Comment simplifier la mise en œuvre d'une sécurité matérielle pour les réseaux d'objets connectés

Alors que les failles de sécurité des systèmes embarqués ouvrent la voie à de nouveaux vecteurs d'attaque pour les pirates, une nouvelle génération de microcontrôleurs facilite la tâche des développeurs d'objets connectés, leur permettant de configurer et de déployer facilement et rapidement des fonctionnalités de sécurité. Dans ce cadre, Microchip montre ici que des microcontrôleurs ad hoc peuvent simplifier la mise en œuvre de la sécurité tout en limitant les connaissances techniques nécessaires et en diminuant les surcoûts éventuels.

AUTEUR

Ramanuja Konreddy, Senior Product Marketing Engineer pour les microcontrôleurs 32 bits, Microchip.

Sous la double pression de la très faible consommation des systèmes et de leur connectivité associée, le monde de l'Internet des objets arrive à un tournant. D'un côté, les réseaux d'objets connectés promettent de révolutionner nombre de secteurs d'activité (automobile, industrie, maisons intelligentes, secteur médical…), et d'un autre côté, les cas de cyberattaques se multiplient. Des injections de code malveillant aux attaques de déni de service distribuées (DDoS), en passant par les attaques visant à décharger les batteries, ce qui jette un voile d'incertitudes sur les belles promesses du monde des objets connectés. Il n'est donc pas surprenant, dans ces conditions, que les failles associées aux violations de sécurité de ces appareils dernier cri deviennent le souci numéro un des développeurs.

En d'autres termes, la vitesse à laquelle les appareils se connectent à Internet est supérieure à la vitesse à laquelle la sécurité est activée lors de leur déploiement. L'une des raisons de ce décalage est liée au fait que la sécurité est longtemps restée au second plan dans le domaine des applications embarquées. Une seconde raison est qu'il n'y a que très peu de microcontrôleurs disponibles sur le marché actuellement qui intègrent une sécurité intrinsèque capable de respecter les contraintes budgétaires des réseaux d'objets connectés.

Dans ce contexte, les cyberpirates ciblent de plus en plus les réseaux d'objets connectés non protégés, comme on a pu le voir récemment quand des hackers ont exploité les failles d'un thermomètre électronique immergé dans le bassin à poissons d'un casino en s'en servant pour accéder à la base de données des plus gros joueurs de l'établissement. Ce qui prouve à quel point les installations de domotique et immotique sont menacées via les failles de sécurité potentielles des appareils tels que les thermostats, les réfrigérateurs et les systèmes de chauffage et de climatisation (HVAC, Heating, Ventilation and Air-Conditioning). Ou bien encore des systèmes de surveillance par caméra en circuit fermé (CCTV, Closed-Circuit TeleVision) des établissements bancaires ou commerciaux qui, s'ils sont mal sécurisés, sont vulnérables car directement connectés au réseau des entreprises (figure 1).

A ce stade, il convient de mentionner que, tandis que les bonnes pratiques conventionnelles en matière de sécurité sont mises en œuvre au niveau des serveurs et des passerelles, la consommation et l'empreinte réduite des objets technologiques de pointe se révèlent être des obstacles à l'ajout de fonctions de sécurité robustes. De plus, le développement d'applications de sécurité peut ajouter un surcoût significatif en termes de temps et de prix de revient. Il s'agit donc de savoir comment les développeurs d'objets connectés peuvent limiter les failles de sécurité tout en maintenant une faible consommation énergétique. Une des réponses est de mettre en place un framework de sécurité à un stade précoce de la phase de conception. Une seconde est de tirer parti des fonctionnalités de microcontrôleurs économiques intégrant nativement des fonctionnalités de sécurité matérielle qu'il est possible de combiner avec le framework de sécurité préalablement implanté.

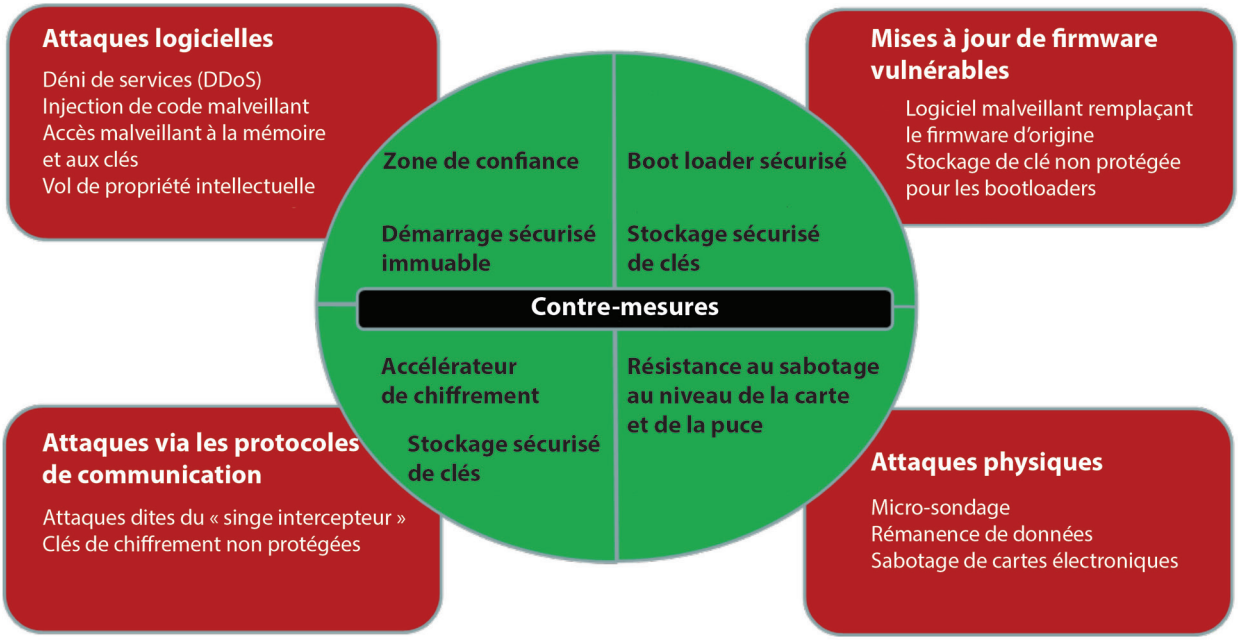
Plusieurs angles de sécurité dans l'Internet des objets

Un réseau d'objets connectés doit être sécurisé contre les attaques via les protocoles de communication, les logiciels malveillants et les attaques physiques. Pour prévenir les attaques via les protocoles de communication ou les attaques dites du « singe intercepteur », on utilise en général un module de chiffrement qui se charge du cryptage, du décryptage et de l'authentification. Par exemple, la technologie Arm TrustZone restreint l'accès à une mémoire spécifique, aux périphériques et aux composants d'entrées/sorties. Elle partitionne le microcontrôleur en zones fiables et zones non fiables et isole les données sensibles des données non critiques. Le démarrage sécurisé garantit que le microcontrôleur démarre dans un état connu et sûr, et, s'il est mis en œuvre avec Arm TrustZone, peut fournir un environnement aidant à contrer les logiciels malveillants.

La sécurité physique d'un réseau d'objets connectés peut aussi être améliorée grâce à des broches dites « anti-sabotage » offrant une protec-

1 APERÇU DES MENACES DE SÉCURITÉ SUR SITE ET À DISTANCE DIRIGÉES CONTRE UN RÉSEAU D'OBJETS CONNECTÉS

On voit ici des exemples de contremesures intégrées à des systèmes embarqués pour les protéger contre d'éventuelles attaques.



tion contre les attaques au niveau de la carte électronique. En cas de tentative de sabotage de la carte ou du châssis, ces broches peuvent être programmées pour fournir des réponses adéquates, y compris l'effacement des données secrètes. Il est important ici d'avoir une résistance au sabotage qui soit opérationnelle également au niveau de la puce, ajoutant ainsi une protection contre la contrefaçon et le vol de propriété intellectuelle.

En plus de ces trois aspects, il est essentiel d'avoir recours à une racine de confiance matérielle, qui peut être mise en œuvre avec un démarrage sécurisé et renforcée par un système d'octroi de clés de sécurité. Les développeurs de réseaux d'objets connectés doivent alors atteindre l'équilibre entre la faible consommation énergétique et la sécurité. Pour les appareils IoT de pointe alimentés par batterie, l'utilisation de l'énergie se révèle de fait capitale, et exige de la part des microcontrôleurs qu'ils puissent réduire de façon drastique la consommation énergétique tout en ajoutant une sécurité robuste.

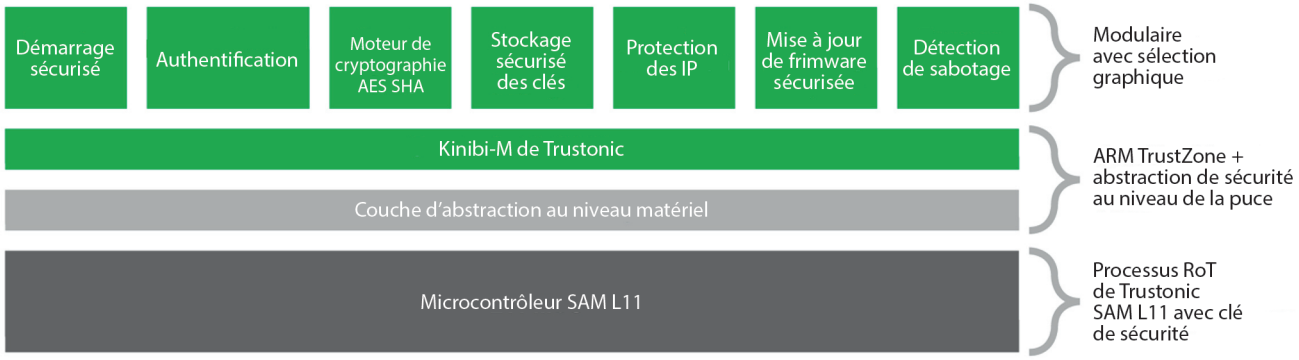
Dernier point, mais non des moindres, les réseaux IoT économiques nécessitent un mécanisme simple pour la mise en œuvre de la sécurité. Un mécanisme qui reprend les détails de sécurité de bas niveau pour éviter toute complexité et qui est capable de réduire les courbes d'apprentissage et tout surcoût substantiel.

Vers une simplification de la sécurité embarquée

Le microcontrôleur SAM L11de Microchip est un exemple d'architecture qui simplifie la mise en œuvre de ces fonctionnalités de sécurité. Il est conçu avec des technologies de sécurisation qui ont été intégrées pendant la phase de conception du circuit, et non rajoutés par la suite. Il fonctionne à 32 MHz avec une configuration de mémoire flash jusqu'à 64 Ko et jusqu'à 16 Ko de SRam. Dans cette

2 UNE SOLUTION DE SÉCURITÉ DE BOUT EN BOUT

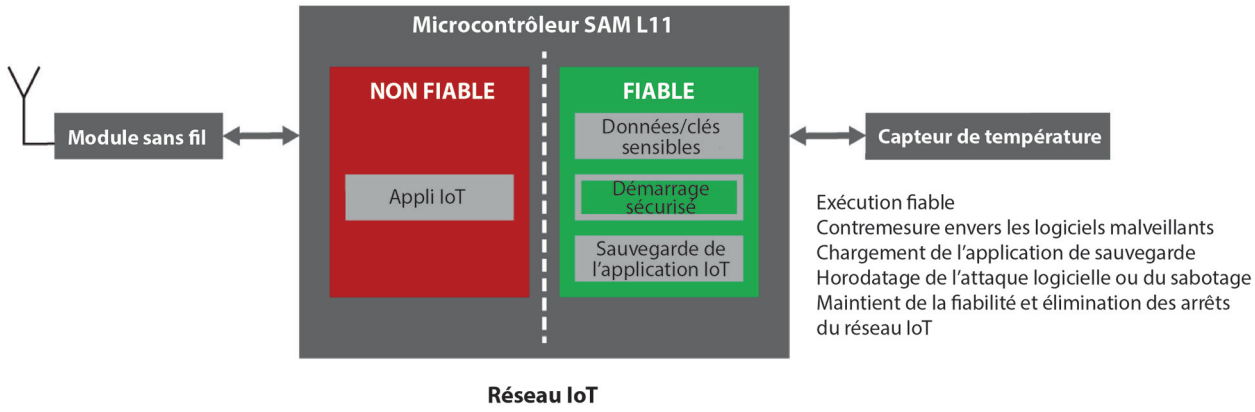
Les différents modules fournis par un framework sont destinés à simplifier la mise en œuvre de la sécurité.



Solution de sécurité de bout en bout

3 EXEMPLE D'UN NŒUD DE L'IOT SÉCURISÉ

Le démarrage sécurisé (bootloader) garantit que le microcontrôleur démarre dans un état connu et sûr.



architecture, quatre éléments de sécurité sont nativement intégrés :

- Démarrage sécurisé

Le SAM L11 intègre un système de démarrage sur une mémoire ROM qui facilite le démarrage sécurisé. Le microcontrôleur possède un accélérateur de chiffrement pour le calcul des algorithmes classiques AES (Advanced Encryption Standard), SHA (Secure Hash Algorithm, fonction de hachage cryptographique conçue par la National Security Agency aux Etats-Unis) et GCM (Galois/Counter Mode, mode d'opération de chiffrement par bloc en cryptographie symétrique) pour le cryptage, décryptage et l'authentification. Il dispose d'un TNRG (True Number Random Generator) conforme aux recommandations du NIST (National Institute of Standards and Technology) pour la génération de nombres aléatoires.

- Environnement d'exécution fiable

La technologie Arm TrustZone permet la création d'une zone sécurisée sur le SAM L11. Celle-ci, quand elle est combinée au démarrage sécurisé, crée alors un « environnement d'exécution sécurisé », ou TEE (Trusted Execution Environment), permettant de contrer efficacement les logiciels malveillants. Le TEE permet aux réseaux d'objets connectés d'entreprendre une action curative quand il contre un logiciel malveillant. Ce qui évite l'arrêt des fonctions critiques et améliore de façon significative la fiabilité des réseaux IoT.

- Stockage sécurisé des clés

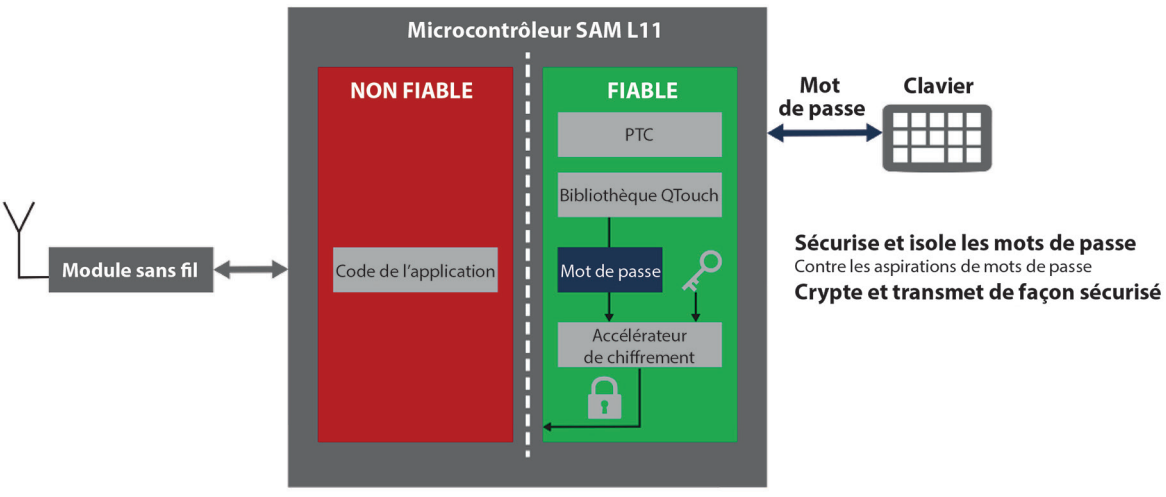
En plus des broches anti-sabotage le protégeant au niveau de la carte, le SAM L11 possède un bouclier actif sur 256 octets de RAM, qui peut résister aux micro-sondages au niveau de la puce et aux problèmes de rémanence des données afin d'offrir un stockage sécurisé pour les clés volatiles. Il intègre également 2 Ko de flash spécifique, qui peuvent être brouillés pour stocker les clés non volatiles, certificats et autres données sensibles. Le stockage des clés sécurisé sur le composant protège les systèmes contre les attaques logicielles et les protocoles de communication et offre aux développeurs une option pour effacer les données sensibles en cas de détection d'une tentative de sabotage.

- Un framework complet de solutions de sécurité

Les SAM L11 sont compatibles avec un framework complet de solutions de sécurité qui offre une solution de bout en bout, depuis l'octroi de la clé de chiffrement sur un site sécurisé, pendant la phase de fabrication des puces, jusqu'à l'implémentation des

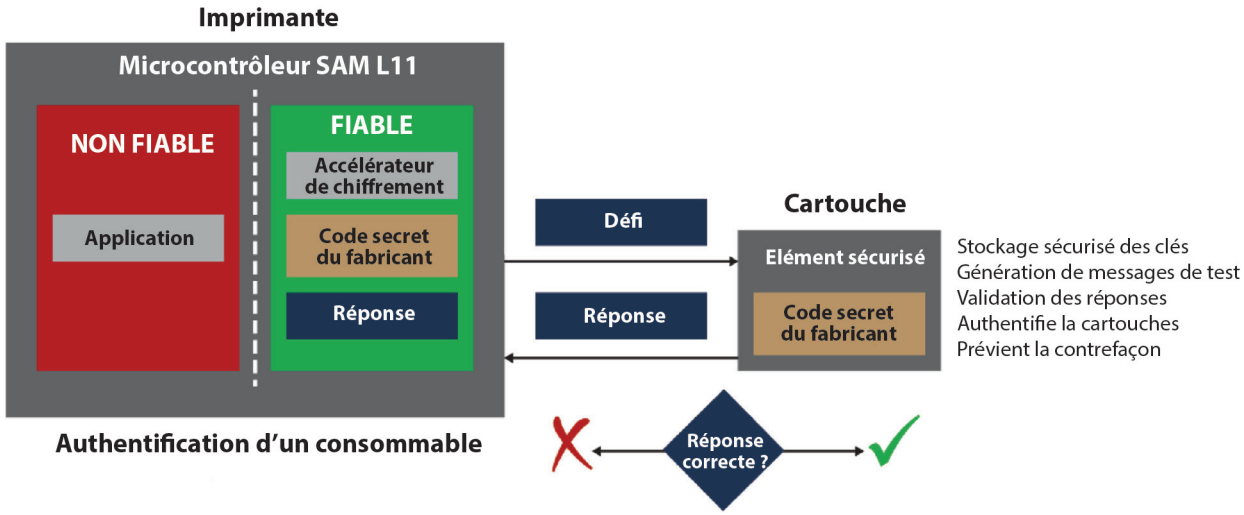
4 EXEMPLE D'UN CLAVIER DISTANT SÉCURISÉ

Pour prévenir les attaques via les protocoles de communication ou les attaques du « singe intercepteur », on utilise un module de chiffrement qui se charge du cryptage, du décryptage et de l'authentification.



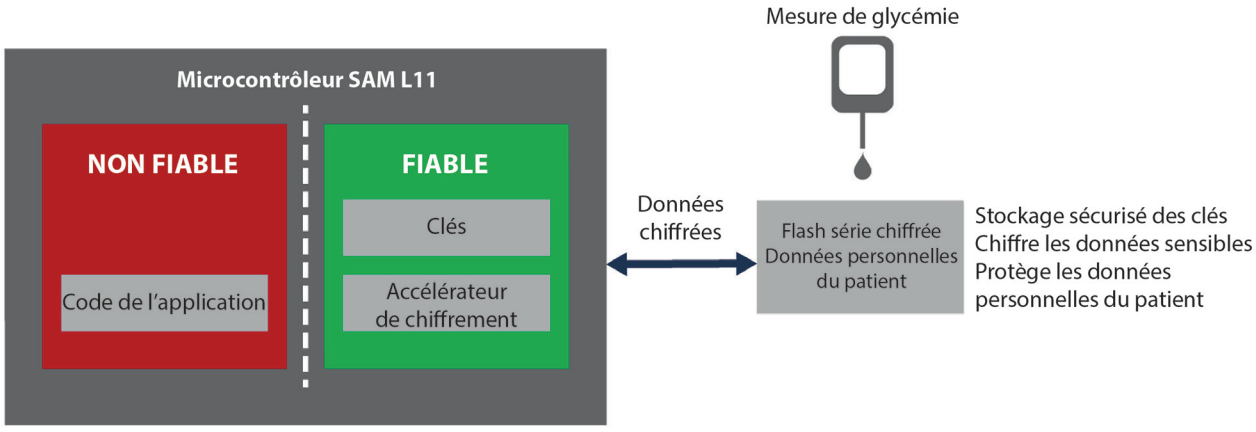
5 AUTHENTIFICATION D'UN CONSOMMABLE

Les fonctionnalités de sécurité matérielle intégrées au microcontrôleur permettent d'effectuer l'octroi de clé sur le site de fabrication de Microchip grâce à la racine de confiance (Root of Trust).



6 EXEMPLE DE CHIFFREMENT DE DONNÉES MÉDICALES

L'accélération du chiffrement et la mise en œuvre de clés cryptographiques sécurisent les données médicales issues de la mesure de glycémie d'un patient.



modules de sécurité pendant le développement de l'application, en passant par la mise à jour à distance du firmware à tout moment pendant le cycle de vie du composant. Le framework comprend le logiciel de sécurité Kinibi-M de Trustonic qui reprend les détails de bas niveau des fonctionnalités de sécurité du composant et qui offre une interface graphique modulaire aux développeurs leur permettant de choisir le module de sécurité adapté à leur application (figure 2). Prenons par exemple, le bootloader utilisé pour sécuriser les mises à jour du firmware. Dans ce cas, les ingénieurs systèmes embarqués n'ont pas besoin de passer au crible des centaines de pages de fiches techniques pour trouver comment créer un bootloader sécurisé. Ainsi, le framework de sécurité, défini avec précision, offre un module aux développeurs leur permettant de mettre en œuvre rapidement un bootloader sécurisé sur leur application (figure 3). Aucune formation sur la sécurité embarquée n'est nécessaire, ce qui fait que le temps de développement et les coûts sont significativement réduits.

Les fonctionnalités de sécurité matérielle, profondément intégrées aux microcontrôleurs SAM L11, permettent en outre aux ingénieurs systèmes embarqués d'effectuer l'octroi de clé sur le site de fabrication de Microchip grâce au processus de racine de confiance (RoT, Root of Trust) de Trustonic (figures 4 et 5)

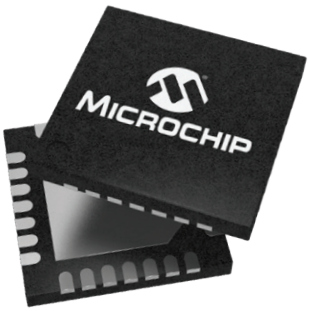
Le framework de solution de sécurité complet permet aux développeurs de systèmes embarqués novices en matière de sécurité de ne pas perdre de temps en formation et d'éviter les surcoûts. En un tournemain, ils peuvent facilement mettre en œuvre une sécurité robuste pour les divers cas d'utilisation de leur application (figures 3, 4, 5 et 6).

Enfin, le composant intègre aussi la technologie picoPower de Microchip qui garantit une faible consommation énergétique en fonctionnement et en mode veille et bénéficie des meilleures notes ULPMark de la part du consortium EEMBC (Embedded Microprocessor Benchmark Consortium). Il offre également plusieurs modes d'économie d'énergie et des techniques de faible consommation, de sorte que les développeurs peuvent facilement mettre en œuvre la sécurité, sans faire de compromis sur la consommation énergétique. ■

Différenciez votre application

Personnalisez votre projet embarqué grâce à nos briques intégrées très souples

Microchip sait que vos impératifs de conception sont uniques. C'est pourquoi nous vous proposons un ensemble robuste de périphériques intégrés pour un large éventail d'applications :



- Ajoutez des affichages percutants et des fonctions tactiles pour une interaction intuitive avec l'utilisateur
- Connectez votre application au monde, avec ou sans fil
- Commandez votre moteur ou votre système de conversion d'énergie
- Protégez les données de votre application

Personnalisez votre produit avec des périphériques intégrés, et réduisez les coûts et le temps de conception.

Personnalisez votre projet sur www.microchip.com/FlexibleFunctions

MICROCHIP

Le nom et le logo Microchip sont des marques commerciales déposées de Microchip Technology Incorporated aux Etats-Unis et dans d'autres pays. Toutes les autres marques commerciales citées appartiennent à leurs entreprises respectives.
© 2019 Microchip Technology Inc. Tous droits réservés. DS30010187A. MEC2287Fre05/19