Aperçu des lignes directrices de sécurité IoT

Aperçu des lignes directrices de sécurité IoT

Version 2.0

26 Octobre 2017

Ce document est une référence permanente non contraignante de la GSMA

Classification de sécurité : Non-confidentiel

Copyright

Avertissement

Avis antitrust

Table des Matières

1 Introduction

1.1 Aperçu général

L'émergence de l'Internet des Objets (IoT) crée de nouveaux fournisseurs de services qui cherchent à développer de nouveaux produits et services connectés et innovateurs. Les analystes ont prédit que des centaines de milliers de nouveaux services IoT connecteront des milliards de nouveaux dispositifs IoT au cours de la prochaine décennie. Cette croissance rapide de l'Internet des Objets représente une grande opportunité pour tous les membres du nouvel écosystème d'élargir leurs offres de services et d'augmenter leur base de clients.

Les analystes ont indiqué que les problèmes de sécurité entravent considérablement le déploiement de nombreux nouveaux services IoT et que la mise en place d'une connectivité de réseaux étendue (WAN) à une gamme de services IoT de plus en plus variée augmentera l'exposition de l'ensemble de l'écosystème à la fraude et aux attaques. Il y a déjà beaucoup de preuves qui montrent que les attaquants commencent à montrer un intérêt toujours plus grand dans ce domaine.

À mesure que ces nouveaux fournisseurs de services développent des services nouveaux et innovants pour des segments de marché particuliers, ils peuvent ne pas être conscients des menaces auxquelles leur service peut être confronté. Dans certains cas, le fournisseur de services n'a peut-être pas développé un service connecté à un réseau de communication ou à Internet et n'a peut-être pas accès aux compétences et à l'expertise nécessaires pour atténuer les risques liés à la connectivité Internet de ses dispositifs. En revanche, leurs adversaires comprennent les faiblesses de la technologie et de la sécurité, profitant rapidement si des vulnérabilités sont découvertes. Il y a une litanie d'attaques qui ont abouti à des dispositifs compromis. Les dispositifs compromis peuvent exposer des données, attaquer d'autres dispositifs ou provoquer des interruptions sur des services associés ou indépendants.

Alors que de nombreux fournisseurs de services, tels que ceux fournis pour l’industrie automobile, dans la santé, dans l'électronique pour le grand public et des services municipaux, considèrent que leurs exigences de sécurité spécifiques sont uniques à leur marché, ce n'est généralement pas le cas. Presque tous les services IoT sont construits à l'aide de composants de terminaux et de plates-formes de services qui contiennent des technologies similaires à de nombreuses autres solutions de communications, informatiques et solutions des technologies de l’information en général. En outre, les menaces auxquelles ces différents services sont confrontés et les solutions potentielles pour les atténuer sont généralement très similaires, même si la motivation de l'attaquant et l'impact des failles de sécurité réussies peuvent varier.

L'industrie des télécommunications, représentée par la GSMA, fournit depuis longtemps des produits et services sécurisés à ses clients. La fourniture de produits et de services sécurisés est autant un processus qu'un objectif en lui-même. La vigilance, l'innovation, la réactivité et l'amélioration continue sont nécessaires pour s'assurer que les solutions répondent aux menaces.

Pour garantir la sécurité des nouveaux services IoT sur le marché, les opérateurs de réseaux, ainsi que leurs partenaires dans les réseaux, services et équipements, souhaitent

partager leur expertise en matière de sécurité avec les prestataires de services qui souhaitent développer des services IoT.

La GSMA a donc créé cet ensemble de lignes directrices de sécurité au profit des fournisseurs de services qui cherchent à développer de nouveaux services IoT.

1.2 Ensemble de documents sur les lignes directrices de sécurité IoT de la GSMA

Ce document constitue la première partie d'un ensemble de documents de lignes directrices de sécurité de la GSMA destinés à aider l'industrie naissante de l 'Internet des Objets à établir une compréhension commune des problèmes de sécurité liés à l'IoT. L'ensemble des documents préconise une méthodologie pour développer des services IoT sécurisés afin de garantir la mise en œuvre des meilleures pratiques de sécurité tout au long du cycle de vie du service. Les documents fournissent des recommandations sur la façon d'atténuer les menaces et les faiblesses courantes en matière de sécurité au sein des services IoT.

La structure du jeu de documents de lignes directrices de sécurité de la GSMA est présentée ci-dessous. Il est recommandé que ce document, (c'est-à-dire le document de synthèse) soit lu comme une amorce avant de lire les pièces justificatives.

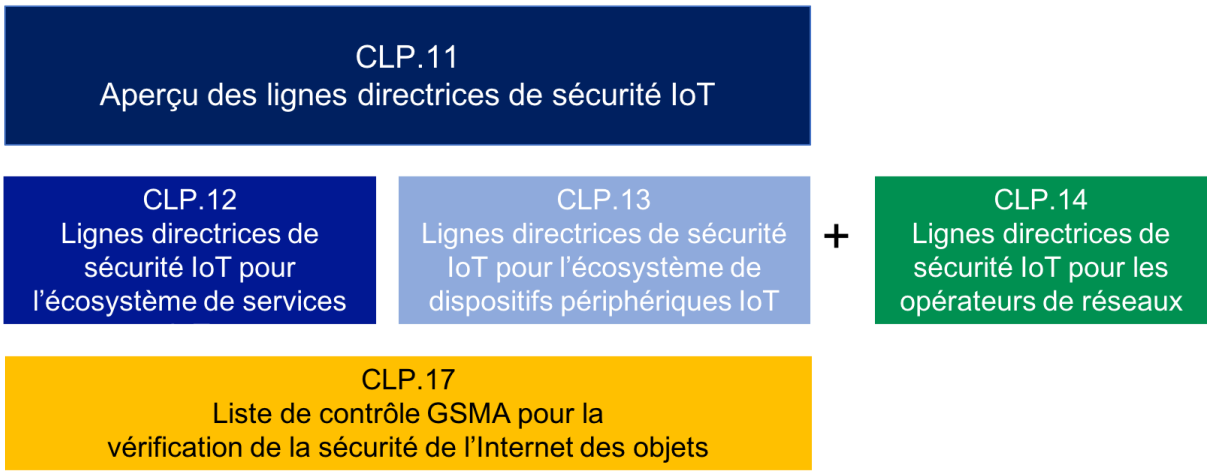

Figure 1 – Structure des documents sur les lignes directrices de sécurité de la GSMA

Les opérateurs de réseau, les fournisseurs de services IoT et les autres partenaires de l'écosystème IoT sont invités à lire le document GSMA CLP.14 "Lignes Directrices de sécurité IoT pour les opérateurs de réseau" [13] qui fournit des orientations de sécurité de haut niveau aux opérateurs de réseau qui veulent être au même temps fournisseurs de services IoT pour assurer la sécurité du système et la confidentialité des données.

1.2.1 Liste de contrôle pour l'évaluation de la sécurité IoT de la GSMA

Une liste de contrôle pour l'évaluation est fournie dans le document CLP.17 [16]. Ce document permet aux fournisseurs de produits, services et composants IoT d'autoévaluer la conformité de leurs produits, services et composants aux Lignes Directrices de Sécurité IoT de la GSMA.

L'achèvement d'une liste de contrôle d'évaluation de la sécurité de l'IoT de la GSMA [16] permettra à une entité de démontrer les mesures de sécurité qu'elle a prises pour protéger ses produits, services et composants contre les risques de cyber sécurité.

Les déclarations d'évaluation peuvent être faites en soumettant une déclaration rempli à la GSMA. Veuillez consulter le processus sur le site Web suivant de la GSMA:

https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

1.3 Objectif du document

L'objectif de l'ensemble de documents sur les lignes directrices en matière de sécurité de l'Internet des Objets est de fournir à l'exécutant d'une technologie ou d'un service IoT un ensemble de lignes directrices pour la conception d'un produit sécurisé. Pour accomplir cette tâche, ce document servira de modèle général pour interpréter les aspects d'une technologie ou d'un service qui sont pertinents pour l'exécutant. Une fois ces aspects, ou composants, identifiés, l'exécutant peut évaluer les risques associés à chaque composant et déterminer comment les compenser. Chaque composant peut être décomposé en sous-composants, où des risques plus granulaires seront décrits. Chaque risque doit se voir attribuer une priorité, afin d'aider le responsable de la mise en œuvre à déterminer le coût de l'attaque, ainsi que le coût de l'assainissement, et le coût, le cas échéant, de ne pas prendre en compte le risque.

La portée de ce document est limitée aux recommandations relatives à la conception et à la mise en œuvre des services IoT.

Ce document ne vise pas à créer de nouvelles spécifications ou normes IoT, mais se référera aux solutions, normes et bonnes pratiques actuellement disponibles.

Ce document n'a pas pour but d'accélérer l'obsolescence des services IoT existants.

Il est noté que le respect des lois et règlements nationaux pour un territoire particulier peut, si nécessaire, annuler les lignes directrices énoncées dans ce document.

1.4 Public visé

Le principal public visé par ce document est:

- Fournisseurs de services IoT - entreprises ou organisations qui cherchent à développer de nouveaux produits et services connectés innovateurs. Parmi les nombreux domaines dans lesquels les fournisseurs de services IoT opèrent, figurent les maisons intelligentes, les villes intelligentes, l'automobile, le transport, la santé, les services publics et l'électronique grand public.
- Fabricants de dispositifs IoT - Fournisseurs de dispositifs IoT aux fournisseurs de services IoT pour activer les services IoT.
- Les développeurs IoT - créent des services IoT pour le compte des fournisseurs de services IoT.
- Les opérateurs de réseau qui sont eux-mêmes des fournisseurs de services IoT ou qui construisent des services IoT au nom des fournisseurs de services IoT.

1.5 Definitions

Terme	Description
Nom du point d'accès réseau	Identifiant d'un point de connexion au réseau, auquel un dispositif périphérique se rattache. Ils sont associés à différents types de services et, dans de nombreux cas, sont configurés par l'opérateur de réseau.
Attaquant	Un pirate informatique, un agent de menace, un acteur de la menace, un fraudeur ou toute autre menace malveillante envers un service IoT généralement dans le but de récupérer, détruire, restreindre ou falsifier des informations. Cette menace pourrait provenir d'un criminel, du crime organisé, du terrorisme, de gouvernements hostiles et de leurs agences, d'espionnage industriel, de groupes de piratage, de militants politiques, de pirates informatiques, de chercheurs, ainsi que d'atteintes involontaires à la sécurité et à la vie privée.
Cloud	Un réseau de serveurs distants sur Internet qui hébergent, stockent, gèrent et traitent les applications et leurs données.
Dispositif Périphérique Complexe	Ce modèle de Dispositif Périphérique dispose d'une connexion permanente à un serveur principal via une liaison de communications longue distance, telle qu'une connexion cellulaire, par satellite ou câblée telle qu'Ethernet. Voir CLP.13 [4] pour plus d'informations.
Composants	Fait référence aux composants contenus dans les documents CLP.12 [3] et CLP.13 [4]
Carte de SIM embarquée	Une carte SIM qui n'est pas destinée à être retirée ou remplacée dans un appareil, et qui permet le changement sécurisé des profils selon la norme GSMA SGP.01 [2].
Dispositif Périphérique	Terme générique désignant un dispositif IoT léger, complexe, une passerelle ou un autre périphérique connecté. Voir CLP.13 [4] pour plus d'informations.
Écosystème de Dispositifs Périphérique	Toute configuration qu'assemble des Dispositifs IoT Périphériques de faible complexité, de périphériques complexe et de passerelles qui relient le monde physique au monde numérique d´une manière innovante. Voir la section 4.2 pour plus d'informations.
Internet des Objets	L'Internet des objets (IoT) décrit la coordination de plusieurs machines, appareils et appareils connectés à Internet via plusieurs réseaux. Ces dispositifs comprennent des objets du quotidien tels que les tablettes et l'électronique grand public, ainsi que d'autres machines telles que des véhicules, des moniteurs et des capteurs dotés de capacités de communication leur permettant d'envoyer et de recevoir des données.
Service IoT	Tout programme informatique qui tire parti des données des périphériques IoT pour rendre un service.
Fournisseurs de Service IoT	Entreprises ou organisations qui cherchent à développer de nouveaux produits et services connectés innovants.
Opérateur de réseau	L'opérateur et le propriétaire du réseau de communication qui connecte un dispositif périphérique IoT à l'écosystème de service IoT.
Racine organisationnelle de la confiance	Un ensemble de politiques et de procédures cryptographiques qui régissent la façon dont les identités, les applications et les communications peuvent et doivent être sécurisées par cryptographie.

Terme	Description
Recommandations	Fait référence aux recommandations contenues dans les documents CLP.12 [3] et CLP.13 [4]
Risque	Fait référence aux risques contenus dans les documents CLP.12 [3] et CLP.13 [4]
Tâches de sécurité	Fait référence aux tâches de sécurité contenues dans les documents CLP.12 [3] et CLP.13 [4]
Point d'accès au service	Un point d'entrée dans l'infrastructure back-end d'un service IoT via un réseau de communication.
Écosystème de Services IoT	Ensemble de services, plates-formes, protocoles et autres technologies requis pour fournir des fonctionnalités et collecter des données à partir des dispositifs périphériques déployés sur le terrain. Voir la section 3.1 pour plus d'informations.
Module d'identité d'abonné (SIM)	La carte à puce utilisée par un réseau mobile pour authentifier les dispositifs de connexion au réseau mobile et d'accès aux services de réseau.
UICC	Plateforme d'élément sécurisé spécifiée dans la norme ETSI TS 102 221 et pouvant prendre en charge plusieurs applications d'authentification de réseau ou de service normalisées dans des domaines de sécurité crypto graphiquement séparés. Il peut être incorporé dans des facteurs de forme incorporés spécifiés dans la norme ETSI TS 102 671.

1.6 Abréviations

Terme	Description
3GPP	Projet de Partenariat sur la Troisième Génération (« 3rd Generation Project Partnership »)
API	Interface de Programmation d'Applications (« Application Program Interface »)
APN	Nom du Point d'Accès (« Access Point Name »)
CERT	Équipe d'Intervention d'Urgence Informatique (« Computer Emergency Response Team »)
CLP	Programme de la Vie Connectée (« GSMA's Connected Living Programme »)
CPU	Unité centrale de traitement (« Central processing Unit »)
EAP	Protocole d'Authentification Extensible (« Extensible Authentication Protocol »)
EEPROM	Mémoire Morte Effaçable Électriquement et Programmable (« Electrically Erasable Programmable Read-Only Memory »)
GBA	Architecture d'Amorçage Générique (« Generic Bootstrapping Architecture »)
GPS	Système de positionnement global (« Global Positioning System »)
GSMA	Association GSM (« GSM Association »)
GUI	Interface Graphique d'Utilisateur (« Graphic User Interface »)
HIPAA	Loi sur la Transférabilité et la Responsabilité en Matière d'Assurance-Maladie (« Health Insurance Portability and Accountability Act »)
IoT	Internet des Objets (« Internet of Things »)
LPWA	Réseau de Longue Portée et faible puissance (« Low Power Wide Area »)
LTE-M	Évolution à long terme pour les machines (« Long Term Evolution for Machines »)

Terme	Description
NB-IoT	Bande étroite- Internet des Objets (« Narrowband-Internet of Things »)
NIST	Institut National des Normes et de la Technologie (« National Institute of Standards and Technology »)
OBD	Diagnostic à Bord (« On Board Diagnostics »)
OCTAVE	Évaluation des menaces, des actifs et des vulnérabilités critiques sur le plan opérationnel (« Operationally Critical Threat, Asset, and Vulnerability Evaluation »)
OMA	Alliance Mobile Ouverte (« Open Mobile Alliance »)
PIA	Évaluation d'Impact sur la Vie Privée (« Privacy Impact Assessment »)
PII	Informations Personnelles Identifiables (« Personally Identifiable Information »)
RAM	Mémoire Vive (« Random Access Memory »)
SIM	Module d'Identité d'Abonné (« Subscriber Identity Module »)

1.7 References

Ref	Numéraux du Doc.	Titre
[1]	n/a	The Mobile Economy 2017 http://www.gsmamobileeconomy.com/
[2]	SGP.01	Embedded SIM Remote Provisioning Architecture https://www.gsma.com/iot/embedded-sim/
[3]	CLP.12	IoT Security Guidelines for IoT Service Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[4]	CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[5]	n/a	NIST Risk Management Framework http://csrc.nist.gov/groups/SMA/fisma/framework.html
[6]	CMU/SEI-2007-TR-012	Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process http://www.cert.org/resilience/products-services/octave/
[7]	Not Used	Not Used
[8]	TS 33.220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) www.3gpp.org
[9]	RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) www.ietf.org
[10]	n/a	Conducting privacy impact assessments code of practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Ref	Numéraux du Doc.	Titre
[11]	n/a	Open Mobile Alliance http://openmobilealliance.org/
[12]	n/a	oneM2M Specifications http://www.onem2m.org/
[13]	CLP.14	IoT Security Guidelines for Network Operators https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[14]	GE.11-13201	Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[15]	n/a	Right to Internet Access https://en.wikipedia.org/wiki/Right_to_Internet_access
[16]	CLP.17	GSMA IoT Security Assessment Checklist https://www.gsma.com/iot/iot-security-assessment/

2 Les défis créés par l'Internet des Objets

Il y a plusieurs années, un rapport spécial des Nations Unies recommandait qu'Internet soit un droit humain fondamental et que tous les peuples du monde aient accès aux services à haut débit [14]. Plus récemment, des lois ont été adoptées dans des pays tels que la France, la Grèce, l'Espagne et d'autres [15], pour garantir un accès à Internet largement disponible et/ou empêcher l'État de restreindre déraisonnablement l'accès à l'information et à Internet.

Ces déclarations sont le résultat des changements sociaux et technologiques rapides qui ont permis la croissance d'Internet. Cela a fait d'Internet un mode de vie, l'une des principales sources de toutes les catégories d'informations, et la méthode la plus courante pour maintenir la connectivité avec les gens en général, les amis et les collègues. L'Internet n'est pas simplement une technologie, il est devenu une partie de nous.

De concert avec le désir croissant de maintenir la connectivité, une explosion technologique s'est produite au cours des dernières années. Alors que les technologues déclarent que « l'Internet des Objets arrive» depuis plus d'une décennie, l'intérêt pour l'accès omniprésent à l'information et le modèle de coûts requis pour le faire ne se sont pas encore fondus dans un modèle commercial pratique au moins dans les cinq dernières années. À ce stade, les coûts des composantes ont fortement diminué, tandis que l'accès aux services sans fil et la vitesse de ces services ont considérablement augmenté. Les protocoles, la durée de vie de la batterie et même les modèles commerciaux ont tous évolué pour répondre à la demande sans cesse croissante d'informations et de connectivité.

Et c'est essentiellement ce qu'est l'Internet des Objets. Ce n'est pas vraiment une question qui vise uniquement aux “choses”. C'est à propos de nous. L'Internet de nous. Les expériences humaines et numériques ne reposent plus côte à côte, elles sont toujours plus étroitement liées à ce nouveau mode de vie.

Et parce que l'expérience physique humaine est plus liée au monde numérique que jamais, elle doit être protégée, car la sécurité numérique a plus que jamais un impact direct sur le monde physique. L'Internet des objets est une excellente opportunité pour le monde d'avancer ensemble, afin de créer des bases de données toujours plus vastes de connaissances, d'expériences partagées et d'explosions d'innovation. Mais pour que cela fonctionne efficacement, les technologies qui génèrent cette connectivité doivent être sécurisées, afin d'assurer la confidentialité, la fiabilité et la qualité des services nécessaires pour que cette grande utilité, ce besoin fondamental impératif, soit disponible pour tous ceux qui en ont besoin.

Pour que l'Internet des Objets évolue efficacement, nous devons résoudre les problèmes de sécurité inhérents à sa croissance. Ces défis sont :

- Disponibilité : assurer une connectivité constante entre les dispositifs périphériques et leurs services respectifs
- Identité : authentification des dispositifs périphériques, des services et du client ou de l'utilisateur final qui administre souvent ce dispositif périphérique
- Confidentialité : réduire le potentiel de dommages pour les utilisateurs finaux
- Sécurité : assurer que l'intégrité du système peut être vérifiée, suivie et surveillée

2.1 Le défi de la disponibilité

Pour que l'Internet des Objets évolue à son rythme, les dispositifs périphériques doivent pouvoir se communiquer en permanence entre eux, avec les utilisateurs finaux et avec les services back-end. Pour accomplir cela, de nouvelles technologies telles que NB-IoT et LTE-M sont déployées, ce qui permet une connectivité persistante pour les dispositifs de faible puissance. Cela correspond bien au défi de l'accès Internet omniprésent dans le monde moderne. Pour que cela réussisse, plusieurs questions doivent être répondues:

- Comment les réseaux LPWA (« Low Power Wide Area ») (par exemple NB-IoT et LTE-M) peuvent-ils être déployés et exploités avec un niveau de sécurité similaire à celui des systèmes cellulaires traditionnels ?
- Comment plusieurs opérateurs mobiles peuvent-ils supporter le même niveau de sécurité dans leurs réseaux quand les dispositifs périphériques ou terminaux IoT migrent à travers les limites du réseau ?
- Comment la confiance réseau peut-elle être transmise aux dispositifs périphériques sur leurs réseaux capillaires qui s'appuient sur des passerelles pour la communication ?
- Comment les contraintes d'alimentation des dispositifs périphériques légers peuvent-elles être traitées dans des environnements de communications sécurisés ?

2.2 Le défi de l'identité

Pour qu'un Dispositif Périphérique fonctionne dans un écosystème de produits ou de services IoT, il doit être capable de s'identifier de manière sécurisée à ses pairs et à ses services. Cet aspect critique et fondamental de la technologie IoT garantit que les services et les pairs sont en mesure de garantir à quoi - et à qui - les données sont livrées. L'accès à l'information et aux services n'est pas le seul problème directement lié à l'identité. Nous devons également poser les questions :

- L'utilisateur qui exploite le dispositif périphérique peut-il être fortement associé à l'identité de ce même dispositif ?
- Comment les services et les pairs dans la communication peuvent-ils vérifier l'identité de l'utilisateur final en vérifiant l'identité du dispositif périphérique ?
- La technologie de sécurité du dispositif périphérique sera-t-elle capable d'authentifier de manière sécurisée les pairs et les services ?
- Les services et les pairs malveillants peuvent-ils usurper l'identité des services autorisés et des pairs ?
- Comment l'identité d'un appareil est-elle protégée contre toute altération ou manipulation ?
- Comment le dispositif périphérique et le réseau peuvent-ils garantir qu'un service IoT est autorisé à accéder ce même dispositif dans l'écosystème IoT ?

2.3 Le défi de la confidentialité

La confidentialité ne peut plus être considérée comme un ajout aux produits et services existants. Parce que le monde physique est directement affecté par les actions du monde numérique, la protection de la vie privée doit être intégrée dans les produits, afin que chaque action soit autorisée et chaque identité vérifiée tout en garantissant que ces actions et les métadonnées associées sont pas exposé à des parties non autorisées. Cela ne peut être réalisé qu'en définissant l'architecture appropriée pour un produit ou un service, et il est exceptionnellement difficile et coûteux d'effectuer un travail rétroactif.

Les dispositifs médicaux, les solutions automobiles, les systèmes de contrôle industriel, la domotique, les systèmes de construction et de sécurité, etc., ont tous un impact direct sur la vie physique des êtres humains. Il est du devoir des ingénieurs de maintenir ces produits et services au niveau d'assurance le plus élevé possible, de réduire le risque de dommages physiques ainsi que l'exposition de données pertinentes à la vie privée.

Par conséquent, nous devons nous demander comment les données par rapport aux renseignements personnels affectent non seulement l'utilisateur final, mais aussi comment les technologies IoT sont conçues:

- L'identité d'un dispositif périphérique est-elle exposée à des utilisateurs non autorisés ?
- Est-ce que les identificateurs de service ou dispositifs périphériques IoT uniques peuvent permettre à cet utilisateur final ou à ce dispositif périphérique d'être surveillé ou suivi physiquement ?
- Les données émanant d'un service du dispositif périphérique ou d'un service IoT indiquent-elles ou sont-elles directement associées à des attributs physiques de l'utilisateur final tels que l'emplacement, l'action ou un mode de fonctionnement concret du dispositif, tels que « sommeil » ou « en-veille » ?
- La confidentialité et l'intégrité sont-elles utilisées avec une sécurité suffisante pour garantir que les modèles du texte chiffré qui en résulte ne peuvent pas être observés ?
- Comment le produit ou le service stocke-t-il ou gère-t-il des données personnelles identifiables (PII) spécifiques à l'utilisateur ?
- L'utilisateur final peut-il contrôler le stockage ou l'utilisation des données personnelles dans le service ou le produit IoT ?

- Les clés de sécurité et les algorithmes de sécurité utilisés pour sécuriser les données peuvent-ils être actualisés ?

2.4 Le défi de la sécurité

Bien que la sécurité sur Internet se soit considérablement améliorée au cours des dernières décennies, il y a eu plusieurs lacunes importantes dans la santé globale de la technologie moderne. Ces lacunes ont été plus évidentes dans les systèmes embarqués et dans les services de cloud - les deux principaux composants de la technologie IoT.

Pour que l'IoT évolue sans exposer des groupes massifs d'utilisateurs et de systèmes physiques à des risques, les pratiques de sécurité de l'information doivent être appliquées sur les deux composants plus importants d'un écosystème IoT : les dispositifs périphériques et les Services IoT.

- Les meilleures pratiques en matière de sécurité sont-elles intégrées sur le produit ou sur le service au début du projet ?
- Le cycle de vie de la sécurité est-il intégré au cycle de vie du logiciel ou du développement du produit ?
- La sécurité de l'application est-elle appliquée aux services et aux applications s'exécutant sur le système intégré ?
- Une base de calcul sécurisée (TCB) est-elle implémentée à la fois dans le dispositif périphérique et dans l'écosystème de service ?
- Comment la TCB impose-t-elle l'auto-vérification des images logicielles de l'application et des services ?
- Le service ou dispositif périphérique IoT peuvent-ils détecter s'il existe une anomalie dans sa configuration ou son application ?
- Comment les dispositifs périphériques sont-ils surveillés en cas d'anomalies indiquant un comportement malveillant ?
- Comment l'authentification et l'identité sont-elles liées au processus de sécurité du produit ou du service ?
- Quel plan d'intervention en cas d'incident est défini pour les anomalies détectées indiquant un compromis ?
- Comment les services et les ressources sont-ils segmentés pour garantir une solution à un compromis rapide et efficace ?
- Comment les services et les ressources sont-ils restaurés après un compromis ?
- Une attaque peut-elle être repérée ?
- Un composant du système IoT compromis peut-il être repéré ?
- Comment les clients peuvent-ils signaler des problèmes de sécurité ?
- Les dispositifs périphériques peuvent-ils être mis à jour ou corrigés pour supprimer les vulnérabilités ?

3 La solution mobile

Bien qu'il y ait eu une myriade de technologies qui offrent des solutions de connectivité pour l'IoT, aucune ne façonne l'avenir de l'IoT mieux que les réseaux mobiles. Les réseaux mobiles ont offert les premiers services sans fil aux consommateurs et à l'industrie il y a plus de vingt ans et ont mis en place depuis des services fiables, disponibles, sécurisés et rentables. L'industrie de la téléphonie mobile possède une vaste expérience de la

disponibilité des réseaux en raison de la nature volatile des réseaux radio sans fil gérés sur de longues distances. L'identité du réseau a été un défi qui a engendré de nombreuses normes, technologies de dispositifs, protocoles et modèles analytiques. La vie privée et la sécurité sont des préoccupations constantes de l'industrie de la téléphonie mobile, qui a travaillé pour réduire le potentiel d'abus, de vol d'identité et de fraude dans toutes les technologies mobiles.

L'industrie de la téléphonie mobile offre des technologies de réseau sans fil à faible consommation d'énergie (LPWA) basées sur des normes, appelées NB-IoT et LTE-M, pour couvrir les besoins des applications et des services IoT. Ces technologies de réseau LPWA offrent la même (et dans de nombreux cas, une plus grande) connectivité sans fil des réseaux mobiles traditionnels à une fraction de la puissance requise pour communiquer efficacement les données du service IoT. De nombreux opérateurs de réseaux déploient des services LPWA, de sorte que NB-IoT et LTE-M deviendront les normes de facto pour le déploiement du réseau LPWA.

De plus amples informations sur le déploiement des réseaux NB-IoT et LTE-M dans les régions du monde peuvent être trouvées sur le site Web de la GSMA : https://www.gsma.com/iot/mobile-iot-initiative/

3.1 Comment répondre au défi de la disponibilité

Selon le rapport "The Mobile Economy 2017" de la GSMA [1] :

- À la fin de l'année 2016, les deux tiers de la population mondiale avaient un abonnement mobile, soit un total de 4,8 milliards d'abonnés uniques. D'ici 2020, près des trois quarts de la population mondiale, soit 5,7 milliards de personnes, seront abonnés aux services mobiles.
- Le passage aux réseaux haut débit mobiles et aux smartphones continue de prendre de l'ampleur. Les connexions haut débit mobiles (technologies 3G et 4G) représentaient 55% du nombre total de connexions en 2016 - un chiffre proche des trois quarts de la base de connexions d'ici 2020. La proportion de connexions 4G devrait presque doubler, passant de 23% à 41% d'ici la fin de la décennie.
- 2,3 milliards de connexions haut débit mobile supplémentaires sont prévues entre 2016 et 2020, la proportion du total passant à 73%. La migration rapide vers la 4G est restée un élément clé en 2016, les connexions 4G ayant augmenté de 55% sur l'année pour atteindre 1,7 milliard. Par conséquent, d'ici 2020, la 2G ne sera plus la technologie dominante en termes de connexions.
- Le marché mondial des dispositifs LPWA est vaste, totalisant environ 1,4 milliard de connexions d'ici à 2020, et certains observateurs de l'industrie en prévoient 5 milliards d'ici 2022.

3.2 Comment répondre au défi de l'identité

La gestion des identités a été un défi pendant des décennies et a considérablement renforcé les normes et les offres technologiques de l'industrie mobile. Alors que l'industrie du mobile est généralement associée à la carte SIM démontable, la GSMA a créé une solution basée sur SIM appelée « Embedded SIM Remote Provisioning Architecture » [2], utilisable en IoT pour permettre une intégration plus poussée des composants dans les appareils, une réduction des coûts de production et une gestion de la connectivité via les plates-formes

“Over-The-Air” (OTA) pour permettre la connectivité des dispositifs périphériques IoT pendant toute leur durée de vie.

Les technologies d'identité, telles que la carte SIM embarquée, sont conçues comme des ancres de confiance intégrant la sécurité par défaut. Elles sont fabriqués pour résister à des attaques telles que :

- Glitching
- Analyse des canaux latéraux
- Interception passive de données
- Altération physique
- Vol d'identité

Un excellent progrès pour cette technologie déjà sécurisée est que les nouvelles générations de ces ancres de confiance intègrent un ajout important dans le paysage IoT. Ces technologies seront à double usage. Elles ne seront pas simplement utilisées pour vérifier la sécurité du réseau, elles seront également capables de sécuriser les communications des applications et l'application elle-même, de la même manière que les ancres traditionnelles de confiance informatique traditionnelles.

Cette capacité d'utilisation double sera encore renforcée par l'intégration des spécifications de sécurité de l'industrie mobile telles que celles fournies par 3GPP GBA [8], OMA [11], oneM2M [12] et d'autres. Ces technologies permettront de provisionner de manière sécurisée les appareils sur le terrain, de sécuriser les mises à jour du firmware sur des protocoles OTA et de gérer les capacités et l'identité des appareils.

Ces technologies, lorsqu'elles sont utilisées ensemble, faciliteront les processus d'ingénierie actuellement complexes et les combineront en un seul composant. Au lieu que les ingénieurs d'application construisent des technologies complexes qu'ils doivent eux-mêmes gérer, l'opérateur de réseau, qui gère déjà l'identité du réseau, peut le faire pour le compte de l'application. Cela réduit non seulement la complexité de l'ingénierie, mais aussi les exigences de gestion quotidiennes de l'entreprise.

3.3 Comment répondre au défi de la confidentialité et de la sécurité

En plus des capacités de la carte SIM, l'industrie de la téléphonie mobile a développé des protocoles, des processus et des systèmes de surveillance résilients pour assurer la sécurité et réduire le potentiel de fraude et d'autres activités malveillantes. Par exemple, les technologies 3G et 4G utilisent l'authentification mutuelle pour vérifier l'identité des terminaux et du réseau. Ce processus permet de s'assurer que les adversaires sont incapables d'intercepter les communications.

En outre, la technologie réseau peut être sécurisée grâce à l'utilisation de la carte SIM et de technologies telles que GBA [8] ou EAP-SIM [9]. En utilisant ces technologies, la carte SIM peut être fournie avec une clé de sécurité de session qui peut être utilisée dans des communications entre dispositifs sur des réseaux d'application en utilisant des protocoles bien connus. Ce processus peut réduire le risque que des adversaires manipulent le protocole d'application pour compromettre les dispositifs périphériques ou les services. Ainsi, il est possible de sécuriser à la fois le réseau et l'application avec ce modèle.

4 Le modèle IoT

La figure ci-dessous montre que le modèle d'IoT standard utilisé dans ces documents est décrit comme des composants des écosystèmes de Services et de Dispositifs Périphériques. Chaque composant est composé de sous-composants, qui sont détaillés dans un document qui se concentre uniquement sur le composant principal. Par exemple, le Dispositif Périphérique et ses risques respectifs sont décrits dans le document Écosystème de Dispositifs Périphériques IoT [3] fourni dans cet ensemble de documents et les composants des Services sont décrits dans le document Écosystème de Services IoT [4].

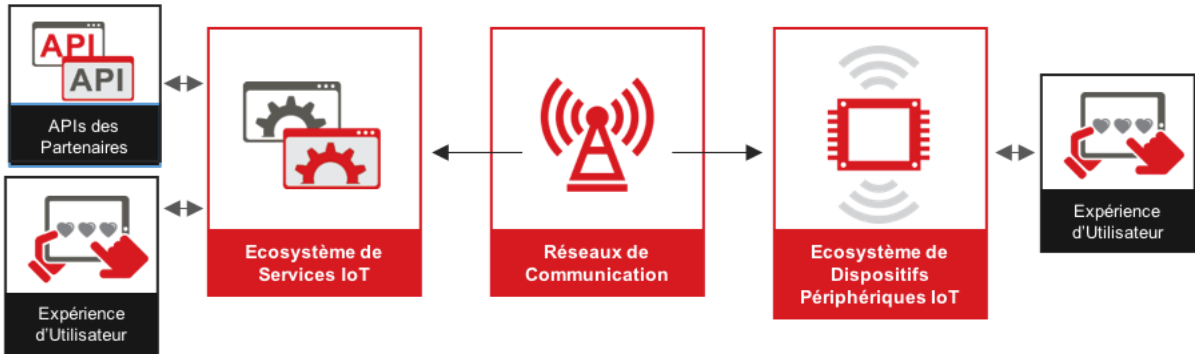

Figure 2 – Exemple du modèle IoT

Dans presque tous les modèles de service ou de produit IoT modernes, ce diagramme définit les principaux composants requis lors du déploiement d'une technologie prête pour la production.
Les composants du réseau de communication sont inhérents à l'IoT et, pour les besoins de ce modèle, fournissent la connexion entre les deux écosystèmes avec chaque « extrémité » du lien de communication discutée dans les documents appropriés : Écosystème de Dispositifs Périphériques IoT et Écosystème de Services IoT.
Des recommandations spécifiques pour les opérateurs de réseau avec les lignes directrices sur la sécurité du réseau figurent dans le document : « Lignes Directrices de Sécurité de l'IoT pour les Opérateurs de Réseau » de la GSMA [13].

4.1 Écosystème de services IoT

L'Écosystème de Services IoT représente l'ensemble des services, plateformes, protocoles et autres technologies requis pour fournir des fonctionnalités et collecter des données à partir des dispositifs périphériques déployés sur le terrain. Cet écosystème collecte généralement les données des dispositifs périphériques et les stocke dans son environnement de serveurs. Ces données peuvent être rendues à l'utilisateur en transmettant des représentations visuelles élégantes des données à diverses interfaces utilisateurs. Ces données, souvent sous forme de métriques, de paramètres ou de commandes, peuvent également être transmises à des tiers autorisés via une API (par exemple oneM2M [12]) provenant de l'infrastructure de services, ce qui est généralement la façon dont les services IoT monétisent le service.

Les lignes directrices de sécurité de l'Écosystème de Services à utiliser en conjonction avec le processus décrit dans ce document d'aperçu peuvent être trouvées dans CLP.12 Lignes Directrices de Sécurité IoT pour l'Écosystème de Services IoT [4].

4.2 Écosystème de dispositifs périphériques IoT

L'Écosystème des Dispositifs Périphériques IoT [4] se compose de dispositifs de faible complexité, de dispositifs riches ou complexes et de passerelles qui relient le monde physique au monde numérique via plusieurs types de réseaux capillaires câblés et sans fil. Des exemples de dispositifs périphériques communs sont les capteurs de mouvement, les verrous de porte numériques, les systèmes télématiques d'automobiles, les systèmes de contrôle industriels pilotés par capteurs, et plusieurs autres... Les dispositifs périphériques collectent des métriques à partir de l'environnement physique qui les entoure et transmettent ces données sous différents formats via un réseau capillaire ou cellulaire à l'écosystème de services, recevant souvent des instructions ou des actions déterminées en réponse. Ils peuvent également inclure des interfaces utilisateur riches qui rendent les données obtenues soit par le dispositif périphérique lui-même, soit à partir de l'Écosystème de Services.

Les lignes directrices sur la sécurité de l'Écosystème des Dispositifs Périphériques à utiliser en conjonction avec le processus décrit dans ce document d'aperçu se trouvent dans CLP.13 Lignes Directrices de Sécurité IoT pour l'Écosystème de Dispositifs Périphériques IoT [13].

5 Évaluations des risques

Bien que le concept d'évaluation des risques existe depuis de nombreuses décennies, de nombreuses entreprises sont plus familiarisées avec l'application du concept aux risques commerciaux généraux qu'à la sécurité de l'information. Cependant, un processus d'évaluation des risques liés à la sécurité de l'information est également impératif pour assurer le fonctionnement sécurisé et la longévité technologique d'une solution pour une entreprise. Évidemment, dans les technologies de l'Internet des Objets, où l'équipe d'ingénierie est un élément essentiel à la réussite de l'entreprise, le processus d'évaluation des risques devrait être la première démarche de l'élaboration d'une pratique de sécurité.

Alors que chaque organisation devrait créer une perspective granulaire du risque technologique, il existe des questions de haut niveau qui servent de point de départ pour le processus d'évaluation des risques.

- Quels actifs (numériques ou physiques) doivent être protégés ?
- Quels groupes de personnes (tangibles ou intangibles) sont des acteurs potentiels de la menace ?
- Qu'est-ce qu'une menace pour l'organisation ?
- Qu'est-ce qu'une vulnérabilité ?
- Quel serait le résultat si un actif protégé était compromis ?
- Quelle est la probabilité que l'actif soit compromis ?
- Quel serait le résultat lorsqu'il est mis en contexte avec différents groupes d'attaquants ?
- Quelle est la valeur de l'actif pour l'organisation et ses partenaires ?
- Quel est l'impact sur la sécurité de l'actif compromis ?
- Que peut-on faire pour corriger ou atténuer le potentiel de vulnérabilité ?
- Comment les nouvelles lacunes ou en évolution dans la sécurité peuvent-elles être surveillées ?

- Quels risques ne peuvent être résolus et que signifient-ils pour l'organisation ?
- Quel budget devrait être appliqué pour la réponse aux incidents, la surveillance et la réparation des risques ?

Ces points de départ aideront les équipes d'ingénierie et de la technologie de l'information à travailler plus efficacement avec l'organisation. L'objectif est de s'assurer que le côté technique de l'entreprise se mettent d'accord sur les risques, les valeurs et les mesures correctives avec la direction de l'entreprise. Forcer les équipes à travailler ensemble aidera à créer une perspective plus réaliste non seulement du risque pour l'entreprise, mais aussi de la valeur des actifs. Cela affectera directement le budget qui devrait être utilisé pour résoudre les lacunes en matière de sécurité.

Il y a des risques qui ne peuvent tout simplement pas être résolus. Certains de ces risques seront abordés dans ces lignes directrices. L'entreprise devrait évaluer ces risques et déterminer s'ils sont acceptables. Cela fournira à l'entreprise une compréhension réaliste de ses limites, des limites de la technologie et de sa capacité à réagir à certains types de menaces. Il n'y a rien de plus épuisant sur le plan monétaire que de supposer que toutes les lacunes en matière de sécurité peuvent être résolues d'une manière rentable.

5.1 Objectif

Le but d'une évaluation des risques est de créer (ou de mettre à jour) un ensemble de politiques, de procédures et de contrôles qui corrigent, surveillent et répondent aux lacunes de sécurité rencontrées par l'organisation technique de l'entreprise. Le résultat de l'évaluation des risques devrait aider l'entreprise à ajuster non seulement sa technologie, mais aussi la façon dont la technologie est gérée, conçue et déployée. Une fois que le résultat de l'évaluation des risques décrit plus adéquatement la valeur de l'information et des ressources utilisées par l'organisation, l'activité globale peut être sécurisée grâce à l'amélioration de son personnel, de ses processus et de ses politiques.

Rappelez-vous, les principaux avantages de l'utilisation d'une évaluation des risques sont les suivants :

- Informer le personnel
- Amélioration des processus
- Définition (ou mise à jour) des politiques
- Exécution de la correction des défauts
- Surveillance des nouvelles lacunes
- Améliorer le produit ou le service

Cela aide essentiellement l'organisation à mettre en place une plateforme de base pour la sécurité du personnel et des processus. Cette plateforme devrait ensuite être intégrée dans un cycle qui évalue et affine constamment les rôles et responsabilités de l'organisation.

5.2 Références du modèle de risques

Plutôt que d'essayer de définir un processus d'évaluation des risques et de modélisation des menaces ici, veuillez passer en revue les références suivantes pour une description et une présentation adéquate du processus d'évaluation des risques :

- Cadre de gestion des risques de l'Institut National des Normes et Technologies (NIST) [5]
- Le modèle OCTAVE de l'Équipe d'Intervention en cas d'Urgence Informatique (CERT) [6]

6 Considérations sur la confidentialité

De nombreux services et produits IoT seront conçus pour créer, collecter ou partager des données. Certaines de ces données peuvent ne pas être considérées comme des « données personnelles » ou avoir un impact sur la vie privée d'un consommateur et ne sont donc pas soumises aux lois sur la protection des données et la vie privée. Ces données peuvent inclure des informations sur l'état physique des machines, des données de diagnostic internes ou des mesures concernant l'état du réseau.

Cependant, de nombreux services IoT impliqueront des données concernant ou liés à des consommateurs individuels et seront soumis aux lois générales sur la protection des données et la vie privée. Lorsque les opérateurs mobiles fournissent des services IoT, ils sont également soumis à des règles de confidentialité et de sécurité spécifiques aux télécommunications. Les services IoT ciblés sur les « consommateurs » impliquent probablement la génération, la distribution et l'utilisation de données détaillées susceptibles d'avoir un impact sur la vie privée des individus. Par exemple, tirer des conclusions sur leur santé ou développer des profils en fonction de leurs habitudes d'achat et de leurs emplacements. Au fur et à mesure que les services IoT des consommateurs gagneront en popularité, davantage de données sur les consommateurs seront créées, analysées en temps réel et partagées entre plusieurs parties à travers les frontières nationales.

Lorsque les données concernent des individus spécifiques, cet écosystème complexe et « connecté » peut susciter des inquiétudes de la part du consommateur sur :

- Qui collecte, partage et utilise les données des individus ?
- Quelles données spécifiques sont acquises ?
- D'où proviennent les données (quelles technologies ou interfaces) ?
- Quand les données sont-elles collectées ?
- Pourquoi les données sont-elles collectées auprès de l'utilisateur ?
- Comment la vie privée (et pas seulement la sécurité) des informations des individus est-elle assurée ?
- Les individus contrôlent-ils la façon dont leurs données sont partagées et comment les entreprises vont les utiliser ?

Tous les fournisseurs de services IoT qui s'appuient sur les données des consommateurs - ainsi que les entreprises partenaires qui capturent ou utilisent ces données - ont l'obligation de respecter la vie privée des individus et de sécuriser les informations personnelles ou intrusives à leur vie privée.

Un défi majeur pour les fournisseurs de services IoT est qu'il existe des lois variées, souvent incohérentes, en matière de confidentialité et de protection de données. Des lois différentes peuvent s'appliquer dans différents pays, en fonction des types de données concernés, ainsi que du secteur d'activité et des services que le prestataire de services propose. Cela a des

implications pour un certain nombre de fournisseurs de services IoT centrés sur le consommateur.

Un véhicule connecté, par exemple, peut se déplacer entre différents pays, ce qui signifie que les transferts de données associés peuvent être régis par plusieurs juridictions différentes. Des capteurs embarqués qui suivent l'emplacement de la voiture (statique ou dynamique) et ses destinations fréquentes peuvent être utilisés pour déduire un certain nombre d'informations sur le mode de vie, les loisirs ou la religion du conducteur, que le conducteur peut prendre en considération comme une représentation/information de sa vie privée. De plus, les connaissances sur les habitudes de conduite au moyen de capteurs de diagnostic embarqués pourraient être partagées avec des compagnies d'assurance qui pourraient utiliser ces informations pour imposer une prime plus élevée et donc discriminer le conducteur à leur insu.

Les services et appareils IoT (y compris les voitures connectées) peuvent également circuler entre différents territoires souverains et donc différentes juridictions. Dans de nombreux cas, les données personnelles d'un individu peuvent transiter ou résider dans des juridictions différentes de l'individu. Ce sont des questions importantes qui doivent être prises en compte avant le déploiement d'un service IoT multinational.

Un autre défi est que la plupart des lois sur la protection des données exigent que les entreprises collectent les données des consommateurs pour obtenir le consentement du consommateur concerné (également appelé « personne concernée ») avant de traiter certaines catégories de données personnelles. La plupart des lois définissent les données personnelles comme toute information relative à une personne physique « identifiée » ou « identifiable ».

Mais au fur et à mesure que de plus en plus d'appareils sont connectés à Internet, de plus en plus de données sur les individus seront collectées et analysées et pourront éventuellement affecter leur vie privée, sans être nécessairement considérées comme « personnelles » par la loi. La combinaison de volumes de données massifs, de stockage dans la Cloud et d'analyses prédictives peut fournir des profils détaillés des utilisateurs. En particulier, il peut devenir difficile de vraiment anonymiser les informations et les informations personnelles peuvent être déduites à partir d'autres types de données.

La nécessité de préserver la confidentialité des données sensibles sur la santé est bien reconnue, notamment en raison de la possibilité d'utilisation abusive de tels enregistrements. Aux États-Unis d'Amérique, la Loi de 1996 sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) comprend des exigences de confidentialité et de sécurité pour atténuer les risques de divulgation non autorisée des dossiers de santé.

HIPAA, comme beaucoup d'autres règlements tels que ceux de l'Union européenne, ne s'applique que si les données de santé sont personnellement identifiables. Les données stockées dans un dispositif de contrôle du sang (qui n'identifie pas l'utilisateur) ne seraient pas couvertes par ces exigences, alors que les mêmes données dans une application smartphone ou dans un serveur Cloud sont susceptibles d'être couvertes car elles peuvent être liées à un individu (dans le cas d'un smartphone car le téléphone contiendra presque certainement d'autres données identifiant l'utilisateur et dans un serveur Cloud car il sera

associé à un compte d'utilisateur identifiable). Les décideurs du monde entier se rendent compte que les informations et les connaissances sur les personnes peuvent avoir un impact sur leur vie privée, même si elles ne sont pas définies comme « identifiables personnellement ». Ils commencent donc à adopter des approches de la réglementation davantage axées sur le risque, mais tiennent également compte des répercussions plus générales de l'utilisation des données sur la protection de la vie privée plutôt que de se concentrer sur les définitions juridiques.

Afin de renforcer la confiance dans l'écosystème de l'IoT, les gouvernements devraient veiller à ce que la législation relative à la protection des données et à la vie privée soit neutre sur le plan technologique et que les règles soient appliquées systématiquement à tous les acteurs de l'écosystème Internet. De plus, pour que les fournisseurs de services IoT minimisent la nécessité d'une intervention réglementaire officielle, nous recommandons qu'ils suivent les pas décrits à l'annexe A dans les premiers stades de développement de leur service ou de leur produit IoT.

7 Utilisation efficace de ce guide

Bien que la sécurité soit mieux mise en œuvre au début d'un projet d'ingénierie, ce guide peut également aider les organisations qui ont déjà conçu, fabriqué et même déployé un produit ou un service IoT. Quelle que soit la phase atteinte par le produit ou le service du lecteur, un processus utile doit être suivi pour tirer le meilleur parti de cet ensemble de documents :

- Évaluer le modèle technique
- Examiner le modèle de sécurité du produit ou du service actuel
- Examiner et évaluer les recommandations
- Mise en œuvre et examen
- Cycle de vie en cours

7.1 Évaluation du modèle technique

La première et la plus importante phase du processus consiste à comprendre le produit lui-même ou le service IoT de l'entreprise. Afin de procéder à un examen de sécurité et à une évaluation des risques, l'équipe doit être familiarisée avec chaque composant utilisé dans la solution ou produit de l’entreprise, l'interaction des composants entre eux et l'interaction des composants avec leur environnement. Sans une compréhension claire de la façon dont le produit ou le service a été (ou sera) construit, une revue sera incomplète.

Commencez par créer un document décrivant chaque composant utilisé dans le système. Identifiez comment le composant est approvisionné, comment il est utilisé, quel niveau de privilège il requiert et comment il est intégré dans la solution globale. Mappez chaque composant aux technologies décrites dans la section « Modèle » de chaque document sur les principes de l'Écosystème des Dispositifs Périphériques IoT [3] et de l'Écosystème de Services IoT [4]. Il est acceptable que le document ne corresponde pas spécifiquement à un composant donné, mais il doit mapper la classe générale du composant. Utilisez simplement la classe de composant, comme un microcontrôleur, un module de communication ou une ancre de confiance, comme contexte. Considérez les questions suivantes :

- Quels composants sont utilisés pour créer le produit ou le service ?

- Quelles entrées et sorties sont applicables au composant donné ?
- Quels contrôles de sécurité sont déjà appliqués à ces entrées et sorties ?
- Quel niveau de privilège est appliqué au composant ?
- Qui dans l'organisation est responsable de l'implémentation du composant ?
- Qui dans l'organisation est responsable de la vérification et de la gestion du composant ?
- Quel processus est en place pour remédier les risques observés pour le composant ?

Ces questions, une fois résolues, permettront de comprendre comment les composants techniques interagissent les uns avec les autres et comment le produit ou le service global est affecté par chaque composant.

Ce processus correspond à la première et à la deuxième phase du modèle d'évaluation des risques CERT OCTAVE [6], ou à la phase du « Cadre de Gestion des Risques » du NIST [5]. Cela aide à l'élaboration d'un profil pour chaque actif commercial essentiel, au développement d'objectifs de sécurité et établit une base pour la façon dont l'entreprise évaluera, surveillera et réagira aux risques.

7.2 Passer en revue le modèle de sécurité actuel

Ensuite, lisez la section sur le modèle de sécurité du dispositif périphérique ou du service en cours d'évaluation. Cette section aidera le lecteur à comprendre le modèle qu'un attaquant utilisera pour compromettre une technologie donnée. Ce modèle est basé sur des années d'expérience en évaluation de sécurité, en ingénierie inverse et en conception de systèmes embarqués.

Une fois le modèle de sécurité revu, le lecteur devrait avoir une meilleure compréhension des technologies les plus vulnérables ou les plus souhaitables pour l'attaquant dans le produit ou le service en cours de développement. Cette information devrait être partagée avec l'organisation, pour s'assurer que les ingénieurs et le leadership comprennent les risques et les menaces pour le modèle actuel.

Cependant, il convient de noter que l'organisation ne devrait pas prendre de mesures pour ajuster son modèle de sécurité en ce moment. Il est trop tôt pour faire des changements architecturaux concis.

Ce processus correspond à nouveau à la première et la deuxième phase du modèle « CERT OCTAVE [6] », ou à la phase Frame du NIST « Risk Management Framework [5] ». L'examen du modèle de sécurité permet d'améliorer le modèle technique en identifiant les lacunes potentielles en matière de sécurité et en mettant en lumière les objectifs de sécurité qui devraient être prioritaires.

7.3 Examiner et évaluer les recommandations

La section « Recommandations » devrait être examinée en ce moment pour évaluer comment les tâches de sécurité peuvent être résolues. Cette section fournira non seulement des méthodologies pour la mise en œuvre des recommandations, mais donnera un aperçu des défis liés à la mise en œuvre d'une recommandation particulière.

Pour chaque recommandation, une section « Méthode » est fournie. Cette section décrira les méthodologies qui aident à la correction ou à la réduction du risque de sécurité

correspondant. Ces méthodes, bien que présentées à un haut niveau, décriront des concepts qui réduisent le risque d'un point de vue holistique, afin de s'assurer que la plus grande partie du bénéfice est acquise grâce à un effort raisonnable et pratique.

Une section « Dépenses » est fournie pour discuter, dans le cas approprié, des dépenses financières supplémentaires que l'organisation devrait préparer pour la mise en œuvre d'une recommandation particulière. Alors que la plupart des dépenses, telles que le temps d'ingénierie et les matières premières, sont assez évidentes, des dépenses moins évidentes peuvent modifier les finances appliquées aux produits et services dont les marges du bénéfice particulier et les limites budgétaires ont déjà été définies par les chefs d'entreprise. Bien que des numéros spécifiques ne soient pas fournis, des technologies et des services sont spécifiés qui peuvent entraîner des coûts supplémentaires.

Une section sur les « Risques » est également fournie afin que le lecteur comprenne les lacunes en matière de sécurité susceptibles de résulter de la non-application d'une recommandation particulière. Alors que l'entreprise peut accepter que certains risques soient dans les lignes directrices opérationnelles de l'entreprise, le lecteur doit examiner chaque section de risque pour s'assurer que l'entreprise comprend parfaitement les effets secondaires de ne pas appliquer (ou de ne pas mettre en œuvre correctement) une recommandation donnée. Cela peut sembler simple pour des recommandations telles que « Crypter les données », mais la subtilité de certaines menaces, telles que les attaques par rejeu contre des messages qui ne sont pas cryptés d’une manière unique, peut surprendre le lecteur à une date ultérieure.

Dans certains cas, des références sont fournies pour un examen plus approfondi. Bien que ce document ne fournisse pas d'informations détaillées sur chaque technologie, sur chaque risque ou plan de restauration, d'autres normes et stratégies éprouvées le font. Cet ensemble de documents fournira des références à ces documents, le cas échéant, dans chaque recommandation.

Les résultats de l'examen de la section « Recommandations » doivent être directement liés à la section « Tâches de Sécurité ». Les tâches de sécurité doivent maintenant être remplies avec les recommandations appropriées pour l'implémentation correcte des tâches de sécurité. Ces tâches de sécurité seront ensuite associées à des composants spécifiques qui sont à leur tour attribuer aux membres responsables de l'organisation.

L'évaluation des recommandations correspond à la phase d'évaluation du cadre de gestion des risques du NIST [5], et aux phases « six, sept et huit » de la méthodologie CERT OCTAVE [6].

7.4 Mise en œuvre et examen

À présent, des tâches de sécurité claires ont été définies et l'entreprise aura une meilleure compréhension de leurs vulnérabilités de sécurité, de leur valeur et de leurs risques. L'entreprise doit maintenant créer un modèle de l’architecture clair pour chaque composant en cours de vérification et utiliser le processus d'évaluation des risques choisi par l'organisation pour développer un modèle de menace pour chaque composant, incorporant les recommandations et les risques appropriés pour chaque composant et tâche de sécurité. Lorsque le modèle de l’architecture est terminé, l'organisation peut commencer à mettre en œuvre chaque recommandation afin de remplir les tâches de sécurité.

Lorsque la mise en œuvre est terminée, l'entreprise doit examiner les risques à la fois dans la sous-section « Recommandations » et dans les section des « Composants ». L'entreprise devrait s'assurer que la mise en œuvre satisfait aux exigences énoncées dans ces sections. L'entreprise doit alors s'assurer que l'implémentation résout la sécurité en ce qui concerne le contexte dans lequel le composant est conçu dans le produit ou le service de l'entreprise, car ces documents ne peuvent pas entièrement traiter chaque produit ou service conçu et installé sur le terrain. Dans la mesure du possible, demandez à un cabinet de consulting extérieure d'évaluer la mise en œuvre afin de vous assurer qu'il adhère effectivement aux meilleures pratiques en matière de sécurité.

La mise en œuvre et la révision correspondent au composant « Respond » du cadre de gestion des risques du NIST [5] et à l'étape huit du modèle CERT OCTAVE [6].

7.5 Cycle de vie en cours

Le cycle de vie par rapport à la sécurité ne s'arrête pas ici. Au contraire, la sécurité est une partie inhérente de l'ingénierie globale d'un processus. Les dispositifs périphériques et les services IoT ont une durée de vie déterminée, et doivent être continuellement entretenus tout au long de cette vie, tout comme un organisme vivant.

Les exigences changent avec le temps. Les algorithmes cryptographiques deviennent démodés ou déconseillés. Les nouveaux protocoles et les technologies radio doivent interagir avec le produit ou le service. Cet écosystème en constante évolution dans lequel nos produits embarqués sont déployés doit être constamment revu pour garantir la confidentialité, l'intégrité, la disponibilité et l'authenticité.

La gestion du cycle de vie de sécurité en cours correspond aux composants « Monitor et Frame » du cadre de gestion des risques NIST [5] et aux étapes « un, quatre et cinq » du modèle CERT OCTAVE [6].

8 Exemple - Moniteur de fréquence cardiaque portable

Dans cet exemple, une conception simple d'un Moniteur de Fréquence Cardiaque (MFC) sera évaluée en utilisant cet ensemble de lignes directrices. Le dispositif périphérique sera évalué à l'aide du document Écosystème des Dispositifs Périphériques IoT, tandis que le côté service de la conception sera évalué à l'aide du document Écosystème de Services IoT.

8.1 Présentation du dispositif périphérique

Commençons par évaluer la conception matérielle du dispositif périphérique.

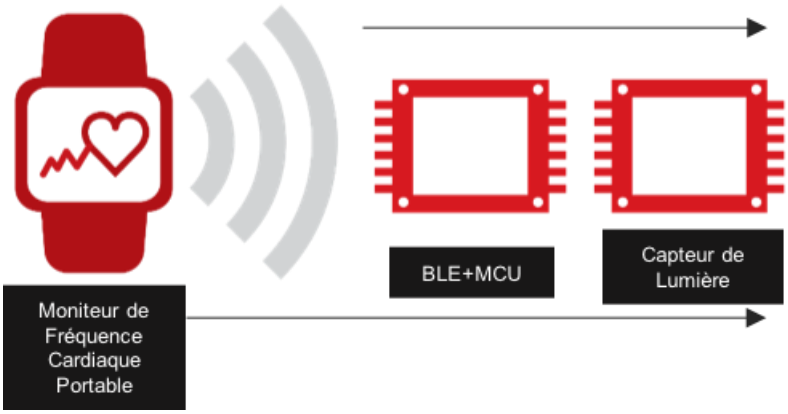

Figure 3– Simple moniteur de frequence cardiaque et composants principaux

Le MFC est formé par de composants standard pour un dispositif portable sans fil simple : un capteur photoélectrique de lumière ambiante et un microcontrôleur « Bluetooth Low Energy » (BLE). Le capteur est utilisé pour capturer les données de fréquence du pouls, tandis que le microcontrôleur analyse les données émises par le capteur et choisit les données à envoyer via l'émetteur-récepteur BLE intégré. Dans cet exemple, la pile du protocole BLE utilisée est la version 4.2.

Dans cet exemple, une pile type bouton est utilisée pour alimenter le dispositif et pouvoir transmettre les données du module MFC à un autre dispositif, tel qu'un téléphone intelligent ou une tablette. Aucun autre composant n'est requis pour que cet appareil fonctionne.

Selon le document, « Écosystème de Dispositifs Périphériques », cet appareil s'intégrerait dans la classe des dispositifs périphériques légers.

8.2 Aperçu du service

Du point de vue du service, l'application sur le smartphone ou la tablette pousse les mesures du dispositif périphérique vers un service back-end sur une connexion réseau disponible. Le service principal de l'application associe simplement le propriétaire du périphérique aux mesures capturées et les stocke dans une base de données locale au serveur d'applications.

La visualisation des données peut être réalisée à l'aide de l'application mobile ou via le site Web du service. Les utilisateurs de la technologie portable peuvent se connecter au site Web du fournisseur de services pour effectuer d’autres fonctions avec les mesures capturées par le dispositif périphérique.

Ceci est un modèle de service très simple et commun sans complexités particulières ou inutiles.

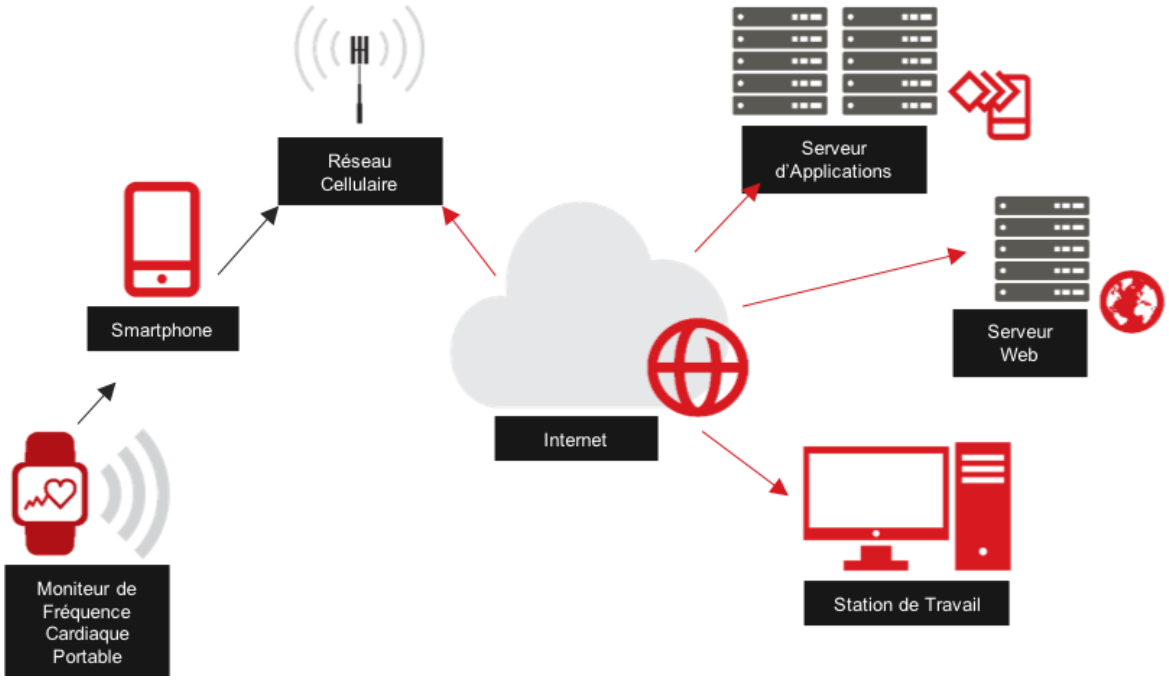

Figure 4– Flux de données vers un service back-end simple

8.3 Le cas d'utilisation

L'entreprise qui développe cette technologie a l'intention de suivre ses données par rapport au rythme cardiaque tout au long de la journée, en les stockant dans l'application et dans la base de données principale. L'intention est de permettre aux utilisateurs de revoir leur fréquence cardiaque au fil du temps pour suivre leur état de santé général. Les utilisateurs peuvent voir leur santé s'améliorer ou s'aggraver au fil du temps, selon leurs styles de vie. Cela permet aux utilisateurs de se motiver en évaluant les tendances positives et négatives dans leurs données du MFC.

L'entreprise a l'intention d'utiliser ces données pour établir des partenariats avec des fabricants d'appareils médicaux, des fournisseurs de soins de santé et d'autres organisations qui peuvent utiliser ces paramètres pour déterminer si un consommateur est plus susceptible d'avoir un événement lié à la santé, comme une crise cardiaque ou un accident vasculaire cérébral.

8.4 Le modèle de sécurité

L'équipe d'ingénierie de cet exemple a utilisé les sections des « Foires aux Questions de sécurité » des documents sur les dispositifs périphériques et les services IoT afin de déterminer les problèmes les plus pertinents pour leurs produits et services.

Du point de vue des dispositifs périphériques, l'équipe a appris que les problèmes suivants sont préoccupants :

- Clonage
- Usurpation d'identité du dispositif périphérique

- Usurpation d'identité du service
- Assurer la confidentialité

Du point de vue du service, l'équipe a décidé que les problèmes suivants sont préoccupants :

- Clonage
- Services piratés
- Identification d'un comportement anormal des dispositifs périphériques
- Limiter les compromis
- Réduire la perte de données
- Réduire l'exploitation
- Gestion de la confidentialité des utilisateurs
- Améliorer la disponibilité

L'équipe a examiné les recommandations pour chacune des questions ci-dessus, comme suggéré par chaque section pertinente des « Foire Aux Questions de Sécurité » de chaque document. L'équipe a ensuite choisi de mettre en œuvre des recommandations qui étaient des améliorations rentables qui assuraient une sécurité plus efficace.

Dans ce modèle d'exemple, le dispositif périphérique n'exigerait pas de changement substantiel. Étant donné que le dispositif périphérique a très peu de fonctionnalités, une sécurité minimale peut être utilisée sur celui-ci pour la sécurité de l'application et la communication. Étant donné que l'application du dispositif périphérique est gravée normalement sur une mémoire EEPROM unique, et tant que le microprogramme du périphérique soit verrouillé, il n'y a aucune menace réelle d'attaque contre le dispositif dans le cas d'utilisation donné.

Cependant, étant donné que la confidentialité est un problème, l'organisation devrait utiliser au moins une version PSK personnalisée d'une base de calcul de confiance (TCB). Cela garantirait que les tokens de chiffrement soient uniques à chaque dispositif périphérique, de sorte qu'un dispositif compromis ne puisse pas compromettre tous les dispositifs périphériques. Si les clés personnalisées (uniques) étaient codées dans le microcontrôleur verrouillé, il serait raisonnable de croire que ce cas d'utilisation était correctement protégé contre les menaces de clonage, d'usurpation d'identité et de confidentialité. Passez en revue les documents de l'IoT Service [3] et Endpoint [4] pour une discussion plus complète sur ce qu'est une base d'informatique de confiance dans le contexte de chaque écosystème.

L'infrastructure du serveur nécessite toutefois un nombre important de modifications. Les ingénieurs se rendent compte que, selon les recommandations, ils courent un risque sérieux d'abus. Les problèmes suivants sont reconnus :

- Il n'y a pas d'interface de sécurité diminuant les effets d'une attaque par déni de service
- Il n'y a pas de contrôle d'entrée ou de sortie limitant le flux de trafic vers ou depuis les services
- Il n'y a pas de séparation des tâches entre les niveaux de service

- Il n'existe pas de base de données sécurisée séparée contenant des jetons PSK personnalisés
- Aucune mesure de sécurité adéquate n'est implémentée dans le système d'exploitation du service
- Aucune mesure n'a été prise pour évaluer un comportement anormal des dispositifs périphériques

8.5 Le résultat

Après la mise en œuvre des recommandations, l'organisation dispose d'une architecture de service back-end bien mieux définie qui répond adéquatement aux risques identifiés par les lignes directrices.

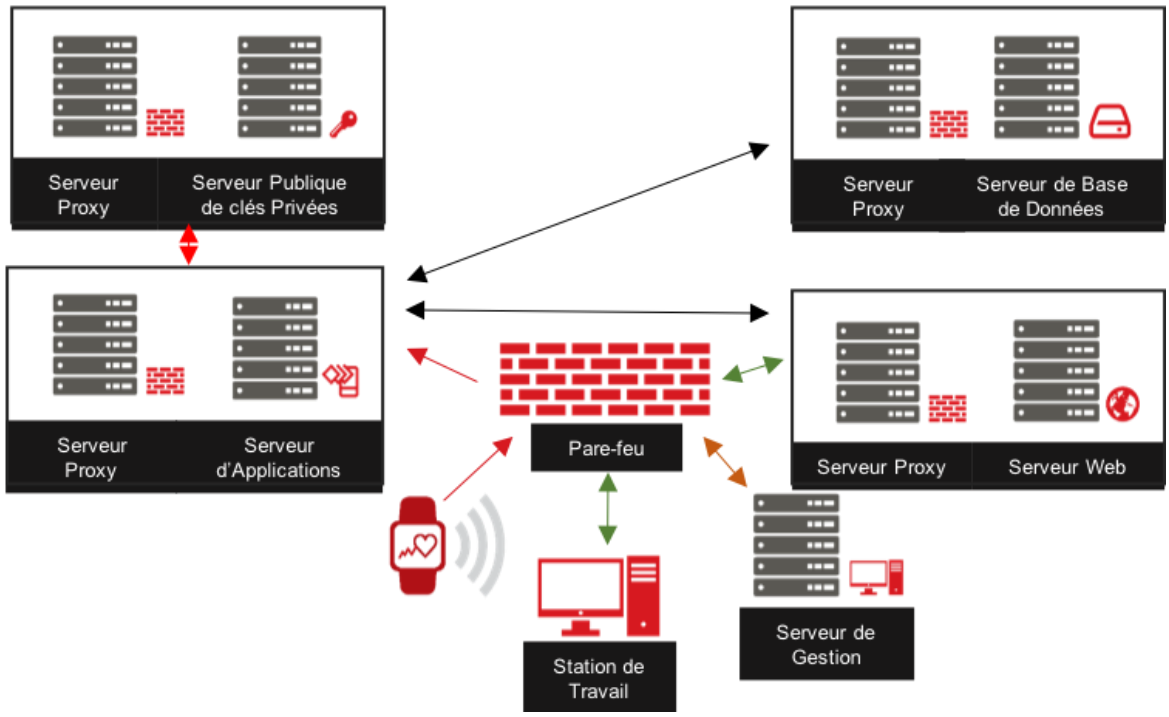

Figure 5– Écosystème de service résultant

Dans la figure ci-dessus, les changements dans l'écosystème de service sont facilement observables. Chaque classe de service a été divisée en plusieurs niveaux pour aider à sécuriser et à adapter facilement la technologie au cas où la demande augmenterait. Deux niveaux supplémentaires ont été ajoutés, un niveau de base de données et un niveau d'authentification, pour séparer les systèmes critiques des services qui interfacent directement avec le monde extérieur. Une interface de sécurité a été implémentée pour aider à protéger le réseau interne de plusieurs types d'attaques, y compris les attaques DoS et DDoS qui réduisent la disponibilité globale du système. Enfin, un modèle administratif a été défini pour permettre à la gestion un accès sécurisé à l'environnement de production. Un composant non représenté dans le diagramme ci-dessus est la présence d'un modèle analytique qui observe lorsque le comportement du dispositif périphérique peut indiquer un compromis, ou une faille dans la conception du firmware ou du matériel.

8.6 Résumé

Dans l'ensemble, cette technologie simple aurait pu être facilement compromise si elle avait été déployée « telle quelle ». Pourtant, avec quelques changements rapides, simples et rentables sur le dispositif périphérique, la technologie est assurée d'avoir des années de longévité sur le terrain sans changement de l'architecture.

Avec l'amélioration en capacités et architecture de l'écosystème des services, les menaces pesant sur les utilisateurs et sur l'entreprise sont bien moindres. Le clonage et l'usurpation d'identité ne sont plus une menace. La confidentialité est garantie en accordant à chaque terminal des tokens cryptographiques uniques. Les systèmes contenant des informations critiques sont séparés et protégés contre les systèmes el les réseaux publics les plus abusés. Ce modèle, bien que légèrement plus complexe, réduit le risque global de l'environnement de production.

9 Exemple - Drone personnel

Dans cet exemple, un petit drone personnel sera évalué en utilisant cet ensemble de lignes directrices. Le dispositif périphérique sera évalué à l'aide du document « Écosystème des Dispositifs Périphériques IoT », tandis que le côté service de la conception sera évalué à l'aide du document « Écosystème de Services IoT ».

9.1 Présentation du dispositif périphérique

Commençons par évaluer la conception matérielle du dispositif périphérique.

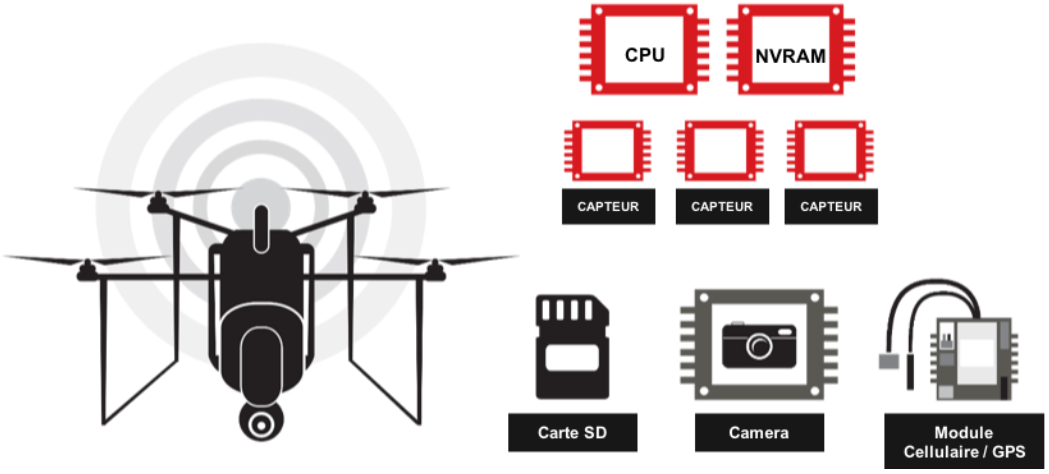

Figure 6– Un drone et ses composants primaires

Ce drone personnel est composé d'un ensemble robuste de composants. Les capacités de traitement du drone doivent être très performantes grâce aux multiples moteurs, capteurs et autres équipements qui doivent tous fonctionner efficacement en parallèle. Ce modèle utilise un processeur ARM Cortex-A8 avec le système de fonctionnement principal (Linux) stocké dans une NVRAM sur une puce séparée. Un ensemble de capteurs variés est nécessaire pour détecter les mouvements, la lumière, la vitesse, etc. Une carte SD/MMC est utilisée pour stocker la vidéo, les métriques de capteur et les métadonnées. Une caméra est utilisée pour permettre à l'opérateur d'observer les parcours du point de vue du drone lui-même. Un module qui combine les technologies cellulaire et GPS est utilisé pour s'assurer que le drone

peut maintenir la connectivité avec son opérateur même lorsqu'il est hors de portée du protocole propriétaire sans fil utilisé pour la communication. Le GPS est également utilisé pour le guidage et pour une automatisation minimale.

Une batterie Lithium Polymer (LiPo) est utilisée pour alimenter le drone. Son temps de vol est d'environ deux heures avant qu'une nouvelle charge soit nécessaire lorsque toutes les fonctions sont actives en même temps.

Selon le document « Écosystème des Dispositifs Périphériques », cet appareil s'intégrerait dans la classe des dispositifs périphériques complexe. Même s'il contient un module cellulaire, il n'est pas considéré comme une passerelle car il n'achemine pas les messages vers ou depuis d'autres dispositifs périphériques.

9.2 Aperçu du service

Du point de vue du service, le back-end est uniquement utilisé pour la connectivité avec l'opérateur lorsqu'une perte de contact est détectée sur l'interface radio propriétaire pendant le vol. Si le drone est en vol et que la connexion cellulaire peut être activée, il tentera d'attendre que son opérateur se connecte via le réseau LTE. Si, toutefois, il ne peut pas être contrôlé par LTE, il tentera un atterrissage automatisé à l'endroit où il a décollé pour la dernière fois.

Cependant, comme le drone a quelques fonctions légères d'automatisation, il peut recevoir des coordonnées et un chemin à parcourir tout en prenant des photos ou de courtes vidéos. Ces fichiers multimédias peuvent être téléchargés en temps réel sur LTE vers le service back-end pour montrer à l'opérateur le cap et le point de vue du drone pendant l'exécution automatisée.

Ainsi, un service back-end robuste est nécessaire pour assurer un haut niveau de disponibilité du service pour chaque drone pouvant se connecter au système. La disponibilité est également nécessaire pour les hauts débits de trafic réseau requis pour transmettre des vidéos et des images haute résolution sur une liaison cellulaire. Il doit également y avoir une interface Web qui permet à l'opérateur de visualiser les téléchargements de médias à partir d'un navigateur Web.

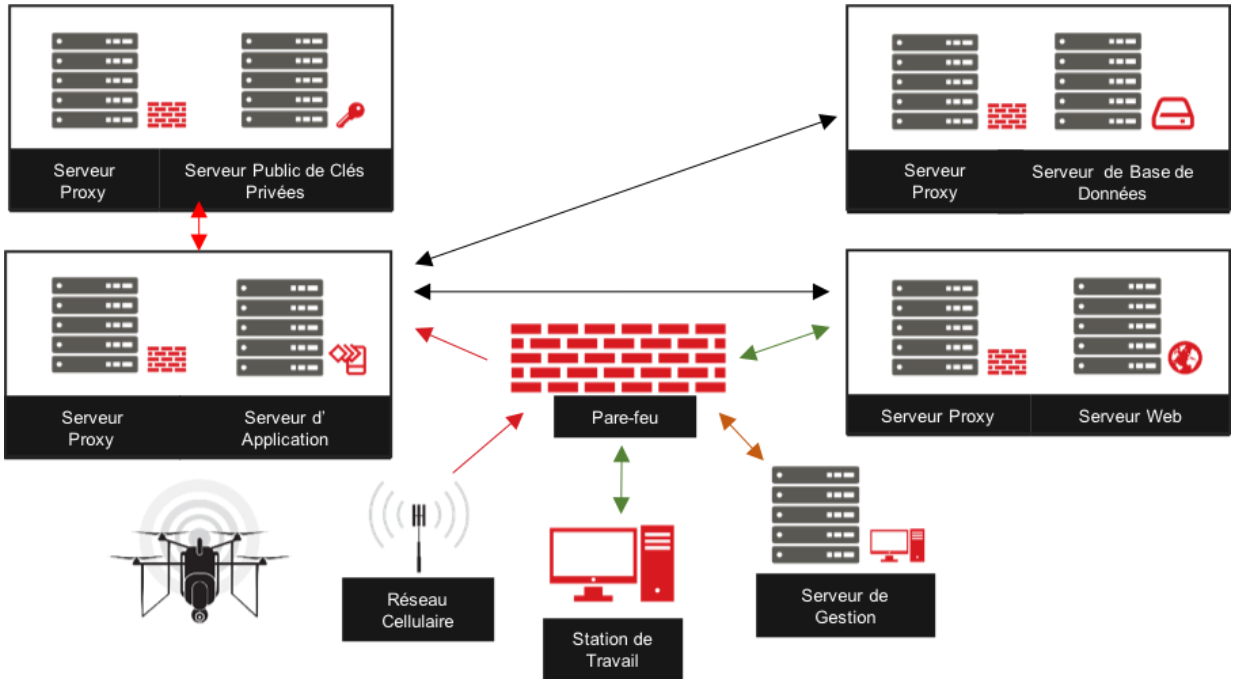

Figure 7– Flux de données vers les services back-end

9.3 Le cas d'utilisation

L'entreprise qui développe cette technologie envisage que l'utilisateur final l'utilise pour filmer dans la nature. Cependant, certains de leurs clients ont utilisé le drone pour filmer des scènes de cinéma, la caméra et les capacités de stabilisation du drone étant exceptionnelles pour le prix. En conséquence, le drone sera utilisé dans des projets de tournage coûteux où la propriété intellectuelle et la vie privée sont des préoccupations majeures.

9.4 Le modèle de sécurité

L'équipe d'ingénierie de cet exemple a exploité les sections « Questions Fréquemment Posées de sécurité » des documents sur les dispositifs périphériques et les services afin de déterminer les problèmes les plus pertinents pour leurs produits et services.

Du point de vue des dispositifs périphériques, l'équipe a appris que les problèmes suivants sont préoccupants :

- Identité du dispositif périphérique
- Usurpation d'identité du dispositif périphérique
- Attaques aux Ancres de Confiance
- Altération du logiciel et du micro-logiciel
- Gestion à distance sécurisée
- Détection des dispositifs périphériques compromis
- Usurpation de l'identité du service
- Assurer la confidentialité

Du point de vue du service, l'équipe a décidé que les problèmes suivants sont préoccupants :

- Gestion de la confidentialité des utilisateurs

- Améliorer la disponibilité

L'équipe a examiné les recommandations pour chacune des questions ci-dessus, comme suggéré par chaque section pertinente de questions fréquemment posées sur la sécurité. L'équipe a ensuite choisi de mettre en œuvre des recommandations qui étaient des améliorations rentables qui assuraient la plus grande sécurité.

Dans cet exemple, l'infrastructure de service ne nécessite pas de changement substantiel. En effet, l'infrastructure de service a déjà dû être construite de manière extensive pour prendre en charge les rafales de trafic nécessaires à l'entretien du produit final. L'architecture exigeait déjà une architecture bien formée et sécurisée simplement afin d'évoluer efficacement et maintenir la disponibilité des ressources même lorsque certains services subissaient des failles temporaires. Cependant, l'entreprise a choisi de rechercher davantage sur la confidentialité de l'utilisateur car cela est devenu un point de discorde principal pour le créneau inattendu commerciale de l'entreprise (dans le monde du cinéma).

L'infrastructure du dispositif périphérique, cependant, nécessite un nombre important de changements. Les ingénieurs se rendent compte que, selon les recommandations, ils courent un risque sérieux d'abus. Les problèmes suivants sont reconnus :

- Le chargeur de démarrage ne valide pas correctement l'application avant l'exécution du noyau du système de fonctionnement, ce qui risque de compromettre la sécurité
- Il n'y a pas de TCB utilisé pour gérer la sécurité de l'application ou des communications
- En raison de l'absence d'une Ancre de Confiance ou de TCB correctement implémenté, l'emprunt d'identité du dispositif périphérique constitue un problème, ce qui peut entraîner une fuite de données.
- Sans un TCB bien implémenté, le drone ne peut pas authentifier correctement les services
- Sans un TCB bien implémenté, le drone ne peut pas authentifier correctement l'opérateur via l'interface radio propriétaire.
- Les ingénieurs se sont fiés à la sécurité de LTE pour s'assurer que le canal de communication ne peut pas être compromis, mais n'a pas considéré la menace d'usurpation d'identité ou de réutilisation d'une Femtocell, qui outrepassent la sécurité de LTE pour compromettre une sécurité faible de service.

9.5 Le résultat

Après la mise en œuvre des recommandations pour les problèmes mentionnés ci-dessus, l'entreprise dispose d'une architecture de dispositif périphérique bien mieux définie qui répond adéquatement aux risques identifiés dans les documents de lignes directrices.

Pour le système de drones existant déjà en production, l'équipe d'ingénierie émet une mise à jour du micro logiciel qui implémente un modèle de sécurité « Pubkey » personnalisé. La mise à jour du firmware améliore le chargeur de démarrage ainsi que la sécurité dans l'architecture de base. Étant donné qu'un modèle Pubkey personnalisé a été utilisé, toute personne tentant d'abuser de l'absence de sécurité initiale du système pour tenter d'usurper l'identité d'un autre utilisateur échouerait, car les ingénieurs ont exploité leur base de données de mappage utilisateur et dispositif périphérique, pour créer des clés personnalisées pour chaque utilisateur. De cette façon, aucun utilisateur sans les identifiants Web appropriés ne peut télécharger et installer la mise à jour personnalisée de Pubkey d'un

autre utilisateur. Même si ce processus était complexe et long à mettre en œuvre, il en vaudra la peine.

Les futures versions de la technologie utilisée sur le drone implémenteront une ancre de confiance de CPU interne. Cette ancre de confiance sera liée à un TCB personnalisé Pubkey, pour s'assurer que chaque dispositif périphérique est unique avec une sécurité exceptionnelle à partir de zéro.

Déployer une cryptographie forte de cette manière est impératif, car elle annule également le potentiel pour les autres classes d'attaque que l'entreprise a identifiées comme une préoccupation. En tirant parti de l'avantage d'une cryptographie robuste et d'un TCB pour la vérification et l'authentification, l'équipe d'ingénierie peut facilement identifier si des services malveillants tâchent d'infecter le drone. Celui-ci, en détectant les services malveillants, peut simplement revenir sur le site d'origine du décollage.

Tout service qui détecte un drone mal sécurisé peut également déclencher des avertissements en interne. L'équipe d'administration, à ce moment-là, peut déterminer comment gérer le drone potentiellement compromis. Cela offre un niveau d'agilité en ce qui concerne les événements de sécurité et permet également à l'entreprise d'évaluer s'il existe des problèmes sur les logiciels ou matériels qui provoquent un comportement anormal sur le dispositif périphérique.

9.6 Résumé

Alors que l'équipe d'ingénierie consacrait évidemment une quantité exceptionnelle de temps à la création d'une architecture résiliente du point de vue de l'ingénierie mécanique et des services back-end, un travail substantiel devait être réalisé pour créer une technologie de dispositifs périphériques sécurisée. Même si ce scénario ne représentait pas une menace critique pour l'ensemble de l'entreprise, il était heureux qu'il y ait une solution qui fonctionnait assez bien pour les besoins de leurs clients. Si cela avait été une technologie plus critique pour la sécurité, même la solution déployée ici n'aurait pas été suffisante.

Pour plus d'informations sur les variantes de base pour réaliser une solution d'informatique de confiance, telles que Pubkey personnalisé TCB ou PSK TCB, veuillez consulter les documents des Écosystèmes de Service IoT [3] et de Dispositifs Périphériques IoT [4].

10 Exemple - Réseau de capteurs sur un véhicule

Dans cet exemple, un réseau de capteurs installés dans un véhicules est déployé dans une nouvelle classe d'automobile qui sera évalué en utilisant l'ensemble des lignes directrices. Le dispositif périphérique sera évalué à l'aide du document sur l'Écosystème des Dispositifs Périphériques, tandis que le côté service de la conception sera évalué à l'aide du document sur l'Écosystème de Services.

10.1 Présentation du dispositif périphérique

Commençons par évaluer la conception matérielle du dispositif périphérique.

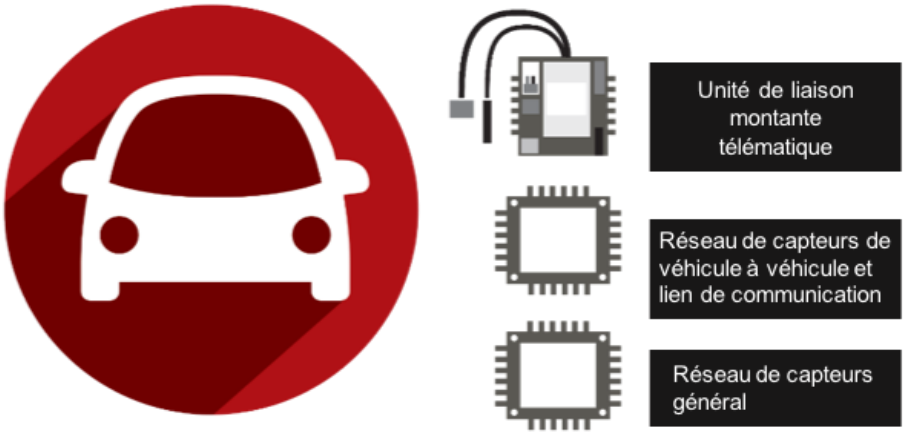

Figure 8– Système complet du réseau de capteurs dans un véhicule et de communications

Alors que le modèle ci-dessus est trop complexe pour le représenter dans un diagramme simple, les trois composants de haut niveau impliqués sont :

- Une unité de liaison télématique montante qui gère le réseau de capteurs, prend des décisions complexes pour le compte du conducteur et maintient une connexion avec l'écosystème de services.
- Un système de véhicule à véhicule (V2V) qui détecte et réagit aux événements V2V
- Un réseau de capteurs général qui fournit des métriques à l'unité de liaison montante télématique

Dans les systèmes automobiles modernes, l'unité télématique fait partie du réseau informatique de l'automobile et prend des décisions basées sur les données des capteurs et les communications back-end. Cette unité prendra des décisions avec ou au nom du consommateur conduisant le véhicule. L'unité s'assure que le véhicule fonctionne correctement, tente de prendre des décisions intelligentes en cas d'urgence et reçoit les commandes du réseau principal.

Le réseau de capteurs V2V identifie les véhicules à proximité et prend des décisions en fonction des mesures recueillies par les capteurs. Alors que l'unité de télématique prend principalement des décisions en fonction de l'état des composants (comme les freins ou les manomètres), le système V2V prend des décisions en fonction de la présence d'autres véhicules ou envoie des alertes aux véhicules voisins en cas d'événement critique.

Le réseau de capteurs général est une série de composants qui fournissent des données à l'unité télématique, et parfois à l'unité V2V. Ces unités utilisent les informations recueillies à partir du réseau de capteurs général pour prendre des décisions précises lors d'événements critiques.

Selon le document « Écosystème de Dispositifs Périphériques », ce système comporte des composants qui s'intègrent à chaque classe de dispositifs périphériques IoT. L'unité de liaison montante télématique agit comme une passerelle. L'unité V2V agit comme un dispositif complexe. Les dispositifs de détection généraux sont effectivement tous des dispositifs périphériques légers.

10.2 Présentation du service

Du point de vue du service, le réseau de capteurs du véhicule fournira des métriques au back-end. Ces données peuvent ou non être fournies au consommateur. Au contraire, les données pourraient être stockées par le fabricant pour observer ou identifier des problèmes potentiels avec les composants. Cela peut déclencher des avertissements de service qui sont ensuite envoyés au consommateur.

Le système peut également être amélioré pour fournir au consommateur des services utiles, tels que « déverrouiller à distance la porte », « démarrer le moteur » et des fonctions similaires. Dans un proche avenir, ces systèmes pourraient permettre de conduire les véhicules à distance à l'aide de systèmes de guidage automatisés.

Bien que les décisions les plus critiques seront prises sur l'unité elle-même, il est raisonnable de penser que certaines décisions seront prises dans le cloud, où plus d'apprentissage automatique (ML) et d'intelligence artificielle (IA) avec des modèles comportementaux ou statistiques peuvent être utilisé pour prendre des décisions plus complexes.

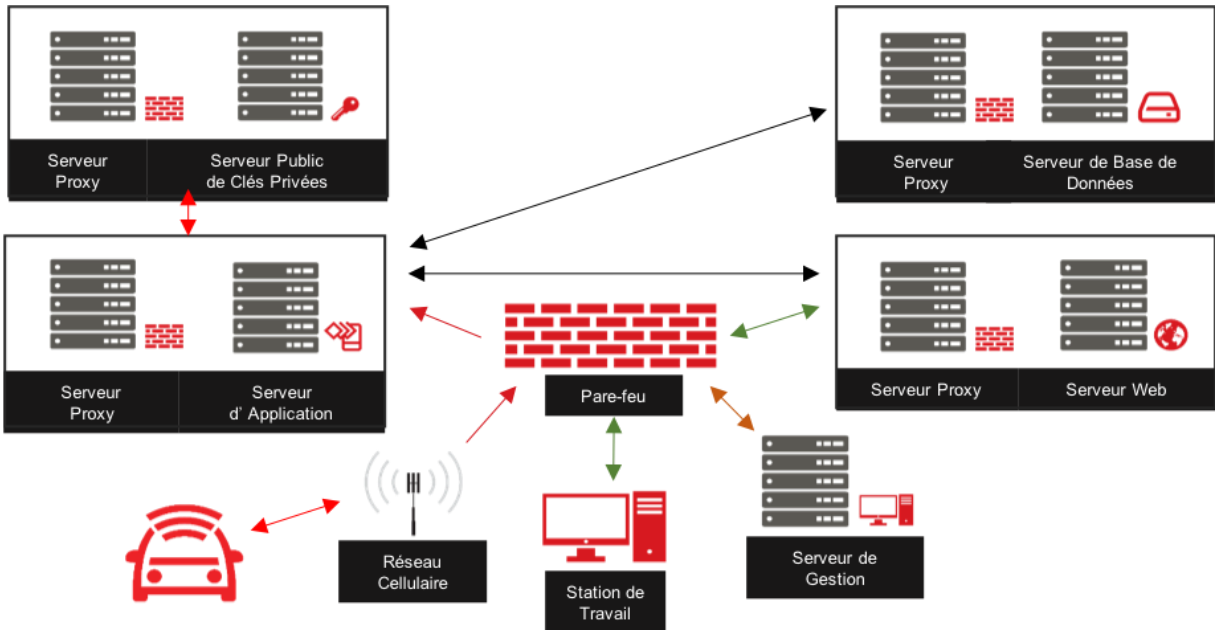

Figure 9– Flux de données vers les services back-end

10.3 Le cas d'utilisation

L'utilisation de cette technologie est évidente : construire des véhicules plus intelligents capables de prendre des décisions complexes dans des scénarios critiques pour la sécurité. L'objectif est de tirer parti de l'intelligence du plus grand nombre possible de capteurs pour prendre des décisions critiques dans de très petites fenêtres de temps. Les alertes de coupure automatique, les alertes de diffusion, les avertissements d'opérateur temporairement désactivés et d'autres scénarios critiques peuvent être résolus grâce à l'utilisation de capteurs et de systèmes informatiques bien conçus.

Une caractéristique intéressante de cette technologie est qu'elle peut être entièrement transparente pour l'utilisateur. L'utilisateur n'aurait pas besoin de configurer ces ordinateurs

pour agir d'une certaine manière. Au lieu de cela, ils devraient être capables de négocier les décisions à prendre à chaque moment en utilisant les mesures des capteurs. Cela permettra aux ordinateurs de se comporter correctement quel que soit l'environnement.

10.4 Le modèle de la sécurité

À l'heure actuelle, l'équipe d'ingénierie a exploité la section sur les “questions plus fréquentes” des documents des Écosystèmes de Dispositifs Périphériques et Services pour déterminer les problèmes les plus pertinents pour leurs produits et services.

Du point de vue des dispositifs périphériques, l'équipe a appris que les problèmes suivants sont préoccupants :

- Usurpation d'identité du dispositif
- Usurpation d'identité des services ou d’autres pairs (dispositifs) de communication
- Attaques par canal auxiliaire
- Détection des dispositifs compromis
- Assurer la sûreté au risque de la sécurité

Du point de vue du service, l'équipe a décidé que les problèmes suivants sont préoccupants :

- Identification du comportement des dispositifs périphériques anormaux
- Gestion de la confidentialité des utilisateurs

Le plus grand risque pour cet environnement qui n'a pas été discuté dans les exemples précédents est le risque d'usurpation d'identité à l'égard des pairs de communication. L'une des préoccupations des ingénieurs dans ce type d'environnement est le risque qu'un ordinateur prenne des décisions critiques en utilisant des données qui ne sont pas correctement authentifiées.

Étant donné que les données des capteurs dans des scénarios critiques nécessitent des temps de traitement extrêmement rapide, il est théorisé qu'il ne peut pas toujours être possible de mettre en œuvre la cryptographie asymétrique ou des communications en utilisant PKI. Cependant, cela peut ne pas être une affirmation précise. Au lieu de cela, un modèle de sécurité précis doit prendre en compte à l'avance les scénarios critiques en termes de temps et les clés de session en cache pour les dispositifs périphériques plus proches. Par exemple, si deux objets se rapprochent à un taux connu, les applications de sécurité dans l'Écosystème de Services peut préparer des clés de session spécifiques à ces deux dispositifs périphériques avant d'atteindre une distance où ils peuvent avoir un impact physique entre eux. Cela assurerait une communication sécurisée entre dispositifs et capteurs, pouvant encore être utilisée dans le cas où il n'y a pas de temps pour renégocier une session sécurisée instantanément quand un scénario critique (comme un accident imminent entre automobiles) est détecté.

Ainsi, une amélioration de l’implémentation du TCB est nécessaire. Une solution intéressante est d’utiliser GBA, avec une puce UICC dans l'unité de liaison montante télématique qui peut distribuer des clés de manière sécurisée aux dispositifs périphériques dans tout le système. Ce protocole permettra même aux dispositifs périphériques légers

d'être ensemencés avec des clés de session sécurisées qui peuvent être utilisées dans plusieurs scénarios critiques. De cette façon, l'environnement peut toujours être sécurisée et ensemencé à partir d'une racine de confiance, même si les dispositifs périphériques légers ne sont pas capables de calculs critiques pour l'initialisation de la session de clé publique.

Un autre problème critique dans ces environnements est la détection des dispositifs périphériques compromis. Par exemple, comment l'environnement peut-il reconnaître si un capteur simple, tel qu'un moniteur de pression des pneus (TPM) a été compromis ? Si l'ordinateur prend une décision critique sur la base de la signalisation TPM qu'un pneu a sauté, un problème de sécurité peut survenir. En conséquence, le comportement des périphériques et leur fiabilité doivent être réévalués à chaque phase de démarrage. Tous les appareils doivent avoir une résistance à l'altération et pouvoir notifier le réseau en cas de compromission. Inversement, les autres appareils du réseau de capteurs devraient pouvoir évaluer la véracité des homologues du réseau.

10.5 Le Résultat

Après la mise en œuvre des recommandations, le réseau de capteurs du véhicule est bien protégé contre les attaques sur le réseau de communication du véhicule. Le protocole GBA est utilisée pour distribuer les clés à tous les dispositifs périphériques dans le système, à chaque démarrage, en veillant à ce que les anciennes clés ne soient pas réutilisées. Ceci, associé à une résistance à l'altération, à un TCB fort dans chaque dispositif périphérique et à une racine organisationnelle de confiance, permet à l'environnement de fonctionner avec beaucoup moins de risques.

Pourtant, indépendamment de ces changements, la sécurité est toujours un facteur critique. L'équipe d'ingénierie et le chef d'entreprise, ainsi que l'équipe juridique et les courtiers d'assurance de l'entreprise, devraient évaluer la technologie critique et déterminer si la sécurité peut être mise en œuvre sans risquer la sécurité des utilisateurs. Alors que la sécurité peut souvent être mise en œuvre, même dans des scénarios critiques pour la sûreté de l’utilisateur, avec quelques ajustements architecturaux, il y a des moments où la sûreté physique doit précéder toutes les autres préoccupations.

10.6 Résumé

Des systèmes comme ceux-ci sont souvent bien conçus et nécessite de beaucoup d'efforts pour qu’un attaque á l'écosystème réussisse. Cependant, des failles subtiles dans l'architecture de communication peuvent conduire à un environnement compromis. Dans les environnements clos, tels que certains réseaux CANbus, un seul dispositif périphérique défectueux peut rendre l'ensemble du système vulnérable. Ceci, dans des environnements critiques pour la sécurité, est inacceptable.

Annexe A Considérations de confidentialité recommandées pour les fournisseurs de services IoT

Afin de renforcer la confiance dans l'écosystème IoT et de minimiser le besoin d'une intervention du régulateur formelle, la GSMA propose les phases schematique suivantes comme guide pour minimiser les risques de confidentialité. Nous recommandons aux fournisseurs de services IoT de suivre ces phases et d'examiner ces questions dès les premières phases de développement de leur service ou de leur produit IoT.

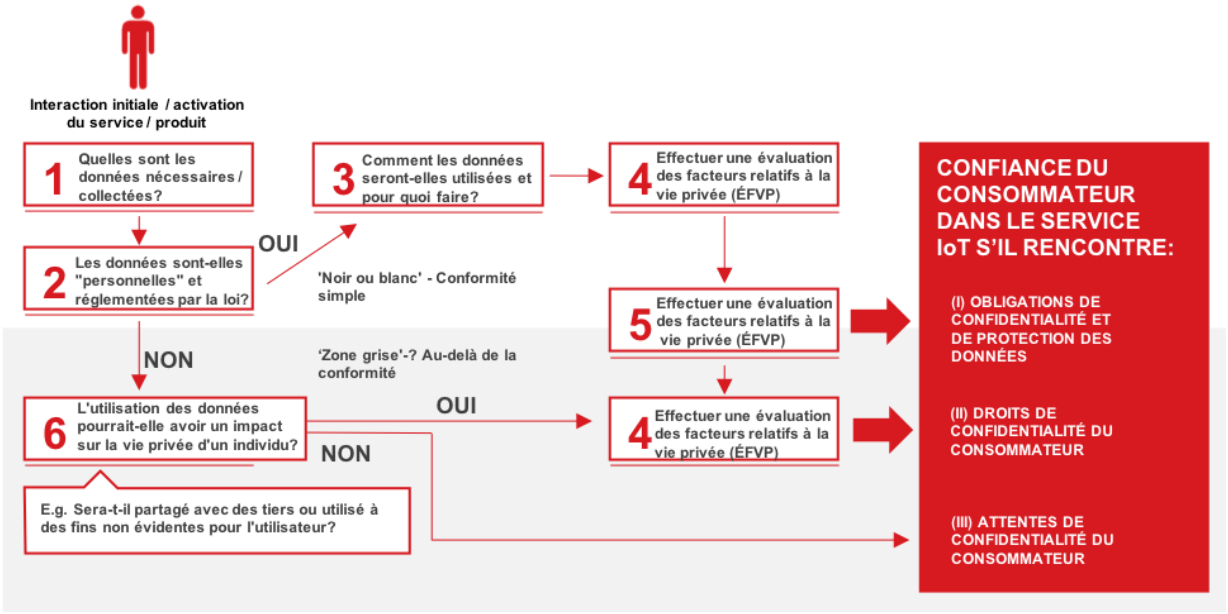

Figure 10– Arbre de décision pour la privacité IoT par conception de la GSMA (« IoT Privacy by Design »)

Étapes	Considération
Étape 1	**Quelles données devez-vous recueillir auprès de l'utilisateur pour que votre service ou produit IoT puisse fonctionner correctement ?** L'une des premières phases de tout modèle commercial reposant sur des données consiste à identifier les informations réellement requises du consommateur ou concernant celui-ci, pour que le service ou le produit fonctionne correctement. Les types de données dont un service a besoin peuvent être catégorisés comme étant statiques - tels que le nom ou l'adresse du domicile du consommateur - et des données dynamiques, telles que l'emplacement en temps réel. Donc, si vous offrez, par exemple, un bracelet de fitness qui suit les pas et les calories de quelqu'un, vous devez connaître le poids, l'âge, le sexe, la distance parcourue et la fréquence cardiaque de l'individu portant le bracelet mais ce n'est pas évident d'avoir besoin de l'emplacement actuel de l'individu. Lors de l'évaluation des types de données nécessaires, il est également important de décider si le consentement des individus est nécessaire pour utiliser ces données et comment vous obtiendriez leur consentement ou si vous leur offriez des options pour contrôler leurs préférences de confidentialité. Un smartphone peut servir de support pour offrir aux utilisateurs des options de confidentialité (par exemple, une application mobile ou un tableau de bord en ligne) lorsque le produit lui-même n'a pas d'écran.

Etape 2	**Les données sont-elles « personnelles » et réglementées par la loi ?**
	La prochaine phase devrait être d'identifier les exigences de protection des données et de confidentialité que la loi vous impose. Les questions à considérer comprennent :
	Quelle est la définition des données « personnelles » dans le pays/marché concerné ?
	• Les données collectées sont-elles « personnelles » et réglementées par la loi ? Si oui, avez-vous identifié la base légale qui vous permet de traiter ces données ?
	• Êtes-vous soumis à des conditions de licence liées à la confidentialité (par exemple, en tant que fournisseur de services de télécommunication) ?
	• Existe-t-il des lois fédérales, départementales, locales ou sectorielles qui s'appliquent à votre modèle de collecte de données proposé, en plus des lois générales sur la protection des données ? par exemple :
	  ○ Services financiers, de paiement, réglementation de la santé
	  ○ Restrictions potentielles sur les transferts de données transfrontaliers

Étape 3	**Comment les données seront-elles utilisées et pour quoi faire ?** Une fois que vous avez établi quelles sont vos exigences légales en matière de conformité, l'étape suivante consiste à déterminer comment les données que vous collectez seront utilisées - et avec qui elles doivent être partagées - pour atteindre les résultats dans le cadre de votre offre de service. Les questions suivantes devraient vous aider à répondre aux questions de sécurité et de confidentialité en relation avec le traitement des données : • Les données sont-elles sécurisées à la fois lorsqu'elles sont stockées et transmises ? • Avez-vous clairement défini les flux de données ? I.e. identifier comment les données seront utilisées et partagées à travers la chaîne de valeur et à quelles fins • Pouvez-vous justifier pourquoi chaque type de données collectées est nécessaire dans le contexte spécifique de l'offre du service prévu ? • Avez-vous défini des responsabilités en matière de protection de la vie privée avec vos partenaires dès le départ (et la conception de votre produit reflète-t-elle ces responsabilités ?) • Existe-t-il des accords contractuels appropriés avec les entreprises avec lesquelles vous partagez les données des consommateurs ? (Par exemple, limiter l'utilisation des données par les fournisseurs d'analyses à leurs propres fins commerciales). De tels accords ou restrictions peuvent être bilatéraux ou vous pourriez établir un code de conduite ou des lignes directrices et demander à vos partenaires de s'engager envers eux avec des conséquences et des responsabilités définies s'ils ne le font pas.

Étape 4	**Effectuer une évaluation des facteurs relatifs à la vie privée** La réalisation d'une évaluation des facteurs relatifs à la vie privée (EFVP) porte sur : • Identifier si des risques pour la vie privée surgissent avec votre produit ou service pour des particuliers • Réduire le risque de préjudice pour les personnes pouvant découler d'une mauvaise utilisation possible de leurs renseignements personnels • Concevoir un processus plus efficace pour gérer les données sur les individus Les exigences d'EFVP deviennent de plus en plus courantes dans les lois sur la protection des données et la vie privée. Il existe un certain nombre de guides sur la façon de mener les EFVP, y compris ceux publiés par le Bureau du Commissaire à l'information du Royaume-Uni [10] et ceux de « l' International Association of Privacy Professionals ». Les questions typiques à aborder lors de la réalisation d'une ÉFVP comprennent : • Le projet aboutira-t-il à ce que vous et vos partenaires prennent des décisions ou prennent des mesures contre des personnes de manière à avoir un impact significatif sur elles ? • L'information sur des personnes d'un genre particulier est-elle susceptible de soulever des préoccupations ou des attentes en matière de protection de la vie privée ? Par exemple, des dossiers de santé, des casiers judiciaires ou d'autres informations que les gens considèrent comme privées ? • Le projet exigera-t-il que vous communiquiez avec des personnes d'une manière qu'elles pourraient trouver intrusive ?

Étape 5	**Concevoir la confidentialité dans l'interface utilisateur** Après avoir évalué les risques pour la vie privée des consommateurs, vous devriez réfléchir à la façon de sensibiliser ces derniers à ces risques et de les atténuer, ainsi que de leur offrir des options pour exprimer leurs préférences en matière de confidentialité. En fin de compte, cette étape consiste à vous assurer que vous offrez un service qui répond aux besoins et aux attentes de vos clients et consommateurs de manière conviviale. Et il s'agit de bâtir leur confiance en les rassurant qu'ils ont plus de contrôle sur leur vie privée. Les questions à considérer comprennent : • Comment les consommateurs peuvent-ils être conscients des risques pour leur vie privée et comment peuvent-ils faire des choix à partir des informations pertinentes ? • Avez-vous obtenu leur consentement, là où la loi l'exige ? Les éléments clés du consentement comprennent : la divulgation, la compréhension, le caractère volontaire, la compétence et l'entente) • Les données sont-elles sécurisées en transit et au repos ? • Existe-t-il une période définie pour laquelle vous devez conserver les données du consommateur (et pourquoi) ? • Le parcours du consommateur aide-t-il à gagner leur confiance? Par exemple: o Comprennent-ils les données qu'ils partagent en échange de l'utilisation du service? o Les consommateurs peuvent-ils exprimer leurs préférences de confidentialité en quelques pas très simples, par ex. via un tableau de bord d'autorisation de données sur le Web, par des messages "juste à temps", par un centre d'appels, sur une application mobile, par des commandes vocales, etc.

Étape 6	**L'utilisation des données pourrait-elle avoir un impact sur la vie privée d'un individu?** Votre produit ou service peut collecter des données qui ne sont pas nécessairement classées comme «personnel» par la loi, mais il peut avoir des implications sur la vie privée pour le consommateur et donc cette possibilité devrait donc être considéré dès le début. Pour vérifier si les données pertinentes pourraient être utilisées pour influencer la vie privée d'un consommateur, tenez compte des éléments suivants: • Des données (non personnelles) provenant de votre service ou produit pourraient-elles être combinées avec d'autres données provenant de différentes sources pour tirer des conclusions sur la vie privée d'un consommateur? Par exemple des inférences sur son style de vie, ses habitudes ou sa religion qui: o Puissent affecter sa capacité à obtenir une assurance santé ? o Être utilisé par des tiers (revendeurs, compagnies d'assurance) pour faire une discrimination par les prix contre le consommateur spécifique ? • Si votre produit ou service est susceptible de changer à un moment donné dans le futur, quelles sont les implications probables d'un tel changement pour le consommateur ? Par exemple : o Le changement implique-t-il la collecte de nouvelles données sur le consommateur (telles que les données de localisation) ? o Existe-t-il des données existantes ou nouvelles du consommateur partagées avec des tiers (par exemple des annonceurs) qui commenceraient à utiliser ces données à des fins différents de ceux initialement obtenus ? • Si de tels changements se produisent, vous devriez : o Vérifiez l'impact possible sur votre entreprise si de nouvelles lois sont invoquées à la suite du changement o Établir des processus pour informer les consommateurs et obtenir leur consentement si nécessaire o Fournir aux consommateurs les moyens de modifier leurs préférences de confidentialité • Certaines considérations supplémentaires que nous recommandons aux fournisseurs de services IoT considèrent : o Assurez-vous que vous avez des accords contractuels appropriés définissant les responsabilités de chaque partenaire dans la chaîne de valeur o Disposer d'un processus de réparation clair afin que les consommateurs sachent à qui s'adresser si les choses tournent mal ou s'ils souffrent d'une atteinte à la vie privée

Annexe B Exemple basé sur un système de suivi automobile

Dans cet exemple, un système de suivi automobile sera évalué du point de vue des lignes directrices de sécurité IoT. Le processus découlera de la section sept de ce document d'aperçu - « Utilisation efficace de ce guide ».

B.1 Évaluation du modèle technique

Dans la première étape, « Évaluation du modèle technique », l'équipe d'ingénierie évalue le fonctionnement du dispositif en fonction de l'architecture de son produit. L'équipe d'ingénierie crée un document qui détaille les technologies utilisées dans la solution afin d'organiser le personnel, d'attribuer des tâches de sécurité et de suivre les progrès.

Par souci de simplicité, notre système de suivi automobile aura les capacités suivantes :

- **Écosystème du Dispositif Périphérique :**
  - Une interface utilisateur graphique simple (GUI) qui permet à un utilisateur de :
    - Se Connecter avec un nom d'utilisateur et un mot de passe
    - Désactiver le suivi
    - Activer le suivi
    - Identifier et visualiser l'emplacement actuel
  - Un module cellulaire pour la connexion aux services back-end
  - Une carte SIM pour le module cellulaire
  - Une batterie Lithium-Polymère comme alimentation de secours
  - Une unité centrale de traitement (CPU)
  - Une application embarquée dans la RAM non-volatile
  - RAM
  - EEPROM

- **Écosystème du service :**
  - Connectivité des données cellulaires
  - APN privé sécuriser
  - Point d'accès au service
  - Service de gestion OTA du modem cellulaire
  - Service de gestion de carte SIM OTA

Après avoir noté les informations pertinentes pour chaque technologie, l'équipe examine la section “Modèle” de chaque document de ligne directrice et identifie le modèle technologique approprié. Ce dispositif périphérique est considéré comme complexe. Le modèle de service et de réseau utilisé dans cet exemple est un service IoT mobile standard.

B.2 Révision du modèle de sécurité

Avec le modèle technique décrit, l'organisation devrait maintenant être prête à faire des progrès avec l'examen du modèle de sécurité. Dans le modèle de sécurité, l'équipe évaluera si un adversaire est susceptible d'attaquer la solution.

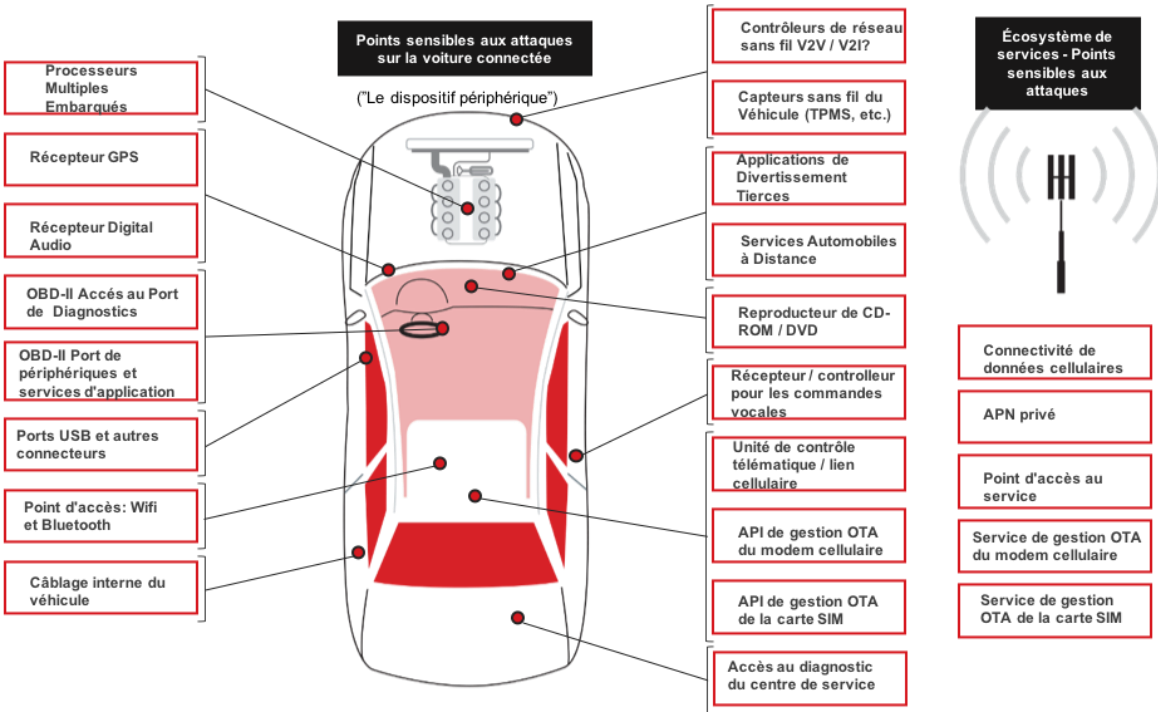

Figure 11– Surfaces d'attaque d'une voiture connectée

Dans notre exemple de solution, il n'y a que deux surfaces de menaces pertinentes pour une attaque :

- Le réseau cellulaire
- Une attaque localisée sur le véhicule

Comme il n'y a pas de connexion sur un réseau locale, seulement une connexion sur un réseau mobile, un attaquant doit : soit compromettre la connexion du réseau cellulaire, entrer via le canal de communication depuis l'APN privé ou entrer via le point d'accès au service, le serveur de gestion OTA du modem cellulaire ou le serveur de gestion OTA de la carte SIM.

Les attaques physiques sont le seul autre moyen de compromettre le dispositif dont il existe plusieurs points d'entrée, comme indiqué dans le diagramme ci-dessus. Dans le cas de ce service IoT, le dispositif périphérique doit être fortement ciblé.

B.3 Examiner et assigner des tâches de sécurité

Avec le modèle de sécurité, il est désormais facile d'assigner des tâches de sécurité. Chaque équipe doit attribuer une personne spécifique à chaque composant de la solution à évaluer. Cela devrait être évalué non seulement d'une perspective générale (dispositif périphérique, réseau et service), mais aussi de la perspective du sous-composant. Cela signifie que le processeur doit être attribuer à une personne de l'équipe technique, ainsi que le système d'exploitation, le service réseau, etc.

Une fois que chaque composant est assigné à un "propriétaire", le processus peut commencer. Cela signifie qu'à ce stade, l'équipe comprend :

- Comment la technologie est composée
- Quelles technologies affectent la sécurité
- Quels sont les ingénieurs/acteurs qui sont responsable de la technologie donnée.

B.4 Révisions des recommandations

Dans la phase d'examen des recommandations, chaque membre de l'équipe devrait lire et comprendre autant de recommandations que possible, ceci par principe d'action. Au lieu de se concentrer uniquement sur les recommandations, les ingénieurs devraient prendre le temps de comprendre autant de recommandations que possible, même d'une façon sommaire pour avoir une meilleure vue de la façon dont leur composant affecte la sécurité globale du produit ou du service. De cette façon, le groupe peut engager une discussion utile sur les stratégies de remédiation ou d'atténuation les plus équilibrées du point de vue de la rentabilité, de la longévité et de la gestion.

Une fois les recommandations examinées, les propriétaires des composants peuvent déterminer si une recommandation a déjà été appliquée ou marquer comme une recommandation en attente. Cela permettra au groupe de discuter de l'applicabilité d'une recommandation avant son déploiement. C'est une meilleure stratégie à suivre, car certaines recommandations peuvent avoir des effets secondaires qui ont une incidence sur la réalisation d'autres recommandations ou sur les contrôles existants.

Dans cet exemple, l'équipe aurait déterminé que :

- Une Base de Confiance pour l'application doit être utilisée
- Une Racine Organisationnelle de Confiance devrait être définie
- La personnalisation de l'appareil doit être implémentée
- Un boîtier inviolable doit être mis en place
- La gestion des mots de passe des Dispositifs Périphériques doit être appliquée
- La sécurité des communications des Dispositifs Périphériques devrait être appliquée
- Les images crypto graphiquement signées devraient être mises en œuvre
- La gestion de la vie privée devrait être mise en œuvre
- Les alertes d'alimentation de l'appareil doivent être intégrées

B.5 Révision du risque sur les composants

Ensuite, chaque composant dans les solutions doit être évaluée pour identifier les différents risques impliqués dans la mise en œuvre ou l'intégration d'un composant particulier dans le produit ou le service. Cette section ne peut être révisée que par le propriétaire du composant afin de minimiser le travail. Cependant, il est toujours bénéfique de lire autant que possible.

Après avoir examiné les recommandations et la section sur les risques liés aux composants, les lacunes de sécurité suivantes ont été identifiées :

- Les secrets ont été stockés sans protection dans l'EEPROM
- Les secrets n'ont pas été traités dans la RAM interne
- L'interface utilisateur doit protéger les mots de passe
- La confidentialité de l'utilisateur doit être définie pour l'utilisateur

B.6 Mise en œuvre et révision

Maintenant, l'équipe peut ajuster la solution pour être conforme aux exigences de sécurité qu'ils ont convenues. L'équipe ré-implémente les composants et ajoute des contrôles de sécurité, si nécessaire.

Dans ce cas particulier, l'équipe a identifié qu'elle travaille avec un membre de la GSMA capable de fournir une carte SIM contenant une technologie d'ancre de confiance compatible avec leurs applications. Ils vont résoudre leur besoin d'intégrer une ancre de confiance en utilisant la carte SIM existante. Cela résout également la personnalisation, car chaque carte SIM peut être personnalisée sur le terrain en utilisant la technologie standard GSMA.

La technologie SIM peut également aider à fournir les clés de la sécurité nécessaire pour les communications OTA, ce qui permet de résoudre le besoin de mettre en œuvre l'authentification et la confidentialité des communications.

La zone spécifique à la société qui fournit la SIM peut être programmée avec une racine de confiance approuvée qui permet à l'entreprise d'authentifier les homologues à l'aide d'une chaîne de certificats. Cela résout le besoin d'une base de racine de confiance organisationnelle et les exigences d'authentification pour les dispositifs se communiquant.

L'emballage du produit est à jour avec un emballage résistant à l'altération appropriée.

L'EEPROM est codée avec des données cryptées et avec des clés de sécurité stockées dans l'ancre de confiance SIM.

Le chargeur de d'amorçage est modifié pour utiliser l'ancre de confiance pour l'authentification de l'image de l'application.

Le dispositif périphérique est reprogrammé pour prendre en charge la saisie de mot de passe sécurisé de l'utilisateur en bloquant les caractères de mot de passe à mesure qu'ils sont saisis.

Une interface graphique de gestion de la confidentialité est créée pour que l'utilisateur puisse voir et contrôler les informations collectées par l'entreprise.

Les secrets sont traités dans la mémoire interne de la même puce.

Une fois ces implémentations définies, l'équipe réévalue toutes les recommandations et tous les risques de sécurité et examine le modèle de sécurité pour déterminer si les modifications ont résolu leurs problèmes.

B.7 Cycle de vie en cours

Maintenant que l'équipe a atteint une configuration approuvée, ils sont prêts à déployer leur technologie. Cependant, la sécurité ne s'arrête pas là. L'équipe négocie une méthodologie de surveillance des dispositifs périphériques pour les anomalies de sécurité et une méthodologie pour déterminer s'ils sont utilisés.

L'équipe planifiera comment chaque incident ou lacune est identifié, réparé et récupéré. Cela garantira que, au fil du temps, l'évolution du paysage technologique et de la sécurité ne prendra pas l'organisation par surprise.

B.8 Gestion du document

Version	Date	Brève description du changement	Autorité d'approbation	Éditeur / Société
1.0	08-Feb-2016	Nouvelle version PRD CLP.11	PSMC	Ian Smith GSMA & Don A. Bailey Lab Mouse Security
1.1	07-Nov-2016	Références au schéma d'évaluation de la sécurité de l'IoT de la GSMA ajoutées. Corrections éditoriales mineures.	PSMC	Ian Smith GSMA
2.0	29-Sep-2017	Ajoutées des informations de réseau LPWA au document et d'autres mises à jour mineures.	IoT Security Group	Rob Childs GSMA

B.9 Autres informations

Type	Description
Propriétaire du document	GSMA IoT Programme
Contact	Rob Childs - GSMA

Nous avons l'intention de fournir un produit de qualité pour votre usage. Si vous trouvez des erreurs ou des omissions, veuillez nous contacter avec vos commentaires. Vous pouvez nous en informer à prd@gsma.com

Vos commentaires ou suggestions et questions sont toujours les bienvenus.