Etude sur la sécurisation des objets connectés

*Thierry Didi,
Avril 2025
Tidiwi*

La sécurité des objets connectés a longtemps été mise de côté par les industriels, mais le contexte géopolitique actuel, ainsi que les évolutions des réglementations, ont placé cette question au centre des préoccupations des fabricants et des utilisateurs.

Au fil de mes expériences professionnelles et de mes recherches personnelles, j'ai eu l'occasion d'explorer plusieurs frameworks de développement créés par des industriels et des organisations à but non lucratif pour assurer la sécurité des logiciels embarqués.

Cet article d'intéresse plus précisément :

- [Aux évolutions réglementaires en Europe](#)
- [Aux frameworks existants](#)
- [Aux bonnes pratiques recommandées par l'ENISA](#)

Il met l'accent sur les aspects opérationnels de la cybersécurité plutôt que sur les aspects organisationnels, sans pour autant négliger l'importance de ces derniers :

- Il est essentiel de développer une culture de la cybersécurité au sein de l'entreprise, impliquant tous les niveaux, des membres du Comité Exécutif aux développeurs, en passant par les acheteurs.
- La formation continue des employés, en particulier des développeurs, est cruciale pour qu'ils restent informés des dernières avancées dans ce domaine en constante évolution.

J'espère que cet article aidera chacun à mieux comprendre les étapes nécessaires pour sécuriser les objets connectés et se conformer aux futures réglementations.

Si vous avez des commentaires, remarques ou des questions, n'hésitez pas à me contacter par email pour m'en faire part : [thierry.didi \[at\] tidiwi \[dot\] com](mailto:thierry.didi[at]tidiwi[dot]com)

Introduction

Avant de rentrer dans le détail des attaques envisageables contre les objets connectés, et des mesures qu'on peut mettre en place pour s'en protéger, il est utile de préciser quelques éléments de langage :

- **Attaque DDOS** (Distributed Denial Of Service) : un grand nombre d'appareils génèrent des requêtes simultanées vers un serveur pour le planter.
- **Attaquant** : un utilisateur malveillant qui cherche à perturber le système.
- **CVE** (Common Vulnerabilities and Exposures) : Quand une faille est détectée dans un logiciel open source ou propriétaire, elle est publiée dans un ou plusieurs bases de données publiques gérées par des entités officiellement reconnues pour gérer ce type de base de données (Microsoft, Google, MITRE, Apache Software Foundation ...). Le gestionnaire de la base de données lui affecte un identifiant unique nommé CVE qui a la forme CVE-YYYY-NNNNN. Dans les bases de données des CVEs, on trouve une description plus précise de la faille de sécurité, son impact, et les correctifs éventuels. MITRE est responsable de l'allocation des CVEs de manière qu'un même CVE se soit pas affecté à deux failles différentes.
- **Cyber Resilience Act** (CRA) : Règlement qui entrera progressivement en vigueur en Europe pour renforcer la sécurité des équipements contenant des éléments (matériels et/ou logiciels) numériques. Le texte complet est accessible à l'adresse https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847
- **Directive RED** (Radio Equipment Directive) : Directive européenne 2014/53/UE qui s'applique aux équipements radioélectriques. Le texte complet est accessible à l'adresse : <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053>
- **ENISA** (European Union Agency for Cybersecurity : <https://www.enisa.europa.eu/>).
- **IoTSEC** (IOT Security Foundation: <https://iotsecurityfoundation.org/>) est une organisation à but non lucratif basée en Grande Bretagne qui s'intéresse à la sécurité des objets connectés.
- **JTAG** : dans ce document, le terme connecteur JTAG représente un connecteur présent sur les cartes électroniques et permettant de lire/écrire dans la mémoire d'un microcontrôleur, et de debugger un programme exécuté par ce microcontrôleur. En règle générale, ce connecteur n'est présent que sur les cartes utilisées par les développeurs, mais son empreinte est présente sur le PCB de toutes les cartes. Il est possible (et même recommandé) de désactiver le JTAG des processeurs une fois que les produits sont mis en production.
- **Marché Gris** : il s'agit d'un marché où on peut se procurer des produits authentiques, mais en dehors des circuits de distribution officiels autorisés par le fabricant.

- **MITRE** (<https://www.mitre.org/>) est une organisation à but non lucratif basée aux Etats Unis qui soutient le gouvernement américain, notamment dans le domaine de la cybersécurité.
- **SBOM** (Software Bill Of Material) : Il s'agit de la liste des composants logiciels tiers (souvent open source), qui entrent dans la composition d'un logiciel. Chaque composant logiciel doit être associé à sa version. L'intérêt de connaître la SBOM d'un logiciel est de permettre d'identifier (et de corriger) rapidement les failles de sécurité introduites par ces logiciels dès que ces failles sont publiées.

VEX (Vulnerability Exploitability Exchange) : il s'agit d'un format standardisé destiné à décrire si un logiciel est vulnérable à une faille de sécurité connue.

Le Contexte

Les fabricants d'objets connectés ont tendance à s'intéresser de près à la sécurité lorsqu'un incident grave fait la une de l'actualité (une attaque *DDOS*¹ générée par des caméras connectées par exemple ...), ou lorsque la mise en application d'une obligation légale approche, comme c'est le cas en Europe avec la directive *RED* en 2025 ou avec le *Cyber Resilience Act* d'ici fin 2027.

Les risques liés au piratage des objets connectés sont souvent sous-estimés, surtout lorsqu'il s'agit d'objets apparemment anodins et non destinés à des environnements critiques. Il est courant de penser à tort que le piratage se limite principalement aux rançongiciels ou au vol de données bancaires et personnelles. Cependant, les motivations des attaquants peuvent être bien plus variées :

- Il peut s'agir simplement de sabotage d'infrastructures, mené par des États ou des organisations puissantes.
- Des concurrents malveillants peuvent lancer des attaques pour nuire à la réputation d'un produit ou d'une entreprise, ou pour « voler » la propriété intellectuelle d'une autre société.
- Des hackers isolés peuvent mener des attaques pour des raisons idéologiques ou par pur divertissement.
- Certains attaquants peuvent chercher à exploiter la connectivité et les processeurs d'une flotte d'objets pour mener des activités illégales, comme des attaques par déni de service (DDoS), ou encore espionner des positions GPS ou des conversations.
- Les attaques peuvent aussi viser des systèmes sans fil (NFC, ondes radio) pour réaliser des effractions, voler des véhicules, ou accéder à des bâtiments en piratant les communications entre un émetteur (badge d'accès, clé de véhicule) et un récepteur.

Enfin, il faut garder à l'esprit que les opérations de piratage peuvent bénéficier de complicités internes, avec des individus au sein de l'entreprise ayant accès à des ressources sensibles.

Les exemples ci-dessous montrent que le piratage d'un objet banal peut entraîner des conséquences importantes :

- Un attaquant capable de prendre le contrôle d'un détecteur d'incendie ou qui parvient à installer un faux détecteur dans un bâtiment pourrait déclencher de fausses alertes incendie, perturbant ainsi le fonctionnement de l'entreprise et entraînant des coûts économiques. Ces alertes erronées nuiraient également à la réputation du fabricant du système de sécurité incendie, dont la fiabilité serait remise en cause. Le client pourrait même demander des compensations financières au fabricant du système.
- Un attaquant capable de pénétrer dans le système de contrôle d'accès d'une entreprise pourrait en perturber considérablement le fonctionnement. En créant de faux badges d'accès ou en clonant des badges authentiques, il pourrait facilement pénétrer dans les locaux de l'entreprise.

¹ Distributed Denial Of Service : un grand nombre d'appareils génèrent des requêtes simultanées vers un serveur pour le surcharger.

- Un attaquant capable de modifier le logiciel d'un compteur d'eau, de gaz ou d'électricité pourrait manipuler le système de facturation, entraînant ainsi des pertes financières importantes pour le fournisseur.
- Un attaquant capable d'installer un nouveau firmware sur un objet connecté pourrait le rendre complètement inutilisable, ou l'utiliser comme point de lancement pour des attaques par déni de service distribué (DDoS), comme cela a déjà été observé. Dans les deux cas, les risques en termes d'image et de coûts financiers pour le fabricant seraient considérables.

Les frameworks

Pour répondre aux besoins de sécurisation des objets connectés, une nouvelle réglementation entrera en vigueur en Europe, concernant tous les objets connectés à l'internet :

- Un amendement à la directive *RED* introduit de nouvelles exigences pour les nouveaux produits dotés d'interfaces sans fil et mis sur le marché à partir d'août 2025.
- Le *Cyber Resilience Act* (CRA) entrera progressivement en vigueur d'ici la fin de l'année 2027, imposant de nouvelles contraintes applicables notamment aux objets connectés. Ces contraintes seront applicables tout au long de leur cycle de vie, et pas seulement lors de leur mise sur le marché.

Par ailleurs, plusieurs organisations ont spécifié des frameworks et des méthodologies visant à améliorer la sécurité des objets connectés. Parmi elles :

- L'*ENISA* a publié un guide à l'intention des fabricants, développeurs et intégrateurs pour les aider à sécuriser les objets connectés : Guidelines for Securing the Internet of Things (<https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Guidelines%20for%20Securing%20the%20Internet%20of%20Things.pdf>).
- L'*IoTSEC* a développé le « IOT Security Framework » dédié à la sécurité des objets connectés : <https://iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSEC-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf>.
- *MITRE* a créé la base de données ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) pour répertorier les attaques des cybercriminels et décrire les techniques utilisées. Cette base de données est accessible à tous : <https://attack.mitre.org/>.
- *MITRE* a également développé le framework EMB3D (<https://emb3d.mitre.org/>), axé sur l'amélioration de la sécurité des systèmes embarqués.
- ARM Limited, dont les cœurs de CPU équipent une grande partie des objets connectés, a créé le framework PSA Certified (<https://www.psacertified.org/>) pour les fabricants d'objets connectés. Ce framework fournit un ensemble de règles de conception visant à garantir la sécurité des objets. Il s'agit d'un framework de très bas niveau, associé à des modules open source (TF-M², TF-A³) permettant de l'implémenter sur des processeurs ARM Cortex M ou Cortex A.

Ce document s'intéresse plus particulièrement au guide publié par l'*ENISA* qui a sans doute servi de base à l'élaboration du *Cyber Resilience Act*.

² <https://www.trustedfirmware.org/projects/tf-m/>

³ <https://www.trustedfirmware.org/projects/tf-a/>

Les évolutions de la réglementation européenne

Les deux évolutions récentes de la réglementation européenne concernent une évolution de la directive *RED*⁴ et l'adoption du *Cyber Resilience Act*⁵.

- La nouvelle directive *RED* entrera en vigueur en Aout 2025 pour tous les nouveaux produits mis sur le marché en Europe. Elle introduit trois nouvelles contraintes dans son article 3 (« Essential Requirements »):
 - 3.38d : « *radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service* »
 - 3.38e : « *radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected* »
 - 3.38f : « *radio equipment supports certain features ensuring protection from fraud* »

Il existe une famille de standards harmonisés permettant de garantir la conformité à ces nouvelles exigences :

- EN 18031-1:2024 : Common Security Requirements for Internet Connected Radio Equipment. Permet de vérifier la conformité à RED 3.3-8d
 - EN 18031-2:2024 : Common Security Requirements Equipment Processing Personal Data : Permet de vérifier la conformité à RED 3.3-8e
 - EN 18031-3:2024 : Common Security Requirements for Equipment Processing Virtual Money or monetary value : Permet de vérifier la conformité à RED 3.3-8f
- Le *Cyber Resilience Act* entrera progressivement en vigueur d'ici à la fin de l'année 2027, imposant de nouvelles contraintes applicables aux produits électroniques, notamment aux objets connectés, tout au long de leur cycle de vie et pas seulement lors de leur mise sur le marché. Ces contraintes ne s'appliquent toutefois pas aux appareils médicaux⁶ à l'industrie automobile⁷, à l'aviation civile, aux équipements militaires ou aux logiciels open source.

En premier lieu, le *CRA* impose (Article 13) de réaliser une analyse de risques et prendre en compte le résultat de cette étude dans toutes les phases de vie du produit, depuis la conception jusqu'au retrait du marché, en incluant la maintenance.

La liste des exigences est facilement consultable dans le texte du *CRA* (Annexes I, II, et III). Les éléments les plus importants sont les suivants :

- Annexe I - Part I : Sécurité du produit
Cette section concerne les mises à jour du logiciel, le contrôle d'accès, la gestion de la confidentialité et de l'intégrité des données critiques stockées dans l'appareil ainsi que des données transmises, la mise en place de mesures pour minimiser l'impact d'un dysfonctionnement d'un produit sur les autres produits

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053>

⁵ https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

⁶ La cybersécurité des équipements médicaux est traitée dans les réglementations (EU) 2017/745 et (EU)2017/746

⁷ La cybersécurité pour l'industrie automobile est traitée dans la réglementation (EU)2019/2144

présents sur le réseau, la limitation de la surface d'attaque (interfaces de type UART, JTAG ... ou ports TCP/UDP ouverts), le monitoring et le reporting d'incidents de sécurité, la possibilité pour un utilisateur de supprimer toutes les données sensibles d'un appareil.

- Annexe I - Part II : Gestion des vulnérabilités

Il s'agit d'implémenter des process pour détecter les vulnérabilités, les corriger, diffuser des correctifs, et rendre ces vulnérabilités publiques (via des CVEs) dès qu'un correctif est identifié. Les incidents de sécurité détectés devront être reportés à l'ENISA. Notamment, cette gestion impose de générer une SBOM (Software Bill Of Material) pour les logiciels intégrés dans le produit. Il n'est pas obligatoire de rendre cette SBOM publique.

Le CRA définit aussi plusieurs classes d'appareils en fonction du risque de sécurité associé à chaque appareil. La majorité des appareils sont des appareils de classe I. La classe II correspond aux équipements de sécurité (hyperviseur, firewalls). Enfin certains appareils sont considérés comme critiques (metering gateways, smart cards). Essentiellement, la classe d'un appareil a une incidence sur la procédure de certification. Il est possible d'appliquer une procédure d'auto-certification à un produit de Classe I qui implémente les standards harmonisés associés au CRA. Ces standards harmonisés n'existent pas encore (en avril 2025) mais ils devraient être publiés bien avant l'échéance de 2027. Cependant le standard « ETSI EN 303 645 V2.1.1 : Baseline Requirements »⁸ et la Spécification Technique « ETSI TS 103 701 V1.1.1 : Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements »⁹ permettent de couvrir une grande partie des exigences de l'Annexe I du CRA.

La plupart des outils d'analyse statique de code (par exemple Sonarqube¹⁰) fournissent, ou vont fournir dans un futur proche, des moyens de générer une SBOM, et de lister les vulnérabilités introduites par des logiciels tiers.

Enfin, les fabricants devront permettre à des utilisateurs de reporter des failles de sécurité qu'ils auraient identifiées, en désignant un point de contact unique à notifier quand une vulnérabilité est détectée.

⁸ https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

⁹ https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

¹⁰ <https://www.sonarsource.com/products/sonarqube/>

Le guide de l'ENISA

La gestion de la sécurité d'un produit se fait tout au long du cycle de vie d'un produit, depuis la phase de conception jusqu'au retrait du marché. Le guide de l'ENISA s'articule autour des concepts suivants :

- [Le cycle de vie du produit](#)
- [Les menaces](#)
- [Les bonnes pratiques](#)

Le Cycle de vie d'un produit

Le concept qui se trouve au cœur de l'approche de l'ENISA est nommé « Secure By Design » : Il s'agit un ensemble de principes et de bonnes pratiques visant à intégrer la sécurité de manière proactive et continue tout au long du cycle de vie d'un produit, de sa conception à son retrait du marché, afin de réduire les risques de vulnérabilités et de protéger contre les menaces potentielles dès le début. Concrètement ce guide définit les étapes suivantes dans la vie d'un produit :

- Conception
 - Développement
 - Production
 - Utilisation
 - Support
 - Retrait
-
- **La conception**
Dès cette étape, la stratégie de sécurité doit inclure l'électronique, le logiciel, le packaging, la plateforme IOT et les services associés, en tenant compte de l'environnement d'utilisation envisagé pour le produit.
 - **Le Développement**
Cette phase inclut le développement logiciel du produit, des services à implémenter dans la plateforme de service, de l'électronique et du packaging. Evidemment, la sécurité doit être prise en compte durant toutes ces phases.
 - **La production**
Cette étape est aussi très importante, car si la chaîne de production n'est pas sécurisée, rien n'empêche un attaquant de voler des données de sécurité avant même que le produit ne soit sur le marché, ou même d'y intégrer un logiciel malveillant.
 - **L'utilisation et le support**
Par ailleurs, la prise en compte de la sécurité ne s'arrête pas lorsque le design est terminé et que le produit est mis sur le marché. Le fabricant doit prendre en compte les phases d'installation, puis de support tout au long de la vie du produit. Notamment, il est important de superviser les produits pour détecter les éventuelles failles ou cyber-attaques, et d'implémenter des mécanismes de mise à jour des logiciels à distance.

- **Le retrait**

Enfin, la phase de retrait du marché doit être étudiée, pour des raisons environnementales dans un premier temps, mais aussi pour éviter qu'un produit en fin de vie ne puisse être analysé pour en extraire des informations confidentielles (informations personnelles, clés de chiffrement ...)

Les menaces

Les menaces les plus importantes concernant les systèmes IOT, telles qu'elles ont été identifiées par des experts sur le terrain sont listées ci-dessous. Cette section est importante puisqu'elle permet de mieux comprendre les risques auxquels un fabricant d'objet connecté sera confronté, surtout s'il ne prête pas attention à la cybersécurité :

○ **Les attaques physiques**

Ces attaques sont destinées à rendre le produit non opérationnel, ou à revendre sur le *marché gris* des produits en fin de vie ou défectueux. Le premier point n'est pas forcément important si l'objet n'est pas utilisé dans un contexte critique car le propriétaire de l'objet est responsable de son intégrité physique. Le second point est beaucoup plus important car il peut entraîner une perte de revenu pour le fabricant, ou une atteinte à sa réputation si des produits défectueux sont revendus sur le *marché gris*.

○ **La perte de propriété intellectuelle**

Récupération par reverse engineering de documents, clés de sécurité, algorithmes embarqués dans le produit. Ces attaques peuvent avoir de graves conséquences légales en cas de vol de données à caractère personnel, ou financières en cas de vol de données industrielles confidentielles.

○ **Le clonage de produit**

Fabrication de faux produits sous la même marque ou sous une autre marque que le produit d'origine. Les faux produits peuvent aussi embarquer des logiciels malveillants, tout en se faisant passer pour des produits d'origine. Ici aussi, ces menaces peuvent entraîner des conséquences financières importantes, ou des conséquences en termes d'image pour le fabricant.

○ **Les abus divers**

Dans la mesure où les attaquants disposent d'un temps infini et d'un accès physique aux appareils, ils peuvent utiliser des outils avancés pour les attaquer. Par génération de champs magnétiques ou par analyse de la consommation de courant d'un appareil pendant une opération de chiffrement, il est possible de récupérer les clés de chiffrement utilisées. En accédant au *JTAG* d'un processeur, ils peuvent insérer des logiciels malveillants dans le produit.

○ **Attaques réseau**

Des appareils mal protégés peuvent servir de base à de larges campagnes d'attaque de type *DDOS*.

- **Attaques du process de manufacturing**
Si un attaquant est capable de s'introduire dans la chaîne de production, il peut insérer dans les produits un logiciel malveillant dès la phase de fabrication, ou bien récupérer les clés de sécurité censées protéger le système.
- **Attaques au niveau de la plateforme IOT**
Si l'authentification des appareils auprès de la plateforme de service n'est pas assez robuste, de faux appareils peuvent se connecter à la plateforme, et transmettre des données erronées, ou même utiliser la plateforme de service comme une passerelle pour des attaques du réseau local auquel les serveurs de la plateforme est connectée.

Les bonnes pratiques

Enfin ce guide définit un ensemble de bonnes pratiques pour se protéger de ces menaces. Ces pratiques peuvent être classifiées suivant les rubriques suivantes :

- [L'identification des risques](#)
- [La protection contre les risques](#)
- [La détection des anomalies](#)
- [La réponse aux anomalies et le retour à la normale](#)

Bonnes pratiques : identification des risques

- **L'analyse de risques**
Une analyse de risques doit être effectuée dès la phase de conception, pour identifier les risques encourus en fonction de l'utilisation prévue pour le produit. Pour chaque risque identifié, les conséquences doivent être évaluées, et des mesures doivent être mises en place en fonction de la gravité de ces conséquences.

Bonnes pratiques : protection contre les risques

- **La culture d'entreprise**
Il est de la plus haute importance de développer une culture de la cybersécurité, aussi bien chez les membres du Comité Exécutif que chez les développeurs ou les acheteurs de logiciels tiers.
- **La gestion des sous-traitants**
Il faut s'assurer des mesures mises en œuvre par les sous-traitants pour garantir la sécurité de leurs procédés. Notamment, les usines de production doivent être en mesure de garantir que des logiciels malveillants ne seront pas introduits dans les produits au moment de la production, ou que les éléments cryptographiques (clés de chiffrement, certificats, ...) ne seront pas divulgués ou altérés pendant la phase de production. Il faut aussi pouvoir s'assurer que les binaires qui seront finalement intégrés dans les appareils sont bien ceux qu'on a fourni à l'entreprise chargée de la production. Ce dernier point peut être réalisé via une inspection d'un échantillon de produits en sortie de chaîne de production par exemple.

- **Génération d'une SBOM (Software Bill Of Material)**
La liste des modules externes intégrés dans le produit doit être générée pour permettre une identification rapide des problèmes associés à des logiciels tiers.

- **Configuration « usine »**
Lorsqu'un produit est restauré dans sa configuration « usine », les fonctionnalités de sécurité doivent être activées par défaut. En effet, de nombreux utilisateurs ne s'intéresseront pas à restaurer les paramètres de sécurité du produit, par ignorance ou par manque de temps. Il est donc important de garantir que si certaines fonctionnalités doivent être désactivées pour exécuter une action particulière, cette désactivation résulte d'une action consciente de l'opérateur de l'objet.

- **De-commissioning**
Lorsqu'un produit est retiré du marché, par exemple parce qu'il est défectueux, il faut s'assurer que toutes les données confidentielles (données personnelles, clés de sécurité ...) sont correctement effacées du produit.

- **L'utilisation de logiciels tiers**
Lors du développement, l'utilisation de logiciels tiers, notamment de logiciels Open Source, introduit un risque de sécurité important. De nouvelles failles de sécurité sont régulièrement identifiées par la communauté Open Source, et des patches sont implémentés. Il faut donc toujours s'assurer que les bibliothèques externes n'ont pas été modifiées par un tiers, que les versions les plus récentes sont utilisées, et d'effectuer une veille et des mises à jour de ces bibliothèques pendant toute la vie du produit.

- **L'implémentation de la cryptographie**
Les algorithmes de chiffrement eux-mêmes sont régulièrement dépréciés quand la puissance de calcul des processeurs augmente, ou quand des failles de sécurité sont découvertes. Par exemple, le protocole WEP est proscrit pour la sécurité des réseaux WIFI, les algorithmes DES ou 3DES sont aussi bannis des protocoles de sécurité.
Par ailleurs, une mauvaise utilisation ou une mauvaise implémentation d'un algorithme de sécurité qui sont pourtant reconnus comme très robustes peut introduire une faille de sécurité. Par exemple, l'algorithme AES-CTR n'offre pas de vraie sécurité si un même IV (Initialization Vector) est utilisé pour plusieurs opérations de chiffrement. De même AES-CBC n'offre aucune garantie de sécurité si l'IV n'est pas choisi aléatoirement à chaque opération de chiffrement. Il faut donc toujours s'assurer d'utiliser les algorithmes en phase avec les recommandations des experts en sécurité, et d'utiliser ces algorithmes suivant les règles de l'art.

- **La chaîne de confiance**

L'implémentation d'une chaîne de confiance (root of trust) est de première importance pour le démarrage du logiciel. Au démarrage d'un processeur, un premier logiciel (bootloader) est exécuté : ce logiciel est responsable de vérifier l'intégrité du prochain logiciel à exécuter (second stage bootloader, ou Operating System ...) qui est lui-même responsable de vérifier l'intégrité du logiciel suivant (application cliente par exemple). Idéalement, cette chaîne de confiance est garantie par un composant de sécurité (Secure Element) qui stockera les clés de chiffrement et exécutera les algorithmes cryptographiques de manière sécurisée. Certains SOCs (Systems On Chip) récents intègrent ce type de composant, mais il est aussi possible d'implémenter ces composants sur le PCB si le SOC n'en intègre pas.
- **Minimisation de la surface d'attaque de l'objet**

Ce point est un des éléments essentiels de l'approche Secure By Design. Il consiste à désactiver toutes les interfaces du produit qui ne sont pas utilisées (JTAG, console UART, ports TCP/UDP ...) qui pourraient servir de point d'entrée à un attaquant.
- **Minimisation de la surface d'attaque de la plateforme IOT**

Les services associés au produit seront souvent implémentés au sein de la Plateforme IOT. Cette plateforme sera donc accessible aux objets (souvent via des ports UDP/TCP) pour que ceux-ci puissent lui transmettre leurs données. Il est très important de vérifier que cette plateforme n'expose que les services utiles au bon fonctionnement du système (notamment que seuls les ports UDP/TCP utiles sont ouverts) pour éviter qu'un attaquant n'utilise des services laissés ouverts par inadvertance (ftp, ssh, telnet, ...).
- **Gestion des accès dans la plateforme IOT**

Dans la mesure où la plateforme IOT est au cœur du système, est de d'une importance capitale d'y gérer correctement le contrôle d'accès. Seuls les appareils correctement authentifiés doivent pouvoir s'y connecter, et ces appareils ne doivent avoir accès qu'au minimum de ressource dont ils ont besoin pour fonctionner, suivant le principe du « moindre privilège » qui est aussi un des éléments clé de l'approche Secure By Design.
- **Utilisation de composants authentifiés**

L'utilisation de composants authentifiés permet d'éviter la contrefaçon. Notamment, certains fournisseurs de SOCs permettent de personnaliser les processeurs de manière que le logiciel ne puisse s'exécuter que sur des processeurs proprement personnalisés par le fabricant de l'objet connecté. C'est-à-dire qu'un contrefacteur qui serait capable d'obtenir une image binaire « officielle » d'un objet ne pourra pas l'exécuter sur un processeur ayant la même référence, mais qu'il aurait acheté en dehors du circuit de vente officiel défini par le fabricant de l'objet.

- **Utilisation d'identifiants uniques par produit**

La génération d'un identifiant unique par appareil lors de la production permettra d'authentifier cet appareil auprès de la plateforme de service, ou de le révoquer en cas de dysfonctionnement.

Bonnes pratiques : détection des anomalies

- **Le monitoring à distance**

Il est impossible de prévoir à l'avance toutes les attaques qui vont arriver durant toute la vie du produit. Il faut donc implémenter des mécanismes de détection des situations anormales. Notamment, on peut utiliser des logs pour tracer tous les événements liés à la sécurité qui peuvent apparaître pendant toute la vie du produit. L'analyse continue des logs (depuis la plateforme de service, et potentiellement grâce à l'IA), va permettre de détecter les menaces dès qu'elles apparaissent en détectant des comportements anormaux.

Bonnes pratiques : réponse aux anomalies

- **La mise à jour du logiciel à distance**

Il est indispensable de pouvoir mettre à jour à distance le logiciel et/ou les éléments de sécurité (clés, certificats ...), pour corriger les failles de sécurité découvertes pendant toute la vie du produit. Mais il faut être absolument certain que la chaîne de mise à jour n'est pas corrompue, ce qui pourrait permettre à un attaquant de télécharger un logiciel malveillant dans l'objet connecté.

- **La correction des failles de sécurité**

Les failles de sécurité doivent être analysées, publiées (dès que possible sans générer de risque supplémentaire) et corrigées via des remote upgrades dès qu'une solution aura été identifiée. Il est à noter que ce mécanisme sera rendu obligatoire quand le *Cyber Resilience Act* entrera en vigueur en Europe.

Conclusion

En conclusion, il est essentiel de sécuriser l'ensemble de la chaîne de développement et de production du produit. Un attaquant ciblera le maillon faible, qui peut se trouver dans une mauvaise implémentation des algorithmes de cryptographie, une protection insuffisante de l'usine de fabrication, ou un processus de mise à jour logicielle à distance mal sécurisé.

L'approche "Secure By Design" permet de réduire considérablement les risques de sécurité. De plus en plus utilisée dans le développement des objets connectés, cette approche n'a pas de définition formelle, mais tous les acteurs qui s'y réfèrent mettent en avant les mêmes principes. Son objectif est d'aborder la sécurité de manière proactive plutôt que réactive. Il s'agit d'identifier dès la phase de conception les risques auxquels l'appareil sera exposé tout au long de sa vie, et de mettre en place des mesures proactives pour détecter et corriger les failles de sécurité dès que possible. Étant donné que les logiciels et les menaces évoluent dans le temps, cette approche ne s'arrête pas à la mise sur le marché mais se prolonge tout au long de la vie du produit. Les éléments clés de cette approche sont les suivants :

- Effectuer une analyse des risques dès la phase de conception pour identifier les menaces auxquelles l'objet sera exposé.
- Minimiser la surface d'attaque en désactivant toutes les interfaces inutilisées (consoles UART, ports TCP/UDP, JTAG, etc.).
- Authentifier les appareils autorisés à se connecter à la plateforme IoT pour éviter les connexions de faux appareils.
- Implémenter un contrôle d'accès aux ressources en appliquant le principe du moindre privilège, garantissant que chaque entité (objet connecté, utilisateur, etc.) n'a accès qu'aux ressources nécessaires.
- Rester vigilant vis-à-vis des services tiers, notamment les bibliothèques externes (open source ou propriétaires) intégrées dans le produit.
- Mettre en place une stratégie de correction des failles de sécurité tout au long de la vie du produit, notamment par des mises à jour logicielles.
- Mettre en place des mesures pour détecter et signaler les intrusions, par exemple en générant des logs en cas de comportement anormal et en analysant ces logs en continu.
- Établir une politique de divulgation des vulnérabilités.

Enfin, au-delà des recommandations de l'*ENISA*, et en attendant la publication de Standards harmonisés, les guides mis en ligne par *IOTSF*¹¹ fournissent une méthodologie détaillée pour analyser les risques et mettre en place des mesures pratiques pour gérer ces risques.

¹¹ <https://iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf>

A propos de TIDIWI

TIDIWI est une société de conseil spécialisée dans la conception et le développement de projets IOT. Notamment, TIDIWI a une forte expérience dans les protocoles de communication sans fil et dans les systèmes à ultra faible consommation d'énergie.

TIDIWI intervient sur des missions de conseil, de développement de logiciel embarqué, de développement de cartes électroniques, le management d'équipes de développement, la gestion de projets.

Pour plus d'information, visitez le site de Tidiwi : www.tidiwi.com

Ou contacter [thierry.didi\[at\]tidiwi\[dot\]com](mailto:thierry.didi@tidiwi.com)