Huit bonnes pratiques pour bien sécuriser les objets connectés

Huit bonnes pratiques pour bien sécuriser les objets connectés

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Le point.

Gartner prédit 26 milliards d'objets connectés d'ici 2020. En 2016 ce sont 4,9 milliards de dispositifs connectés qui devraient être déployés. Des objets qui seront potentiellement confrontés à un grand nombre d'attaques. En effet, le volume des cyber-attaques recensé par l'étude The Global State of Information Security® Survey 2016, réalisée par le cabinet d'audit et de conseil PwC en collaboration avec CIO et CSO, a progressé de 38 % dans le monde en 2015. Comment alors sécuriser au mieux ses objets connectés ?

En appliquant quelques bonnes pratiques.

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Plusieurs zones « sensibles » sont donc à surveiller au sein des objets connectés notamment au niveau du capteur et au niveau du transfert des données.

Pour le capteur, l'un des moyens les plus efficaces pour se protéger consiste à sécuriser le hardware grâce à un Secure Element, qui empêche tout accès à l'information lorsqu'on se connecte au capteur. Un élément sécurisé repose sur une plate-forme matérielle inviolable qui héberge des données, cryptées ou non, en toute sécurité et en conformité avec les règles de sécurité fixées par les autorités de confiance. Certains de ces éléments, comme les cartes microSD, peuvent même être amovibles.

Pour sécuriser les données, il est indispensable d'utiliser des technologies de chiffrement robustes afin de lutter contre le piratage ou les interceptions. En effet, le chiffrement rend les données impossibles à lire pour qui ne possède pas la clé de déchiffrement de 128 bits ! Efficace pour repousser les hackers même les plus coriaces.

Une fois le capteur protégé et les données chiffrées, il est important d'assurer la sécurité de l'information lors de son transfert de bout en bout : du capteur jusqu'au portail client.

L'utilisation d'un système de clés multiples géré par un tiers de confiance tel que le propose le protocole LoRa s'avère une solution des plus fiables.

Un tiers de confiance fournit un système de gestion de clé – Key Management System (KMS) – qui permet de générer une AppKey unique pour chaque capteur. A chaque nouvelle session, une AppSKey – Application Session Key – dérivée de l'AppKey sert au chiffrement des données du client. L'opérateur n'a pas accès à ces 2 clés, elles ne sont connues que du tiers de confiance dans le KMS et du client bien sûr pour déchiffrer les données.

Une fois les données récupérées, l'utilisation d'un VPN est bien sûr conseillé.

En agissant à ces différents niveaux, vous appliquez une sécurité optimale à vos objets connectés. De plus, vous pouvez appliquer quelques conseils pour assurer une sécurité de bout en bout des processus :

1. Évaluez le bon degré de sécurité sur le capteur en fonction de la criticité de la donnée : selon l'information concernée, il n'est pas forcément nécessaire d'insérer un Secure Element dans le capteur.
2. Utilisez une technologie avec un protocole de chiffrement robuste de type AES128 par exemple.
3. Mettez en place des infrastructures intégrant l'état de l'art en termes de chiffrement.
4. N'écrivez pas vos clés de cryptage sur disque dur : privilégiez les éléments de sécurité non stockés et volatiles. Calculées « à la demande » par un algorithme, elles ne peuvent donc pas être piratées en cas d'attaque sur la base de données.
5. Optez pour un renouvellement de la clé de chiffrement à chaque connexion du capteur sur le réseau. Une clé renouvelée régulièrement à moins de risque d'être piratée.
6. Utilisez un portail sécurisé pour accéder à vos données applicatives chiffrées : vous avez ainsi, seul, la possibilité de déchiffrer les données. Toutefois, si vous choisissez de ne pas les déchiffrer vous-même, assurez-vous que votre prestataire le fasse sur un cloud sécurisé.
7. Choisissez des technologies en perpétuelle évolution : au sein de la LoRa Alliance, un groupe dédié fait évoluer en permanence le protocole afin d'être toujours à la pointe de la sécurité.
8. Optez pour un opérateur qui intègre les processus de sécurité recommandés par l'ANSSI dans la conception et l'exploitation de son réseau.

Article original de Franck Moine

Réagissez à cet article

Original de l'article mis en page : Huit bonnes pratiques pour bien sécuriser les objets connectés – JDN