Comment sécuriser votre équipement IoT à l'épreuve du temps

De nos jours, chaque équipement embarqué développé requiert un système de sécurité. En raison de la topographie évolutive des menaces touchant les dispositifs IoT, ce système de sécurité se doit d'être complet et opérationnel dès l'expédition de l'appareil. Mouser donne ici des indications sur la démarche à suivre pour disposer dès le départ d'une protection robuste contre des attaques logicielles qui n'en finissent pas d'évoluer.

La mise en œuvre de la sécurité dans une conception embarquée, quelle qu'elle soit, représente une tâche ardue. Tous les jours on entend parler de vol d'informations sensibles par des pirates, ou d'un site Internet obligé d'interrompre ses services parce que les données de ses clients ont été compromises. Qui plus est, la topographie des menaces évolue en permanence et les vecteurs d'attaques et les adversaires se multiplient. Cela ne concerne pas uniquement les failles de sécurité repérées dans les équipements grand public. Fin 2020, un fournisseur de semi-conducteurs a vu l'intégralité de sa production mise à l'arrêt par des pirates informatiques réclamant une rançon. Un coup dur pour un secteur industriel qui prône les meilleures pratiques dans le domaine de la sécurité.

Pour les pirates, viser les particuliers n'apporte généralement que de petits bénéfices. S'attaquer à de grandes entreprises et organisations peut en revanche rapporter gros, d'autant plus que les cibles concernées préfèrent en général éviter toute publicité négative. De nos jours, les développeurs actifs dans le domaine des technologies opérationnelles (OT) – dont fait partie l'Internet des objets industriel (IIoT) – sont sommés de mettre en œuvre les niveaux de sécurité les plus élevés dans tous les équipements qu'ils conçoivent. De fait, alors que les attaques étaient auparavant dirigées généralement contre les serveurs et centres de données distants des entreprises, elles affectent à présent les équipements opérationnels au niveau local tels que capteurs, nœuds de périphérie de réseau et passerelles. Cette évolution indique un changement dans les vecteurs d'attaque. Par exemple, une faille de sécurité au niveau d'un nœud de capteur de température en périphérie ne compromet pas seulement l'équipement lui-même. Elle constitue une porte d'entrée pour attaquer toute l'infrastructure étendue à partir de ce seul capteur.

AUTEUR

Simon Holt, Supplier Maketing Manager, Mouser Electronics.

Une réglementation en évolution

La réglementation en la matière subit elle aussi des changements. De récentes lois promulguées tant aux Etats-Unis qu'en Europe établissent un cadre pour la conception d'appareils grand public et industriels. Ainsi, l'Institut américain des normes et de la technologie, le NIST, prépare une réglementation fédérale, la norme NIST.IR 8259, dont l'objectif est de relever les problèmes de sécurité affectant les appareils IoT et de formuler des recommandations afin de les résoudre. Une fois ratifiée, cette norme NIST deviendra un standard ISO de sécurité des appareils IoT internationalement reconnu. Plusieurs Etats américains sont d'ailleurs déjà à un stade avancé dans l'adoption des exigences de la NIST. IR 8259. La figure 1 met en évidence quelques-uns des principes de base

1 CADRE ÉTABLI PAR LA NORME NIST.IR8259 POUR LA SÉCURITÉ DES APPAREILS IOT

L'Institut américain des normes et de la technologie, le NIST, prépare une réglementation fédérale, la norme NIST.IR 8259, dont l'objectif est de relever les problèmes de sécurité affectant les appareils IoT et de formuler des recommandations afin de les résoudre.

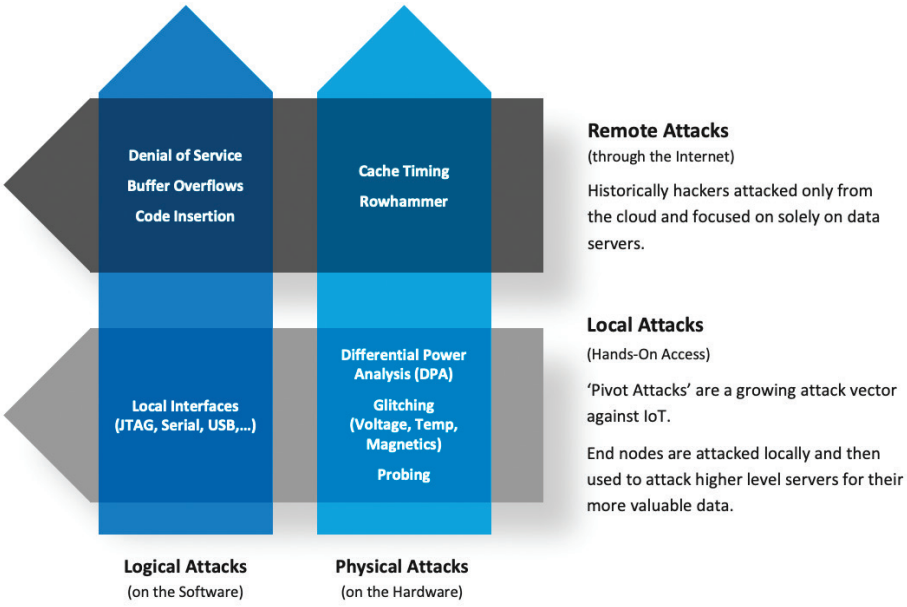
(source : Silicon Labs)

Concern	Federal Requirement
Device Identification	The IoT device can be uniquely identified logically and physically.
Device Configuration	The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.
Data Protection	The IoT device can protect the data it stores and transmits from unauthorized access and modification.
Logical Access to Interfaces	The IoT device can limit logical access to its local and network interfaces to authorized entities only.
Software and Firmware Update	The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.
Cybersecurity Event Logging	The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.

de la sécurité visés par cette réglementation.
L'Europe n'est pas en reste. L'organisme de normalisation ETSI a publié une réglementation similaire nommée TS 103 645. Devenu par la suite la norme européenne EN 303 645 sur la cybersécurité dans l'Internet des objets grand public, ce nouveau standard devrait être largement adopté par les Etats européens ainsi que par quelques autres pays comme l'Australie.
Dans ce cadre, le présent article détaille les étapes de mise en œuvre d'une sécurité plus robuste au sein des appareils IoT, explique les différents concepts de la sécurité embarquée et aborde la mise en œuvre d'une approche globale cohérente de la sécurité des équipements embarqués.

2 EVOLUTION DES VECTEURS D'ATTAQUE DANS LE DOMAINE DE L'IOT INDUSTRIEL

Alors que les attaques étaient auparavant dirigées généralement contre les serveurs et centres de données distants des entreprises, elles affectent à présent les équipements opérationnels au niveau local tels que capteurs, nœuds de périphérie de réseau et passerelles . (source : Silicon Labs)



Découvrir les failles de sécurité des appareils IoT

Les développeurs de systèmes embarqués ont parfaitement conscience des exigences en matière de sécurité. Cependant, elles s'avèrent parfois difficiles, voire complexes, à mettre en œuvre. L'exercice était certainement bien moins contraignant à l'époque où les dispositifs embarqués étaient autonomes. Or, de nos jours, tout fonctionne en réseau et les appareils IoT sont particulièrement exposés aux attaques. En outre, les pirates ont eux aussi acquis de l'expérience. Le trafic de données et les ports TCP/IP ne sont plus les seuls points d'entrée des attaques : chaque aspect d'un dispositif embarqué est susceptible de présenter une surface d'attaque. Il importe dès lors de connaître les éventuelles surfaces d'attaque pour décider de la méthode de protection la plus appropriée.
La figure 2 distingue les attaques locales selon qu'elles ciblent les dispositifs IoT au niveau logiciel ou matériel. Certains types d'attaques s'avèrent sophistiqués, comme l'analyse de consommation différentielle (DPA), ou au contraire relativement simples comme peut être un accès physique au port JTAG pour le reprogrammer avec un code malveillant. La DPA consiste à « mettre sur écoute » la consommation électrique d'un appareil à un niveau granulaire et en temps réel afin d'en déduire la nature des opérations de l'appareil. Cette technique permet, au bout d'un certain temps, de générer une image numérique des opérations réalisées par un processeur embarqué. Les opérations cryptographiques, par exemple, sont particulièrement gourmandes en ressources de calcul et en énergie.
En surveillant ces activités, un pirate pourrait détecter de fréquentes tâches de chiffrement et de déchiffrement numériques. Une fois que le pirate a compris le fonctionnement d'un processeur, il peut alors provoquer une panne qui rendrait les ports et les registres accessibles. D'autres techniques fréquemment utilisées par les pirates consistent à dérégler les horloges système, injecter de faux signaux sur des broches périphériques ou encore baisser la tension de l'alimentation électrique au point de provoquer l'instabilité du processeur, ce qui peut entraîner l'exposition de clés secrètes ou l'ouverture de ports verrouillés.

Sécuriser votre équipement

Lorsqu'il s'agit de mettre en œuvre un régime de sécurité dans un appareil IoT, les équipes d'ingénieurs peuvent s'appuyer sur des frameworks industriels tels que celui proposé par l'alliance IoXT. Il s'agit d'une initiative fondée par des acteurs de l'industrie qui vise à faciliter la tâche des développeurs de systèmes embarqués chargés de la programmation dans le cadre de la sécurisation d'un dispositif IoT. L'IoXT fournit donc un cadre auquel les ingénieurs peuvent se référer lors de la conception d'appareils IoT. Ce cadre repose sur huit principes couvrant la sécurité IoT, l'évolutivité et la transparence.

1 - Pas de mots de passe universels
Il faut commercialiser les appareils avec un mot de passe par défaut unique plutôt qu'avec un mot de passe identique pour tous les appareils, de telle sorte que les pirates ne puissent pas prendre le contrôle généralisé de centaines d'appareils.

2 - Sécuriser chaque interface
Toutes les interfaces doivent être chiffrées et authentifiées pendant leur utilisation, quel que soit leur objectif.

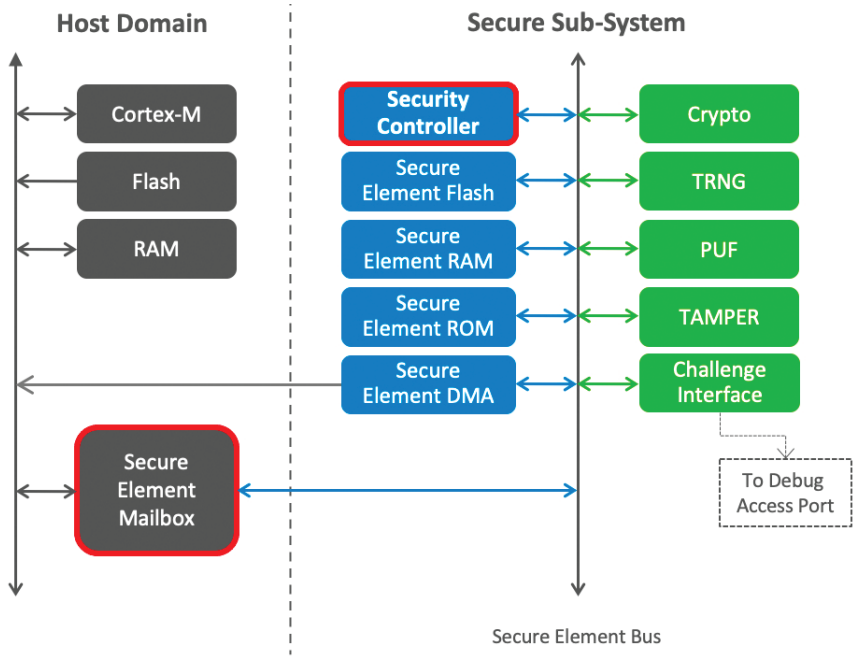
3 - Utiliser des méthodes de cryptographie éprouvées
Il est recommandé d'utiliser des normes et des algorithmes cryptographiques ouverts et validés par l'industrie.

4 - Sécurité par défaut
Les appareils doivent être livrés avec la sécurité activée au plus haut niveau possible.

5 - Mises à jour logicielles signées
Les mises à jour logicielles à distance over-the-air doivent être signées de telle sorte que l'appareil récepteur

3 SECURE VAULT DE SILICON LABS : UN SECURE ELEMENT AU SEIN D'UNE PUCE

Secure Vault utilise une combinaison de fonctionnalités matérielles et logicielles pour fournir un sous-système de sécurité complet dans une puce-système (SoC). Le premier circuit intégré Silicon Labs à intégrer Secure Vault est le SoC sans fil multiprotocole EFM32MG21B.



puisse authentifier la mise à jour avant de l'appliquer.

6 - Mises à jour logicielles automatiques

Plutôt que de laisser à l'utilisateur le choix d'installer ou non la mise à jour, l'appareil doit appliquer d'office les mises à jour logicielles authentifiées afin de toujours bénéficier des derniers correctifs de sécurité.

7 - Système de signalement des failles de sécurité

Les fabricants d'appareils doivent fournir aux utilisateurs un moyen de signaler les problèmes de sécurité potentiels afin d'accélérer la mise au point d'un correctif.

8 - Date d'expiration de la sécurité

A l'instar des systèmes de garantie, la fourniture de services de sécurité devrait également être limitée dans le temps. Les fabricants peuvent proposer des programmes d'assistance étendus afin d'aider à différer les coûts liés au maintien continu de la sécurité et aux mises à jour.

Mise en œuvre d'une approche globale de la sécurité

Le paysage de la sécurité de l'IoT évolue à toute vitesse et les équipes de conception de produits IoT ont parfois du mal à tenir à jour la liste croissante des fonctionnalités de sécurité nécessaires. La plate-forme Secure Vault développée par Silicon Labs répond à ce défi. Secure Vault utilise une combinaison de fonctionnalités matérielles et logicielles pour fournir un sous-système de sécurité complet dans une puce-système (SoC). Le premier circuit intégré Silicon Labs à intégrer Secure Vault est le SoC sans fil multiprotocole EFM32MG21B.

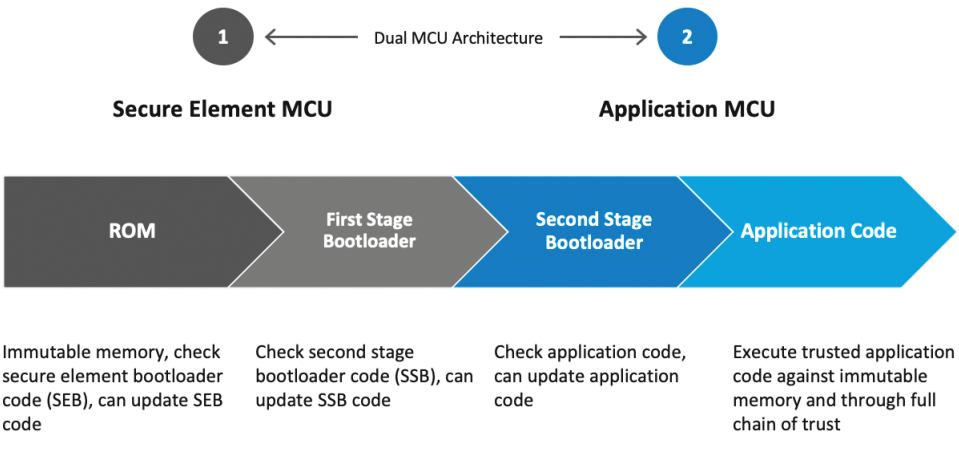
Secure Vault a obtenu la certification des groupes de sécurité industriels PSA Certified et IoXt Alliance. La certification PSA Certified Level 2 repose sur un framework de standards de sécurité cofondé par Arm. Un SoC Secure Vault comprend toutes les fonctions de sécurité auxquelles un développeur peut s'attendre dans un circuit intégré, comme un générateur de vrais nombres aléatoires, un moteur de chiffrement, une racine de confiance et l'aptitude à effectuer un démarrage sécurisé. Secure Vault va plus loin en proposant en outre un démarrage sécurisé amélioré, une série de mesures destinées à contrer la DPA, un système de détection préventive des manipulations malveillantes, une gestion sécurisée des clés et des fonctionnalités d'obtention d'attestations sécurisées. Dans la pratique, au sein de Secure Vault, toutes les fonctions de sécurité sont intégrées dans un élément sécurisé SE (figure 3).

Un vecteur d'attaque couramment utilisé par les pirates consiste à falsifier le code de démarrage en remplaçant le code par des instructions qui semblent normales, mais qui fonctionnent différemment et redirigent les données vers des serveurs distants. Afin de prévenir ce type d'attaque, Secure Vault utilise un processus de démarrage amélioré faisant à la fois appel au microcontrôleur d'application et au microcontrôleur de l'élément sécurisé. Il intègre une racine de confiance et une fonction de chargeur sécurisé afin d'autoriser uniquement l'exécution de code provenant d'applications de confiance (figure 4).

Une autre technique de piratage consiste à essayer de retourner à une version précédente du micrologiciel

4 PROCESSUS DE DÉMARRAGE SÉCURISÉ DU SECURE VAULT DE SILICON LABS

Secure Vault utilise un processus de démarrage amélioré faisant à la fois appel au microcontrôleur d'application et au microcontrôleur de l'élément sécurisé.



installé qui présentait des failles de sécurité et ce en vue de les exploiter. Avec Secure Vault, le système de prévention contre les « rollbacks » utilise des versions signées numériquement du micrologiciel afin de déterminer si le micrologiciel doit être réinstallé (figure 5).

Enfin, certains systèmes utilisaient auparavant un identifiant unique (UID) accessible au public pour identifier les appareils IoT individuels. Du point de vue des développeurs, ces UID étaient une porte ouverte à la contrefaçon de leurs produits et n'étaient plus une garantie suffisante de l'authenticité d'un produit. Pour y remédier, Secure Vault génère une paire de clés ECC (une publique, une secrète) et stocke la clé secrète directement sur la puce en toute sécurité. De cette manière, les applications peuvent demander le certificat de l'appareil, mais la réponse à la requête est signée avec la clé secrète de l'appareil et non pas envoyée telle quelle avec le certificat. Avec Secure Vault, les équipes de développement de produits et leurs clients ont donc l'assurance de disposer dès le départ d'un système de protection robuste contre des attaques logicielles qui n'en finissent pas d'évoluer. ■

5 LA SIGNATURE NUMÉRIQUE POUR ÉVITER LES ROLLBACKS

Le système de prévention de Secure Vault contre le rollback (retour à une version ancienne du firmware dotée de failles de sécurité) utilise des signatures numériques pour authentifier les mises à jour du micrologiciel. (source : Silicon Labs)