Concevoir des systèmes IoT sécurisés, résilients et robustes… avec une racine de confiance

La conception d'un système embarqué pour l'Internet des objets (IoT) nécessite une approche différente de celle d'une conception embarquée classique… du fait de la connectivité à Internet. Ce genre de dispositif doit notamment suivre le rythme des changements rapides du monde de l'informatique et des technologies de sécurité de l'information, tout en étant aussi facile à mettre à jour qu'un PC et aussi sécurisé qu'un centre de données surveillé en permanence. Difficile ? Oui, mais réalisable avec une approche de conception système adaptée, fondée sur la mise en œuvre d'une racine de confiance, comme l'explique ici Microchip.

AUTEUR

Ian Pearson, ingénieur en chef, Applications - Systèmes sans fil, Cloud et IoT, Microchip Technology.

Avec un dispositif embarqué pour l'IoT, il est primordial de vérifier comment le dispositif s'intègre dans l›ensemble du système en modélisant les menaces et en analysant les risques, afin de déterminer ses performances et les fonctionnalités qu'il doit impérativement posséder. Qu'il se connecte par voie filaire ou sans fil, le dispositif peut avoir une durée de vie de un à vingt ans, au cours de laquelle il pourra être l'objet d'attaques. Pour parer à cela, la sécurité doit être une priorité majeure lors de la conception du système, sans oublier d'y intégrer la problématique liée aux opérations de maintenance et de mise à jour de logiciels de manière sécurisée, tout au long de la vie du produit.

Etant donné que n'importe quel dispositif IoT nécessite l'intervention de plusieurs acteurs (informatique, marketing, ingénierie, ventes, personnel de direction, finances et juridique), ceux-ci doivent tous définir et comprendre les besoins, les attentes, les coûts et les éléments livrables du dispositif. Les points à prendre en compte sont notamment la conformité des produits (respect des normes), la responsabilité (analyse légale, comme les législations RGPD, Réglementation générale sur la protection des données), la collecte des données, leur stockage et leur utilisation ainsi que la manière de traiter les éventuels cas d'intrusion ou de violation d'intégrité. Il faut aussi définir le modèle économique permettant de couvrir les coûts d'exploitation à long terme du dispositif dans le cadre d'un système connecté au cloud, et bien identifier les avantages pour l'utilisateur. La façon dont un produit est conçu et maintenu sur le long terme dépend directement de ces décisions initiales.

Dans ce cadre, la facilité d'utilisation et le besoin de renforcer la sécurité sont souvent en contradiction lors de la conception, tout comme les mots de passe complexes et les processus d'enregistrement des dispositifs. Ce qui signifie que sécurité et simplicité doivent être prises en compte dès le début de la conception.

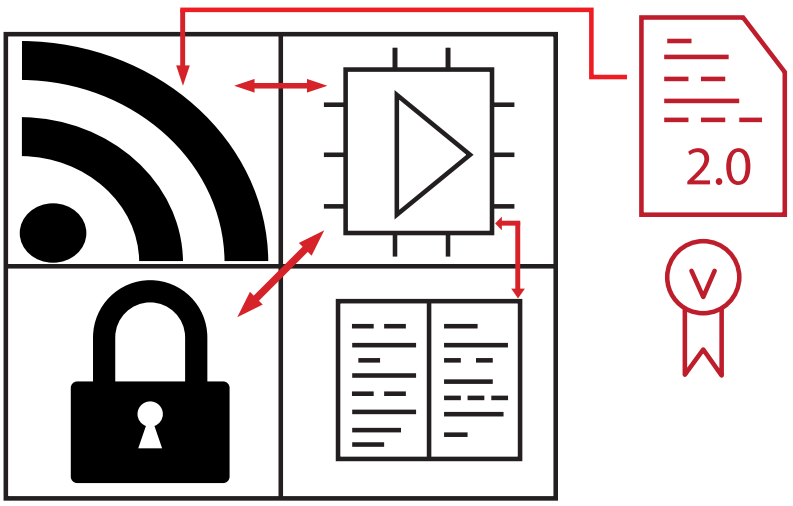
Si l'on regarde de plus près un produit embarqué connecté, il fait appel à quatre composants de base - processeur, mémoire, communications et composant sécurisé – auxquels il faut ajouter le logiciel (figure 1).

Ces composants de base sont communs à tous les systèmes, et la manière précise dont ils sont mis en œuvre est un choix de conception qui doit se faire en fonction de l'utilisation exacte du produit, de l'estimation des risques et de l'attitude face à ces risques, mais aussi des coûts, des capacités de développement, de la sécurité et de la maintenabilité.

L'objectif doit être une conception robuste, fiable, résiliente, récupé-

1 LES CINQ PILIERS D'UN SYSTÈME EMBARQUÉ

L'analyse des interactions entre les composants de base d'une solution IoT est un préalable la conception proprement dite.



rable, sécurisée, digne de confiance, évolutive, maintenable, fabricable et utilisable. L'intégrité de la marque doit être préservée et les objectifs de coût doivent être atteints en fonction des demandes auxquelles le système sera confronté. Il faut accepter que les coûts de conception, de développement et de fabrication d'un dispositif connecté soient plus élevés que ceux d'un dispositif embarqué classique, autonome et que l'on ne peut pas mettre à jour. Cependant, si le produit est bien conçu, la valeur qu'il fournira sur le long terme dépassera de loin les montants investis. Il est donc logique, d'un point de vue financier, de développer correctement le dispositif IoT plutôt que de tenter de le réparer plus tard si les choses tournent mal (figure 2).

Un point d'ancrage : la racine de confiance

Un système sécurisé a besoin d'un moyen digne de confiance pour stocker des informations secrètes et authentifier certains éléments, tout en s'assurant que les secrets eux-mêmes ne soient jamais révélés. Un «ancrage de confiance», généralement sous la forme d'un composant sécurisé, permettra cela. Ces dispositifs offrent plusieurs méthodes physiques pour prévenir les attaques matérielles connues tout en offrant des fonctions telles que la génération de nombres aléatoires (RNG, Random Number Generator) de qualité (voir à ce sujet la norme NIST SP 800) et des algorithmes de chiffrement, tels que l'ECDSA-P256 (Elliptic Curve Digital Signature Algorithm, ou algorithme de signature numérique à courbe elliptique), conformes à la norme FIPS.

Ce composant sécurisé permet en premier lieu d'authentifier un dispositif auprès de services dans le cloud à l›aide de méthodologies de type PKI (Public Key Infrastructure, ou infrastructure à clé publique) à la fois éprouvées et bien comprises. Une manière de faire qui permet de préenregistrer les dispositifs dans le système lors de la fabrication, avec des certificats individuels pour chaque dispositif, et de générer un code QR lors de la fabrication pour relier le produit final à son certificat spécifique. L'utilisateur n'a plus alors qu'à lire le code QR chez lui lors de la mise en service. Le système backend sécurisé relie ensuite les certificats au compte du client, ce qui garantit une mise en service simple et sécurisée, tout en respectant les exigences réglementaires. Pour cette approche, Microchip a récemment présenté une solution à clé sécurisée pré-fournie, disponible avec un minimum de commandes de seulement 10 pièces. L'objectif étant d'aider les développeurs à automatiser l'authentification sécurisée dans le cloud, quelle que soit la taille de leur projet. Connu sous le nom de Trust-Platform (Plate-forme de confiance), cette offre à trois niveaux propose des composants sécurisés prêts à l'emploi, pré-approvisionnés, préconfigurés ou entièrement personnalisables, et permet l'authentification auprès de toute infrastructure de cloud public ou privé, ou auprès d'un réseau LoRaWAN (protocole de communication bas débit à très faible consommation) (photo).

Ensuite, le composant sécurisé authentifie des données. Car grâce à l'ancrage de confiance, on peut s'assurer que les mesures proviennent bien d'un dispositif spécifique et qu'elles n'ont pas été «trafiquées». Ce qui permet aussi de repérer des anomalies dans les données grâce à l'analyse cloud, dans la mesure où une intervention physique à grande échelle est difficile.

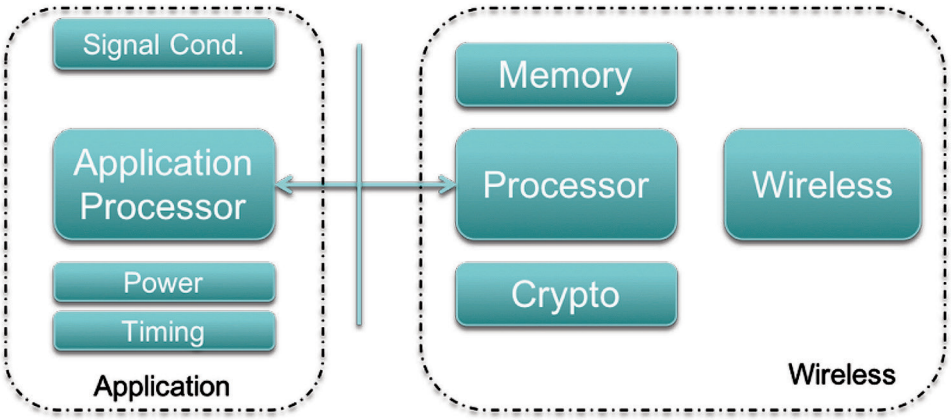
Autre point important, la technologie gère des amorçages sécurisés, ce qui signifie que l'on s'appuie sur un secret stocké dans le composant sécurisé pour identifier d'éventuelles modifications de la signature chiffrée du microcontrôleur hôte ou de fichiers de mise à jour du micrologiciel (firmware). D'autres contrôles d'intégrité en cours d'exécution, utilisant les méthodes des bibliothèques de sécurité de classe B, peuvent également être utilisés.

Côté logiciel, la mise à jour du firmware par voie hertzienne (FUOTA, pour Firmware Upgrade Over The Air) est sécurisée. Dans ce cas, le secret stocké dans le composant sécurisé sert à vérifier l'intégrité de la source de la mise à jour, et aussi à vérifier la signature de la mise à jour envoyée au dispositif pour confirmer sa validité avant le nouvel amorçage. Enfin, si la fabrication est bien gérée, le composant sécurisé permet d'empêcher le clonage et la contrefaçon du matériel.

Mais pouvoir stocker les secrets correspondant à un produit donné dans un composant matériel sécurisé exige aussi que les dispositifs soient programmés dans un environnement de fabrication sécurisé. Ce qui peut souvent poser des problèmes d'évolutivité et de confiance, notamment lorsque la fabrication est sous-traitée. La flexibilité de la fabrication et la facilité de mise en service sont assurées par l'achat de dispositifs contenant des informations privées, préprogrammées par le fournisseur du dispositif dans un environnement sécurisé, avec la possibilité de charger des informations publiques vers votre service cloud, selon un processus simple et automatisable.

2 EXEMPLE D'ANALYSE D'UNE SOLUTION CONNECTÉE SANS FIL

Dans de nombreux cas, un dispositif IoT fait appel à plusieurs processeurs. Un dispositif sans fil prendra souvent en charge certaines parties du traitement, en particulier dans le cas du Wi-Fi et du Bluetooth, afin de gérer les protocoles complexes sous-jacents. Ici l'architecture choisie dépendra notamment de l'utilisation finale, des besoins de l'utilisateur et de son comportement face aux risques.



Prêter attention aux mémoires de masse et aux alimentations

Les mises à jour de micrologiciels se font en général à l'aide d'un câble, relié directement à l'appareil, via un port série, une pratique mise en œuvre de depuis de nombreuses années. Mais alors comment une telle approche peut-elle fonctionner avec des dispositifs connectés, éventuellement installés dans des endroits inaccessibles, et déployés à grande échelle?

En cas de problème nécessitant le déploiement rapide d'une mise à jour en dehors des cycles de maintenance de routine, il est préférable d'éviter toute approche nécessitant une intervention physique. La solution consiste à lancer une mise à jour FUOTA, voire idéalement FUOTA sécurisée. Etant donné qu'il s'agit d'une approche sans manipulation physique, le système doit s'appuyer sur une authentification par le composant sécurisé pour empêcher les mises à jour malveillantes provenant d'une source inconnue ou non digne de confiance.

Mais comment effectuer la mise à jour elle-même? Idéalement, les mises à jour FUOTA sécurisées doivent se faire sans solliciter le microcontrôleur hôte. L'exécution d'une mise à jour directement sur la mémoire flash de l'appareil, sans sauvegarde locale, risque de provoquer le redoutable scénario de «bricking» (plantage mortel définitif) selon lequel une erreur irrécupérable se produit pendant la mise à jour.

La méthode FUOTA retenue doit donc être «agnostique» en termes de support physique. C'est-à-dire que le processus de mise à jour doit pouvoir fonctionner indépendamment de la bande passante, de la latence, des pertes et des abandons, quel que soit le support physique. Ainsi, le même processus back-end, côté serveur, et les mêmes mécanismes de téléchargement, de stockage et de contrôle d›intégrité, côté dispositif, peuvent servir sur un grand nombre de supports différents. Inévitablement, il y aura une certaine variabilité de cette «méthode unique pour tous» dans le cas d'un déploiement sur l'ensemble du système. Néanmoins, conserver autant que possible une approche standard, utilisant des méthodes modulaires, facilite la maintenance du code à long terme.

Si l'on déploie des dispositifs dans le monde entier et qu'il est impératif de réaliser une mise à jour contrôlée vers certains groupes de dispositifs, il est parfois difficile de connaître exactement les conditions d'alimentation et d'environnement de chaque dispositif concerné. On s'attend à ce que tout fonctionne exactement comme en laboratoire lors des tests, et que les dispositifs soient maintenus dans des conditions de fonctionnement idéales. Mais si ce n'est pas le cas? Que faire si un événement de type décharge électrostatique se produit sur un certain groupe de dispositifs et pas sur un autre? La conception de l'alimentation joue ici un rôle capital et doit faire partie des scénarios «et si...» et s'inscrire dans une stratégie globale de résilience et de récupération.

● La plate-forme de confiance de Microchip pour sa famille CryptoAuthentication permet aux OEM de toute taille et de toute expertise en sécurité de mettre en œuvre une authentification sécurisée pour des périphériques matériels.

Si ça n'arrive jamais, et que le système n'est jamais piraté…

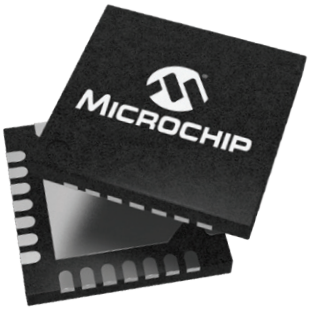
Tant mieux si rien n'arrive! Peut-être la chance est-elle de la partie, mais peut-être aussi que la planification de la conception préventive a rendu le défi suffisamment difficile pour que le pirate occasionnel trouve plus facile d'attaquer un autre système. Cependant il faut avoir à l'esprit qu'aucune sécurité n'est parfaite et peut toujours être remise en question ultérieurement. Ce qui ne doit pas empêcher, au contraire, de mettre en œuvre les meilleures techniques et fonctionnalités disponibles aujourd'hui, ni d'essayer de prévoir un certain nombre d'attaques à venir. Si le système s'appuie sur des dispositifs dignes de confiance et qu'il peut être mis à jour de manière sécurisée, on peut utiliser le côté cloud du système – par essence plus souple – pour gérer la plus grande partie de la charge, à condition que le système ait été conçu dans cette optique.

Dans ce cadre, il convient d'aborder la conception en utilisant les techniques recommandées par des organisations telles que l'IoT Security Foundation, Secure by Design du gouvernement britannique, UL2900, ISA 62443, ISA Secure et autres, au fur et à mesure de leur publication. Il faut aussi prévoir une marge suffisante pour permettre l'inévitable inflation du volume de code. Le mieux est encore de concevoir le système en envisageant le pire, puis de faire des compromis en conscience, plutôt que de rechercher le moindre coût sans tenir compte des scénarios «et si...». Car les dispositifs IoT représentent une surface d'attaque potentielle énorme pour les pirates, les acteurs malveillants, et même pour les petits malins qui veulent s'amuser un peu. ■

Défendez votre propriété intellectuelle, votre marque et votre chiffre d'affaires

Des solutions de sécurité faciles à ajouter et difficiles à pirater

Laissez Microchip vous aider à sécuriser non seulement vos systèmes, mais aussi votre marque et votre chiffre d'affaires. Forts de deux décennies d'expérience dans la sécurité, nos experts vous permettent d'intégrer la sécurité à vos systèmes sans aucune appréhension et en vous passant d'une expertise coûteuse en interne. Combinez cette expertise avec nos sites de production sécurisés et nos services d'approvisionnement et vous comprendrez pourquoi tant d'entreprises font confiance aux experts de Microchip pour les guider dans la conception de leurs systèmes.



Du chiffrage sécurisé jusqu'aux environnements d'exécution de confiance, trouvez les mises en œuvre de sécurité qui répondent à vos besoins spécifiques grâce à notre large éventail de solutions logicielles et matérielles.

SMART | CONNECTED | SECURE

Sécurisez votre système en allant sur www.microchip.com/Secure

MICROCHIP