste, il est devenu une réalité tangible et quotidienne. Cette veille technologique consacrée à la domotique Do It Yourself, apparaît clairement que l'on peut trouver des alternatives aux solutions commerciales fermées. Cela garanti une certaine liberté et un contrôle de ses données et de sa vie privée. En s'appuyant sur des équipements modulables tels que les Raspberry Pi, les mini-PCs ou les microcontrôleurs ESP32, couplés à des systèmes d'exploitation open-source puissants comme Home Assistant ou Jeedom, l'utilisateur a désormais la capacité de reprendre la mainmise totale sur ses données et sur son environnement.

Il faut toutefois ne pas négliger un point important à une installation personnel, la sécurité. Comme l'ont démontré les nombreux incidents documentés au fil de notre analyse allant du célèbre botnet Mirai aux intrusions angoissantes via des caméras Nest, en passant par le piratage de robots aspirateurs et les failles de puces massivement utilisées, l'Internet des Objets (IoT) constitue une surface d'attaque extrêmement vulnérable. Ces cas concrets illustrent que les menaces sont protéiformes. Elles peuvent cibler la couche physique (sabotage, puces corrompues), exploiter des faiblesses dans les protocoles de communication (brouillage radio, interception sans fil) ou tirer parti de logiciels et micrologiciels non mis à jour.

Dans le modèle de la domotique commerciale, la gestion des risques est déléguée aux constructeurs et aux serveurs Cloud, avec les dérives de confidentialité et de disponibilité que cela implique (comme les pannes des serveurs AWS affectant des appareils vitaux). Dans le modèle DIY, le créateur devient l'architecte, l'administrateur et le garant exclusif de sa cybersécurité. De ce fait, il est nécessaire d’appliquer de manière rigoureuse les normes et les recommandations. Il est nécessaire de bien prendre en compte les recommandations de l'ANSSI ou l'ETSI. Le cloisonnement des réseaux, la robustesse des mots de passe, la gestion assidue des correctifs, la limitation de la surface d'attaque et l'utilisation de chiffrements forts sont les piliers indispensables pour éviter qu'une simple ampoule connectée ne devienne la porte d'entrée de cybercriminels dans la sphère privée.

Heureusement, le marché de la domotique DIY tend vers la maturité. L'arrivée de standards unificateurs et sécurisés par conception, comme Matter et Thread, promet de simplifier l'interopérabilité tout en élevant le niveau de protection par défaut. De plus, la tendance à relocaliser l'intelligence logicielle – notamment via des IA fonctionnant en local – permet aujourd'hui d'allier l'automatisation avancée à une confidentialité totale, s'affranchissant ainsi des risques liés à l'exposition sur Internet.

En définitive, la création de sa propre infrastructure domotique est une démarche qui dépasse le simple cadre de l'informatique de loisir. Elle exige une véritable acculturation aux enjeux de la cybersécurité. Si le défi est de taille, les opportunités le sont tout autant. Le DIY permet de bâtir une maison connectée sur mesure, évolutive et respectueuse de la vie privée. L'enjeu de

demain ne sera plus seulement de connecter notre habitat, mais de le faire avec la certitude que la technologie restera à notre service, sans jamais se retourner contre nous. Une véritable maison intelligente est, avant tout, une maison sécurisée.

BIBLIOGRAPHIE

ANSSI : Guide – Recommandations relatives à la sécurité des objets connectés
ETSI : EN 303 645 – Cyber Security for Consumer Internet Of Things : Baseline Requirements
ENISA : Baseline Security Recommendations for IoT

WEBOGRAPHIE

2009
IEEE SA :
- https://standards.ieee.org/ieee/802.3at/4553/

2013
IEEE Xplore :
- https://ieeexplore.ieee.org/document/6615591

2015
IEEE Communications Surveys & Tutorials :
- https://ieeexplore.ieee.org/document/7123563
- https://ieeexplore.ieee.org/document/7395614

2016
Mirai :
- https://www.cloudflare.com/fr-fr/learning/ddos/glossary/mirai-botnet/
- https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets
- https://medium.com/@d21dcs151/a-case-study-on-mirai-botnet-attack-of-2016-4b66630e6508

2017
IEEE Xplore :
- https://ieeexplore.ieee.org/document/8255054

2018
ANSSI MesServicesCyber :
- https://messervices.cyber.gouv.fr/documents-guides/guide_802.1x_anssi_pa_043_v1.pdf

White Hat :
- https://www.cbc.ca/news/science/smart-home-hack-marketplace-1.4837963

2019
Fausse Alerte nucléaire :
- https://www.securityweek.com/hacker-uses-nest-camera-broadcast-hoax-nuke-alert/

Incident sur les caméras Nest du domicile
- https://1440wrok.com/computer-hacker-takes-over-milwaukee-couples-home/

2020
ENISA :

- https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

PubMed Central:

- https://pmc.ncbi.nlm.nih.gov/articles/PMC7508411/

e-Spacio UNED :

- https://oai.e-spacio.uned.es/server/api/core/bitstreams/2c51072f-39d2-4744-9d7e-8bed71736b3c/content

Caméra Xiaomi affichant des images d'autres caméras hors du domicile :

- https://www.welivesecurity.com/2020/01/03/google-disables-xiaomi-smart-home-integration/

Tester la faiblesse des firmware lors d'attaques :

- https://blog.avast.com/avast-proves-iot-firmware-can-be-hacked-avast

Incident de swatting :

- https://www.justice.gov/usao-cdca/pr/wisconsin-man-pleads-guilty-swatting-scheme-took-over-ring-doorbell-cameras-livestream

2023

Tom's Hardware :

- https://www.tomshardware.com/news/orange-pi-5-plus-rk3588

GARALOV Toghrul "Raspberry-Pi based IDS for IoT":

- https://essay.utwente.nl/fileshare/file/95931/Garalov_BA_EEMCS.pdf

CSA-IoT :

- https://csa-iot.org/newsroom/matter-1-1-release/

Box Android TV avec malware préinstaller :

- https://www.bleepingcomputer.com/news/security/android-tv-box-on-amazon-came-pre-installed-with-malware/

2024

1NCE « Raspberry Pi Boards »:

- https://www.1nce.com/en-eu/resources/iot-knowledge-base/raspberry-pi-iot-boards

PARLEMENT EUROPÉEN :

- https://www.europarl.europa.eu/news/fr/press-room/20240308IPR19013/

Faille de sécurité sur le site de Kia :

- https://www.kaspersky.fr/blog/tracking-and-hacking-kia-cars-via-internet/22339/

2025

Capteurs de diabète défectueux :

- https://www.lemonde.fr/societe/article/2025/12/04/diabete-des-capteurs-de-glycemie-font-l-objet-d-une-campagne-de-rappel-massive-apres-plusieurs-morts_6655952_3224.html

L'utilisation de nos données personnelles à travers les objets connectés :

- https://www.rts.ch/info/sciences-tech/2025/article/toilettes-connectees-vos-donnees-intimes-en-danger-29089854.html

Panne des serveurs AWS empêchant le sommeil :

- https://www.neozone.org/innovation/les-problemes-daws-ont-transforme-les-lits-connectes-en-cauchemar-pour-leurs-utilisateurs/

Piratage de robots aspirateurs :

- https://www.kaspersky.fr/blog/ecovacs-robot-vacuums-hacked-in-real-life/22471/

Faille sur les puces wifi et bluetooth :

- https://www.lesalexiens.fr/actualites/domotique-une-faille-decouverte-sur-les-puces-esp32-de-plus-dun-milliard-dappareils/

2026

Microsoft Learn :

- https://learn.microsoft.com/fr-fr/windows-hardware/design/device-experiences/oem-secure-boot

officiel Espressif Documentation :

- https://docs.espressif.com/projects/esp-idf/en/latest/esp32/security/security.html
- https://docs.espressif.com/projects/esp-iot-solution/en/latest/display/pwm.html

CSA-IoT :

- https://csa-iot.org/all-solutions/zigbee/

Shelly Knowledge Base :

- https://kb.shelly.cloud/knowledge-base/hardware-architecture

Panne d'un serveur empêchant une application de fonctionner :

- https://next.ink/217301/panne-chez-netatmo-les-applications-et-le-controle-a-distance-ne-sont-pas-disponibles/

Faille de sécurité sur un robot aspirateur :

- https://meilleure-innovation.com/maison/aspirateur/aspirateur-robot-piratable-le-cas-dji-romo/

Faille dans un système de sécurité domestique :

- https://fr.euronews.com/next/2026/02/11/et-si-votre-systeme-de-securite-domestique-etait-votre-pire-ennemi

Position du Porte avion Charles-de-gaulle dévoilé :

- https://www.mac4ever.com/divers/195262-comment-une-course-sur-strava-a-permis-de-localiser-le-porte-avions-charles-de-gaulle

Faille home assistant :

- https://www.cve.org/CVERecord?id=CVE-2026-33045
- https://nvd.nist.gov/vuln/detail/CVE-2026-34205

Home Assistant Documentation :

- https://www.home-assistant.io/integrations/zha/

Silicon Labs :

- https://www.silabs.com/wireless/zigbee/efr32mg21-series-2-socs

FCC :

- https://www.fcc.gov/CyberTrustMark

Label France Cybersecurity :

- https://www.francecybersecurity.fr/

Source :

- https://infos-digital.fr/wifi-domotique-comment-ca-marche/ (*18 juillet 2025 article*)

- https://forumdomotique.com/guides-tutoriels/debuter-domotique/quel-protocole-domotique-choisir-2025-comparatif-zigbee-zwave-wifi-thread-matter/ (*8 septembre 2025 article*)
- https://materiels-electriques.fr/z-wave-le-protocole-domotique-de-reference-pour-la-fiabilite.htm (*28/11/2025 article par Jonathan GEYLER*)
- https://zigbee.readthedocs.io/fr/latest/reseaux-sans-fil.html
- https://wikimemoires.net/2022/11/domotique-et-maison-intelligente/ (« Implémentation d'un système de contrôle d'accès à une maison et à son éclairage (Domotique) » par MWEPU MWANSA Andy)
- https://zigbee.readthedocs.io/_/downloads/fr/latest/pdf/ (Documentation Zigbee par Rémy HUBSCHER le 27/09/2017)
- https://csa-iot.org/newsroom/the-connectivity-standards-alliance-announces-zigbee-4-0-and-suzi-empowering-the-next-generation-of-secure-interoperable-iot-devices/ (Article CSA 11/18/2025)
- http://domo-blog.fr/matter-nouveau-protocole-domotique-maison-connectee-objets-connectes-simplement/ (Article du 01/02/2022 par Aurélien BRUNET)
- https://www.figer.com/Publications/mattter.htm (Article du 19/06/2022 par Jean-Paul FIGER)
- https://project-chip.github.io/connectedhomeip-doc/index.html (Documentation GitHub de Matter)
- https://github.com/openthread/ot-docs/blob/main/site/en/guides/thread-primer/index.md (Documentation Thread)
- https://www.home-assistant.io/blog/2026/03/04/release-20263/ (Article du 04/03/2026 par Franck NIJHOF)
- https://actualite-domotique.fr/home-assistant-hub-automatisation/ (Article du 22/05/2025)
- https://lunarok-domotique.com/2017/05/pourquoi-choisir-jeedom-domotique/ (Article du 16/05/2017 et mis à jour en 2026)
- https://www.elecstore.fr/jeedom-installation-guide-domotiser-maison-connectee/ (Article du 07/09/2025)
- https://blog.domadoo.fr/33379-utilisation-du-logiciel-domoticz-sur-raspberry-pi/ (Article du 27/02/2017)
- https://www.scaleway.com/fr/blog/decouverte-du-protocole-mqtt/ (Article du 01/09/2020 par Luiza del Giúdice de Carvalho)
- https://www.domo-blog.fr/pourquoi-vous-devriez-effectuer-la-sauvegarde-de-votre-domotique-dans-le-cloud/ (Article du 17/02/2026 par Aurélien BRUNET)
- https://www.sqlite.org/docs.html (Documentation du site SQLite)

Index Alphabétique

- **Connectivity Standards Alliance (CSA)** : Organisation à l'origine du protocole Matter et des certifications Zigbee[cite: 1].

D

- **Déni de service (DDoS / DoS)** : Brouillage des ondes (Jamming) et attaques massives perpétrées par le botnet Mirai[cite: 1].
- **DJI (Romo)** : Incident de sécurité sur un robot aspirateur exposant la cartographie des domiciles[cite: 1].
- **Do It Yourself (DIY)** : Approche consistant à créer sa domotique personnelle (matériel, logiciel, réseau) pour plus d'indépendance et de confidentialité[cite: 1].
- **Domoticz** : Logiciel domotique léger et open source écrit en C++[cite: 1].
- **Dongles USB** : Contrôleurs de protocoles radio, équipés d'antennes gravées ou externes[cite: 1].
- **Données** : Cycle de vie (acquisition, traitement, stockage, archivage) et protection RGPD[cite: 1].

E

- **Ecovacs** : Incidents de piratage de robots aspirateurs (insultes racistes, accès caméra, accès root)[cite: 1].
- **Eight Sleep** : Lits connectés devenus incontrôlables suite à la panne des serveurs AWS[cite: 1].
- **EN 303 645 (ETSI)** : Guide de cybersécurité fondamental destiné aux consommateurs d'objets connectés (IoT)[cite: 1].
- **ENISA** : Agence de l'UE soulignant les vulnérabilités liées à la non-traçabilité des composants matériels[cite: 1].
- **ESP32 (Espressif Systems)** : Microcontrôleurs Wi-Fi/Bluetooth peu coûteux[cite: 1].
- **ESP32 (Vulnérabilité)** : Faille critique découverte à la RootedCON 2025 permettant l'exécution de code malveillant à distance[cite: 1].
- **Ethernet (RJ45 / PoE)** : Solutions de connexion filaire directes limitant la surface d'attaque radio[cite: 1].

F

- **Fail-open** : Vulnérabilité (point de défaillance silencieux) causée par l'arrêt d'un capteur fonctionnant sur batterie[cite: 1].
- **Firmware (Micrologiciel)** : Cible d'attaques démontrée par l'infection d'une machine à café par un chercheur d'Avast[cite: 1].

G

- **GATT (Generic Attribute Profile)** : Profil Bluetooth utilisé par de nombreux capteurs domotiques[cite: 1].

- **Google (Home, Nest)** : Interopérabilité limitée face à des failles (alertes nucléaires factices, affichage des flux Xiaomi)[cite: 1].
- **GPIO (Broches)** : Connectique matérielle vulnérable aux surtensions et permettant des connexions directes au réseau[cite: 1].

H

- **Hardkernel (Odroid)** : Fabricant alternatif d'ordinateurs à carte unique (SBC)[cite: 1].
- **Home Assistant** : Système d'exploitation (OS) domotique open-source très populaire, axé sur le fonctionnement local et la confidentialité[cite: 1].
- **Home Assistant (Vulnérabilité)** : Faille XSS documentée via l'intégration d'Android Auto en mars 2026[cite: 1].
- **Hyperviseur (Type 1)** : Utilisation de Mini-PC pour virtualiser et isoler les environnements domotiques de façon sécurisée[cite: 1].

I - J

- **IEEE 802.15.4** : Standard radio basse consommation sur lequel se basent Zigbee et Thread[cite: 1].
- **Intelligence Artificielle (IA locale)** : Solution (ex: SwitchBot AI Hub) pour traiter des données en local sans cloud et analyser les comportements anormaux[cite: 1].
- **Jamming (Brouillage)** : Technique de saturation des fréquences radio pour empêcher la communication des capteurs[cite: 1].
- **Jeedom** : Logiciel domotique concurrent de Home Assistant, basé sur des plugins et une architecture PHP[cite: 1].
- **Journalisation** : Objectif crucial de la sécurité pour analyser les événements du système (selon l'ANSSI)[cite: 1].

K - L

- **Kia** : Faille logicielle ayant permis de démarrer des véhicules et traquer leurs propriétaires avec une simple plaque d'immatriculation[cite: 1].
- **Kohler** : Toilettes connectées posant des problèmes de confidentialité de données soi-disant "chiffrées de bout en bout"[cite: 1].
- **Labels (Cybersécurité)** : Initiatives naissantes pour la certification (ex: U.S Cyber Trust Mark, France Cybersecurity)[cite: 1].

M

- **Matter** : Nouveau standard unificateur visant l'interopérabilité universelle des appareils IoT en local[cite: 1].
- **Mini-PC (x86)** : Appareils plus puissants et fiables que les cartes SBC pour la domotique complexe (Lenovo Tiny, Dell, HP)[cite: 1].

- **Mirai (Botnet)** : Logiciel malveillant historique (2016) ayant orchestré des attaques DDoS colossales (Krebs, OVH, Dyn)[cite: 1].
- **Mosquitto** : Logiciel agissant comme centre de tri (Broker) pour le protocole MQTT[cite: 1].
- **MQTT** : Protocole de messagerie asynchrone fonctionnant avec un système de Broker, Clients, et Topics[cite: 1].

N - O

- **NAS** : Dispositif de stockage en réseau pour des sauvegardes locales redondantes et sécurisées[cite: 1].
- **Netatmo** : Pannes de serveurs en 2025/2026 rendant le contrôle du chauffage à distance impossible[cite: 1].
- **Odroid** : Ordinateur à carte unique concurrent du Raspberry Pi[cite: 1].
- **OpenHAB** : OS domotique open source basé sur Java, destiné aux utilisateurs avancés[cite: 1].
- **Orange Pi** : Ordinateur monocarte utilisant des processeurs Rockchip et des ports NVMe[cite: 1].

P

- **Phishing** : Technique utilisée lors d'un test d'intrusion (par Marketplace) pour voler les accès d'une serrure connectée via l'app Wink[cite: 1].
- **PIR (Infrarouge passif)** : Capteur de détection de mouvement vulnérable au masquage thermique[cite: 1].
- **Protocoles** : Règles de communication classées par type (ouvert/fermé, portée, unidirectionnel/bidirectionnel)[cite: 1].

R

- **Radxa (Rock Pi)** : Alternative matérielle sur le marché des ordinateurs à carte unique[cite: 1].
- **Raspberry Pi** : Ordinateur à carte unique phare de la domotique, mais physiquement limité (usure des cartes micro SD, port GPIO)[cite: 1].
- **Réseau maillé (Mesh)** : Topologie réseau où les appareils relaient l'information pour accroître la portée (utilisé par Zigbee, Z-Wave, Thread)[cite: 1].
- **Ring LLC** : Marque de sonnettes connectées impliquée dans des incidents de "swatting"[cite: 1].

S

- **Sabotage physique** : Destruction de capteurs, vol d'ampoules pour extraction de mot de passe Wi-Fi/Zigbee, ou masquage thermique[cite: 1].

- **SBC (Single Board Computers)** : Appareils monocartes exécutant un OS complet (Raspberry Pi, Orange Pi, Odroid)[cite: 1].
- **Shelly (Gen 4)** : Incident critique en février 2026 où un réseau Wi-Fi de configuration restait ouvert, offrant un point d'accès persistant aux pirates[cite: 1].
- **SQLite** : Système de gestion de base de données privilégié en domotique DIY pour sa légèreté[cite: 1].
- **Strava** : Application de course ayant exposé involontairement des données militaires critiques[cite: 1].
- **Swatting** : Canular criminel visant à envoyer les forces de l'ordre lourdement armées au domicile d'une victime, favorisé par la compromission de caméras[cite: 1].
- **SwitchBot AI Hub** : Solution matérielle exploitant l'intelligence artificielle en local[cite: 1].

T - U - V

- **Thingsbot** : Réseau de 100 000 objets connectés compromis lors de la première cyberattaque officielle documentée (2013-2014)[cite: 1].
- **Thread** : Protocole réseau maillé basé sur l'IPv6, accompagnant la norme Matter[cite: 1].
- **Trojans (Matériels)** : Risques de sécurité sur des cartes SBC assemblées sans processus transparents[cite: 1].
- **UTEC Melun** : Centre de formation d'où est issu le document[cite: 1].
- **Virtualisation** : Déploiement de machines virtuelles pour isoler et sécuriser les sous-systèmes domotiques[cite: 1].

W - X - Z

- **Wi-Fi** : Protocole de communication standard, mais énergivore et dépendant du réseau existant[cite: 1].
- **Wink** : Application de gestion domestique victime d'usurpation d'identité (Phishing)[cite: 1].
- **Xiaomi** : Caméras impliquées dans une faille affichant des flux vidéo chez des voisins sur des écrans Google Nest[cite: 1].
- **XSS (Cross-Site Scripting)** : Injection de code malveillant (faille de mars 2026 sur Home Assistant)[cite: 1].
- **Z-Wave** : Protocole radio propriétaire européen à moyenne portée (868,4 MHz), avec chiffrement natif (Framework S2)[cite: 1].
- **Zero Day** : Type de faille logicielle non connue exploitable par des attaquants[cite: 1].
- **Zigbee (IEEE 802.15.4)** : Protocole ouvert sur la fréquence 2,4 GHz, permettant de gérer jusqu'à 65 000 appareils avec une sécurité décentralisée (version 4.0)[cite: 1].

Glossaire

DIY: Littralement “Do It YourSelf”

Raspberry Pi: Ordinateur à carte unique utilisé comme cœur d'une installation domotique DIY.

SBC: Ordinateur à carte unique (Single Board Computer) intégrant tous les composants essentiels.

GPIO: Broches d'entrée/sortie utilisées pour connecter des périphériques électroniques.

ESP32: Microcontrôleur avec Wi-Fi et Bluetooth intégré, utilisé pour des tâches simples.

MQTT: Protocole de messagerie léger utilisé pour la communication entre objets connectés.

Zigbee: Protocole radio maillé basé sur IEEE 802.15.4 pour la communication entre objets connectés.

Z-Wave: Protocole de communication sans fil pour la domotique, concurrent de Zigbee.

Thread: Protocole de communication maillé pour objets connectés, basé sur IPv6.

Matter: Standard unificateur pour la domotique visant l'interopérabilité entre appareils.

Home Assistant: Système domotique open-source pour la gestion locale des équipements.

Jeedom: Plateforme domotique française open-source pour le contrôle des objets connectés.

Domoticz: Système domotique open-source léger pour la gestion des capteurs et actionneurs.

OpenHAB: Plateforme domotique open-source orientée vers l'interopérabilité des objets connectés.

Broker: Serveur central qui gère la communication entre les clients dans un système MQTT.

Mosquitto: Implémentation open-source populaire d'un broker MQTT.

Mesh: Topologie de réseau où chaque nœud peut relayer les données, augmentant la portée et la fiabilité.

BLE: Bluetooth Low Energy, protocole sans fil à faible consommation pour objets connectés.

PoE: Power over Ethernet, technologie permettant d'alimenter un appareil via un câble Ethernet.

TRIM: Commande utilisée par les SSD pour gérer l'usure du disque et améliorer sa durée de vie.

Botnet: Réseau d'appareils compromis contrôlés à distance pour mener des attaques.

Mirai: Botnet célèbre ayant exploité des objets connectés vulnérables pour lancer des attaques DDoS.

S2 Framework: Cadre de sécurité pour le protocole Z-Wave visant à renforcer la protection des données.

AES-128: Algorithme de chiffrement symétrique utilisé pour sécuriser les communications.

OTA: Over-The-Air, méthode de mise à jour logicielle à distance des appareils connectés.

Anti-rollback: Mécanisme empêchant l'installation de versions antérieures de firmware vulnérables.