CYBERSÉCURITÉ

DES RÉSEAUX D'OBJETS CONNECTÉS PLUS SÛRS GRÂCE À TIEMPO SECURE

La révolution de l'Internet des objets (IoT) pose de grands défis sécuritaires au vu du nombre croissant de cyberattaques opérées via les objets connectés. D'où la nécessité de proposer des solutions adaptées à ces enjeux parfois vitaux. Explications avec Serge Maginot (82), Co-fondateur et CEO de Tiempo Secure, PME figurant parmi les leaders mondiaux des processus de sécurisation des objets connectés.

Serge Maginot (82)

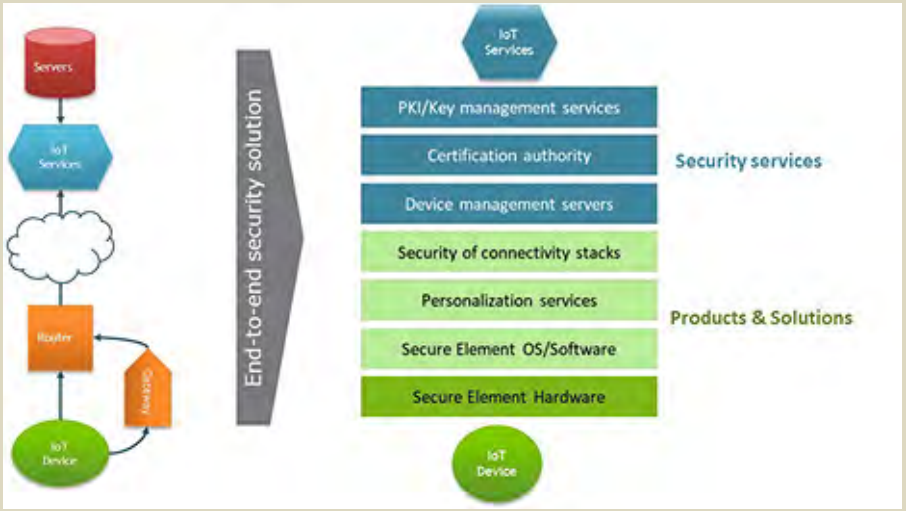
Il existe un consensus à l'heure actuelle sur la nécessité de sécuriser les objets connectés. Qu'en est-il des modalités de mise en œuvre ?

Si la sécurisation des objets connectés fait effectivement l'objet d'un consensus, il en est autrement de la manière employée pour assurer cette sécurisation. Un certain nombre de parties prenantes dans le domaine avancent qu'elle s'opère grâce aux logiciels, sans matériel spécifique. Chez Tiempo, nous sommes convaincus au contraire qu'une approche mixte hardware & software est indispensable pour réellement protéger les objets connectés et les données qu'ils transmettent contre les tentatives d'attaque des cybercriminels. Dans l'approche software pure, la protection des données transmises sur un réseau s'effectue via un microcontrôleur standard qui exécute du code embarqué, grâce auquel se fait le cryptage des données via des algorithmes de chiffrement standard avec clef unique (typiquement un AES avec une clé de chiffrement de 128 bits). Or, il est possible aujourd'hui avec un équipement qui coûte moins d'un millier d'euros de retrouver en quelques minutes les clés de chiffrement utilisées dans ce type de microcontrôleur standard (par des attaques d'observation de type « side-channel attacks ») et de décoder ainsi toutes les informations transmises sur le réseau en question. Dans l'approche combinée hardware & software, l'objet connecté contient un microcontrôleur sécurisé spécifique appelé Secure Element, équivalent d'un « coffre-fort matériel » dans lequel les clefs sont stockées et protégées des attaques les plus agressives grâce à des contre-mesures matérielles (secondées par des contre-mesures logicielles) très efficaces implantées dans ce type de microcontrôleur. C'est à l'intérieur de ce Secure Element que va se faire le chiffrement des données, les clefs privées ne quittant ainsi jamais ce « coffre-fort matériel ». Cette technologie est utilisée depuis des décennies pour les cartes bancaires et les documents d'identité sécurisés, passeports ou autres. Il est important de s'inspirer de ces expériences réussies pour garantir la sécurité des objets connectés.

Comment assurez-vous le développement de circuits intégrés permettant le chiffrement des données sensibles et leur stockage sécurisé ?

Face aux menaces exécutées par les hackers, les autorités ont développé des standards permettant de graduer les niveaux de résistance aux attaques des systèmes électroniques faisant du chiffrement sécurisé. Appelés Critères Communs (CC), ils sont classés par ordre croissant de résistance : EAL 2/3/4/5/5+/6/6+. Le niveau CC EAL5+ est ainsi exigé pour les documents d'identité au niveau international. La vérification de la conformité des systèmes à ces standards est assurée par des laboratoires indépendants, les laboratoires CESTI en France qui sont eux-mêmes certifiés par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), expert en France de ces normes Critères Communs. Ces laboratoires mènent des campagnes d'attaques, attaques

End-to-end security solution for the IoT



intrusives (par injection de fautes par laser par exemple) ou attaques par observation (de la consommation électrique du système, les fameuses « side-channel attacks », très performantes), sur les systèmes électroniques pour tester leur niveau de résistance face à ces attaques. Le matériel est certifié s'il résiste à ces attaques. Les laboratoires d'évaluation anticipent même les nouvelles attaques potentielles et les intègrent à leurs campagnes. Actuellement, seule une dizaine de sociétés de microélectronique dans le monde, dont la société Tiempo, sont en mesure de concevoir des circuits intégrés certifiés au niveau CC EAL5+ et donc capables de résister à ce niveau d'attaque.

Quelles en sont les applications concrètes dans le domaine des objets connectés ?

Tiempo utilise son expertise, ses produits et sa propriété intellectuelle, validés dans les domaines de sécurisation les plus exigeants que sont le bancaire et l'identification gouvernementale, pour décliner une offre de sécurisation flexible qui soit adaptée à l'Internet des Objets. Contrairement aux domaines précédents, les besoins en sécurité pour les objets connectés sont très différents en fonction du type d'application et du marché visé. Il est important que les objets connectés aient une sécurisation minimum qui passe par un hardware, mais celle-ci doit être adaptée à l'usage de l'objet. Certaines applications doivent être extrêmement sécurisées lorsqu'elles mettent en jeu la vie humaine, comme les voitures connectées ou certains équipements médicaux par exemple. L'enjeu est légèrement différent lorsqu'on ne parle plus de sécurité vitale, mais de protection des données personnelles. À l'autre bout de la chaîne, un bracelet connecté pour le sport ne nécessitera pas le même matériel de sécurité. Il s'agit donc pour les producteurs d'objets connectés de parvenir à un équilibre économique adapté au niveau de sécurité demandé.

Vous proposez une nouvelle offre de sécurisation des objets connectés sur Internet. Pouvez-vous nous expliquer en quoi consiste cette « end-to-end security solution » ?

Les acteurs industriels qui intègrent des Secure Elements dans le domaine bancaire et gouvernemental sont des experts en sécurité. Ce n'est pas le cas de la plupart des sociétés qui produisent et déploient des objets connectés. Tiempo travaille en coopération avec ces sociétés, notamment des fabricants d'équipements pour la domotique, les compteurs intelligents et des objets portables de surveillance médicale, dans le cadre d'un projet de R&D collaboratif pour définir une offre de sécurisation des objets connectés adaptée à leurs besoins.

Une « end-to-end security solution » vise ainsi à fournir une solution clé en main à nos clients qui développent et déploient des objets connectés pour sécuriser leur application au niveau de l'objet connecté, de la transmission (chiffrée) de l'information sur le réseau jusqu'à la gestion de l'objet par des serveurs sécurisés disponibles sur le Cloud (d'où la dénomination « end-to-end »). Pour nos clients de l'IoT, il est important d'introduire cette sécurité au niveau de la fabrication de l'objet autant que d'en permettre la gestion par des serveurs sécurisés, une fois la flotte d'objets connectés déployée sur le terrain, dans une voiture, une maison, une entreprise ou une ville, par exemple pour permettre la mise à jour des clefs de chiffrement et des logiciels embarqués sur ces objets de manière sécurisée et via le Cloud (« Over-The-Air », ou OTA). Le client est ainsi assuré d'une gestion sécurisée de ses objets connectés durant tout leur cycle de vie.

Pour finir, quels sont vos prochains challenges au vu du développement exponentiel de l'IoT ?

La typologie des acteurs de l'Internet des Objets est très variable. On trouve des grands groupes dans certains segments de marché comme le secteur automobile, mais aussi une majorité de start-ups, TPE, PME et ETI fournissant des services ou objets connectés sur l'IoT. Nous souhaitons adresser nos produits et solutions à ces clients en priorité car nous sommes particulièrement sensibilisés à leurs problématiques spécifiques, étant nous-mêmes une PME. Pour cela, nous allons donc proposer des solutions dimensionnées aux besoins divers de ces sociétés, différents en termes de sécurité et d'enjeux. Un vaste programme donc, mais plein d'opportunités passionnantes... ■