Opinions Libres
le blog d'Olivier Ezratty

Peut-on sécuriser l'Internet des objets ?

Je suis intervenu en ouverture de la **Conférence Cybersécurité – IOT et Systèmes Embarqués** organisée à Toulouse le 18 février 2016. Organisée par Captronic et la société de conseil G-Echo, cette conférence rassemblait une centaine de personnes au laboratoire du LAAS-CNRS de Toulouse et voyait intervenir des spécialistes des questions de sécurité. C'était une belle occasion de faire le point sur le sujet. Ce compte-rendu utilise des informations glanées dans les interventions de cette conférence, complétées de quelques recherches en ligne. La conférence était sponsorisée par AllianTech (outils de mesure et capteurs), Digital Security (services et conseil), HSC/Deloitte (la filiale de conseil en sécurité de Deloitte issue de l'acquisition de Hervé Schauer Consultants en 2014), ISIT (développement temps-réel) et NeoTech (services et conseils).

Ce n'était pas la seule conférence sur le sujet en France. Le **8e Forum International de la Cybersécurité** avait eu lieu au Grand Palais de Lille les 25 et 26 janvier 2016. Il y avait aussi eu les **Journée sur l'Internet des Objets et la Cybersécurité/Cyberdéfense** en juin 2015 au CNAM à Paris. Le sujet monte en puissance ! La sécurité de l'Internet des objets est devenue un sujet majeur des grandes conférences sur la sécurité comme dans les fameuses **Defcon** aux USA.

Chaque nouvelle vague technologique apporte son lot de vulnérabilités. Il a fallut des décennies pour sécuriser les transports ferroviaires, aériens et automobiles. La ceinture de sécurité, inventée à la fin du 19e siècle, n'est devenue obligatoire en France qu'en 1973. Dans le numérique, ces cycles innovation-sécurisation se sont accélérés. La micro-informatique a vu très rapidement naitre le business des anti-virus. Celui-ci s'est accéléré avec l'arrivée d'Internet. La mobilité et les systèmes de paiement ont alors apporté leur lot de vulnérabilités et de nouvelles solutions.

NB: j'utilise souvent le terme "hack" pour décrire des actions techniques permettant d'attaquer un objet connecté. Oui, je sais, le hacking peut avoir une connotation positive, mais il est aussi appliqué dans le domaine du piratage !

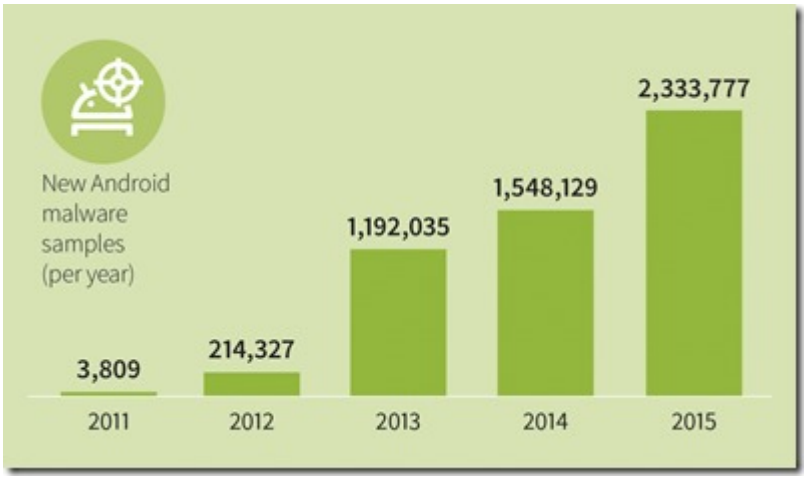
Les fragilités connues des objets connectés

L'univers des objets connectés va probablement suivre un scénario voisin : un développement des usages, la découverte de (nombreuses) vulnérabilités, des attaques symboliques générant un écho dans les médias et l'émergence puis le déploiement de solutions de sécurisation. On assistera à une inévitable course contre la montre entre sécurité et contre-attaques des pirates.

Ceux qui prétendent pouvoir sécuriser intégralement leur site web ou leur micro-ordinateur sont souvent surpris des vulnérabilités qui peuvent être mises à jour par des spécialistes. La perception du risque est une affaire d'information. Par défaut, on ne craint pas grand chose. Mais

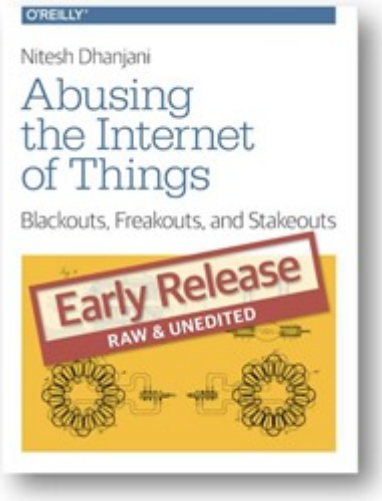
au gré de la mise en avant des failles de sécurité et de leurs conséquences, la perception augmente et peut générer l'attente d'une plus grande sécurisation des systèmes. Sans compter le cas d'attaques subies.

Dans l'univers des objets connectés, les **smartphones** sont en première ligne. Ils sont à ce jour les objets les plus connectés du grand public et sujets à un nombre croissant d'attaques liées à leurs différentes vulnérabilités. Ainsi, le Mobile Malware Report Q4 2015 de G-DATA évoque le nombre de **2,3 millions de nouveaux dangers** identifiés sur Android en 2015, en augmentation de 32% par rapport au trimestre précédent. Cela concerne les 66% d'utilisateurs de smartphones qui utilisent Android. iOS est également sujet à diverses vulnérabilités même si son côté plus fermé le protège partiellement.



Mais les vulnérabilités commencent à toucher de nombreuses catégories d'objets connectés. Les vulnérabilités sont multipliées par les points de contact et les capteurs comme les actuateurs. Et côté couverture médiatique, on commence à être servi. A commencer par les déclarations de responsables de l'ANSSI, l'agence du gouvernement qui dépend du SGDN et gère la sécurité des systèmes d'information de l'Etat, après la publication du **Rapport Cybersécurité des objets connectés** de Vincent Strubel **en juin 2015**.

Le catalogue des menaces concernant les objets connectés est pour le moins fascinant ! Dans "**Abusing the Internet of Things**", Nitesh Dhanjani en fait un premier inventaire avec le hacking intégrant les codes sources associés pour des éclairages connectés, générant un black-out, des serrures connectées (**source**), facilitant les cambriolages, des baby monitors, des TV connectées et des voitures connectées.



L'inventaire du "Hou ! Fais-moi peur" est déjà des plus riche :

- Les **voitures** possèdent une bonne douzaine de sous-systèmes et supportent divers protocoles réseaux (GSM/2G/3G/4G, Bluetooth, NFC, Wi-Fi sans compter l'USB et le port ODB-II). Même les informations RDS transmises dans la bande FM peuvent perturber le système de navigation ! Les autoradios sont vulnérables aux fichiers audio WAV vérolés. Il est aussi possible de créer une impulsion électromagnétique pour détruire l'électronique de bord d'un véhicule, via un **générateur de Marx** placé au bord de la route. Des problèmes de ce genre sont inventoriés dans le rapport du sénateur américain Edward Markey **Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk** publié début 2015. Le schéma ci-dessous qui liste les nombreuses zones de vulnérabilités des véhicules modernes provient de la **GSMA**.

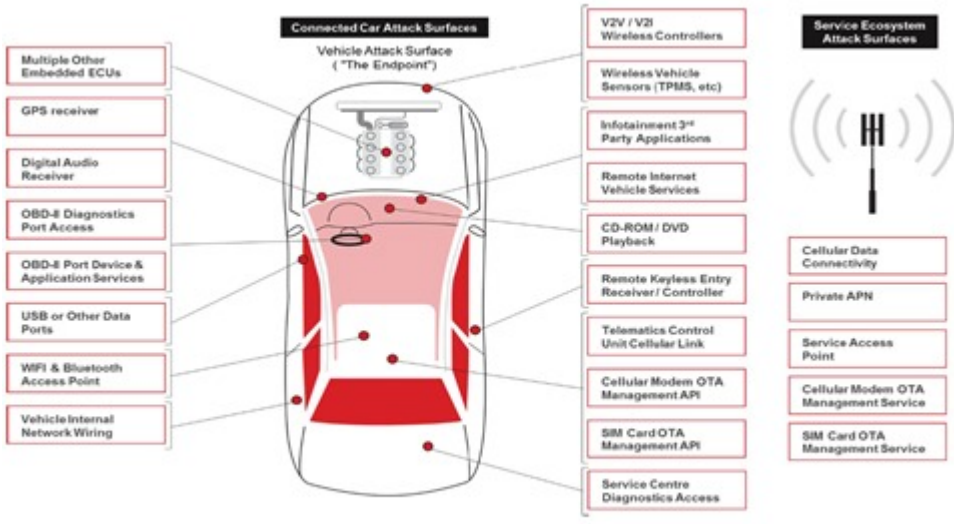


Figure 11– Connected Car Attack Surfaces

- Le piratage de **connexions Wi-Fi** via l'accès aux ondes de radio fréquences et l'interception de certains mots de passe qui circulent en clair est déjà bien courant. Des logiciels de hack de réseaux Wi-Fi sont faciles à trouver sur Internet et sont qui plus est gratuits ! La protection ? Au minimum, utiliser des mots de passe compliqués avec minuscules, majuscules, chiffres et

caractères spéciaux empêchant les systèmes de hacking d'exploiter des dictionnaires de mots couramment utilisés.

- Les **caméras de surveillance** peuvent être attaquées avec des lasers ou via leurs liaisons Wi-Fi, surtout si le réseau Wi-Fi a été précédemment attaqué par les outils précédents. Il en va de même pour les caméras **GoPro** qui peuvent être hackées à distance via leur liaison Wi-Fi (**source**).

- Dans la **santé**, des risques sont identifiés aussi bien avec les appareils connectés qui se contentent de prendre des mesures comme la tension ou la glycémie ou ceux qui agissent sur la santé comme les pacemakers.

- Les **moyens de paiement**, notamment sans contacts, sont très vulnérables. Ceci étant, la vulnérabilité la plus forte est celle des hommes eux-mêmes, en témoigne les fameuses fraudes "au président" qui relèvent de l'ingénierie sociale et pousse des services de comptabilité à effectuer des virements de très fortes sommes à des destinataires inconnus sans que cela n'éveille de soupçons dans les entreprises. L'objet connecté le plus fragile est en fait… l'homme !

- Les **compteurs électriques** peuvent être attaqués, tout du moins en Espagne, pour compromettre la **sécurité du réseau électrique** du pays. C'est lié à l'inter connectivité massive d'appareils faiblement sécurisés avec des réseaux d'infrastructure.

- Les **thermostats de Nest** sont vulnérables, tout du moins, ils l'étaient **en 2014**.

- Un **haut fourneau** a aussi été attaqué **en Allemagne** en 2014 sans compter les centrifugeuses d'uranium iraniennes, attaquées par le virus **Stuxnet** co-conçu par la NSA et le service de renseignement israélien 8200, et exploitant une vulnérabilité de Windows. Le ver reprogrammait des machines industrielles sans laisser de traces ! Il va sans dire que c'était une attaque des plus sophistiquées avec un niveau d'intégration très important. Le scénario est facilement réplicable et s'appuie sur la connaissance publique de failles connues dans les systèmes d'exploitation, Linux compris. Les systèmes d'exploitation sont rarement patchés instantanément après la découverte de vulnérabilités.

- Il y a quelques années, l'expert en sécurité **Chris Roberts** avait montré comment il avait détourné la **route d'un avion** à partir de son siège de passager, en hackant physiquement puis logiquement le système de vidéo du siège. Il avait aussi modifié la température de la

station spatiale ISS, ce qui lui a évidemment attiré les foudres de la NASA alors qu'il cherchait surtout à montrer leur incurie en termes de sécurité.

- Mieux, les **bracelets de détenus** en liberté surveillée sont aussi hackables (**source**).

- Dans la conférence de Toulouse, Eric ALATA, un chercheur du LAAS-CNRS montrait comment il avait hacké à distance la **box opérateur** d'un utilisateur ainsi que des objets connectés via un **réseau LoRa** avec une petite antenne permettant d'avoir une portée de 1km.

- A contrario, des rumeurs circulent sur une entreprise dont le réseau informatique aurait été hacké via une vulnérabilité d'un grille pain connecté. Je l'ai vu évoqué dans différentes conférences en France. J'ai l'impression qu'il s'agit en fait d'une légende urbaine et plutôt d'un cas théorique. Il est évoqué dans une présentation de Checkpoint pendant la **conférence Defcon 2015**. On trouve des traces de grille pain connecté sur Internet en **1990** et en **2014**. A chaque fois, il ne s'agissait que de prototypes, pas de produit commercial, donc à fortiori, avec peu de chances d'être installés dans des entreprises lambda. J'en même trouvé un historique des grille pains connectés **ici** qui confirme qu'il ne s'agit pas de produits commerciaux (même si l'article date de 2012). Une agence de communication américaine dénommée **SocialToaster** utilise même le concept du grille pain connecté pour décrire ses campagnes de buzz sur réseaux sociaux. Ils ont lancé un grille pain connecté le 1ier avril 2012 (*photo ci-dessous*) ! Il ne me semble jamais avoir vu de grille pain connecté en visitant le CES de Las Vegas. Et pourtant, on y trouve chaque année plein de choses bizarres comme vous avez pu le constater dans le dernier **Rapport du CES 2016** ! Les évangélistes de l'IoT et autres experts en sécurité **continuent** malgré tout de brandir la menace du hack des grilles pain connectés, les utilisant comme de simples et efficaces artifices de communication pour sensibiliser le public ! Un peu de fact checking ne fait pas de mal !

- Les attaques sont aussi très souvent mises en scène dans la **fiction** au cinéma ou dans les séries TV. Elles étaient innombrables et provoquées par la NASA dans "Ennemy of the State" en 1999, qui n'avait pas l'équipement adapté à l'époque mais s'est largement rattrapée depuis comme l'a révélé Edward Snowden, avec les neuf saisons de "24 Chrono" et les bidouilles de Jack Bauer utilisant un smartphone pré-iPhone, puis dans "Die Hard 4" avec une cyber-attaque globale touchant les infrastructures de New York, la cyberattaque d'Air Force

One par des ukrainiens au début de la seconde saison de la série “Madam Secretary” ou encore l’assassinat du Vice Président US via une attaque de son pacemaker dans le **10ième épisode** de la seconde saison de la série “Homeland”. Ces nombreuses attaques sont en fait des demi-fictions car elles s’appuient en général sur scénarios plutôt plausibles. Dans le pire des cas, les scénaristes n’étaient qu’un peu en avance sur leur temps. Mais moins en avance que les scénaristes de films de science-fiction genre Star Wars ou Star Trek. En effet, on ne se déplace toujours pas plus vite que la lumière, même au niveau des particules les plus élémentaires !

Une bonne partie des cyber-attaques n’ont pas attendu les objets connectés pour se développer. Leurs principales cibles étaient au départ les micro-ordinateurs puis les serveurs. Se sont ensuite adjoints les smartphones et tablettes. Les objets connectés ajoutent maintenant leurs lots de vulnérabilités liés à leurs spécificités, qui s’additionnent aux vulnérabilités existantes :

- Les **systèmes d’exploitation** des objets connectés sont nombreux et pas toujours bien connus. Ils ont pour la plupart été lancés en 2015 : Brillo (Google), LiteOS (Huawei), Windows 10 IoT Core (lancé en partenariat avec Raspberry), Mbed OS (ARM). Ils n’ont pas de référentiels connus de sécurité et utilisent beaucoup de protocoles propriétaires. Et même Linux n’est pas à l’abri de hacks. “*Au niveau de l’OS, sur un Linux par exemple, 4000 à 5000 vulnérabilités sont recensées publiquement chaque année. Il n’est pas possible de sécuriser un tel OS même dégrossi à 300 000 lignes de code*” (lu sur le **blog d’Octo**).

- Les **architectures** sont très hétérogènes. C’est à la fois dangereux et sécurisant. En effet, ce sont les plateformes les plus utilisées qui sont le plus attaquées en général comme nous l’avons tout juste vu avec Android.

- Les objets connectés sont parfois oubliés avec leurs piles et batteries toujours en état de marche. Cela créé des situations de failles de sécurité **différées dans le temps**.

- Leur **sécurité physique** est souvent compromise. Les objets connectés peuvent être hackés physiquement relativement facilement dans pas mal de situations.

- L'**intégrité logicielle** des objets connectés lors de la mise à jour des objets n'est pas bien garantie, notamment en raison des failles de sécurité des réseaux sans fil utilisés. La sécurité des données stockées ne l'est pas plus côté serveurs. Cela peut compromettre la vie privée des utilisateurs même si celle-ci est autant menacée par l'usage des données qui en est fait par des sociétés commerciales classiques telles que Google que par des hackers.

- Les objets connectés peuvent être piratés pour **accéder aux réseaux** dans lesquels ils sont intégrés comme au sein des entreprises. Les exemples qui circulent pour l'instant comme ceux concernant les grille-pain et autres ventilateurs connectés restent pour l'instant fictifs, mais la menace existe.

- Une bonne part des objets connectés contenant des capteurs utilisent de **faibles ressources**, coutent peu cher, ont de simples micro-contrôleurs en guise de CPU ce qui limite l'usage de la cryptographie pour sécuriser leurs communications.

- Des vulnérabilités sont déjà détectées dans les **réseaux M2M** du marché, et notamment dans celui de Sigfox. Dans son intervention à Toulouse, Renaud Lifchitz de **Digital Security**, une filiale d'Econocom, présentait la première étude réalisée sur la sécurité des réseaux Sigfox. Sans rentrer ici dans le détail, l'étude s'appuyait sur un détournement d'usage d'une clé **TNT USB** à 15€ qui scanne les bandes de fréquences de 50 MHz à 2,2 GHz, équipée d'un chipset de démodulation Realtek RTL2832U. Elle montrait que la formule de génération du code de contrôle d'erreurs (CRC) était facilement récupérable et que le numéro de périphérique était diffusé en clair. Bref, une belle ouverture à des hacks potentiels.

- A plus long terme, les risques et failles de sécurité des réseaux et objets connectés atteindront les solutions d'**intelligence artificielles** qui pourront être trompées sur les données concernant la réalité !

Les solutions de sécurisation de l'IOT

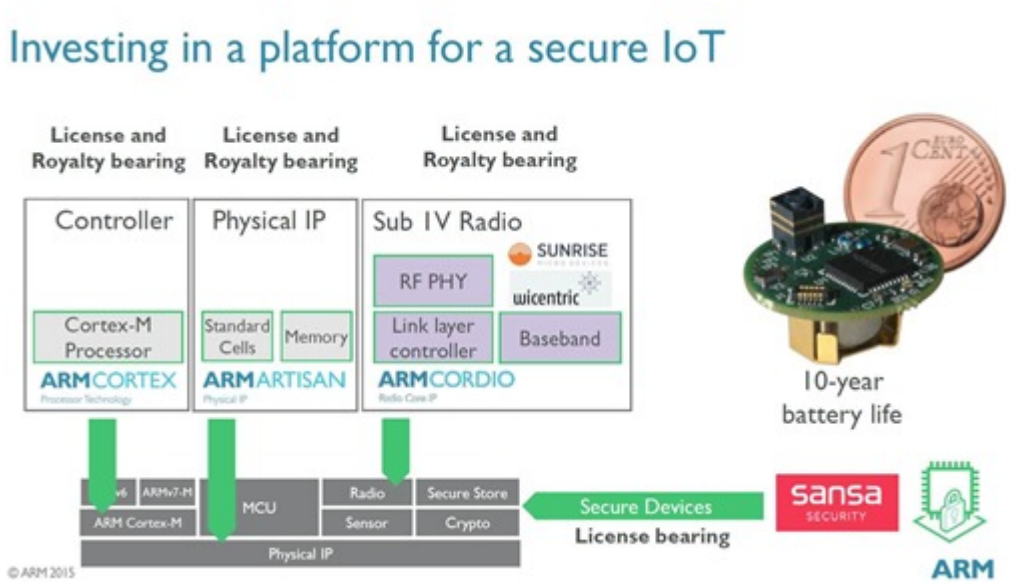
Réduire la surface d'exposition des objets connectés aux attaques est une tâche complexe. Elle requiert une connaissance architecturale de la chaine de valeur qui relie les objets au cloud. Il faut s'intéresser aux objets eux-mêmes, à leurs capteurs et processeurs, aux réseaux locaux et distants, aux protocoles de tout niveau, puis aux serveurs, à leurs logiciels et aux traitements des données qui y sont réalisés. Les besoins sont bien connus depuis des années (cf "**Security needs in embedded systems**" paru… en 2008). De nombreuses sociétés proposent des outils permettant de sécuriser telle ou telle partie de la chaine de valeur mais elles se positionnent depuis assez peu de temps dans les objets connectés.

Avec les technologies existantes, la sécurité est une affaire de méthodes et de processus. C'est ce qu'expliquait très bien Yann Allain de la société de conseil **Opale Security** à la conférence de Toulouse. Il expliquait le besoin de bien sécuriser toute la chaine de valeur et pas simplement l'objet lui-même. Il évoquait la menace globale provenant de l'absence de chiffrage des données de nombreux objets connectés, du manque de web sécurisé, du manque de confidentialité des données, de la sécurité des mises à jour des firmware des objets, des couches électroniques. Il

mettait en évidence le fait que nombre d'industriels ne savent pas évaluer la robustesse de leurs produits et que les outils de tests ne son pas encore répandus dans l'IOT. Il évoquait des standards de tests de sécurisation d'objets, aussi bien le **JTAG** que l'**OWASP IoT**.

Aviram Jenik, CEO de la startup israélienne **Beyond Security**, basée à cheval entre Israël et la Silicon Valley, présentait ses outils qui permettent d'analyser les risques d'objets connectés en tout genre et d'identifier des failles de sécurité inconnues grâce à d'ingénieux mécanismes d'automatisation et de ciblage. Le système génère par exemple automatiquement des dépassements de buffers (buffers overflow), des chaines spécifiques (avec des %d, ...), des chaines vides, des attaques et encodages divers. Il en déduit une cartographie des risques par objet et logiciels dans des systèmes complexes. Le CEO indiquait faire plus confiance aux machines qu'aux hommes pour identifier de manière systémique des failles de sécurité ! Il n'a probablement pas tort même si cela fait un peu froid dans le dos socialement parlant.

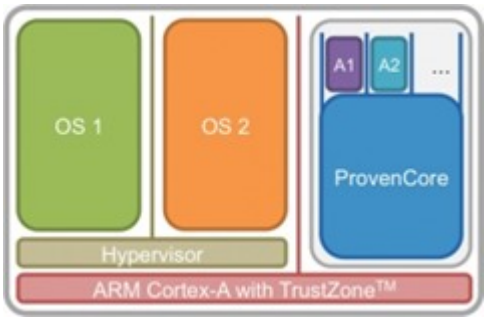
Dans la chaine de valeur des objets connectés, il faut commencer par les objets eux-mêmes. Ils comprennent souvent un chipset ou un micro-contrôleur à base de **noyaux ARM**. Les noyaux ARM les plus courants sont ceux de la série A que l'on trouve dans les chipsets de smartphones et tablettes et qui peuvent valoir plus de $10 et ceux de la série M que l'on trouve dans les micro-contrôleurs d'objets connectés qui valent autour de $1. Jusqu'à présent, ARM proposait de sécuriser les chipsets utilisant des noyaux de la série A avec sa TrustZone, une zone sécurisée permettant d'exécuter des traitements protégés, comme les systèmes de contrôle d'accès conditionnels dans les set-top-boxes de TV payante. ARM annonçait fin 2015 que cette technologie devrait aussi être intégrable dans les micro-contrôleurs à base de noyaux Cortex-M. En juillet 2015, ARM faisait l'acquisition de la startup israélienne **Sansa** qui leur permettra de compléter la TrustZone avec une architecture de sécurité complémentaire logicielle et matérielle. Tout ceci arrivera dans la roadmap ARM en 2016 et donc, probablement, dans des chipsets sécurisés commerciaux en 2017 qui seront intégrés dans des objets connectés grand public d'ici 2018. Le processus prendra un peu de temps !



La chaine de valeur de conception et de production des chipsets embarqués est cependant fragile. Elle s'appuie sur l'intégration de blocs fonctionnels d'origines variées ("blocs d'IP"), avec des logiciels d'intégration divers et une fabrication dans des usines en Chine ou ailleurs qui ne sont pas forcément bien sécurisées. D'où l'émergence de solutions technologiques qui permettent

de créer des chipsets ultra-sécurisés, surtout adaptées du fait de leur coût aux applications professionnelles. Dans le cas présent, les menaces ne proviennent pas de hackers mais plutôt d'Etats et de grandes sociétés impliquées dans de l'espionnage industriel.

Afin de sécuriser les chipsets d'objets connectés pour les applications exigeantes, la société française **Prove & Run** propose Provencore, un micro-noyau sécurisé et formellement prouvé. Il tourne sur des architectures matérielles à base de noyaux ARM et Intel x86. Dans les processeurs à noyaux ARM, Provencore tourne dans la TrustZone sur chipsets à base de noyaux Cortex A, mais fonctionne aussi sur architectures à base de Cortex M utilisée dans les micro-contrôleurs d'objets connectés. Cela semble être une alternative à la solution de Sansa, acquise par ARM. On ne risque en tout cas pas de voir apparaître ce genre de technologie dans sa brosse à dent connectée !



On retrouve une offre assez riche et du même genre chez **Inside Secure**, une société située à Aix en Provence. Elle aussi propose des blocs d'IP divers et noyaux sécurisés pour chipsets, utilisables notamment dans les systèmes de paiement sécurisés.

L'Institut de Recherche Technologique **SystemX** travaille de son côté sur son "chipset du futur" sécurisé dans le cadre du projet EIC et de la plateforme expérimentale CHESS (Cybersecurity Hardening Environment for Systems of Systems) qui doit servir à évaluer la cybersécurité de plateformes ciblant les marchés des des SmartGrids, de l'Usine du Futur, des transports connectés et autonomes ainsi que des services de l'Internet des Objets (voir leur **vidéo de présentation**).

En fait, les principales solutions de sécurisation du marché concernent les PC, smartphones et tablettes. C'est à la fois lié à la relative nouveauté des objets connectés mais aussi à la valeur marchande des cibles. Les pirates informatiques s'intéressent en premier lieu à l'opportunité de gagner de l'argent de manière frauduleuse ! D'où l'intérêt de solutions qui sécurisent les moyens de paiement.

Ercom présentait au MWC de Barcelone sa solution Cryptosmart de sécurisation par chiffrement du stockage et des communications des smartphones et tablettes Samsung. Ercom est labellisé France Cybersecurity, membre de l'Association HexaTrust. CryptoSmart s'appuie sur une carte à puce certifié EAL5+ et une applette certifiée EAL4+. Il suffit de composer son code pour activer la sécurité par chiffrement local du terminal. Ercom propose aussi Mobipass, une solution en cloud de simulation et de tests de réseaux mobiles. Elle simule le fonctionnement de milliers de terminaux. En octobre 2015, Ercom et Samsung annonçaient l'intégration de la solution de chiffrement d'Ercom dans les nouveaux smartphones du coréen.

Le français **Famoco** propose quant à lui le FX100+, un terminal sécurisé fonctionnant sous Android et supportant le NFC, pouvant notamment servir de terminal de paiement. La société

exposait à la fois au CES 2016 de Las Vegas et au MWC. C'est une manière d'isoler dans un terminal spécifique des fonctions qui requièrent un haut niveau de sécurité. Il est ciblé sur les applications professionnelles. On ne peut en effet pas raisonnablement attendre que les consommateurs utilisent ce genre de terminal en plus de leur smartphone.

L'univers des opérateurs télécoms n'est pas en reste. La **GSMA** a publié début 2016 des **guidelines** pour sécuriser les architectures IoT, en partenariat avec des opérateurs télécoms issus de plusieurs continents : AT&T, Verizon, China Telecom, Etisalat, KDDI, NTT Docomo, Orange, Telefonica, Telenon ainsi que Gemalto. Les équipementiers télécoms ambitionnent aussi de compléter leurs offres pour sécuriser les réseaux de bout en bout, en plus de leur investissement conséquent pour se préparer aux déploiements à venir de la 5G. **Ericsson** présentait au MWC 2015 ses solutions de sécurisation orientées sur le stockage des données dans le cloud. De son côté, **Nokia** vient ainsi d'acquérir le canadien **Nakina Systems**, afin de sécuriser les réseaux 5G et de l'Internet des Objets. Ils ciblent comme les autres l'IoT grand public, les voitures connectées, la e-santé et le big data. **Huawei** veut aussi avoir son mot à dire dans la sécurisation des objets connectés. Il promeut une approche collaborative et la standardisation avec le reste de l'industrie.

J'ai aussi entendu parler de sécurisation de l'IoT via l'usage de **BlockChains**. Pourquoi pas. C'est séduisant d'un point de vue intellectuel. Mais cela pose des problèmes liés à la taille grandissante des BlockChains avec leur usage. Celle-ci peut facilement atteindre une taille bien trop grande, incompatible avec les réseaux M2M LPWAN (longue portée + bas débit comme Sigfox ou LoRa) dont les débits sont assez faibles.

Pour les startups de l'IoT, **BuiltItSecure.ly** est une initiative américaine intéressante. Elle vise à rapprocher des créateurs d'objets connectés et spécialistes de la sécurité pour identifier et corriger rapidement les vulnérabilités identifiées et partager les bonnes pratiques en matière de sécurisation. Elle rassemble à ce jour huit constructeurs dont Belkin et Dropcam (qui fait partie de Nest / Google). Il reste du chemin à faire pour sensibiliser un plus grand nombre de sociétés du secteur !

En matière de sécurité de l'IOT se pose bien évidemment la question de la préservation de la vie privée pour les données collectées par les objets et consolidées dans des serveurs et dans le cloud. Cela peut aussi bien être dans le cloud de votre fournisseur d'objet connecté que dans iCloud d'**Apple** (pour iHealth). La sécurité pour l'utilisateur est dans ce cas à la fois une question technique (les serveurs sont-ils bien sécurisés ?) tout comme juridique et marketing (qu'en font les sociétés qui hébergent ces données ?).

Cet inventaire de solutions de sécurisation de l'IoT est certainement très incomplet. Je n'ai pas mené une recherche exhaustive du secteur. Cet article est surtout là pour poser le problème. Après avoir assisté à la conférence de Toulouse, je me suis rendu compte que les solutions de sécurisation de l'IOT existantes étaient surtout utilisées par les concepteurs de systèmes embarqués critiques liés à l'aérospatial, à la sécurité et à la défense. Qu'en est-il des startups qui créent des objets connectés grand public avec de faibles financements et après un simple prototypage en Fablab ? On est loin dans ce cas des méthodes des sociétés établies de l'embarqué ! Il existe donc une opportunité pour créer des solutions très packagées de sécurisation d'objets connectés grand public et aussi pour l'accompagnement des startups du secteur. Les accélérateurs et Fablabs vont avoir besoin d'experts en sécurité !

Cet article a été publié le 23 février 2016 et édité en PDF le 9 septembre 2020.