L'authentification matérielle est la clé pour un Internet des objets sécurisé

La problématique de la sécurité devient un enjeu crucial pour l'Internet des objets, comme l'ont démontré récemment un certain nombre d'attaques malveillantes fortement médiatisées. Pour pallier ce problème, les appareils connectés doivent disposer d'une architecture basée sur une véritable « racine de confiance » qui fournit un moyen d'établir des communications sécurisées uniquement avec les utilisateurs et applications dument certifiés. Explications du distributeur de composants et sous-systèmes électroniques Mouser.

Alors que l'Internet des objets (IoT) se développe, la problématique de la sécurité devient un enjeu crucial. La standardisation de la connectivité et des protocoles que génère l'IoT augmente en effet les risques pour les appareils, dispositifs et équipements connectés, et, au travers d'eux, pour les réseaux de service auxquels ils donnent accès. Un certain nombre de menaces se sont déjà manifestées, telles que le piratage de véhicules au travers de leurs systèmes d'info-divertissement connectés à Internet ou diverses attaques ciblant des appareils industriels ou grand public, voire même des jouets.

Dans bien des cas, ces attaques malveillantes se sont avérées relativement élémentaires pour la simple et bonne raison que les fabricants n'avaient guère pris de précautions. Les appareils sont en effet bien souvent fournis avec un mot de passe par défaut simple à deviner. Et les applications utilisées pour programmer les appareils IoT contiennent fréquemment des informations sur leurs structures de données internes, fournissant ainsi aux hackers de précieuses ressources.

• La standardisation de la connectivité et des protocoles que génère l'Internet des objets augmente les risques de sécurité pour les appareils, dispositifs et équipements connectés, et, au travers d'eux, pour les réseaux de service auxquels ils donnent accès.

AUTEUR

Mark Patrick, Supplier Marketing Manager, EMEA, Mouser Electronics.

En se concentrant sur les nœuds d'extrémité IoT et les appareils connectés, les hackers peuvent mettre au point divers types d'attaques, d'une simple observation visant à récupérer des informations utiles pour lancer une attaque infrastructurelle de plus grande envergure, à la manipulation directe de l'appareil ou du réseau. Pour pallier ce problème, les appareils connectés doivent disposer d'une architecture basée sur une véritable racine de confiance.

Authentifier les appareils connectés

Une racine de confiance (root of trust) fournit un moyen d'établir des communications sécurisées uniquement avec les utilisateurs et applications dument certifiés, limitant ainsi la capacité des hackers à envoyer des messages à un appareil susceptibles de compromettre sa sécurité. Elle permet également au réseau d'authentifier les appareils, empêchant ainsi les hackers d'utiliser leurs propres dispositifs pour accéder aux systèmes en usurpant l'identité d'appareils approuvés.

Les clés et certificats utilisés par les protocoles sécurisés doivent être stockés en mémoire. Néanmoins, cette zone mémoire doit être distincte de celle utilisée pour stocker les données d'application. Pour être approuvés et dignes de confiance, ces clés et certificats doivent non seulement être valides, mais également protégés contre toute analyse via des circuits matériels sécurisés empêchant leur lecture par des utilisateurs non autorisés. Les processeurs cryptographiques complètent

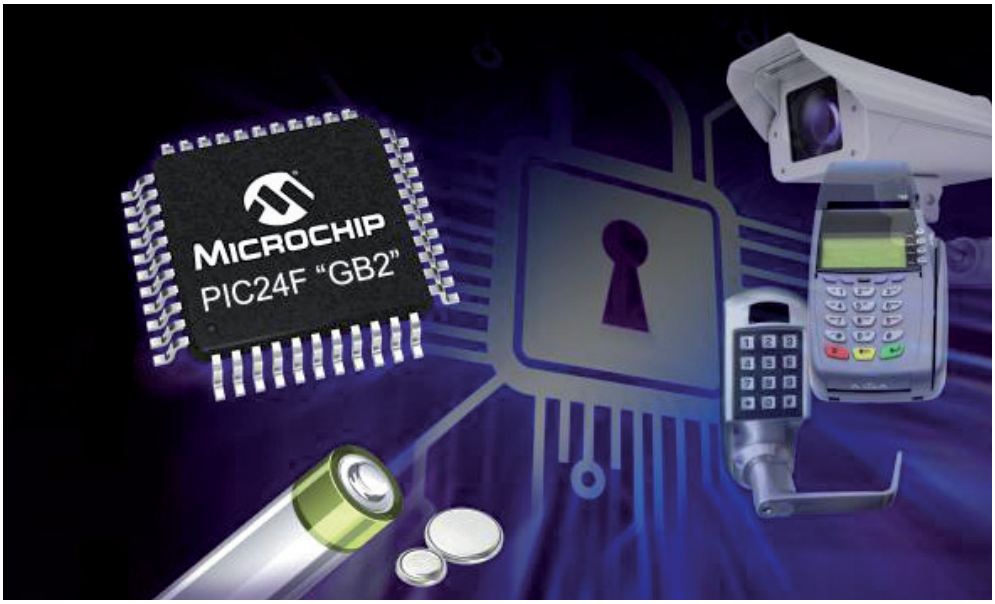
cette implémentation en fournissant un support direct aux protocoles nécessaires à l'authentification et à la communication sécurisées avec l'appareil, sans risquer d'exposer l'ensemble des clés et certificats confidentiels aux autres logiciels s'exécutant sur ce dernier.

Bien que les premiers produits connectés via l'IoT aient fait l'objet de nombreuses critiques en raison de leur faible niveau de sécurité, les infrastructures basées sur le concept de racine de confiance existent déjà et sont produites en masse. Les téléphones mobiles numériques, compatibles avec le standard GSM et les normes 3GPP ultérieures, et développés dans une perspective de sécurité renforcée, en sont un bon exemple.

Pour pouvoir accéder au réseau cellulaire sans fil, chaque téléphone doit disposer d'un module d'identité d'abonné (SIM, Subscriber Identity Module) permettant aux opérateurs d'authentifier et de communiquer avec le terminal. Basé sur une conception matérielle similaire et initialement développé pour les ordinateurs personnels, le Trusted Processor Module (TPM) est désormais intégré aux produits embarqués tels que les terminaux de point de vente (POS, Point-Of-Sale). Ces modules s'appuient sur une architecture d'infrastructure à clé publique (PKI, Public Key Infrastructure), offrant un ensemble de fonctions permettant de répondre aux divers besoins de sécurité des appareils connectés. Cette architecture est déjà utilisée dans des composants destinés aux téléphones et ordinateurs, mais également au sein de systèmes embarqués plus pointus.

Le concept de cryptographie asymétrique

L'infrastructure PKI gravite autour du concept de cryptographie asymétrique, dans lequel les documents et autres objets logiciels sont signés et vérifiés via une combinaison clé publique/clé privée. Le modèle mathématique PKI repose sur l'incapacité à dériver facilement une clé privée à partir d'une clé publique associée. La clé publique peut quant à elle être divulguée librement. Mais la clé privée doit être protégée. Dans un équipement embarqué, un processeur de cryptage sécurisé doté d'une mémoire protégée offre un



● Dans un équipement embarqué, un processeur de cryptage sécurisé doté d'une mémoire protégée offre un support idéal pour la protection des clés privées. Membre de la famille PIC24F GB2 de Microchip, le microcontrôleur PIC24FJ128GB204 doté de 128 Ko de mémoire RAM intégrée et d'un support cryptographique matériel en est un exemple.

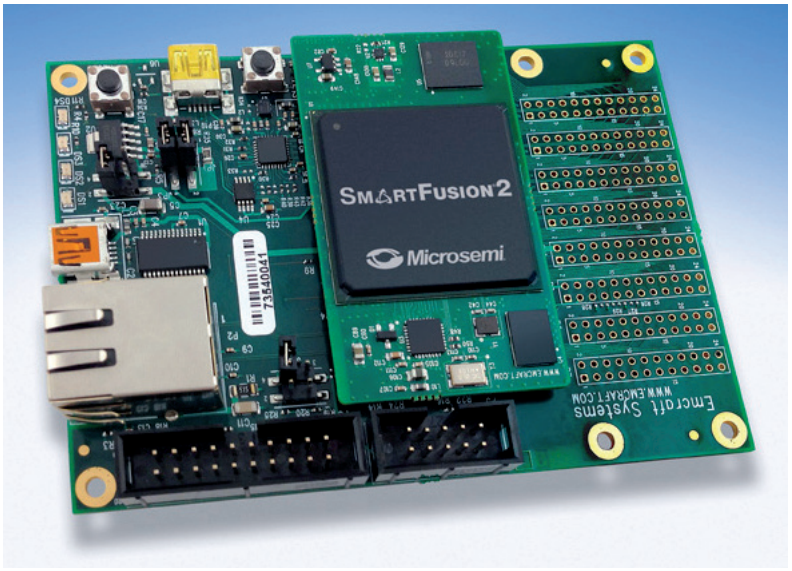
support idéal. Le microcontrôleur PIC24FJ128GB204 doté de 128 Ko de mémoire RAM intégrée et d'un support cryptographique matériel en est un exemple. Il fait partie de la famille des microcontrôleurs PIC24F GB2 développés par Microchip Technology.

L'une des fonctions clés du processeur au cœur des modules d'authentification matériels est de garantir qu'au démarrage, l'appareil exécute uniquement du code approuvé et qu'aucun utilisateur non autorisé ne l'a altéré. Cette fonction est connue sous le nom de démarrage sécurisé (secure boot). Lorsque l'appareil démarre et lit le code depuis la mémoire en lecture seule (ROM, Read Only Memory) intégrée, il vérifie que chaque segment majeur a été signé par un fournisseur autorisé. Le fournisseur utilise une clé privée pour signer le bloc de code. Ce processus de signature crée un hachage unilatéral combinant le code et la clé privée. Le composant d'authentification matériel examine ce hachage pour vérifier son authenticité. Toute modification apportée au code original doit être signée à l'aide de la clé pertinente, vérifiée par le module d'authentification avant la poursuite de l'installation ou de la mise à jour. Si l'appareil détecte un bloc de code dont la signature est incorrecte, il interrompt généralement le chargement du logiciel affecté et peut passer en état de reprise sur faute pour tenter d'obtenir le code autorisé auprès du fournisseur d'origine (éventuellement en rechargeant le code d'usine stocké dans la mémoire ROM), et, le cas échéant, envoyer une alerte à un serveur.

Bien qu'il soit possible de mettre en œuvre certains types de démarrage sécurisé sans module d'authentification matériel, il est difficile de certifier l'arrêt correct du processus si le hacker s'est infiltré suffisamment profondément dans le micrologiciel (firmware). Le processeur du module d'authentification matériel peut garantir la sécurité en décryptant uniquement les segments clés du micrologiciel pour le compte du processeur hôte si le hachage est correct et en refusant le service de décryptage à tout composant logiciel exempt de hachage ou de clé conforme. Grâce à cette capacité à protéger les clés embarquées et à interdire toute modification ou lecture par un attaquant, la gamme de FPGA flash de Microsemi (comme les SmartFusion 2) peut être utilisée pour mettre en œuvre un démarrage sécurisé, ainsi que d'autres fonctions de sécurité.

Des protocoles de communication sécurisés

Une fois que l'appareil a démarré correctement, celui-ci est en mesure de s'authentifier sur le réseau via des mécanismes PKI. En règle générale, l'appareil établit des communica-



● Grâce à la capacité à protéger les clés embarquées et à interdire toute modification ou lecture par un attaquant, la gamme de FPGA flash de Microsemi (comme les SmartFusion 2) peut être utilisée pour mettre en œuvre un démarrage sécurisé, ainsi que d'autres fonctions de sécurité.

tions sécurisées via un protocole tel que TLS (Transport Layer Security), un complément au protocole HTTP (HyperText Transfer Protocol) désormais standard. Les certificats à signature numérique stockés dans le module d'authentification matériel garantissent que les serveurs distants communiquent avec une ressource connue. Le certificat réel est stocké dans le module d'authentification afin que seules les données publiquement accessibles soient transmises via le réseau et le bus de données interne de l'appareil pour empêcher toute tentative d'espionnage de la part des hackers.

Sans module d'authentification matériel, un hacker peut utiliser un analyseur logique ou un autre instrument pour sonder la mémoire de l'appareil et obtenir les clés et certificats confidentiels afin de mystifier les serveurs réseau.

À l'inverse, l'appareil connecté doit être certain que les commandes qu'il accepte proviennent uniquement d'équipements ou de serveurs dignes de confiance. En utilisant le module d'authentification matériel pour s'assurer que les certificats de ces derniers correspondent aux clés stockées dans la mémoire protégée, l'appareil connecté a la garantie de communiquer uniquement avec des systèmes autorisés.

Avec l'évolution des profils de service, l'utilisation des échanges PKI permet d'ajouter ou de supprimer des certificats, ce qui garantit non seulement que les services peuvent être améliorés au fil du temps, mais aussi que les systèmes qui ne font plus partie du réseau ou qui présentent une vulnérabilité connue peuvent être retirés de la liste d'approbation.

En tirant parti de l'expérience et de l'infrastructure technologique développées pour la téléphonie mobile et l'informatique, les fabricants d'appareils connectés via l'Internet des objets peuvent donc prendre une longueur d'avance en dotant leurs produits d'une solide base de sécurité. L'existence de composants tels que les produits de la famille PIC24 GB2 de Microchip et les FPGA flash de Microsemi leur permet d'accéder facilement à ces technologies et de bénéficier d'une infrastructure de sécurité renforcée pour l'IoT. ■