Peut-on se fier à l'Internet des objets ?

Plus les équipements connectés à l'IoT (Internet of Things ou Internet des objets) prennent d'importance dans nos vies, plus notre confiance en leur sécurité et leur fiabilité devient critique. Toutefois, pour que les bienfaits de l'IoT puissent s'accommoder du nombre croissant d'équipements connectés, les développeurs ont la responsabilité de préserver cette confiance en mettant en place une stratégie de sécurité de bout en bout.

Par essence, les équipements IoT restent des systèmes embarqués, soumis aux mêmes impératifs de fiabilité et de sécurité que les systèmes critiques d'autres secteurs. Sous leurs couches logicielles se trouvent des entrées, des sorties, des machines d'état et des données, le tout conçu dans un but spécifique. Les systèmes complexes contiennent plusieurs sous-systèmes développés par différents partenaires, chacun avec ses propres interfaces réseau externes (figure 1 ci-contre). L'IoT consiste également en une multitude d'appareils reliés en réseau qui échangent des données en tant que capteurs ou en tant que contrôleurs, et qui sont limités en taille, en poids et en consommation. Quelle que soit l'application – énergie intelligente, réseau, automobile ou dispositifs électroniques portés sur soi – la confiance dans ces équipements repose sur leur sécurité et leur fiabilité en cours de fonctionnement.

Types d'attaques

Les architectures de sécurité de bout en bout défendent les systèmes embarqués contre trois grandes catégories d'attaques, le « reniflage » réseau (sniffing), l'usurpation d'identité (spoofing) et les attaques par injection. Ces attaques décrites dans le tableau I utilisent une combinaison de ces différentes catégories pour accéder aux données sensibles et altérer le fonctionnement de ces systèmes. Les attaques de type réseau sont menées au niveau « boîte noire » depuis les interfaces réseau externes pour accéder au système d'exploitation, aux piles logicielles et aux applications. Les attaques physiques portent directement sur le matériel accessible à l'intérieur du châssis. Bien que les attaques de type réseau aient une plus grande portée et soient les plus dangereuses, il est plus difficile de se défendre contre les attaques physiques. Si le système est éteint, un logiciel de protection n'est, de fait, d'aucune utilité pour contrer les logiciels malveillants.

AUTEUR

Gregory Rudy, directeur Business Development de l'activité Integrity Security Services, Green Hills Software.

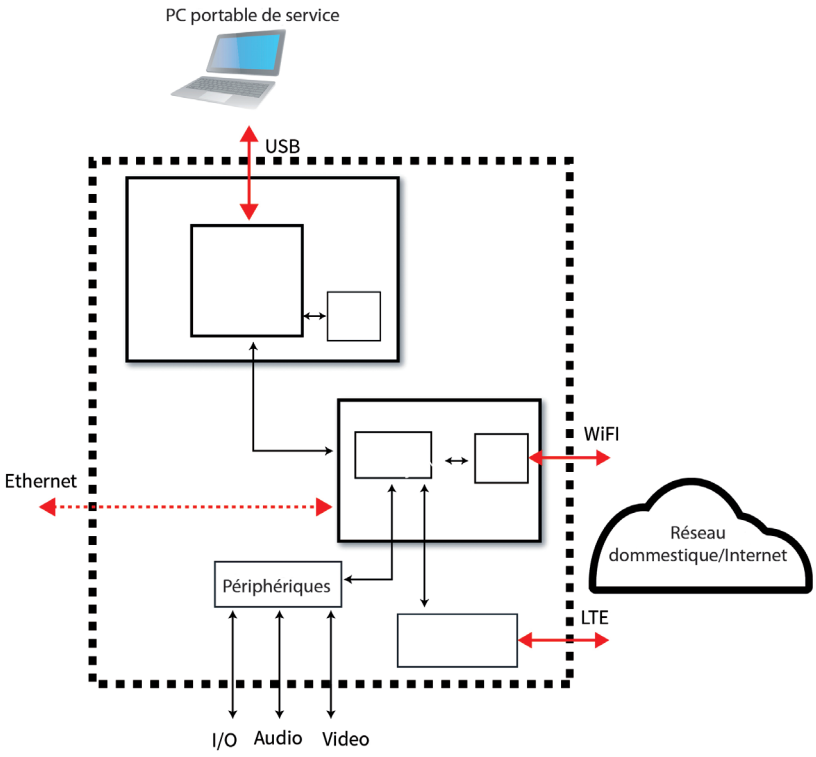
Évaluation du risque

La conception d'une stratégie de sécurité de bout en bout démarre avant la sélection du matériel et du logiciel, par l'évaluation de l'impact de toutes ces menaces. Durant le processus d'évaluation du risque, les architectes du système de sécurité examinent la vulnérabilité des données, des interfaces et du logiciel aux menaces de type réseau et de type physique au sein de l'environnement cible.

Considérons un simple équipement connecté à l'Internet des objets, du type grille-pain intelligent. On ne peut parler ici de vulnérabilité des données. De même, le risque lié à des commandes éventuellement usurpées est minimal. Toutefois, quels sont les effets possibles de la présence d'un logiciel malveillant ? La surveillance du réseau, la mise en place de portes dérobées Internet et l'aptitude à utiliser ce premier point d'entrée pour attaquer d'autres équi-

1 SCHÉMA FONCTIONNEL DES SYSTÈMES IOT COMPLEXES

Les systèmes complexes contiennent plusieurs sous-systèmes développés par différents partenaires, chacun avec ses propres interfaces réseau externes.



I.- MEILLEURES PRATIQUES DE SÉCURITÉ EMBARQUÉE CONTRE LES ATTAQUES RÉSEAU ET PHYSIQUES

ATTAQUE	DESCRIPTION	MÉTHODES		CONTRE-MESURES
		RÉSEAU	PHYSIQUE	
Reniflage (sniffing)	Collecte passive des données protocolaires et des informations échangées entre les systèmes. Les assaillants l'utilisent pour comprendre les protocoles et monter des attaques du type usurpation d'identité	Collecte des données en s'insérant entre une interface réseau privée et l'extérieur ou via un équipement connecté au même réseau	Analyse des données entre les sous-systèmes en utilisant des équipements de débogage (ex. sondes et analyseurs logiques); peut inclure l'interception des ondes émises ou d'autres attaques indirectes	Cryptage
Usurpation d'identité (spoofing)	Reproduction et corruption de messages par une source invalide afin de forcer l'accès ou d'impacter le fonctionnement	Par connexion directe à une interface réseau cible ou via un « homme du milieu » (man-in-the-middle)	Généralement commise par un logiciel corrompu sur un sous-système connecté	Authentification
Attaque par injection	Chargement et exécution d'un logiciel malveillant destiné à remplacer ou ajouter une fonction telle que des portes d'accès dérobées (backdoors)	Utilisation d'anomalies logicielles, de contournement de contrôle d'accès par usurpation d'identité ou de corruption de piles de protocoles de bas niveau afin de lancer un nouveau logiciel	Modification du contenu de la mémoire programme par un logiciel malveillant via un programmateur ou les ports de débogage (ex. chargement via JTAG et USB de logiciels malveillants furtifs - Root Kits).	Analyse de vulnérabilités & vérification par un processus de démarrage sécurisé (Secure Boot)

pements ! Tout ceci induit un risque financier maintenant considérable. Ce n'est pas tant dû à l'attaque d'un unique système embarqué, mais au fait qu'il existe une grande quantité d'équipements reliés à ce premier système. Ces systèmes embarqués – appareils médicaux, automobiles, alarmes, ordinateurs domestiques – cessent d'être des équipements isolés. Ce sont des points d'accès à tous les réseaux dont dépendent votre existence numérique et vos moyens de subsistance.

Comment établir la confiance en l'Internet des objets

Par « confiance » dans la sécurité embarquée, nous entendons ici la foi en l'intégrité et la fiabilité d'un système. Le processus utilisé pour établir cette confiance se nomme authentification. La confiance en un système (root of trust) trouve sa racine dans le point où démarre ce processus d'authentification, puis se déploie à travers chaque couche du logiciel (figure 2). Les solutions à haut niveau d'assurance possèdent soit une racine de confiance de type matériel, soit une mémoire inaltérable (impossible à modifier).

A chaque mise sous tension, le processus de démarrage sécurisé (Secure Boot) vérifie l'authenticité de chaque couche du logiciel avant de l'autoriser à s'exécuter. Cette caractéristique garantit que le logiciel n'est pas corrompu et provient d'une source valide. Un composant n'est exécuté qu'une fois qu'il a été approuvé comme étant « digne de confiance » (trustworthy).

L'objectif du démarrage sécurisé est d'éliminer le risque d'injection de code par le réseau ou au niveau physique, et ce en vérifiant à chaque mise sous tension que le logiciel est exempt de tout logiciel malveillant.

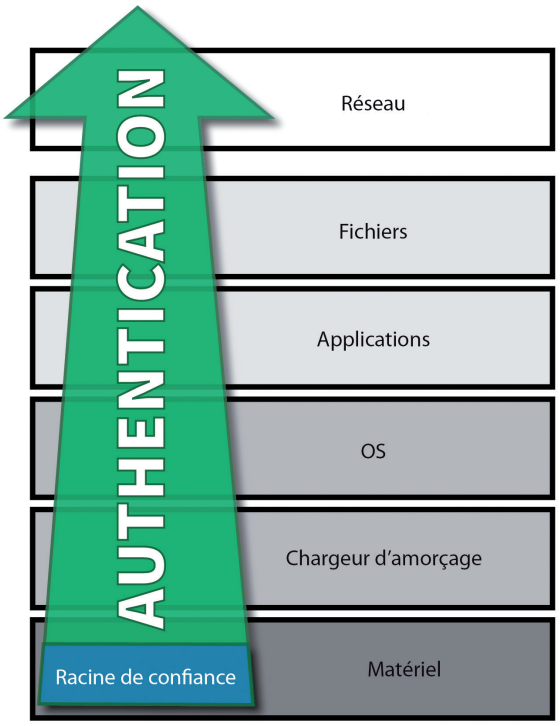
Extension du domaine de la confiance

Il ne faut jamais se fier à un réseau, mais toujours supposer que derrière chaque connexion se tient un pirate qui essaie de s'emparer des données, de lancer des commandes et de jouer le rôle de « l'homme du milieu » (man-in-the-middle) avec vos équipements. La figure 3 de la page suivante illustre ce dernier type d'attaque. Au minimum, l'assaillant se bornera à analyser l'ensemble des données et commandes entre deux équipements (ici un portable et une caméra). Les communications entre les équipements peuvent également être transférées à des systèmes de collecte de données non autorisés. Enfin, le pirate peut détourner les deux équipements ; éteindre la caméra et falsifier son état tout en remplaçant le flux vidéo.

La cryptographie reposant sur une infrastructure à clés publiques (Public Key Infrastructure ou PKI) élimine la menace de l'« homme du milieu » en utilisant des certificats afin de permettre aux points d'extrémité de s'authentifier mutuellement. Une autorité de certification (Certificate Authority ou CA) génère les certificats pour chaque équipement – dont l'identité est attestée par une signature numérique apposée sur chaque certificat. Ces signatures numériques sont générées par une clé privée et n'ont besoin que de la clé publique correspondante pour être vérifiées. Le certificat émis par

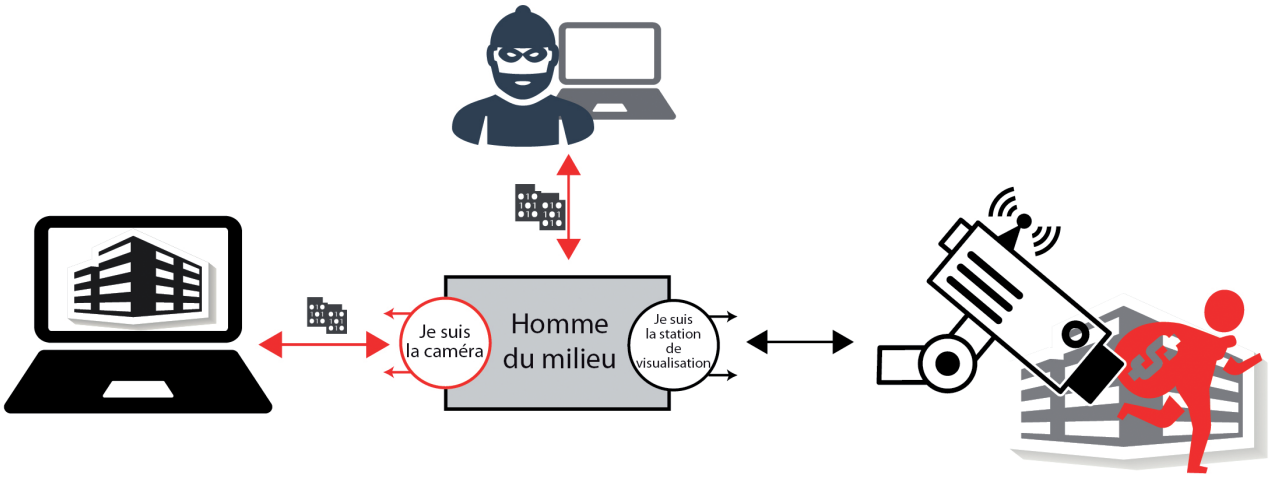
2 AUTHENTIFIER L'ENSEMBLE DU LOGICIEL À PARTIR DE LA RACINE DE CONFIANCE

La confiance en un système (root of trust) trouve sa racine dans le point où démarre le processus d'authentification, puis se déploie à travers chaque couche du logiciel.



3 PRINCIPE DE L'ATTAQUE DIT DE L'HOMME DU MILIEU

Il ne faut jamais se fier à un réseau, mais toujours supposer que derrière chaque connexion se tient un pirate qui essaie de s'emparer des données, de lancer des commandes et de jouer le rôle de « l'homme du milieu » (man-in-the-middle) avec vos équipements.



la CA permet ainsi à chaque équipement d'authentifier l'identité d'un autre système avant d'en accepter les données.

L'authenticité du logiciel

Mais qu'est-ce qui empêche quiconque d'ouvrir le capot d'un système une fois celui-ci mis hors tension et d'accéder à sa mémoire flash pour y injecter du code ou la falsifier ? En utilisant des principes similaires aux certificats PKI, les développeurs peuvent signer des images logicielles pour prouver l'authenticité de leurs produits au lancement et durant le fonctionnement en utilisant un démarrage sécurisé (Secure Boot). Pour la signature du code, on utilise une clé privée asymétrique à laquelle correspond une « ancre de sécurité » (trust anchor) qui permet de vérifier ce dernier à l'exécution (figure 4).

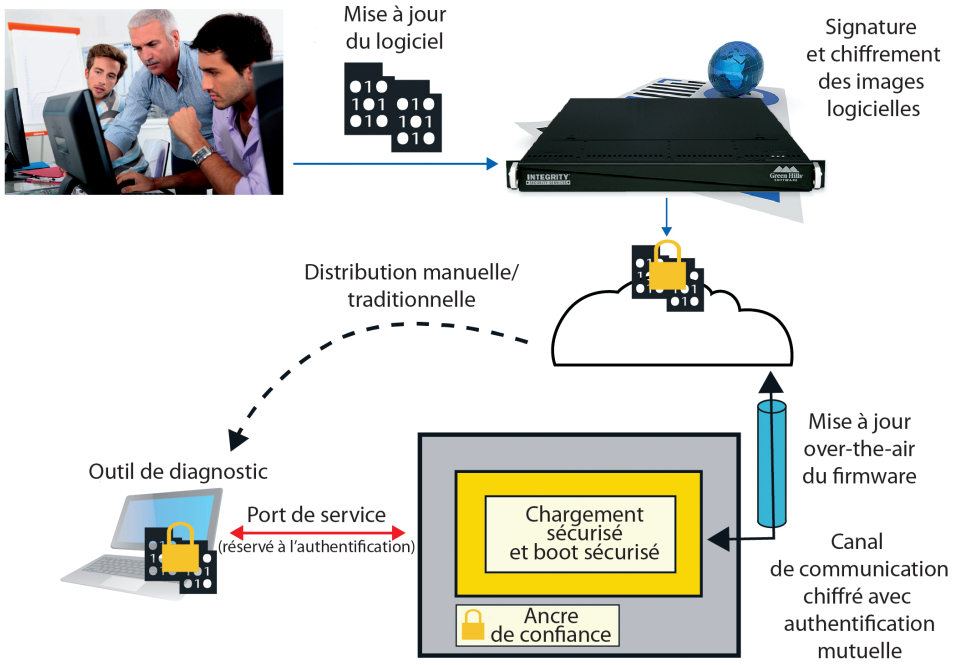
Les infrastructures de sécurité d'entreprise

Grâce à la cryptographie, les développeurs de l'Internet des objets sont en mesure de créer des systèmes d'équipements interconnectés « de confiance » sur des réseaux publics peu fiables. La mise en œuvre d'une stratégie de sécurité de bout en bout exige une plate-forme intégrant un module cryptographique, des protocoles de sécurité réseau, une protection par clés et un démarrage sécurisé. Toutefois, quel que soit le temps passé à sécuriser les équipements, cet investissement sera mis en péril si les clés des certificats et les clés de signature du logiciel sont piratées.

Dans le cas d'un piratage des clés PKI racines, c'est l'ensemble des équipements mis en fabrication qui est menacé. Par conséquent, la protection des clés racines est la fonction la plus critique du système et doit bénéficier d'une priorité absolue. Vu la complexité des chaînes de fabrication et d'approvisionnement actuelles, s'équiper d'un poste de travail intégrant un module de sécurité matériel est insuffisant. Les chaînes logistiques de l'IoT combinent de nombreux sites de fabrication offshore et/ou dépendants de tiers. Ici les partenaires de l'entreprise ont besoin d'ajouter des logiciels à la plate-forme de sécurité sans que leur propriété intellectuelle soit menacée par des concurrents partageant le même site. L'Infrastructure de Sécurité leur permet d'utiliser des clés pour éliminer tout risque de piratage (figure 5).

4 UNE INFRASTRUCTURE DE SÉCURITÉ DE BOUT EN BOUT

Grâce aux autorités de certification et aux services de signature de code, les infrastructures de sécurité d'entreprise établissent la confiance dans l'IoT.



Pour éviter les erreurs logicielles

Si la qualité du logiciel laisse à désirer, le niveau de confiance en sera nécessairement affecté. C'est pourquoi Green Hills Software promeut

II.- ORGANISATION PRATIQUE D'UNE STRATÉGIE DE SÉCURITÉ DE BOUT EN BOUT

RÈGLE	SOLUTION
1. Communiquer sans faire confiance au réseau	Authentifier tous les points terminaux distants à l'aide de certificats pour éviter les attaques de type « homme du milieu » et crypter la communication des données sensibles
2. Veiller à ce que le logiciel ne soit pas altéré	Signer numériquement et vérifier le logiciel au démarrage, ainsi qu'à intervalles réguliers, pour s'assurer qu'il n'a pas été modifié
3. Protéger les données critiques	Crypter les données sensibles stockées dans la mémoire non volatile, et placer des « ancres » de sécurité (trust anchors) dans la mémoire protégé en écriture.
4. Séparer pour sécuriser	Isoler les clés dans une enceinte cryptographique protégée des attaques physiques et réseau.
5. Fonctionner de manière fiable	Considérer l'impact d'une vulnérabilité dans le système d'exploitation et dans les applications. Utiliser la méthodologie PHASE pour développer des logiciels à haut niveau d'assurance.

une méthodologie de conception de logiciel à haut niveau d'assurance qualité dénommée PHASE. PHASE consiste en une implémentation minimale, la séparation en composants logiciels, l'application du principe du « privilège minimal », un processus de développement sécurisé et la validation par un expert indépendant. Ces mêmes principes, utilisés dans le développement du système d'exploitation temps réel INTEGRITY, s'appliquent au développement d'applications afin de minimiser le risque et l'impact d'erreurs logicielles.

Développement d'une stratégie de sécurité de bout en bout

INTEGRITY Security Services (ISS), filiale de Green Hills Software, participe dans ce cadre à la révolution de l'Internet des objets. Elle aide ses clients à concevoir des produits fiables grâce à une stratégie de sécurité embarquée de bout en bout.

En partant d'une évaluation des risques (afin de mesurer l'impact de tout événement indésirable), une entreprise peut wbâtir une stratégie de sécurité qui réponde aux cinq règles de la Sécurité Embarquée conçues par ISS (tableau II). En conclusion, les perspectives de l'Internet des objets et son impact sont exponentiels et phénoménaux, mais la sécurité n'a rien d'un luxe –c'est une exigence. La sécurité de bout en bout est la base fondatrice d'un monde d'appareils qui nous connectent. ■

5 UNE INFRASTRUCTURE DE SÉCURITÉ D'ENTREPRISE SÉCURISE L'ÉCHANGE DE CLÉS DE CHIFFREMENT AU TRAVERS DE CHAÎNES LOGISTIQUES DISTRIBUÉES

Vu la complexité des chaînes de fabrication et d'approvisionnement actuelles, s'équiper d'un poste de travail intégrant un module de sécurité matériel est insuffisant. Une infrastructure de sécurité d'entreprise de bout en bout permet d'utiliser des clés pour éliminer tout risque de piratage dans des chaînes logistiques qui combinent de nombreux sites de fabrication offshore et/ou dépendants de tiers