A N D S I

Association Nationale des Directeurs des Systèmes d'Information
www.andsi.fr

La sécurité de l'Internet des Objets ; menaces, nouveaux risques, impacts et tendances.

Compte rendu de la présentation du 9 janvier 2018, Maison des Polytechniciens.

Compte rendu rédigé par ANDSI

En bref…

Xavier AGHINA, expert en cybersécurité chez Orange Labs, nous présente un panorama de l'IoT ; définition et taxonomie de l'IoT, les standards… pour amener aux risques posés par les objets. Les objets sont tout à la fois vulnérables à des attaques (par exemple en e-santé, modifiant des posologies, en Ransomware) et peuvent également, une fois leur vulnérabilité identifiée et utilisée, mener des attaques, par exemple en déni de service massivement distribué (MIRAI …). La sécurité de l'IoT est aujourd'hui en équilibre entre facilité d'emploi, coût, durabilité et… sécurité. Les menaces incluent les attaques matérielles sur les périphériques (side channel attack pour extraire les clefs…), l'OS, les communication radio (Sigfox, LoRa…). La conclusion inclut les tendances que X. AGHINA voit se développer (OS dédié à un objet…) ainsi que les actions de réduction des risques.

Mais qu'est-ce que l'IoT ?

Les utilisateurs disposent d'une gamme de petits appareils informatiques, dont l'utilisation fait maintenant partie de leur vie quotidienne et qui forment un environnement pervasif. Cela permet à des objets de se reconnaître et de se localiser automatiquement avec une capacité d'intelligence distribuée. Mais au vu de ces possibilités avancées, qu'en est-il réellement, de la sécurité de ces systèmes qui peuvent être instrumentés et le seront à plus ou moins brève échéance ? Ces appareils ne disposent pas des ressources avancées pour prendre en charge la sécurité et ces risques ne doivent plus être ignorés, et deviennent un défi pour l'entreprise. Les risques de sécurité associés aux dispositifs IoT ont le potentiel de devenir le risque de sécurité le plus important du réseau : l'entreprise n'a aucune visibilité sur le niveau de protection à mettre en œuvre et ne dispose pas de la technologie en adéquation pour évaluer la sécurité.

Définition de l'IoT ; plusieurs, dont celle de Wikipedia et du Gartner « : L'Internet des Objets est le réseau des objets physiques qui embarquent des technologies pour communiquer et interagir avec l'environnement externe selon leurs états internes. », simple et claire.

L'écosystème IoT se décline en 3 catégories :

1) Léger :

   - Dispositif physique simple, typiquement un capteur, qui a peu de fonctions
   - Protocole de réseau local à court ou à long terme pour la connectivité
   - Système d'exploitation minimal ou non

2) Complexe (connecté à un Back End) :

- Connecté à un serveur de back-end sur une liaison de communication longue distance
- Peut effectuer des opérations cryptographiques symétriques ou asymétriques

3) Passerelle :

- Petit périphérique, généralement connecté à l'alimentation secteur, qui gère la communication entre les points d'extrémité légers et le back-end.

Les objets pouvant interagir avec leur environnement à travers le cloud et dont les fonctionnalités sont enrichies par un applicatif ou un capteur offrent un panorama d'usages multiples avec en tête celui de la domotique et de la maison connectée. Sur le plan économique les capteurs sont toujours de moins en moins chers (souvent <1€ et parfois >10€ pour les complexes) une marge confortable pour les constructeurs sur des projections de baisse des coûts d'infrastructure à 2020.

La croissance très importante de l'IoT implique un modèle de cloud distribué, proche des frontières du réseau, et cela paraît techniquement plus logique pour agréger et traiter les quantités massives d'informations. Les grands acteurs IT comme Oracle, IBM, Microsoft et autres AWS entendent profiter de l'explosion des objets connectés pour apporter leur savoir-faire et leurs solutions, et en cela la situation est analogue à celle présente au début du Cloud.

L'Internet des objets couvre une vaste gamme d'industries et de cas d'utilisation, allant d'un seul dispositif contraint (dans le sens des ressources CPU, fonctionnalités, communication et énergétique) à des déploiements massifs multiplateformes de technologies intégrées et de systèmes de cloud se connectant en temps réel. Tout cela est lié à de nombreux protocoles de communication hérités (les plus connus ou fondamentaux – radio, infrarouge,wifi, bluetooth,) et émergents (toute la classe 802.15.4) qui permettent aux appareils et aux serveurs de communiquer entre eux et de manière plus interconnectée. Dans le même temps, des dizaines d'alliances et de coalitions se forment dans l'espoir d'unifier le paysage IoT, aujourd'hui fracturé et organique.

L'IoT devra donc combiner plusieurs normes et plusieurs approches qui répondent à des cas d'utilisation très différents, par la mise en place des « passerelles fondamentales » standardisées entre les différentes normes ces passerelles pouvant fournir une interopérabilité syntaxique sans compromettre la fidélité des aspects fonctionnels de la technologie spécifique au domaine. Les standards techniques sont :

- Architectures : ETSI, oneM2M
- Protocoles : MQTT, 6LoWPAN
- Consortiums : IICF, GSMA, Allsen, OpenInterconnect

Les utilisateurs prennent conscience de « certains » risques.

Pour une certaine catégorie d'objets connectés les utilisateurs sont conscients des risques, notamment concernant l'usage des caméras de surveillances de leur domicile, les « nouveaux » risques de l'IoT seront toujours plus nombreux :

- un grand nombre de caméras IP non sécurisées ont permis d'ouvrir la voie au botnet Mirai, l'un des plus performants jamais enregistrés. Les caméras IP continueront à représenter une menace importante étant donné le grand nombre de caméras avec des mots de passe par défaut (ou non) qui offrent également la bande passante et l'informatique toutes deux pouvant être utilisées abusivement pour les réseaux de zombies. Les pirates recherchent constamment d'autres moyens de construire des botnets en utilisant d'autres types d'appareils. Ceux-ci pourraient être des imprimantes sans mot de passe ou faible, des verrous intelligents….
- Développement des ransomware et malware - Les caméras IP peuvent capturer des images sensibles à partir d'une gamme d'emplacements, allant d'une usine à l'intérieur d'une maison, les pirates pourraient proposer : « à moins que vous ne me donniez des Bitcoins, je distribuerai ces images ».
- Les botnets IoT visent à la crypto-monnaie - Beaucoup croient que la blockchain est impossible à pirater, mais nous constatons déjà une augmentation des attaques contre les applications basées sur la blockchain. La vulnérabilité centrale ici n'est pas la blockchain elle-même, mais plutôt les applications qui s'exécutent au-dessus.

- De nombreuses attaques IoT vont passer sous le radar - en 2016, le malware le plus mémorable basé sur l'IoT était très nettement le botnet Mirai, qui a paralysé de nombreux sites Web grand public. L'un des botnets les plus mémorables de 2017 est probablement Reaper. Les menaces de sécurité IoT les plus importantes pourraient être des attaques assez petites pour échapper à la détection. "Nous verrons de plus en plus de ce que j'appellerai des - micro-violations -, c'est-à-dire des vulnérabilités et des compromissions de petite taille passant sous le contrôle des technologies actuelles de surveillance et de détection de sécurité".
- La confidentialité deviendra une partie essentielle de la conversation IoT - les entreprises installent un nombre croissant d'appareils IoT - thermostats connectés et systèmes HVAC, téléviseurs intelligents dans les salles de conférence, imprimantes connectées et éclairage intelligent… Pendant ce temps, les industriels de l'IoT continue à étendre leur offre et les consommateurs utilisent des appareils tels que des haut-parleurs intelligents. Malgré cette hausse de la connectivité, les ramifications de la vie privée de nos environnements hyper-connectés sont incertaines et « l'avenir de l'IoT, tirer parti de la transition vers un monde centré sur les données » se confirme.
- L'augmentation du suivi des données sensibles par les grandes entreprises constitue déjà le moteur de la méfiance du public. Des événements récents aux Etats-Unis impliquant des sites de médias sociaux importants viennent s'ajouter à cette conversation, mais l'événement très réel et imminent est le règlement général de protection des données de l'Union européenne (GDPR) qui entrera en vigueur en mai 2018. Essentiellement, ce règlement est conçu pour protéger les informations personnelles, et les entreprises qui violent le GDPR peuvent faire face à des amendes allant jusqu'à 4 pour cent de leurs revenus annuels.

Dans les soins de santé, l'Internet des Objets offre de nombreux avantages, allant de la possibilité de surveiller de plus près les patients à l'utilisation des données générées pour l'analyse. Mais ce flux accru d'informations comporte également des risques auxquels les professionnels de la santé doivent faire face. Ces nouveaux appareils connectés présentent de nombreux avantages, mais ils présentent également de nouveaux risques et de nouvelles vulnérabilités que nous n'avons pas traités.

> Deux personnes dans un hôpital qui ont été branchés à une pompe à perfusion et ont estimé que leur gestion de la douleur n'était pas sous contrôle sont allées en ligne, ont trouvé la documentation de service, ont obtenu les identifiants de service codés en dur dans leurs pompes à perfusion, ont ouvert une session et ont augmenté leurs doses - les surdoses qui ont suivi ont causé des problèmes respiratoires.

Malgré ces risques, il semble que la communauté des soins de santé a accepté le fait que l'IoT arrive. Afin de se préparer et de rester aussi sûrs que possible, les fournisseurs et les fabricants peuvent prendre des mesures comme l'authentification, l'accès aux informations et le chiffrement des données.

La sécurité des systèmes IoT peut être exceptionnellement complexe en raison du grand nombre de composants, d'une surface d'attaque potentiellement étendue et des interactions entre les différentes parties du système. La modélisation des menaces est un excellent point de départ pour comprendre les risques associés aux systèmes IoT et comment ces risques peuvent être atténués.

Le périphérique IoT se compose de matériel exécutant un système d'exploitation dépouillé ainsi que des capteurs, des pilotes, au moins une application spécifique, et une de stockage local. Du point de vue de la sécurité, le périphérique IoT est important, mais il est également essentiel de savoir que la sécurité du système dans son ensemble dépend de bien plus que le code personnalisé (ou le système d'exploitation) exécuté sur le périphérique. Ce n'est qu'une facette d'un système qui est beaucoup plus complexe.

Néanmoins, les contraintes des capteurs peuvent rendre la démarche de sécurisation par cryptographie complexe. En effet, ces derniers présentent :

- Une faible puissance de calcul, difficile à concilier avec la capacité requise par la cryptographie,
- Un espace de stockage réduit,
- Des ressources énergétiques limitées,

Une bande passante réduite pour les réseaux IoT rendant délicates les mises à jour d'informations indispensables (comme les clés de chiffrement) au bon fonctionnement d'une protection cryptographique évolutive.

La comparaison technologique SigFox – Lora qui appartiennent toutes deux à la famille des LPWA (technologies de communication à faible consommation) avec leurs propres spécificités, qui vont co-exister sur les prochaines années et répondent à des besoins différents. Elles permettent de couvrir un large besoin pour envoyer des données depuis l'objet connecté, en petit volume et à des fréquences régulières (température, relevé d'utilisation d'un objet ou de fréquentation d'un espace…). L'avantage clef de ces deux technologies réside dans la très faible consommation énergétique, permettant de ne pas remplacer la batterie du capteur communicant durant 10 ou15 ans.

Relativement à des employés apportant des dispositifs IoT dans le réseau, il est possible de sécuriser l'entreprise. Mais qu'en est-il de tous ces appareils connectés sur des réseaux distant externes de type cloud que les employés utilisent ; le «BYOIoT» (Bring Your Own IoT) en référence au précèdent BYOD (Bring Your Own Device). Les dispositifs IoT ont déjà fait leur chemin sur la scène du réseau d'entreprise, et il faut faire en sorte que le réseau ne soit pas dégradé et sans fuite de données confidentielles due à la connexion d'un périphérique compromis. Les entreprises doivent aussi penser à ce type scénario.

En conclusion

L'Internet des objets peut être un concept puissant, cependant, comme tout nouveau déploiement technologique, le risque doit être évalué dans sa globalité d'usage, pour s'assurer que l'entreprise a maximisé son savoir-faire entre usages – fonctionnalités – choix techniques et informationnel, pour que les risques soient minimisés. L'IoT a un énorme potentiel qui a déjà modifié le comportement des personnes dans leurs vies quotidiennes, aussi bien professionnellement que personnellement. Les avantages sont nombreux mais l'IoT génère de nouveaux risques et problèmes complexes. C'est un concept chamboulant dont l'usage nécessite une réflexion responsable et prospective afin de préserver les usages et la société.

Débat

Intervenant :
Où les antennes LoRa sont elles situées, sachant qu'il y en a environ 10 fois moins (4 000 pour le France) que les BTS 3G ?
Xavier Aghina:
A coté d'une BTS, et reliée à Internet.

Int. : Les réseaux, pénétrants les cloisons comme SigFox & LoRa ne sont ils pas dangereux pour la santé ?
X.A.: C'est possible, mais comme pour la téléphonie mobile, peut on encore s'en passer ?

Int. : Y a t il des labels ou méthodes validées et sur la sécurité de l'IoT ?
X.A.: Oui, il en existe, voir sur le site de l'ANSSI, dont des entreprises de pentest (test de pénétration).

Int. : En analogie à passer de la domotique à la gestion d'un usine dans un endroit isolé d'Argentine, va t on avoir des offres de solution (pilotage de ligne …) qui le fassent localement (empêcher les données de sortir….)
X.A.: Il est aujourd'hui de plus en plus difficile de contenir l'information en ayant des systèmes d'information utilisant des vecteurs de communication « sans-fil », la seule solution étant l'adoption du chiffrement qui n'interdit pas l'écoute, mais rend impossible la compréhension des échanges.

Int. : Le chiffrement est il possible ?
X.A.: Oui, ceci dit le facteur limitant est l'énergie disponible sur le système pour permettre le fonctionnement du « cryptoprocesseur ».

Int. : Y a t il un marché du capteur ?
X.A.: Oui mais les entreprises qui en proposent ne savent pas toujours en gérer la sécurité, comme par exemple ceux qui ne peuvent être mis-à-jour.

Int. : L'industrie 4.0 repose sur des capteurs, mais la sécurité fait peur à tout le monde….

X.A.: Oui, car le sans-fil va très souvent s'imposer. Le LiFi a fait l'objet d'une étude chez Orange, car offrant une grande bande passante, aucun risque d'impact sur la santé avec une distance de transmission (et donc d'interception) limitée.

Int. : Est il facile d'inclure une puce wifi dans un capteur ?
X.A.: Oui, le sans-fils est de facto intégré sur les composants, pour les capteurs ce sera plutôt des protocoles 802.15.4, mais tout est possible ; bluetooth, wifi, NFC, modulo la constante de l'énergie embarquée…

Int. : Est il possible d'avoir le mode de communication finement déterminé ?
X.A.: Une firme comme NXP (Qualcomm) fournit le chipset qui inclut n'importe quel mode de communication : - 802.11, 802.15.11, 802.15.4 …

Int. : L'Internet tel qu'aujourd'hui pourrait-il supporter la charge de communication de milliards d'objets ?
X.A.: oui, car le débit de chaque objet est faible ; Il ne s'agit pas de vidéo en 4k. Des concentrateurs d'objets seront mis en place car des plans d'adressage incluant tous les objets seraient compliqués à mettre en œuvre

Int. : Chez Orange, l'IoT va il être vu plutôt en domotique, en industriel …. ?
X.A.: Des terrains seront privilégiés; pour Orange la domotique est l'extension des services de la box, comme l'assistant vocal « Djingo » puis la santé, avec le marché des wearable… .

Int. : Et l'armée ?
X.A.: Elle a ses propres protocoles et se situent en marge de ce fait pour en conserver la maîtrise et le « confidentiel défense » . Ils ont adoptés la « security by design » depuis longtemps, sans avoir de nom pour le définir.

Présentation de l'orateur

Xavier AGHINA est expert en cybersécurité chez Orange Labs.

Dans le département sécurité chez Orange Labs, Xavier AGHINA conduit des projets techniques et un programme de recherche sur le paiement mobile et la protection des objets connectés. Son objectif principal est de concevoir et de mettre en œuvre des solutions de sécurité. Il fournit également un soutien actif et de conseils dans les domaines d'audit de sécurité, l'analyse des risques, l'évaluation de la vulnérabilité et des recommandations. Il anime des formations à Telecom ParisTech ainsi que des séminaires de sensibilisation à la sécurité IT en entreprise.