

Plus de sécurité pour les systèmes IoT

Christian Kriebler, directeur Sécurité et Identification, EBV Elektronik
Thibault Richard, FAE spécialisé Connectivité et Sécurité, EBV Elektronik

La croissance rapide de l'Internet des objets (IoT) multiplie les besoins en performance et en connectivité dans les microcontrôleurs embarqués (MCU). En effet, le volume d'information généré par les capteurs nécessite un traitement local des données (edge node) où fleurit notamment l'utilisation d'algorithmes de type machine learning. Le volume de données est ainsi réduit, puis acheminé vers le cloud où les données sont protégées, stockées et analysées plus en détail. Cette infrastructure allant de l'objet connecté vers le cloud nécessite un niveau de sécurité élevé pour garantir l'intégrité des données envoyées, mais également pour protéger ces objets connectés contre les attaques et les malwares. La sécurité est essentielle pour authentifier les objets connectés ainsi que pour garantir la confidentialité des données. Elle devient également un enjeu majeur dans les systèmes critiques, comme par exemple les systèmes d'aide à la conduite ou le véhicule autonome afin de garantir que les fonctions critiques ne sont pas compromises.

Exigences de sécurité dans l'IoT

Nous avons régulièrement connaissance de nouvelles cyberattaques, conduites par des hackers ou des gouvernements sur les systèmes industriels et commerciaux. Celles-ci sont de plus en plus élaborées et ciblent un nombre croissant d'appareils. En 2010, le ver Stuxnet aurait causé de lourds préjudices aux sites de traitement nucléaires iraniens. Il pourrait s'agir d'une attaque délibérée conduite par un autre état. Le bug Heartbleed qui affecte le logiciel de sécurité OpenSSL (utilisé par de nombreux sites web) a été découvert en 2014. Il a permis de dérober des informations sur de nombreux systèmes, notamment celui du Canada Revenue Service ainsi qu'un important prestataire de service de santé aux États-Unis. En 2016, le malware Mirai a transformé en « bots » un grand nombre d'appareils connectés grand public, comme des caméras de surveillance et des routeurs. Ces machines zombies ont ensuite servi à lancer des attaques par déni de service distribué (DDoS) sur de nombreux systèmes informatiques.

Les chercheurs trouvent régulièrement de nouvelles vulnérabilités. Il peut s'agir de bugs logiciels, comme Heartbleed, ou de problèmes matériels, comme la faille Meltdown détectée dans divers microprocesseurs, notamment certains cœurs ARM.

Un accès malveillant à un seul objet connecté est déjà dommageable en soi. Mais le véritable risque est qu'une faille de sécurité permette de compromettre un nombre illimité d'appareils, et donc de favoriser la prolifération d'attaques (DDoS, malwares, rançongiciels, etc).

Un certain nombre de fonctionnalités peuvent améliorer la sécurité d'un objet connecté : doter chaque appareil d'une identité unique rend possible l'authentification sécurisée avec le cloud. Ce procédé d'authentification permet également l'échange de données cryptées sur le réseau ainsi que l'authentification des logiciels et de leurs mises à jour. Enfin, au niveau local, la mémoire des objets connectés peut être protégée en utilisant des algorithmes de cryptographie.

Pour parvenir au niveau de sécurité requis, la conception d'un MCU doit prendre en considération de multiples paramètres : logiciels, sécurité, analyse des systèmes, etc. Il ne s'agit plus d'un simple problème de conception de la puce. Les concepteurs doivent aussi tenir compte des facteurs humains et des interactions avec le monde extérieur.

Toutefois, le prix est un facteur déterminant sur le marché de l'IoT, et les mesures de sécurité supplémentaires ne doivent pas entraîner une hausse significative du prix ou de la complexité.

Fonctionnalités de sécurité matérielle

De nombreuses fonctionnalités matérielles peuvent être utilisées pour renforcer la sécurité d'un objet connecté. Suivant les cas, on pourra recommander l'utilisation d'un secure element (élément sécurisé), d'un MCU avec des fonctionnalités de sécurité, ou bien les deux.

Le secure boot (amorçage ou démarrage sécurisé) est une fonctionnalité essentielle qui permet au MCU de garantir que le logiciel du fabricant est authentique et qu'il n'a pas été altéré. Le MCU commence par exécuter un bootloader depuis la mémoire ROM qui vient ensuite vérifier la signature du logiciel dans la mémoire Flash avant d'exécuter ce dernier. La mémoire Flash peut également être

chiffré afin d'apporter un niveau de protection supplémentaire.

Le PUF (Physically Unclonable Function) utilise un processus de variations aléatoires lors de la conception de la puce afin de lui donner une identité unique, à l'instar d'une empreinte digitale. Cette technologie peut être utilisée pour générer une clé afin d'encrypter des données, authentifier l'objet sécurisé sur le cloud, ou encore pour injecter des secrets de manière sécurisée (provisioning). Les données protégées par le PUF ne peuvent être déchiffrées que par le même équipement, garantissant ainsi la sécurité des données même si elles sont copiées vers un autre système.

Les processeurs ARM de dernière génération implémentent un système de sécurité appelé TrustZone. Celui-ci peut être utilisé pour protéger des ressources, comme par exemple les données privées et les mots de passe, en s'assurant qu'ils ne puissent être manipulés que dans un environnement sécurisé.

TrustZone permet de segmenter l'espace d'adressage en deux environnements : un environnement sécurisé et un autre non sécurisé. L'environnement non sécurisé procure un accès limité aux données ainsi qu'aux registres non-critiques pour le système. Le code non sécurisé ne peut accéder aux ressources sécurisées que par le biais d'interfaces spécifiques exposées par l'environnement sécurisé. Le système d'exploitation et les applications s'exécutent généralement dans l'environnement non sécurisé, tandis que les fonctionnalités critiques de sécurité s'exécutent dans l'environnement sécurisé. Ce qui réduit la quantité de code devant être soigneusement écrit et vérifié afin de garantir un niveau de sécurité optimal.

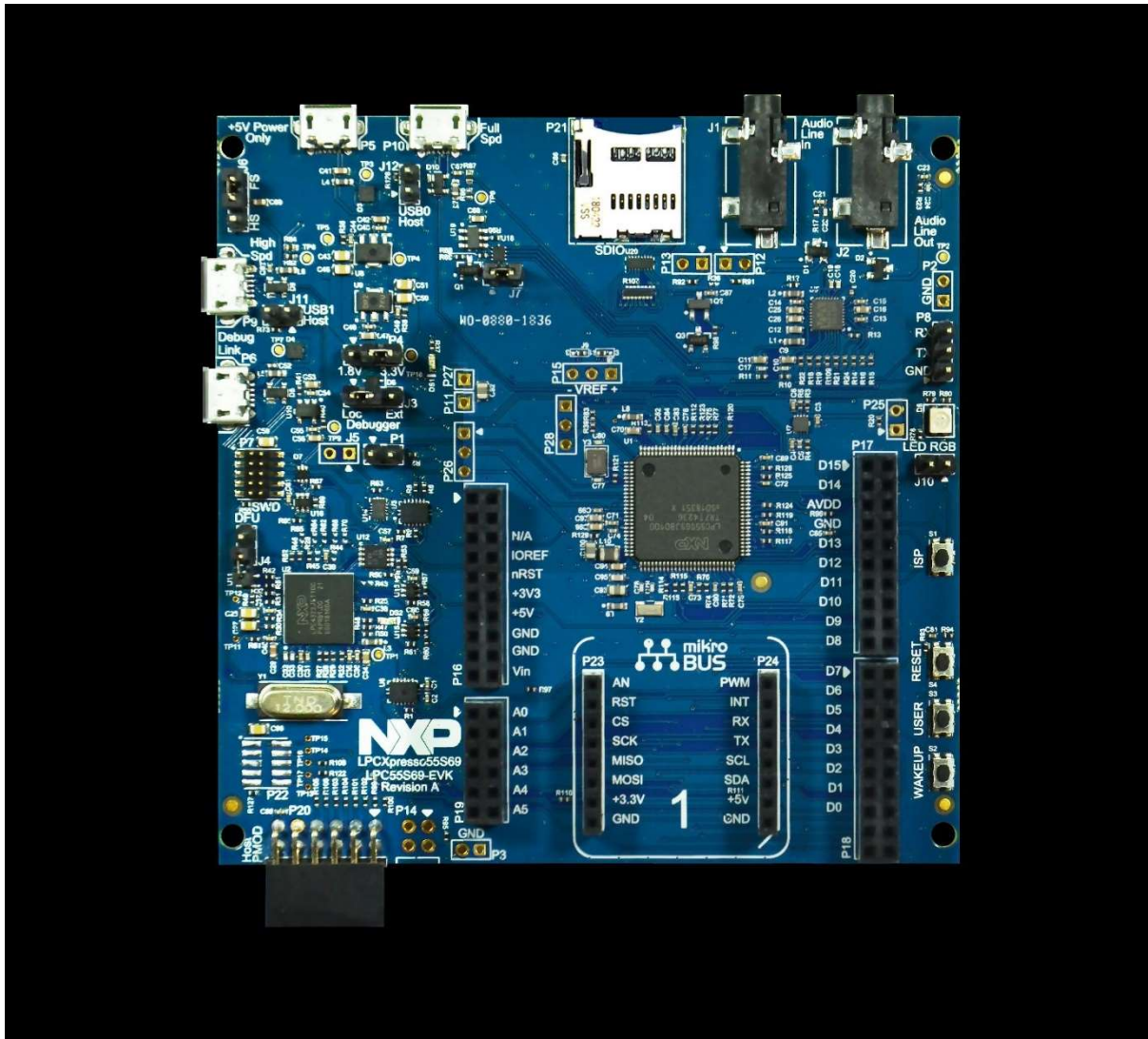
Un générateur de nombres aléatoires (TRNG) est nécessaire pour obtenir une entropie élevée et protéger les procédures de handshake contre les attaques de replay. Parmi les autres fonctionnalités possibles figurent la détection d'accès physique à la puce grâce à l'utilisation de tamper pin, l'utilisation d'accélérateurs hardwares pour les fonctions de chiffrement, ou encore l'utilisation d'une couche de protection supplémentaire au niveau du silicium pour protéger les parties sensibles de la puce (typiquement dans les produits secure element ou smart card). Les fonctions implémentées dans un système donné devront tenir compte du niveau de sécurité requis et du coût supplémentaire du hardware.

Exemple



Le microcontrôleur LPC55S6x qu'a récemment sorti NXP intègre de nombreuses fonctionnalités de sécurité hardware comme décrit plus haut, ce qui le rend unique sur le marché des MCU. Il est doté d'un double cœur ARM Cortex-M33, supportant la fonctionnalité TrustZone ainsi que plusieurs coprocesseurs pour accélérer les fonctions cryptographiques. Tandis que la puce permet un secure boot avec une protection anti-rollback, le hardware supporte également l'exécution en temps réel des images chiffrées à partir de la mémoire Flash. Le contenu de la mémoire Flash est déchiffré uniquement dans le chemin d'exécution du cœur (instruction fetch). Par conséquent, les tentatives malveillantes de lecture directe de la mémoire Flash n'exposeront que des données chiffrées. La propriété intellectuelle du logiciel et les données associées sont donc protégées.

Le MCU LPC55S6x utilise la technologie PUF, basée sur un bloc dédié de la mémoire SRAM. Lors de la mise sous tension, chaque cellule de cette mémoire SRAM s'affiche sous forme de 1 ou de 0, de sorte que ces valeurs de démarrage créent un schéma aléatoire, répétable et propre à chaque puce. Cette empreinte digitale peut ensuite être utilisée comme une clé secrète afin d'identifier de manière unique un équipement et fournir un hardware root of trust pour les autres fonctions de sécurité. Des accélérateurs hardwares sont également présents pour permettre le chiffrement/déchiffrement des données pour une multitude d'algorithmes cryptographiques symétriques et asymétriques. Cette puce dispose de tamper pin, de GPIO et DMA sécurisés ainsi qu'un système de débogage JTAG sécurisé activé par authentification.



Le MCU LPC55S6x est le premier à combiner toutes ces fonctionnalités dans un package de sécurité complet. Il offre un haut niveau de sécurité avancé pour de nombreuses applications IoT et embarquées, pour un coût minime.

Le second cœur ARM et le coprocesseur DSP peuvent alors être utilisés pour exécuter des logiciels applicatifs complexes. Par exemple, les systèmes de machine learning et d'inférence peuvent être implémentés à l'aide de la librairie CMSIS-NN ARM. Il s'agit d'un ensemble de routines permettant de faire fonctionner un réseau de neurones optimisé en performance et taille mémoire pour le cœur Cortex-M. Cette librairie peut être utilisée avec les Framework standard d'Intelligence Artificielle comme par exemple Caffe pour les applications nécessitant de la classification d'images, de la reconnaissance vocale ou encore pour le traitement automatique du langage naturel en vue d'améliorer les interfaces utilisateur.

C'est cette même technologie que l'on retrouve dans des applications telles que les voitures qui peuvent identifier le conducteur et régler automatiquement la position du siège et autres paramètres de conduite. Les robots capables de reconnaître les objets et les personnes dans leur environnement peuvent travailler de façon plus sûre. Un automate pourrait ainsi reconnaître les clients et leur demander s'ils veulent leur boisson chaude habituelle. La capacité de traitement du signal pourrait être utilisée, avec la reconnaissance faciale, pour implémenter le beam forming (filtrage spatial) en utilisant plusieurs microphones afin d'isoler les voix dans un environnement bruyant et d'identifier la personne qui parle.

Conclusion

L'ajout des fonctions de sécurité dans les microcontrôleurs modernes permet de répondre aux besoins croissants en sécurité. La sécurité embarquée devient possible grâce à l'intégration d'un root of trust hardware qui permet l'authentification, la communication et le stockage sécurisé des données. Le MCU LPC55S6x intègre l'ensemble des fonctionnalités de sécurité nécessaire pour l'IoT, tant en répondant aux contraintes de coût et de performances.

EBV est un distributeur de composants microélectroniques. Son expertise dans les marchés industriels, automobiles, et des technologies comme la sécurité, la communication sans fil, etc. lui a permis de développer une parfaite compréhension des besoins de l'IoT. Par ailleurs, EBV est en mesure de fournir une assistance technique complète à chaque étape du processus de conception.

LPC55S6X MCU FAMILY BLOCK DIAGRAM

