note n°15/18

3 septembre 2018

FONDATION pour la RECHERCHE STRATÉGIQUE

Eric Hazane
Membre de la Chaire St-Cyr de cyberdéfense et de cybersécurité

Sécurité numérique des objets connectés, l'heure des choix

« C'est avoir tort que d'avoir raison trop tôt ». Jamais cette citation des *Mémoires d'Hadrien* de Marguerite Yourcenar n'a semblé aussi contemporaine des questions voire des inquiétudes, certaines de portée véritablement stratégique, que suscitent les objets connectés. Leur diffusion qui s'accélère, devrait même se « massifier » au tournant de la prochaine décennie. Peu visibles, à l'exception des plus populaires d'entre eux comme les montres connectées, ils scrutent et interrogent pourtant en permanence[1] et depuis presque une décennie notre environnement, bien au-delà du seul horizon numérique.

En regard des enjeux majeurs qu'ils soulèvent, les objets connectés détournés de leurs indéniables usages positifs et bénéfiques, peuvent introduire par malveillance de nouveaux risques d'atteinte numérique mais aussi économique. Cette note cherche à interroger la sécurité de ces objets connectés. Nécessitent-ils une approche particulière ou, à l'inverse, simples objets « informatiques », les règles générales de sécurité numérique qui devraient s'appliquer aux systèmes d'information leurs sont-elles suffisantes ?

Les objets connectés, quelle(s) définition(s) ?

Les objets connectés sont la partie visible et multiple de l'Internet des objets (IoT en anglais, IdO en français) qui, de manière simplifiée, englobe les infrastructures de communication et de transport des données et les objets connectés eux-mêmes. L'IoT/IdO est un concept apparu en 1999 par l'entremise d'un entrepreneur britannique, Kevin Ashton, qui désignait alors la possibilité de connecter n'importe quel appareil électronique à Internet[2].

1. Anthony Levandowski, l'un des responsables du projet Google car : « nous analysons et prédisons le monde 20 fois par seconde » in http://www.wired.com/2012/01/ff_autonomouscars/all/1

2. Voir E. Hazane « L'Internet des objets et le décuplement des données » paru dans l'ouvrage collectif *La donnée n'est pas donnée* en juin 2016 aux éditions Kawa : https://www.editions-kawa.com/home/157-la-donnee-n-est-pas-donnee-strategie-big-data.html

Concernant les seuls objets connectés, les définitions sont aussi nombreuses que leurs auteurs. Celle du guide[3] publié par Captronic en 2017 apparaît précise et exhaustive. Aussi, elle est choisie dans le cadre de cette note : « Un objet connecté est composé d'une logique de traitement, d'un capteur et/ou d'un actionneur, d'une interface de communication et éventuellement d'interfaces physiques comme des connecteurs, des prises et des boutons. En général, un objet connecté recueille des données locales, transmet ces données à un service via un réseau local ou d'infrastructure, reçoit des commandes de la part d'un serveur de gestion et émet des états vers ce même serveur ».

Du virtuel au monde physique, la frontière abolie

Si plusieurs éléments de la définition sont importants, il en est un qui attire un peu plus l'attention. Un objet connecté peut être doté d'un actionneur c'est-à-dire qu'il est susceptible de réaliser une action concrète dans le monde physique. Cette possibilité constituant une sorte de *continuum* cyberespace-espaces physiques[4] est le point d'inflexion des objets connectés : s'ils peuvent générer et transmettre des données qu'il est possible d'intercepter, de modifier voire de manipuler, plus dangereuse encore est la possibilité offerte par leur capacité singulière d'agir dans le monde physique. Celui-ci est d'ailleurs, d'un point de vue cyber, composé de systèmes industriels, de systèmes de systèmes, bref, de systèmes qui environnent et facilitent notre quotidien (santé, transport, énergie, etc.)[5], ce qui laisse entrevoir l'éventail des possibilités offertes par les objets connectés, autant que leur dangerosité éventuelle.

Un contexte dynamique, des enjeux multiples et (parfois) systémiques

Au risque d'énoncer une évidence, il demeure néanmoins utile de rappeler que la numérisation croissante de la société, associée au développement des objets connectés, est porteuse de nouveaux enjeux ainsi que de nouveaux risques. Sans être exhaustif, nous pouvons indiquer les suivants :

- ◊ La faible sécurisation des objets connectés eux-mêmes et leur (absence de) maintien en condition de sécurité (MCS) tout au long de leur cycle de vie[6],
- ◊ Un risque systémique croissant[7] relatif au déploiement massif d'objets connectés qui embarqueraient la même vulnérabilité technique,
- ◊ La généralisation des objets connectés de type « actionneurs » porteurs d'une rupture dans la maîtrise des risques en matière de sécurité numérique par leur action potentielle sur l'espace physique.

Concernant les nouveaux risques :

- ◊ Des difficultés voire de potentielles impossibilités à réguler et à réglementer un écosystème anarchique qui se caractérise par une massification exponentielle, associée à une pénétration invisible mais profonde de notre environnement quotidien,
- ◊ La fragilité de nombreuses entreprises créatrices d'objets connectés qui, économiquement peu voire non pérennes, fragilisent un peu plus encore le MCS,
- ◊ Sur les systèmes de systèmes comme les villes et les territoires intelligents, les risques numériques pourraient générer des troubles majeurs d'ordre systémique. L'absence de vision globale à moyen et à long terme, tant par la puissance publique que par les industriels et les donneurs d'ordre, est lourde de conséquences potentielles en termes de sécurité publique.

Même si aucun secteur d'activité n'est épargné par le développement des objets connectés et de services associés, il est possible de catégoriser quatre de ces secteurs :

- ◊ Le secteur sensible de la santé[8], de la dépendance et du bien-être,
- ◊ Les villes et les territoires intelligents fortement structurés par la gestion de différents flux (énergie[9], transport, eau, déchets et population),
- ◊ Le commerce, la production et l'industrie (suivant les modèles dits « Usine 4.0 »)[10] notamment *via* la gestion des commandes, des stocks et du marketing,
- ◊ Le secteur « grand public » qui englobe

3. https://www.captronic.fr/Sortie-du-guide-Cybersecurite-des-produits-connectes-a-destination-des-PME.html

4. Avec l'apparition récente – et discutable - du terme « systèmes cyber-physiques » - Voir page 7 de http://www.lirmm.fr/~reitz/di-marel/20160219-expose-GL-SCP.pdf

5. P. Davadie, *L'entreprise, nouveaux défis cyber,* Paris, Economica, 2014.

6. https://www.schneier.com/blog/archives/2017/02/security_and_th.html

7. https://www.contrepoints.org/2016/10/14/268831-internet-objets-eldorado-hackers

8. https://fr.slideshare.net/AntoineVigneron/iot-scurit-et-sant-un-cocktail-dtonnant

9. http://www.smartgrids-cre.fr/index.php?p=objets-connectes-seidolab

10. http://usinedufutur.insa-rennes.fr/lusine-4-0/

la domotique (*smart home*[11]) et les objets du quotidien comme les montres ou les vêtements connectés.

Objets connectés : quelles menaces ?

Du point de vue macroscopique, les menaces qui pèsent sur les objets connectés sont globalement de même nature que celles qui pèsent sur la plupart des systèmes d'information. Au regard du contexte décrit précédemment, il est cependant possible de postuler qu'il existe des menaces plus prégnantes ou qui font peser un risque systémique sur tout ou partie des réseaux :

◊ Dysfonctionnement : perturbations[12] du fonctionnement nominal d'un objet connecté en l'empêchant de transmettre des données, en perturbant ses capteurs voire en provoquant sa panne. Type d'attaque très difficile à détecter du fait de certaines caractéristiques propres aux objets connectés : non connectés en permanence, mobiles, etc. Paradoxalement, l'hétérogénéité des objets connectés déployés peut contribuer à une meilleure résilience du système face à ce type de menace en offrant des systèmes différents donc n'ayant pas les mêmes vulnérabilités (principe de dissimilarité). Dans ce contexte l'anarchie apparente du secteur des objets connectés, vulnérabilité au niveau normatif, deviendrait en soi un facteur de résistance.

◊ Atteinte aux données personnelles et à la vie privée : consiste pour un attaquant à obtenir des informations personnelles sur des individus[13] au travers des objets connectés de celui-ci. La méthode peut être directe (atteinte à la confidentialité des données) ou indirecte (observation du comportement ou du déplacement de l'objet). Combiné à la prise de contrôle (expliquée ci-dessous), un attaquant peut aussi détourner l'usage d'un objet en récupérant des données qui n'étaient pas initialement collectées (*via* une caméra ou un micro d'ambiance, par exemple). Les récentes démonstrations d'attaques sur des assistants domestiques vocaux, pourtant proposés par les plus importantes entreprises du secteur (Alphabet/Google, Amazon, etc.), confirment par ailleurs cette hypothèse.

◊ Accès illégal aux informations stockées ou échangées : c'est la compromission des données qui transitent par les objets connectés ou qui y sont stockées[14]. L'utilisation généralisée des protocoles de liaison sans-fil et la multiplicité de ceux-ci (Wifi, 3G, 4G, LoRa, Sigfox, ZigBee, etc.), aggravent cette menace du fait de vulnérabilités ou d'une sécurisation moindre ou mal implémentée. Pour les plus petits objets connectés qui possèdent donc des capacités rudimentaires de calcul et de communication, la mise en œuvre de méthodes de chiffrement considérées comme robustes est peu ou pas applicable.

◊ Prise de contrôle (logique ou physique) : la prise de contrôle par un attaquant d'un objet connecté lui permet ensuite d'accéder aux fonctions légitimes de l'objet connecté. Déployés en masse, extrêmement répartis sur un territoire, peu voire pas surveillés, les objets connectés sont extrêmement vulnérables à des formes de harcèlement[15] voire représenteraient une menace physique. L'agresseur peut alors se servir d'eux comme première porte d'entrée dans un système d'information, lui-même *a priori* mieux protégé. On parle alors d'attaque sur la chaîne de valeur d'un système ; ce type d'attaque étant en croissance exponentielle[16]. Leur hétérogénéité, si elle peut être positive dans le cas de dysfonctionnements, devient une faiblesse en matière de MCS et d'application des patchs de sécurité.

◊ Manipulation et détournement : utilisation du fonctionnement nominal d'un ou plusieurs objets connectés par un attaquant à son propre profit (*spam*, attaques par dénis de services distribués (DDoS[17]) etc.). Le déploiement massif de

11. https://ec.europa.eu/digital-single-market/en/blog/new-standard-smart-appliances-smart-home

12. https://www.francetvinfo.fr/replay-radio/nouveau-monde/nouveau-monde-pourquoi-les-objets-connectes-ne-decollent-ils-pas_2054649.html

13. https://www.labri.fr/images/uploads/2015_FKrief.pdf

14. Comme le thermomètre d'un aquarium connecté, par exemple : https://www.numerama.com/tech/345446-objets-connectes-casino-pirate-a-cause-dun-thermometre-aquarium.html

15. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

16. Voir l'*Internet Security Threat Report 2018* de la firme Symantec : https://www.symantec.com/security-center/threat-report

17. « Une attaque par déni de service vise à rendre indisponible un ou plusieurs services. Un déni de service peut consister à exploiter, par exemple, une vulnérabilité logicielle ou matérielle. L'interruption de service peut également s'effectuer en empêchant l'accès à ce service, par exemple en saturant la bande passante du réseau : on parle alors d'attaques volumétriques. On parle de « déni de service distribué » (de l'anglais Distributed Denial of Service ou DDoS) lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés. » In https://www.ssi.gouv.fr/guide/comprendre-

certains objets peut permettre à un attaquant de disposer de capacités de calcul distribuées - et donc de capacités d'attaque - très importantes, comme l'a montré le cas de l'attaque contre OVH en septembre 2016, réalisée au travers d'un nombre très important d'objets connectés, en particulier des caméras[18]. L'injection de données erronées dans un système d'information compromis au moyen d'objets connectés peut être très difficile à détecter.

Quelles recommandations en matière de sécurité ?

On sent bien que les besoins de sécurité vont varier en fonction du domaine d'application de l'objet connecté et du type de menace qui peut s'exercer. Même si elles ne sont pas exhaustives ou simples à mettre en œuvre, voici une liste des recommandations qui peuvent être formulées afin de rendre mieux sécurisés les objets connectés.

- ◊ Cycle de vie : alors que sont très souvent évoquées la sécurité native (*security by design*) et, de plus en plus, la sécurité des données personnelles (*privacy by design*), l'émergence des technologies d'apprentissage machine (*machine learning)*, de *Big Data* et de réseaux neuronaux, qui vont de plus en plus s'appuyer sur des capteurs intelligents et des objets connectés, nécessitent l'intégration d'une dimension éthique. Dès lors, introduire la notion de « Sécurité, éthique et protection des données personnelles natives » (*security, ethics and privacy by design*) apparaît pertinent. Pour se faire, une analyse des risques multidimensionnelle (technique, organisationnelle, juridique et éthique) doit guider le projet dès la phase de conception. Cette analyse de risques portera notamment sur les donnés manipulées, l'environnement de l'objet et, de manière encore plus essentielle, les tiers de traitement massif de données (fournisseurs de *cloud* notamment).

A ce stade, un focus sur l'analyse de risques à double-dimension semble utile :

- ◊ Dès la conception (*security by design*) sur l'objet lui-même afin d'identifier les conséquences d'un fonctionnement anormal de l'objet, incluant une prise de contrôle partielle ou totale de l'objet par un attaquant,
- ◊ Sur l'environnement d'intégration où la couverture des risques (à graduer) identifiés peut être assurée par l'environnement[19] de l'objet au lieu de l'objet lui-même.

Ajoutons en complément que l'obtention d'un niveau de certification minimum à l'échelle européenne[20] propose une piste intéressante vis-à-vis des objets connectés à faible coût et à faible valeur ajoutée (mais pouvant intéresser un attaquant par l'effet de levier lié à la masse). La principale difficulté étant ici de s'entendre au niveau communautaire sur le standard à appliquer.

Un effort particulier devra être évidemment porté sur l'architecture de l'objet, l'utilisation d'outils et de standards existants, l'intégration d'un processus de type homologation de sécurité / démarche agile[21].

Côté support, l'entreprise devra réfléchir à l'élaboration d'un engagement pour assurer la disponibilité du concepteur et du fabricant, en tenant cependant compte des aléas de pérennité des différents acteurs, souvent des *start-ups*. La gestion et la publication des vulnérabilités (corrigées) devront faire également partie de cet engagement tout comme la possibilité sera proposée d'offrir des sensibilisations voire des formations à l'exploitation « sûre et sécurisée » de l'objet connecté proposé.

Plusieurs éléments de l'objet doivent ainsi faire l'objet de politiques différenciées pour en assurer la meilleure sécurité possible :

- ◊ Mécanismes de sécurisation : authentification, chiffrement (*secure elements*[22], mémoire(s), etc.) et gestion des clefs de chiffrement devront être réalisés à l'état de l'art ou en s'appuyant sur les recommandations existantes, émises notamment par les agences nationales de cybersécurité.
- ◊ Logiciel / micrologiciel : la mise en œuvre de mécanismes de sécurité des outils et de l'environnement de développement sont un préalable auquel

et-anticiper-les-attaques-ddos/

18. https://www.ovh.com/fr/blog/ovh-resiste-attaque-ddos-vac/

19. Cela signifie que l'infrastructure qui permet la transmission des données de et vers l'objet est sécurisée sur l'ensemble de son cycle de vie (donc auditée et surveillée en temps réel).

20. Si la réflexion est en cours depuis plusieurs mois, la régulation se fait encore attendre. Lire https://www.objetconnecte.com/parlement-europeen-danger-iot/

21. Si l'homologation de sécurité va permettre d'identifier et de traiter les risques, elle peut être difficile à appliquer à un développement en cycle en V. Y adjoindre une démarche agile doit permettre un développement itératif, incrémental, adaptatif et intégré ; voir https://www.ssi.gouv.fr/guide/integrer-la-securite-numerique-dans-une-demarche-agile/

22. https://www.supinfo.com/articles/single/4651-hce-host-card-emulation-se-secure-element

s'ajouteront la gestion et la minimisation des droits d'accès du personnel, ainsi que la journalisation et l'analyse systématique des incidents de sécurité. Du côté des composants les mises à jour logicielles devront être possibles, à condition que leur origine soit authentifiée. La compartimentation mémoire s'appuyant par exemple sur l'emploi d'un noyau système[23] est aussi fortement recommandée lorsqu'elle est possible. Enfin, des tests systématiques de qualité comme de sécurité devront être réalisés.

- ◊ Réseau : les comptes et mots de passe par défaut de type « administrateur » devront être systématiquement modifiés, ce qui est encore loin d'être le cas actuellement et constitue une faille de sécurité majeure, pourtant facilement corrigeable. Un filtrage très fin notamment des services d'administration[24] et des pare-feux devra être réalisé. Les ports et services accessibles non-nécessaires devront être désactivés. Un mécanisme de résistance aux attaques par déni de service devra être étudié et mis en œuvre dans la mesure du possible. Enfin, la sécurité de l'interface radio devra être étudiée.
- ◊ Matériel : des mesures contre les attaques physiques devront être mises en œuvre comme de la détection d'ouverture, par exemple. Une attention particulière sera portée sur l'implémentation des fonctions des *secure elements*. La génération d'aléas[25] devra en outre être de qualité cryptographique.

Conclusion

La diffusion massive et en profondeur de la société et de l'économie par les objets connectés comporte de nombreux bienfaits[26] mais aussi des risques multiples que cette note a présenté. De nombreuses mesures tant physiques que logiques mais aussi juridiques et éthiques, pour améliorer la sécurité unitaire ainsi que la sécurité systémique, doivent intégrer le cycle de vie des objets connectés. De leur conception à leur retrait en passant par leur exploitation.

Les pouvoirs publics, les industriels et les syndicats d'entrepreneurs voire les citoyens, également usagers et clients, devraient réfléchir ensemble et sans tarder à une concertation où la sécurité des objets sera au centre des préoccupations. De la conformité agile avec plusieurs niveaux allant, par exemple, d'un label européen de certification de type CE, jusqu'à un haut niveau de confiance de type « Secure + », pourrait être décrite et mise en œuvre en 18 mois. L'élaboration d'une régulation pro-innovation c'est-à-dire légère mais robuste, devrait également être intégrée à cette réflexion autant de niveau national qu'européen.◊

23. Les solutions techniques dédiées à l'IdO restent encore aujourd'hui très hétérogènes. Les systèmes d'exploitation sont peu ou pas connus : FreeRTOS, RIOT, eCos, Lepton, Contiki, REMS, TinyOS, Brillo (Google), Windows 10 IoT Core (Microsoft). Les normes de radiofréquence sont elles aussi, diverses et variées : WiFi, Bluetooth LE, NFC, RFID, SigFox, LoRa, LoRaWAN, ZigBee, Z-Wave, normes propriétaires in https://infoguerre.fr/2018/04/affrontements-autour-de-linternet-objets/

24. https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/

25. La qualité de l'aléa qui va permettre la sécurité des échanges de données est un important problème soulevé par la cryptographie, en particulier celles embarquées dans des cartes à puces, des smartphones ou des logiciels donc des objets connectés. Les défauts des générateurs d'aléa peuvent conduire à des failles de sécurité exploitable sous forme d'utilisations frauduleuses d'un composant matériel ou logiciel. Pour réduire voire empêcher ce risque, l'aléa cryptographique doit être parfaitement imprédictible. Lire http://www.webreview.dz/IMG/pdf/fr03-rist19-2.pdf

26. https://www.industrie-techno.com/objets-connectes-les-capteurs-facilitent-la-maintenance-predictive.52705

Auteur

Eric Hazane est membre de la Chaire St-Cyr de cyberdéfense et de cybersécurité, co-animateur du groupe cybersécurité du Hub France Intelligence Artificielle.

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.

Dernières publications

2018

- Emmanuelle Maitre, « La communication dans le domaine de la « dissuasion stratégique » : le cas des Etats-Unis », note n° 14/201/, 6 août 2018
- François Christophe, « La crise centrafricaine, révélatuer des nouvelles ambitions africaines de la Russie », note n° 13/2018, 26 juillet 2018
- Nicolas Mazzucchi, « Les données sont-elles une marchandise comme les autres ?, note n° 12/2018, 25 juillet 2018
- Thrassy N. Marketos, « Eastern mediterranean energy geostrategy on proposed gas export routes », note n° 11/2018, 4 July 2018
- Emmanuelle Maitre, « Kazakhstan's nuclear policy: an efficient niche diplomacy?, note n° 10/2018, 1st July 2018
- François-Albert Stauder, « Tchad : une nouvelle République sans état de droit, note n° 09/2018, 12 juin 2018
- Nicolas Mazzucchi, « Perspectives in gas security of supply: the role of Greece in the Mediterranean », note n° 08/2018, 24 mai 2018
- Juan José Riva, « The Impact of Organized Crime on Peacekeeping Operations: The Case of Minustah in Haiti », note n° 07/2018, 9 April 2018
- Régis Genté, « La question libérale en Russie », note n° 06/2018, 22 mars 2018
- Valérie Niquet, « Testing Times for Security in East Asia: Evaluating one Year of the Trump Presidency, » note n° 05/2018, 19 March 2018
- Isabelle Facon, « Le 'discours du 1er mars' de Vladimir Poutine : quels messages ?, note n° 04/2018, 12 mars 2018
- Valérie Niquet, « Chinese Objectives in High Technology Acquisitions and Integration of Military and Civilian Capabilities: A Global Challenge, note n° 03/2018, 7 March 2018
- Benjamin Hautecouverture, « L'interdiction des armes chimiques en question », note n° 02/2018, 6 mars 2018
- Nicolas Mazzucchi, « 2018, année charnière pour l'Europe dans le cyber ?, note n° 01/2018, 22 janvier 2018

2017

- Benjamin Hautecouverture, « Why must the sanctions against Pyongyang be strengthened ? », note n° 22/2017, 19 December 2017
- Mohamed Ben Lamma, « Face au chaos libyen, l'Europe se cherche encore », note n° 21/2017, 14 décembre 2017
- Benjamin Hautecouverture, « Pourquoi il faut renforcer les sanctions contre Pyongyang », note n° 20/2017, 6 décembre 2017
- Benjamin Hautecouverture, « Crise nucléaire nord-coréenne : que peut faire l'UE ? », note n° 19/2017, 15 novembre 2017
- Emmanuelle Maitre, « Le couple franco-allemand et les questions nucléaires : vers un rapprochement ? », note n° 18/2017, 7 novembre 2017
- Monika Chansoria, « Indo-Japanese Strategic Partnership : Scope and Future Avenues », note n° 17/2017, 19 September 2017
- Antoine Vagneur-Jones, Can Kasapoglu, « Bridging the Gulf: Turkey's forward base in Qatar », note n° 16/2014, 11 August 2017
- Patrick Hébrard, « Pérennité du groupe aéronaval : enjeux stratégiques et industriels », note n° 15/2017, 10 août 2017
- Régis Genté, « Le jeu russe en Libye, élément du dialogue avec Washington », note n° 14/2017, 26 juillet 2017
- Antoine Vagneur-Jones, « Global Britain in the Gulf: Brexit and relations with the GCC », note n° 13/2017, 18 July 2017

La Fondation pour la Recherche Stratégique est une fondation reconnue d'utilité publique. Centre de recherche indépendant, elle réalise des études pour les ministères et agences français, les institutions européennes, les organisations internationales et les entreprises. Elle contribue au débat stratégique en France et à l'étranger.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643
© FRS–TOUS DROITS RÉSERVÉS