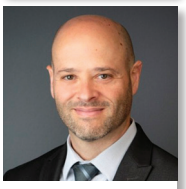
Construire une chaîne d'approvisionnement sécurisée pour faciliter la gestion d'actifs

L'un des avantages de l'Internet des objets est qu'il permet de recevoir des données directement depuis des dispositifs connectés, non seulement sur leur état mais aussi sur leur localisation. Les opérateurs peuvent ainsi savoir où se trouvent leurs actifs, comment ils sont utilisés, et si cette utilisation est conforme au cahier des charges. Cependant, la connectivité nécessaire pour que les appareils signalent leur emplacement à intervalles réguliers entraîne des vulnérabilités susceptibles d'être exploitées par des pirates. Semtech explique ici comment affronter cette difficulté dans le cadre de l'utilisation du protocole LoRaWAN.

AUTEUR



Shahar Feldman, Senior Director Product Marketing, Semtech.

La sécurité est indispensable dans tout système nécessitant une gestion pilotée des actifs en service sur le terrain. Les opérateurs doivent absolument être certains que leurs informations concernant les actifs sur le terrain sont valables et n'ont pas été altérées. Si ce n'est pas le cas, ils exposent à des risques à la fois leur modèle économique mais aussi leur capacité à servir correctement leurs clients.En l'absence de sécurité efficace, un type de piratage qui peut perturber la gestion des actifs est l'attaque dite par rejeu (« replay »). Avec ce type d'attaque, le pirate « écoute » les paquets de données qu'un appareil émet pour signaler son état à une passerelle ou à un autre dispositif du réseau. Il analyse ensuite ces données à la recherche de modèles pour tenter d'effectuer une rétro-ingénierie du protocole utilisé pour les mises à jour de statut, et in fine l'utiliser ultérieurement dans le cadre d'une attaque.

Des attaques potentielles multiples

L'une des attaques possibles est l'attaque par déni de service (DoS) qui inonde le réseau de messages qui semblent authentiques, contenant des mises à jour de localisation fallacieuses et autres données, afin de corrompre la base de données. Une attaque plus subtile et plus simple consiste à désactiver l'étiquette d'un actif avant qu'il ne soit déplacé à l'insu de son propriétaire légitime, puis à faire un replay des messages pour faire croire au système que l'actif se trouve toujours là où il se trouvait.

Une autre forme d'attaque difficile à détecter mais qui peut avoir de graves conséquences pour les utilisateurs et les opérateurs légitimes est l'attaque dite de l'« homme du milieu » (man-in-the-middle). Dans ce scénario, le pirate introduit sa propre passerelle sans fil pour intercepter les messages des dispositifs. La fausse passerelle manipule les données avant de les transmettre au serveur. Les réponses du serveur via cette passerelle peuvent elles aussi être modifiées. Une telle attaque peut avoir de graves conséquences puisqu'elle permet au pirate de prendre le contrôle d'une partie du système et, à partir de là, de lancer d'autres attaques sur le service.

Un impératif : sécuriser les systèmes IoT de bout en bout

Pour prévenir ces attaques, la sécurité de bout en bout est un élément essentiel de tout système basé sur

- Les systèmes IoT qui ont besoin de mises à jour de localisation précises doivent être sécurisés de bout en bout, des badges ou tags utilisés sur le terrain jusqu'à l'application dans le cloud.

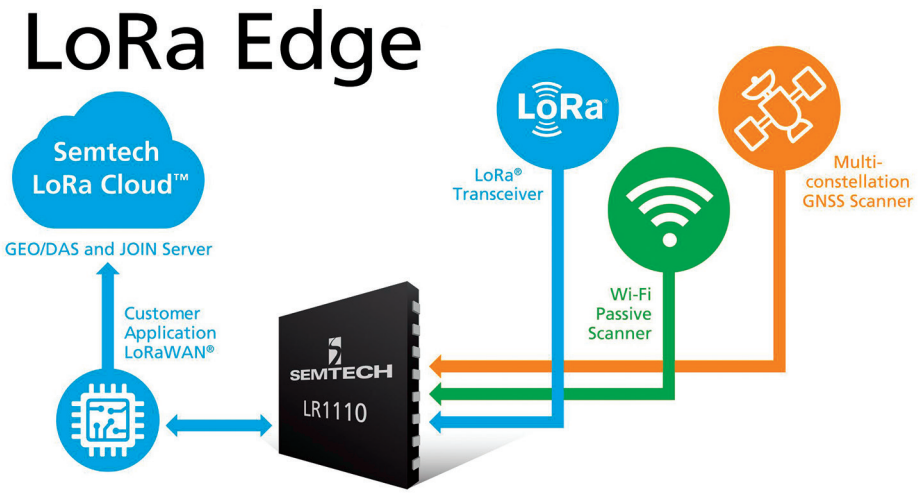
l'IoT, en particulier les systèmes qui ont besoin de mises à jour de localisation précises (photo). Le problème des dispositifs IoT, et en particulier des badges, ou tags, de localisation est qu'ils font l'objet de fortes contraintes en matière d'utilisation d'énergie. Il faut donc des technologies de localisation et une infrastructure de sécurité capable de fonctionner de manière aussi efficiente que possible. Il s'agit d'une contrainte de conception qui exclut d'emblée les technologies et composants développés pour les téléphones portables et les tablettes, même si de nombreux appareils peuvent, lorsqu'ils sont utilisés ensemble, répondre aux principaux besoins de ce type d'application.

L'un des points forts du protocole LoRaWAN est sa sécurité intrinsèque. Contrairement à de nombreux autres réseaux orientés IoT, LoRaWAN met en œuvre un chiffrement de bout en bout pour les données d'application transférées entre les nœuds de capteurs et les serveurs d'application. Un appareil ne peut même pas rejoindre un réseau LoRaWAN s'il n'est pas en mesure de fournir certaines informations d'identification qui devront être approuvées par un serveur contrôlant l'accès. Etant donné que ce protocole a été spécialement conçu pour les dispositifs IoT dont l'enveloppe énergétique est limitée, les architectes de LoRaWAN ont opté pour un cadre dont l'efficacité énergétique est l'un des principaux objectifs, sans pour autant sacrifier l'adhésion à des normes industrielles. La meilleure combinaison de sécurité et d'efficacité énergétique trouvée par les architectes correspond aux algorithmes de chiffrement AES (*) qui sont reconnus comme fiables et efficaces pour les nœuds et les réseaux sous contrainte.

Chaque dispositif compatible LoRaWAN doit donc être personnalisé avec un jeu d›identifiants uniques et des clés de chiffrement AES qui servent non seulement aux applications pour protéger les données qu'elles envoient, mais aussi à rejoindre le réseau lorsque le dispositif est mis en service et qu'il tente de se connecter. La mise en service implique une demande à un serveur de connexion qui exécute les routines d'authentification initiales et vérifie les informations d'identification du dispositif. Il effectue cette vérification en utilisant le protocole CMAC (code d'authentification de message à chiffrement AES). Une fois le code d'authentification calculé et vérifié, le serveur de connexion et le dispositif échangent pour créer un jeu de clés de session. Les clés sont distribuées au dispositif et aux serveurs d'application concernés, afin de garantir une séparation entre les données d'application et les messages de gestion du réseau. De cette manière, les applications et l'opérateur du réseau n'ont pas besoin de partager les clés.

1 ARCHITECTURE LORA EDGE

Semtech a intégré un module de sécurité matériel (HSM, Hardware Security Module) dans le flux de production des dispositifs LoRa Edge afin de garantir que les clés privées et les identifiants de réseau personnalisés soient injectés en toute sécurité avant la livraison à l'équipementier ou au sous-traitant.



Vers un stockage sécurisé et une programmation des clés

De facto, tout le trafic est protégé par les clés de session. En outre, les charges utiles sont protégées à l'aide du mode compteur AES-CTR (**) qui intègre des codes d'intégrité dans chaque paquet. Cette combinaison de protections permet d'éviter les attaques par « replay » de paquets et les attaques de type « homme du milieu ». Toutefois, étant donné qu'il faut intégrer les clés dans l'appareil avant qu'il ne puisse se connecter à l'IoT et commencer à fonctionner, la sécurité de tout appareil est étroitement liée à sa chaîne d'approvisionnement. Pour optimiser la sécurité, la clé racine ne doit donc jamais être utilisée directement. Elle doit plutôt servir à générer des clés dérivées qui peuvent être utilisées pendant de courtes périodes, pour des usages spécifiques. Le dispositif lui-même doit être conçu de telle manière qu'une fois la clé racine injectée, cette clé et ses dérivées ne puissent plus être lues en accédant à la mémoire. Au lieu de cela, le dispositif ne doit utiliser la clé que pour chiffrer les données, ou générer des hachages ou des signatures numériques servant à vérifier l'authenticité. La conception de la pile réseau LoRaWAN va dans ce sens, grâce à l›utilisation de protocoles permettant de lier les clés de chiffrement à des identifiants, pour identifier les dispositifs et les applications à distance.

Afin de garantir que les clés soient protégées et ne risquent pas d'être divulguées par inadvertance ou par cybercriminalité, l'organisation de la chaîne d'approvisionnement est ici d'une importance capitale. Une clé AES, en particulier celle qui fournit les identifiants de base d'un disposi-

(*) Advanced Encryption Standard, algorithme dit à clé symétrique, a été inventé en 2000 par deux ingénieurs, Joan Daemen de STMicroelectronics et Vincent Rijmen de l'université K.U. Leuven. Il existe trois versions de clés AES, sur 128, 192 or 256 bits. C'est le format de clé sur 128 bits qui est le plus utilisé dans le monde.

(**) Dans le mode CTR (CounTeR), le flux de clé est obtenu en chiffrant les valeurs successives d'un compteur. Ce mode qui permet le chiffrement par flot est pré-calculable. De plus, il permet un accès aléatoire aux données et n'utilise que la fonction de chiffrement.

tif, doit être protégée en permanence, à chaque étape, depuis la génération de la clé, en passant par son insertion dans le dispositif, jusqu'à la mise hors service finale après que toute trace, que ce soit dans le dispositif ou dans les systèmes de communication, a été supprimée. Le problème pour bon nombre d'équipementiers et d'intégrateurs est qu'ils n'ont pas le contrôle total de la chaîne d'approvisionnement. La plupart d'entre eux ont recours à un sous-traitant pour faire fabriquer leur matériel à un prix compétitif. Pour programmer les clés dans les dispositifs, à moins de déployer leurs propres programmateurs de dispositifs en interne, les équipementiers devront révéler les données des clés à des tiers. Un pirate ayant accès au programmateur utilisé par le sous-traitant sera en mesure d'intercepter les clés et de les copier pour les utiliser ultérieurement.

Cependant, il existe des mécanismes permettant de prendre en charge le transfert et la programmation sécurisés des clés. Il s'agit généralement d'un module de sécurité matériel intégré à la ligne de fabrication. Mais, même si ce module permet de protéger les données des clés, son intégration dans la chaîne d'approvisionnement implique souvent des coûts d'installation et de gestion élevés, qui restent difficiles à justifier pour de nombreux utilisateurs.

Optimiser la sécurité à moindre coût

Conçu pour être utilisé avec LoRaWAN, le LoRa Edge (LR1110) de Semtech (figure 1) a pour objectif de résoudre ces problèmes du stockage sécurisé et celui de la programmation des clés. Semtech a pour ce faire intégré un module de sécurité matériel (HSM, Hardware Security Module) dans le flux de production de base des dispositifs LoRa Edge afin de garantir que les clés privées et les identifiants de réseau personnalisés soient injectés en toute sécurité avant la livraison à l'équipementier ou au sous-traitant. L'utilisateur n'est pas obligé d'utiliser ces clés programmées. Il peut les écraser en usine lui-même ou avec l'aide de ses partenaires de la chaîne d'approvisionnement s'il préfère utiliser des codes spécifiques. Toutes les clés, qu'elles soient programmées par un client dans son usine ou grâce au HSM de Semtech, ne sont accessibles que par un crypto-moteur embarqué et ne peuvent être lues par l'intermédiaire d'un bus ou d'un port externe.

Ainsi, la configuration par défaut de la solution proposée fournit à chaque dispositif les identifiants de base nécessaires pour rejoindre LoRaWAN à l'aide d'un code identifiant transmis à l'équipementier, qui garantit que le dispositif pourra s'identifier correctement auprès du serveur de connexion lors de sa mise en service quel que soit le domaine d'application (figure 2) .

Pensé pour n'autoriser que les connexions sécurisées nécessaires à LoRaWAN, ce crypto-moteur met en œuvre un jeu standard de routines de sécurité qui sont utilisées par un microcontrôleur externe pour mettre en œuvre des fonctions IoT et de localisation. L'API simple proposée par LoRa Edge permet de chiffrer les données d'une application avant leur transmission, et aussi d'exécuter d'autres services comme des calculs de hachage pour vérifier l'intégrité des données. Étant donné que le moteur de chiffrement se trouve sur la même puce que la mémoire sécurisée, et que les protocoles sécurisés comme ceux utilisés pour LoRaWAN n'utilisent jamais directement les clés stockées, mais génèrent des clés dérivées pour chiffrer les messages, cette architecture assure un haut niveau de protection.

Comme le protocole LoRaWAN lui-même, le crypto-moteur est optimisé pour une consommation d'énergie minimale. Ce qui permet de mieux répondre aux besoins de dispositifs comme les tags de gestion d'actifs. A l'inverse, de nombreux circuits intégrés du marché dotés d'un composant sécurisé sont conçus pour gérer un large éventail de technologies de chiffrement, ce qui tend à augmenter leur coût et leur consommation.

Outre ses fonctions LoRaWAN et de sécurité, LoRa Edge met aussi en œuvre les fonctionnalités de base nécessaires pour recevoir les données des émetteurs-récepteurs GNSS et Wi-Fi, ce qui permet de réaliser des économies de coûts et d'énergie supplémentaires grâce à une solution innovante installée dans le cloud. Par exemple, plutôt que de subir la surcharge de traitement nécessaire pour décoder et interpréter les paquets GNSS, le dispositif peut utiliser le service LoRa Cloud pour traiter ces informations à distance et assurer les mises à jour de localisation via la connexion LoRaWAN. Ce faisant, la conception optimise l'autonomie de la batterie. Un tag de gestion d'actifs typique peut ainsi avoir une durée de vie de plusieurs années à partir d'une seule charge, par opposition aux seulement 3 à 6 mois typiques des conceptions non intégrées, qui utilisent un composant sécurisé et des frontaux silicium séparés pour les signaux GNSS et le Wi-Fi. Le résultat est une solution qui optimise la sécurité à moindre coût, tout en facilitant l'intégration des systèmes et de la chaîne d'approvisionnement par rapport aux autres approches disponibles. ■

2 CHAÎNE D'APPROVISIONNEMENT SÉCURISÉE

La configuration par défaut de LoRa Edge fournit à chaque dispositif les identifiants de base nécessaires pour rejoindre LoRaWAN à l'aide d'un code transmis à l'équipementier qui garantit que le dispositif pourra s'identifier correctement auprès du serveur de connexion lors de sa mise en service, quel que soit le domaine d'application.