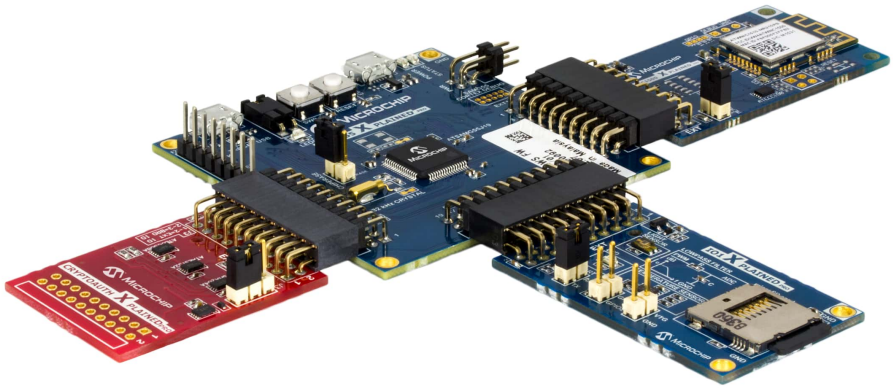
Garantir la sécurité lors de la connexion au cloud des systèmes embarqués industriels

Xavier Bignalet, responsable marketing des produits de sécurité chez Microchip Technology

L'aube de l'Industrie 4.0 a vu les unités de production devenir bien plus automatisées, avec des concepts de fabrication et de commande à distance. Alors que ces concepts apportent des bénéfices en termes d'efficacité de production, ils exposent par ailleurs des actifs très onéreux à un risque d'accès non autorisé. Ce n'est pas seulement la valeur financière des machines qui est menacée, c'est également le chiffre d'affaires généré à partir des biens produits dans l'usine, à un moment donné, qui peut également se voir compromis.

Si, comme c'est souvent le cas, le site de production est connecté à un serveur public ou privé, alors il existe des risques de sécurité inhérents. Cette situation se produit dès lors qu'une usine intelligente est reliée à un réseau, tel qu'un centre de données externe, par exemple. Le défi consiste alors à conserver les bénéfices de l'élasticité d'un site de production connecté, tout en maintenant une sécurité adaptée sur les différents réseaux.

Un bon point de départ consiste à déterminer si la solution utilisera la communication filaire, sans fil ou une combinaison des deux. À partir de là, il est recommandé d'utiliser une technologie de connectivité qui possède des protocoles standard, comme le Wi-Fi, le Bluetooth ou l'Ethernet, pour ne citer que les plus connues dans le secteur industriel. L'utilisation de pratiques standard en matière de sécurité diminue le risque que les connexions soient compromises. Parfois, cela va à l'encontre des pratiques habituelles des milieux industriels, qui affectionnent les solutions propriétaires. L'infrastructure doit être construite pour durer de nombreuses années. Alors que de nombreux réseaux respectent quelques protocoles propriétaires, ceux-ci devraient être réservés à un usage interne et non pour des connexions externes.



L’un des problèmes, cependant, réside dans le fait que la plupart des ingénieurs embarqués les plus qualifiés ne possèdent qu’une connaissance limitée en matière de concepts de sécurité IT. Ce ne sont en effet pas des experts des technologies de l’information, et ce manque de connaissances les empêche d’être capables de créer une infrastructure robuste et sûre pour les objets connectés. Aussitôt que l’établissement de la connexion est réalisé entre l’usine et le serveur distant, les ingénieurs sont soudain propulsés dans le monde d’Amazon Web Services (AWS), Google, Microsoft Azure et autres géants des services de clouding, et se rendent vite compte qu’ils ont besoin de l’aide d’experts en technologie de l’information pour gérer le large éventail de menaces de sécurité auxquels ils doivent désormais faire face.

Pour les pirates, l’une des principales méthodes consiste à s’introduire par un seul point d’accès pour obtenir l’accès distant à une grande partie des systèmes. Les attaques distantes peuvent causer des dommages à grande échelle, comme l’ont prouvé les récentes attaques de déni de service distribuées DDoS *(Distributed Denial of Services)*. Pour un réseau d’objets connectés, le point le plus faible est habituellement le matériel et son utilisateur en fin de nœud, car les ingénieurs qui s’occupent de cette partie du réseau manquent en en général des connaissances IT nécessaires pour résoudre ce problème.

Cela est en train de changer. Des entreprises comme Microchip Technology considèrent en effet comme faisant partie de leur mission le fait de combler ces lacunes, en formant les ingénieurs, en leur enseignant à quoi doit ressembler une infrastructure sécurisée de bout en bout. De plus, les grandes entreprises de clouding telles qu’AWS, Google et Microsoft constituent une importante source d’expertise. La leçon à retenir est qu’il ne faut pas négliger la sécurité, ni considérer qu’elle peut être mise en œuvre dans un deuxième temps, une fois que le réseau d’objets connectés a été conçu. Car, à ce stade, il

est déjà trop tard. La sécurité est un aspect qui doit être mis en œuvre de façon stratégique, dès le début de la conception de tout système IoT. La sécurité commence au niveau matériel, et n'est pas un paramètre qu'on peut ajouter après coup, ni mettre en œuvre au niveau logiciel.

Authentification

La partie la plus importante du casse-tête de la sécurité est l'authentification. Un concepteur de système doit commencer par le concept que chaque nœud connecté à un réseau doit avoir une identité unique, protégée et fiable. En effet, savoir qu'une personne sur le réseau est bien la personne qu'elle affirme être et qu'il s'agit de quelqu'un de confiance est capital. Pour ce faire, l'utilisation traditionnelle de l'authentification TLS 1.2 ou de l'authentification mutuelle doit avoir lieu entre le serveur et le nœud d'extrémité du réseau IoT. Cela est réalisé en utilisant des informations dans lesquelles les deux parties ont confiance, c'est-à-dire une autorité de certification.

Cependant, ceci ne fonctionne que si la confiance qui émane de l'autorité de certification est protégée à tout moment : dès le début du projet, pendant la fabrication et une fois que le système est déployé dans l'unité de production intelligente. La clé privée, qui est utilisée pour reconnaître l'authenticité du nœud d'extrémité du réseau IoT, doit être sécurisée et protégée. Aujourd'hui, une méthode d'implémentation vulnérable, quoique courante, utilisée à ces fins, consiste à stocker la clé privée dans un microcontrôleur dans un espace libre d'une mémoire Flash, où elle peut être exposée à des manipulations logicielles. Or, quiconque ayant accès à cette zone de la mémoire ou la consultant, peut la contrôler et ainsi obtenir la clé privée. Il s'agit d'une mise en œuvre faussée, qui offre aux développeurs un faux sentiment de sécurité. C'est dans ce cas que les dommages et les problèmes sérieux surviennent.

Élément sécurisé

Pour qu'une solution soit sécurisée, la clé et les autres données critiques ne doivent pas seulement être retirées du microcontrôleur, elles doivent également être isolées du microcontrôleur ainsi que de toute exposition logicielle. C'est là que le concept d'élément sécurisé entre en jeu. L'idée sous-jacente aux éléments sécurisés consiste essentiellement à offrir un emplacement sûr pour stocker et protéger la clé, auquel personne ne peut accéder. Les commandes de la bibliothèque CryptoAuthLib permettent d'envoyer les demandes/réponses appropriées depuis le microcontrôleur vers l'élément sécurisé, afin de valider l'authentification. À aucun moment du processus de développement du produit ni de son cycle de vie la clé privée n'est exposée ni ne quitte l'élément sécurisé. En conséquence, une chaîne de sécurité peut être établie de bout en bout.

Les éléments sécurisés sont des circuits intégrés CryptoAuthentication autonomes que l'on peut considérer comme un coffre-fort où l'entreprise conserve ses documents sensibles. Dans le cas présent, les éléments sécurisés renferment les clés privées nécessaires à l'authentification IoT.

Octroi des clés :

Le deuxième concept important concerne la façon dont les clés privées et autres autorisations sont stockées par le client dans le composant CryptoAuthentication. Pour ce faire, Microchip offre une plateforme qui permet au client de créer et organiser en toute sécurité la programmation de ses données sensibles pendant la fabrication de ses puces, sans qu'elles soient exposées à quiconque, y compris au personnel de Microchip. Microchip fabrique ensuite l'élément sécurisé dans ses usines et c'est uniquement au moment de quitter lesdites usines, certifiées sécurisées selon les critères courants, que l'élément sécurisé reçoit les informations sensibles avant d'être envoyé à l'utilisateur final.

Quand les clients ouvrent les comptes IoT AWS, ils fournissent les certificats client que Microchip a créé en leur nom, à l'aide de la fonction Use Your Own Certificate (« utilisez votre propre certificat ») d'AWS. Ensuite, ils utilisent la fonction IoT AWS nommée Just-In-Time Registration (JITR), pour télécharger en une fois tous les certificats au niveau système stockés et pourvus dans les éléments sécurisés vers leur compte d'utilisateur AWS IoT. Le certificat au niveau client peut alors vérifier le certificat niveau système, de sorte que la boucle de la chaîne de confiance est bouclée. Cette fonction est ce qui permet la véritable évolutivité IoT d'une entreprise, avec la sécurité à l'esprit. Des milliers de certificats peuvent être gérés à l'aide du processus d'enregistrement JITR. Ils peuvent être gérés sous forme de paquet, plutôt qu'un par un, sans aucune intervention de l'utilisateur. Au lieu de devoir charger les certificats manuellement depuis les systèmes associés vers un compte en ligne, et ainsi les exposer à des tiers, les utilisateurs peuvent dorénavant décider d'enregistrer les certificats des nouveaux systèmes automatiquement, comme faisant partie des communications initiales entre le système et AWS IoT, le tout sans compromettre la sécurité.

Démarrez avec la nouvelle version du kit AT88CKECC-AWS-XSTK-B

Intégré au kit de d'octroi de clé Zero Touch se trouve le composant Cryptoauthentication ATECC508AMAHAW, livré préconfiguré pour faire fonctionner le processus d'authentification avec le compte AWS IoT de l'utilisateur. La première étape consiste à apprendre ce qu'est une chaîne de confiance en utilisant les nouveaux scripts Python, ainsi qu'à comprendre le processus d'octroi de clé qui s'opère dans les sites de production de Microchip, pendant toute la phase d'octroi de clé. Le kit montre comment fonctionne le processus d'octroi de clé pendant la fabrication, jusqu'à un certain point. De plus, le système possède une grande résistance contre les intrusions physiques, y compris des contremesures contre les attaques latérales. Il possède également un générateur de nombres aléatoire conforme à la norme américaine FIPS *(Federal Information Processing Standard)*, un accélérateur de chiffrement pour une large compatibilité avec de nombreux systèmes IoT limités en ressources, et la capacité de s'adapter facilement à plusieurs flux de production avec un bon rapport bon rapport coût/efficacité.

Pour combler l'écart existant entre les ingénieurs embarqués et les professionnels des technologies de l'information, en plus de l'expérience des scripts Python intégrés, le kit comprend un script CloudFormation pour accélérer le paramétrage du compte AWS et rendre l'expérience avec le Cloud plus formatrice. En utilisant le script CloudFormation,

l'utilisateur peut définir une interface utilisateur dans l'environnement AWS en quelques minutes seulement.

Conclusion

Grâce à l'association de l'enregistrement JITR d'ASW IoT, du composant CryptoAuthentication ATECC508MAHAW et du processus d'octroi de clé sécurisé pendant la fabrication des composants de Microchip, la meilleure sécurité IoT est assurée. Cette solution de sécurité IoT de bout en bout permet l'avènement de l'industrie 4.0 sécurisée, en assurant une croissance sûre et efficace.