Du concept au déploiement, la sécurité passe par une plate-forme de confiance

Par le biais d'une plate-forme de confiance, les utilisateurs ont accès à des mécanismes de sécurité personnalisables combinant outils, codes source et infrastructure de provisionnement. Une approche qui assure aux développeurs de systèmes embarqués l'accès à un système complet et sécurisé, allant de la conception jusqu'au déploiement, comme l'explique ici Microchip.

AUTEUR

Nicolas Demoulin, directeur marketing EMEA (Europe, Moyen-Orient & Asie), groupe Produits sécurisés, Microchip Technology

La sécurité est aujourd'hui une exigence primordiale pour les systèmes embarqués. Le désir de connecter des dispositifs à Internet pour en faciliter la commande, et de pouvoir accéder en direct aux données de leurs capteurs, entraîne en effet un risque élevé de piratage. Piratage qui ne met pas seulement en danger ces dispositifs individuels, mais aussi des réseaux entiers. Les choses sont claires : un fournisseur ne peut plus commercialiser un produit IoT qui ne soit pas sécurisé par conception. Le problème pour les fabricants souhaitant exploiter la puissance de l'Internet des objets (IoT) dans leurs systèmes est la complexité de mise en œuvre de mécanismes de sécurité efficaces et pertinents. On perçoit bien le besoin fondamental d'authentification et de chiffrement de ces systèmes. Mais la mise en œuvre reste difficile.

Concrètement, de nombreux composants, tant logiciels que matériels, sont nécessaires pour créer la base sécurisée d'un système embarqué. Une faiblesse dans n'importe lequel de ces composants peut facilement conduire à la compromission du matériel et au chargement de logiciels malveillants qui peuvent servir à attaquer le réseau d'un opérateur ou donner l'opportunité à des cybercriminels de mettre la main sur des données sensibles. Dans le même temps, de nombreuses équipes de concepteurs sont confrontées pour la première fois aux problèmes de développement inhérents aux sujets de sécurité.

Un impératif : à chaque dispositif son identité unique

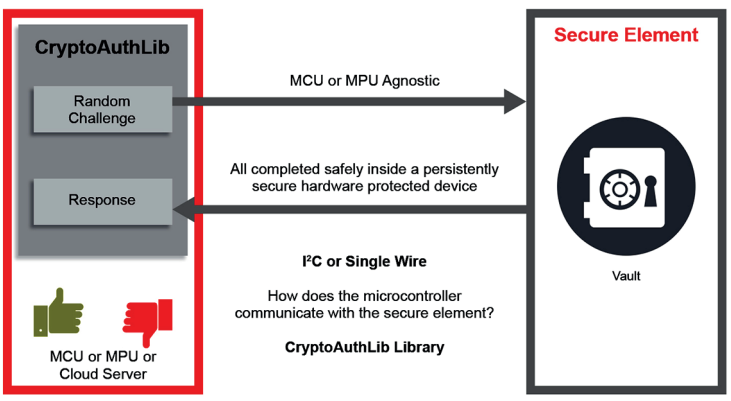
L'une des premières exigences d'une sécurité efficace est que chaque dispositif déployé dispose d'une identité unique. Une faille courante exploitée par les pirates consiste à faire en sorte que les dispositifs fournissent un mot de passe ou un identifiant générique destiné aux techniciens d'entretien et de maintenance. De tels identifiants sont souvent faciles à deviner, et même s'ils ne le sont pas, ils sont généralement faciles à obtenir pour un pirate informatique. Avec ce genre d'identifiant, on peut non seulement accéder à un dispositif donné, mais aussi à l'ensemble de la flotte. Les cybercriminels ont ainsi pu créer des « botnets » – réseaux d'ordinateurs identiques contrôlés par un pirate et servant par exemple à lancer des attaques par déni de service DoS (Denial of Service) – via l'utilisation de simples scripts automatisés. Ces scripts identifient et se connectent à tous les dispositifs d'un certain type disposant d'une connexion Internet.

Avec une identité unique, il est possible de donner à chaque système des codes d'accès uniques, et ainsi de réduire considérablement le risque de permettre aux pirates de construire des botnets. L'accès à un dispositif ne doit être autorisé à un utilisateur que s'il possède les codes d'accès de ce dispositif, sous réserve que l'utilisateur ait le droit d'accéder au dispositif concerné. Toutefois, ce niveau de protection accru a des implications au niveau de la conception, du développement et de la gestion des services.

Mettre en œuvre une sécurité efficace de telle sorte à faciliter plutôt qu'à entraver le développement implique des choix judicieux. Le premier choix concerne la fondation matérielle qui devra protéger l'intégrité du dispositif cible. Cette fondation doit garantir non seulement qu'il soit impossible d'accéder au micrologiciel du dispositif sans autorisation, mais aussi que ses différentes fonctions ne puissent être subverties et que le dispositif en question ne puisse pas servir à attaquer le réseau. Par exemple, si un pirate informatique a réussi à obtenir les codes d'accès d'un dispositif, il doit lui être

1 ELÉMENT SÉCURISÉ

Un composant sécurisé, dispositif compagnon du microcontrôleur, est un coffre-fort qui protège notamment les secrets des clés privées.



UNE PLATE-FORME DE CONFIANCE À TROIS PILIERS

■ La plate-forme de confiance de Microchip est constituée de trois offres principales. La plus simple est Trust&GO qui fournit un ensemble fixe de fonctions, telles que permettre à un appareil d'accéder à des services cloud hébergés sur AWS (Amazon Web Services), Google Cloud, Microsoft Azure ou un cloud privé. Une autre composante de Trust&GO est une solution complète d'authentification sécurisée pour les appareils qui doivent se connecter à un réseau sans fil, comme LoRaWAN. Second pilier, TrustFLEX fournit un niveau de personnalisation supplémentaire avec la prise en charge d'un large éventail d'opérations, qui vont de l'amorçage sécurisé à la génération de certificats.

■ Le troisième pilier, TrustCUSTOM, permet aux utilisateurs d'ajuster la création et l'intégration de composants sécurisés dans le modèle de sécurité qu'ils souhaitent (figure 3).

■ Un point important de cette plate-forme de confiance est la manière dont est déployé le service de fourniture de clés sécurisées sur des applications à faible volume. Avec les offres concurrentes de composants sécurisés, le minimum de commande peut être de 100 000 pièces, en raison des frais liés à la mise en place des certificats et des clés initiales qu'il faut programmer en dur dans la chaîne de production sécurisée du fournisseur. Avec Trust&GO, les concepteurs peuvent acheter des composants sécurisés à partir de 10 pièces par commande, et bénéficier de tout le support de l'infrastructure de la plate-forme de confiance, y compris le provisionnement. Avec TrustFLEX, le minimum de commande est de 2 000 pièces, y compris le provisionnement, mais l'utilisateur a un plus grand contrôle sur les certificats, les clés et les applications, typique de ce que l'on peut attendre de solutions de provisionnement sécurisées sur mesure.

impossible d'intervenir sur un autre dispositif pour que celui-ci accepte ces mêmes codes d'accès dans le but, par exemple, de constituer un « botnet ». Par conséquent, identité et intégrité sont ici intimement liées.

Des schémas d'authentification via une infrastructure PKI

L'infrastructure à clé publique PKI (Public Key Infrastructure) fournit un moyen d'établir et d'authentifier une identité de confiance unique, non seulement au niveau du dispositif lui-même, mais aussi au niveau de l'ensemble d'un réseau. La technologie PKI repose sur le concept de chiffrement asymétrique, une technique qui relie mathématiquement deux clés numériques entre elles. L'une de ces clés est dite publique et sert en général à authentifier les messages. Comme son nom l'indique, cette clé peut être largement distribuée sans compromettre la sécurité. Elle fournit un moyen facile d'envoyer des messages sécurisés à un dispositif, pour autant que l'on sache quelle clé publique utiliser. Le dispositif lui-même a besoin de la clé privée pour signer les messages qu'il envoie et dont l'authenticité pourra être vérifiée à l'aide de la clé publique correspondante.

A partir des opérations PKI de base, on peut élaborer des schémas d'authentification plus structurés, comme des certificats numériques capables d'authentifier l'identité d'un dispositif. Pour créer un certificat numérique, un dispositif signe un message ou lance un défi en générant une signature à l'aide de sa clé privée. La clé publique correspondante est utilisée par le destinataire pour vérifier l'authenticité de la signature. La clé privée a clairement besoin d'une protection forte. Il ne suffit pas de programmer une clé dans la mémoire non volatile d'un dispositif avant son déploiement, car cette mémoire est facilement accessible. La clé privée ne doit jamais être divulguée. S'il y a divulgation, des pirates seront alors en mesure de construire leurs propres clones du dispositif. Ces clones pourront alors se faire passer pour le dispositif authentique et ainsi compromettre la sécurité des applications réseau dépendant des données envoyées par le dispositif.

Le problème avec une conception conventionnelle à microcontrôleur est qu'un logiciel de chiffrement tournant sur le cœur du processeur doit avoir accès à la clé privée pour pouvoir effectuer les calculs nécessaires, en supposant que la clé se trouve dans le contrôleur. Le cœur du matériel nécessaire est donc un composant sécurisé regroupant ces éléments de chiffrement dans un même composant matériel, autonome, protégé et permettant un stockage sécurisé des clés privées. Etant donné que la clé et les fonctions de chiffrement sont stockées ensemble à l'intérieur d'une même enceinte physique sécurisée, aucune donnée sensible n'est envoyée sur le bus interne du système (figure 1).

Un coffre-fort numérique à côté du cœur du microcontrôleur

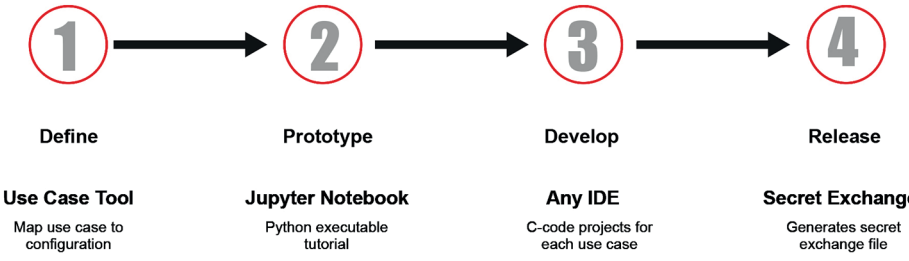
Lorsque le système doit communiquer de manière sécurisée ou prouver son identité, il fait appel au composant sécurisé pour répondre à une énigme aléatoire. La réponse à cette énigme est un code calculé arithmétiquement à partir, d'une part, de la partie aléatoire de l'énigme et, d'autre part, de la clé privée stockée à l'intérieur du composant sécurisé. En d'autres termes, l'énigme aléatoire est « signée » à l'aide de la clé privée. De cette façon, le composant sécurisé peut prouver qu'il connaît le secret approprié, sans avoir à divulguer la clé privée elle-même.

Le composant de sécurité peut également protéger le dispositif d'éventuels codes contrefaits qu'un attaquant pourrait tenter d'exécuter pour compromettre le système. Le mécanisme de protection nécessaire pour empêcher cela est une vérification du code, aussi appelée amorçage sécurisé, ou une vérification du code à l'exécution. Dans ce cas, l'énigme envoyée au composant sécurisé est une signature obtenue à partir de l'image d'amorçage signée et stockée dans le dispositif. Toute mise à jour du logiciel doit être signée par le fabricant à l'aide de sa clé privée. Grâce à des procédures d'amorçage sécurisé et de vérification à l'exécution, le système peut alors accepter les mises à jour OTA (Over-The-Air, par voie radio) fournies par le fabricant, sans risque d'exécuter une mise à jour pirate envoyée par un tiers grâce à une attaque de type « man-in-the-middle » (« homme du milieu » ou pirate intercepteur) ou à une approche similaire.

La clé servant à signer le code pour l'authentifier est un code d'accès sensible, qui doit être conservé dans une zone mémoire protégée et immuable. Si cette clé peut être modifiée, le système ne peut simple-

2 FLUX DE DÉVELOPPEMENT AVEC UNE PLATE-FORME DE CONFIANCE

Un flux de travail guide l'utilisateur, depuis le concept jusqu'à la mise en œuvre, en s'appuyant sur un matériel comprenant un composant sécurisé.



ment pas fonctionner. Si la paire de clés peut être modifiée, alors le code peut également être altéré.

Un exemple de protection efficace est celle que fournit le circuit ATECC608A de Microchip Technology. Il s'agit d'un composant sécurisé utilisable dans tout système à microcontrôleur, grâce à une interface de communication standard I²C ou à une liaison 1-Wire. Le dispositif combine une mémoire non volatile et plusieurs crypto-accélérateurs supportant notamment les algorithmes ECC (Elliptic Curve Cryptography, ou chiffrement à courbe elliptique) dans une puce silicium sécurisée. Le dispositif ne révèle jamais les clés privées sur la liaison de communication et dispose de caractéristiques matérielles anti-effraction qui rendent pratiquement impossible la découverte de son contenu.

Une chaine de sécurité complète

Bien qu'un composant de sécurité associé à un microcontrôleur constitue une fondation efficace pour des dispositifs embarqués connectés qui doivent garantir un niveau de sécurité élevé, cette combinaison n'est qu'une partie de la solution globale. Il y a de nombreuses utilisations qui nécessitent l'élaboration de protocoles complexes dans les logiciels embarqués à partir des fonctions de base fournies par le composant sécurisé. Par exemple, en plus d'un amorçage sécurisé, un dispositif IoT devra être capable de communiquer avec des hôtes distants, en utilisant des protocoles chiffrés comme TLS, et de générer des certificats à la demande, comme preuve de son intégrité avant toute connexion à un nouveau service. Quand le fabricant ou l'opérateur d'un service veut effectuer une mise à jour du micrologiciel, la signature de ce micrologiciel doit être authentifiée pour autoriser la mise à jour de la mémoire flash et le réamorçage du système.

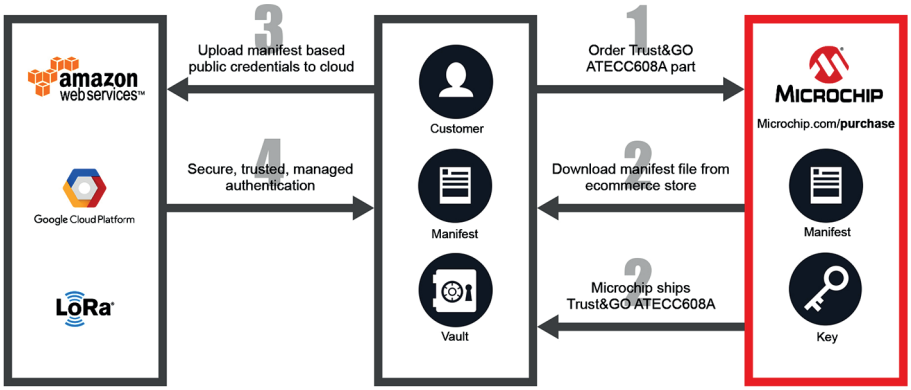
Une autre exigence peut être la détection d'accessoires système ou d'éléments consommables pour vérifier qu'ils soient bien authentiques. Cette fonction peut être réalisée grâce à des protocoles similaires à ceux servant à la vérification du code, mais avec quelques différences essentielles. Par exemple, chaque périphérique peut disposer de son propre composant de sécurité pour vérifier que le système hôte auquel il est branché est lui-même authentique. Bien que les principes de chacun des protocoles permettant la mise en œuvre de ces fonctions soient relativement simples, leur implémentation peut s'avérer délicate dans la mesure où le débogage est soumis aux contraintes de protocoles sécurisés.

Une hypothèse courante en phase de développement est qu'en faisant un Reset ou en vidant la mémoire, il est possible d'accéder à un dispositif qui ne répond pas. En général, les modes de débogage donnent au développeur un accès privilégié au système. Mais lorsque des niveaux de sécurité supérieurs sont imposés à des systèmes qui se connectent à Internet, certaines de ces hypothèses ne seront plus valables. Si le logiciel n'est pas implémenté correctement, le dispositif prototype peut devenir inaccessible. L'un des plus gros problèmes de développement que pose un système sécurisé est le débogage des protocoles de base. Par exemple, il est facile d'introduire des bogues dans le code utilisé pour traiter les mots de passe ou le certificat de sécurité, qui empêcheront le dispositif de répondre à des requêtes illégitimes. S'il était possible de réinitialiser le dispositif pour y accéder, cela fournirait aux pirates informatiques une «backdoor» (littéralement une «porte de derrière» c'est-à-dire une entrée cachée) permettant d'entrer facilement dans le système. Par conséquent, un développement axé sur la sécurité rend inévitablement plus complexe le processus de développement. Ces difficultés sont difficiles à gérer si l'équipe n'a pas l'expérience des techniques requises.

Cependant, l'un des avantages des systèmes à infrastructure PKI est que les applications s'appuient sur les protocoles de base et sur des types d'utilisation, comme l'authentification d'exécutables signés ou la création de certificats, que l'on peut réutiliser dans d'autres projets. Cette vision a permis à Microchip de créer sa plate-forme de confiance (voir encadré). Cette plate-forme fournit un ensemble de configurations, de codes source, de matériels et d'outils logiciels facilitant l'implémentation de nombreux types d'utilisation dans le cadre d'un flux de travail qui guide l'utilisateur, depuis le concept jusqu'à la mise en œuvre, en s'appuyant sur un matériel comprenant un composant sécurisé comme l'ATECC608A (figure 2). ■

3 FLUX DE COMMANDE ET DE LIVRAISON D'UNE PLATE-FORME DE CONFIANCE

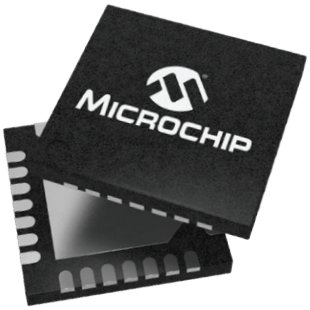
Pour un minimum de commande de 2 000 pièces, y compris le provisionnement, l'utilisateur a un contrôle sur les certificats, les clés et les applications dans le cadre d'une solution de provisionnement sécurisée sur mesure.



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