

De nouvelles techniques pour défendre et protéger les nœuds connectés à l'Internet des objets

Par Stephane di Vito, Senior Principal Micros, Security & Software ; Robert Muchsel, Fellow, Micros, Security & Software ; et Don Loomis, Vice President, Micros, Security & Software, Analog Devices

Quelque dix milliards de nœuds sont actuellement connectés à l'Internet des objets (IoT), soit dix fois plus qu'il y a une dizaine d'années, et cette tendance se poursuit sans relâche. Or, cette croissance va de pair avec une augmentation tout aussi importante des opportunités de cyberattaque — un « marché » dont le coût annuel est compris entre quelques dizaines et plus d'un millier de milliards de dollars, et qui ne montre pas le moindre signe d'essoufflement. Dans ce contexte, la sécurité représente un enjeu essentiel pour poursuivre avec succès la montée en échelle de l'Internet des objets. En d'autres termes, la sécurité de l'Internet des objets commence par la sécurité des nœuds connectés.

Aucune entreprise ne souhaite être connue comme « *une société qui a subi une cyberattaque et dont les données clients ont été subtilisées* ». De plus, les appareils connectés sont également soumis à des réglementations gouvernementales, telles que les règles définies par la FDA américaine pour les équipements médicaux, les exigences de cybersécurité applicables aux usines connectées (Industrie 4.0) aux États-Unis et en Europe, et de multiples standards émergents dans le secteur automobile. Ces contraintes poussent en faveur d'une sécurité avancée, sans pour autant stipuler de manière explicite l'utilisation de moyens de sécurité matériels. Or, les nœuds IoT sont très souvent des appareils produits en grande série au coût optimisé, ce qui soulève des défis pour atteindre un équilibre optimum entre le coût et la sécurité.

Sécuriser les nœuds connectés à l'aide d'une « racine de confiance »

Comment concevoir un nœud IoT à la fois rentable et sécurisé ? La création d'un nœud IoT sécurisé commence par une « racine de confiance » (également appelée « élément sécurisé »), c'est-à-dire un circuit intégré compact et peu onéreux conçu pour sécuriser le nœud connecté. Parmi les fonctions d'une racine de confiance, citons le chiffrement des données pour maximiser la confidentialité des informations, ou les signatures numériques qui en garantissent l'authenticité et l'intégrité. L'objectif ultime de la racine de confiance est de faire en sorte que les clés secrètes utilisées pour le chiffrement des données ou les signatures numériques soient protégées contre tout risque de divulgation.

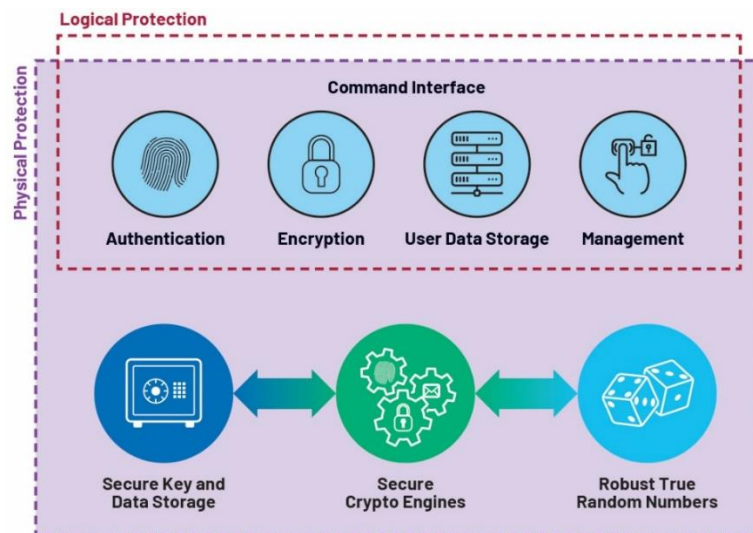


Figure 1. Le concept de « racine de confiance » garantit l'authenticité et l'intégrité des services liés à la sécurité.

La résistance aux attaques physiques menées par sondage direct (méthode dite du « *direct probing* ») ou par canal auxiliaire (*Side Channel Attacks* — SCA) constitue le principal danger pour les circuits de sécurité.

Fonction physique non clonable (PUF)

Malheureusement, face aux tentatives d'attaque par « *direct probing* » qui cherchent à observer l'intérieur des microcircuits, les technologies mémoire généralement utilisées dans les microcontrôleurs à usage général (EEPROM ou Flash) ne sont pas suffisamment sûres. Un agresseur peut observer directement le contenu d'une mémoire moyennant un coût relativement modeste en utilisant un microscope électronique à balayage (SEM — *Scanning Electron Microscopy*). Pour atténuer ce risque, les fabricants des semiconducteurs ont mis au point la « fonction physique non clonable » (PUF — *Physically Unclonable Function*), une technologie utilisée pour dériver une clé unique des propriétés physiques intrinsèques de la puce. Ces propriétés sont beaucoup plus difficiles à sonder selon la méthode du « *direct probing* », ce qui complique l'extraction de la clé générée. Dans certains cas, la clé dérivée à l'aide de la fonction PUF chiffre le reste de la mémoire interne de la racine de confiance, ce qui protège la totalité des autres clés et identifiants stockés sur l'appareil.

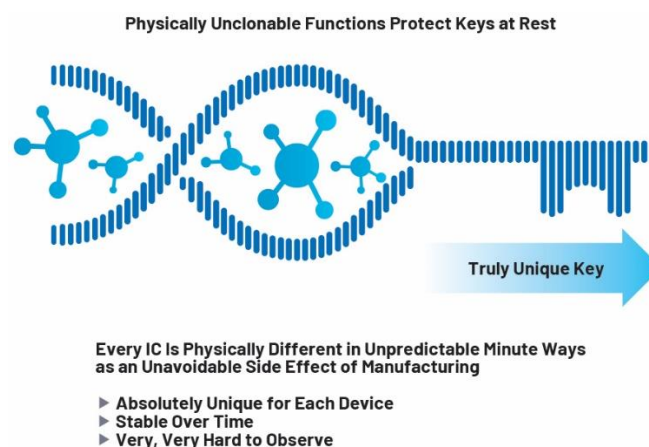


Figure 2. La fonction physique non clonable (PUF) minimise les risques liés au sondage direct des microcircuits.

Les attaques par canal auxiliaire (SCA — *Side Channel Attacks*) sont encore moins onéreuses et moins intrusives. Elles exploitent le fait que les circuits électroniques ont tendance à laisser échapper une signature des données qu'ils manipulent — par exemple par le biais de l'alimentation électrique, d'une liaison radio ou des émissions thermiques. Dans certains cas, la corrélation subtile entre les signaux mesurés et les données traitées permet de deviner avec succès la valeur d'une clé secrète après avoir procédé à une analyse statistique modérément complexe lorsque le circuit utilise cette clé, par exemple pour déchiffrer des données. Une racine de confiance est explicitement conçue pour empêcher que de telles fuites de données puissent se produire et ce, grâce à l'application de diverses contre-mesures.

Exemple d'application utilisant un élément sécurisé (SE)

Les avantages d'une « racine de confiance » matérielle apparaissent clairement dans les applications sécurisées représentées à la figure 3. Le protocole utilisé est un simple protocole d'authentification par défi/réponse :

- ▶ le compteur lance un défi à la pompe à insuline dans l'optique d'envoyer une commande ;
- ▶ la pompe envoie au demandeur un nombre aléatoire R ;
- ▶ le compteur utilise sa clé privée pour signer la commande, le nombre aléatoire R, et un remplissage fixe (« *fixed padding* »). Cette opération est reportée à la « racine de confiance » du compteur ;
- ▶ la pompe vérifie que la signature est correcte et que le nombre aléatoire correspond à celui qu'elle a envoyé précédemment afin d'éviter de renvoyer une commande valide. Cette opération est reportée sur le CI « racine de confiance » de la pompe.

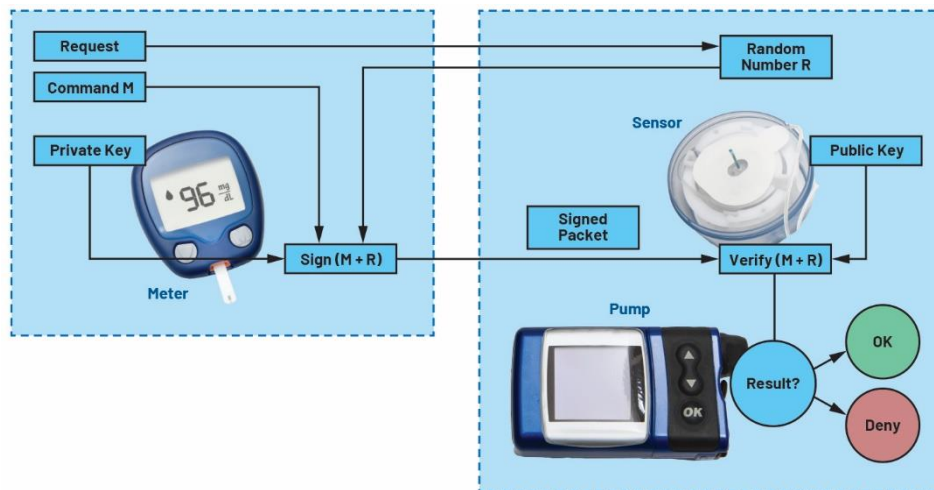


Figure 3. L'authentification de la pompe à insuline est un exemple simplifié d'une « racine de confiance ».

Outre le fait que toute nouvelle tentative d'envoi d'une commande nécessite un nouveau nombre aléatoire, la sécurité de ce protocole réside dans le secret de la clé privée qui est utilisée pour autoriser les commandes et dans l'intégrité de la clé publique employée pour vérifier les autorisations. Si elles étaient stockées à l'intérieur de microcontrôleurs ordinaires, ces clés pourraient être extraites ou manipulées, et de faux compteurs ou de fausses pompes facilement fabriqués, mettant potentiellement en danger la sécurité des patients. Dans ce cas, les éléments sécurisés minimisent les risques de contrefaçon des compteurs ou des pompes, ce qui rend la manipulation des identifiants et l'altération du protocole de communications nettement plus complexes.

Avantages des circuits intégrés dédiés à la sécurité

De manière générale, si un nœud IoT est bien conçu, le coût de la fraude sera nettement supérieur aux avantages que peut en tirer un attaquant. Les atouts d'une architecture basée sur un circuit de sécurité dédié ne manquent pas :

- la sécurité de l'IoT est une lutte sans fin. Alors que les techniques d'attaque ne cessent de s'améliorer, les fabricants de circuits intégrés de sécurité continuent de perfectionner les contre-mesures, rendant les attaques extrêmement onéreuses. La sécurité d'un appareil connecté peut être améliorée en utilisant un circuit intégré de sécurité plus performant, ce qui n'a guère de conséquences sur la conception et le coût global de l'appareil ;
- la concentration des fonctions critiques dans un environnement physique robuste, inviolable et isolé du processeur d'applications permet d'obtenir plus facilement une « preuve de sécurité » dans l'optique de valider la conformité réglementaire. En raison de cette séparation, il est également plus compliqué d'exploiter les points faibles du processeur d'application de l'appareil, lesquels sont très difficiles à détecter et à éliminer entièrement.

Il est plus facile de garantir la sécurité d'un nœud IoT d'un bout à l'autre de son cycle de vie lorsque le circuit intégré de sécurité est implémenté de façon précoce par son fabricant. Cette approche évite de partager des informations critiques avec les sous-traitants, tandis qu'un flux de personnalisation sécurisé et des mises à jour sécurisées effectuées par voie hertzienne OTA (« *Over The Air* ») deviennent possibles. Le vol de propriété intellectuelle (« *overbuilding* ») et le clonage deviennent également beaucoup plus complexes.

Conclusion

Un système connecté classique contient de nombreux composants, et la sécurité doit être intégrée dès la phase de conception. Si la sécurisation des nœuds IoT n'est pas la seule étape, elle est absolument indispensable.

Pour de plus amples informations sur les composants de sécurité embarqués d'Analog Devices, cliquez [ici](#).