IoT : Vers un contrôle des fonctionnalités au vu des menaces liées

Tanguy Godquin*†, Morgan Barbier*, Chrystel Gaber†
Jean-Luc Grimault†, Jean-Marie Le Bars*
*Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen
†Orange Labs, France

***Résumé*—Le nombre de fonctionnalités offertes par l'IOT croît fortement. Dans ce papier, nous mettons en évidence les problèmes de sécurité engendrés par cette tendance. Pour ce faire, nous proposons une mise en relation des fonctionnalités principales des objets de l'IoT avec une taxonomie des menaces. Finalement, nous introduisons une méthodologie pour limiter les menaces passant par un contrôle des fonctionnalités.**

I. Introduction

L'Internet des objets (IoT) connaît une forte croissance ces dernières années. Gartner [1] prévoit 25 milliards d'objets connectés d'ici 2020. La popularité de ce domaine engendre une forte concurrence des solutions proposées par l'industrie et une médiatisation importante.

Les récents problèmes de sécurité, dus au *botnet* Mirai [2], [3] ou à l'attaque de Target [4], pour ne citer que les cas les plus connus, amènent à s'interroger sur la sécurité des objets connectés et plus particulièrement sur ce qu'implique en termes de sécurité l'ajout de fonctionnalités à l'objet.

Le document présente d'abord une problématique des acteurs du domaine, puis une taxonomie des menaces liées à l'IoT est décrite.

Une synthèse des principales fonctionnalités des objets connectés est ensuite proposée. Celle-ci est reliée à une taxonomie des menaces liées à l'IoT. Nous terminerons en proposant une méthodologie pour contrôler les fonctionnalités selon le besoin de sécurisation qu'elles introduisent.

II. Problématique des acteurs

La popularité de l'IoT s'accroît et de nombreux projets se forment autour de cette thématique. La course à l'innovation entre les acteurs encourage une sortie de solutions toujours plus rapide. La sécurisation est perçue comme la dernière étape avant la commercialisation d'un produit. Afin de réduire les temps de conception, la sécurité est souvent négligée.

L'entreprise Serma rapporte [5], d'après ses retours de missions IoT, que 84% des industriels n'évaluent jamais la sécurité de leur produit et que 90% de leurs ingénieurs ne connaissent pas les menaces réelles liées aux IoTs. Ces statistiques concordent avec les résultats de l'étude menée par HP en 2014 [6] au-cours de laquelle les 10 appareils connectés les plus populaires ont été analysés. Lors de cette étude, HP a révélé que 70% des appareils évalués possédaient des vulnérabilités avec en moyenne 25 failles différentes par appareil.

Le cryptologue Bruce Schneier [2] affirme que le marché actuel favorise une commercialisation plus rapide au détriment de la sécurité. Cette tendance a conduit à la rédaction du Règlement européen sur la Protection des Données [7], permettant notamment la mise en place d'une sanction administrative de l'ordre de 2 à 4% du chiffre d'affaire annuel mondial d'une entreprise pour manquement aux droits des personnes (en particulier droit à l'oubli et droits de rectification) et à la protection de leurs données. Les acteurs doivent changer de méthodologie dans la réalisation de leurs solutions afin de respecter cette réglementation.

III. Taxonomie des menaces

Une taxonomie des menaces liées aux éléments de l'IoT a été effectuée par Babar et al. en 2010 [8]. Cette taxonomie se représente sous la forme de 5 catégories:

1) Communication : comprenant les différentes menaces associées aux attaques sur les canaux de communications. Cela comprend notamment les attaques par déni de service (DOS), les attaques dites *man-in-the-middle* (MITM) ou encore les attaques par injections réseau.

2) Identification : représente les menaces liées aux mécanismes de gestion de l'identité dont l'authentification, le contrôle d'accès ou encore le provisionnement.

3) Physique : catégorie spécifique au domaine de l'IoT. L'objet pouvant se retrouver dans les mains d'un client mal-intentionné ou exposé à des tiers (environnement hostile), la menace de l'accès physique à l'objet n'est pas à négliger. Le *reverse engineering* ou l'injection de fautes sont des attaques représentatives de cette menace.

4) Sécurité embarquée : regroupe l'ensemble des menaces au niveau des couches *Physical* et *Media Access Control* (du modèle OSI) mises en œuvre dans l'objet. Cela comprend la falsification des données à ce niveau, les menaces portant sur un environnement ou un élément de sécurité, ainsi que les attaques par canaux auxiliaires.

5) Stockage : catégorie de menaces fortement liée à la présence de l'objet dans un environnement hostile. Elle comprend les menaces liées à la gestion de clés cryptographiques et celles concernant l'intégrité et la confidentialité.

La sécurité absolue n'existe pas. À ce titre il est impossible d'affirmer qu'un système est exempt de menace. Il est nécessaire d'adapter le niveau de sécurité du système selon

les fonctionnalités mises en œuvre et les menaces considérées. L'environnement est également un facteur important dans l'évaluation des besoins sécuritaires et influe sur les menaces affectant une fonctionnalité.

IV. Fonctionnalités et menaces liées

Les solutions IoT offrent une multitude de fonctionnalités via un ou plusieurs objets connectés (constitués de capteurs et/ou d'actuateurs [9]). Chaque fonctionnalité possède des menaces associées et le cumul des fonctionnalités est sujet à une multiplication des menaces.

Nous proposons ci-après un découpage non exhaustif des fonctionnalités principales des objets connectés (monitoring / gestion, interface web, cloud, wireless, firmware update et applications mobiles) et nous rapprochons ces fonctionnalités des menaces de la taxonomie présentée en III.

A. Monitoring / Gestion

Le *monitoring* est utilisé dans les objets connectés afin de faire remonter des informations auprès de leur constructeur, distributeur ou vers un autre objet. Cela peut consister à prévenir un utilisateur que son appareil n'est plus à jour, analyser sa consommation ou encore aider à la construction de statistiques pour l'évolution du produit.

Cette fonctionnalité est particulièrement sensible aux menaces sur la communication(III-1) et le stockage(III-5). Effectuer une attaque sur le système est possible avec un faible coût et un gain potentiel important. L'attaque de Target [4] démontre une vulnérabilité pouvant affecter un système mettant en œuvre ce type de fonctionnalité. L'attaque de cette fonction de *monitoring* permet à un attaquant de bénéficier d'un accès au système pour le détourner à son profit.

Les règlementations pour cette catégorie de systèmes (besoin d'une authentification double facteur) n'ont pas été respectées ouvrant ainsi l'ensemble de l'architecture réseau à cette attaque.

B. Interface Web

Les objets connectés bénéficient rarement d'interface utilisateur physique (écran ou clavier). Afin de combler cette absence, les constructeurs proposent communément une interface web consultable depuis un navigateur internet. Elle est principalement utilisée afin d'interagir avec l'objet (configuration et envoi de commandes).

Une interface utilisateur web introduit dans le système des menaces relatives aux communications(III-1), à la gestion d'identité(III-2) et au stockage(III-5). Les interfaces de ce type rencontrent les mêmes problématiques que les pages web traditionnelles ainsi que celles associées à une communication avec un serveur. Lors de l'étude effectuée par HP en 2014 [6], sur les 10 appareils les plus populaires, 6 d'entre eux bénéficiaient d'une interface utilisateur web vulnérable. Le système s'ouvre ainsi à des attaques faiblement couteuses telle que les injections SQL ou encore les attaques par *Cross-Site Scripting*. Le gain de l'attaquant est important car il bénéficie alors d'un contrôle total sur le ou les appareils.

Il est possible de minimiser les vecteurs d'attaques possibles en respectant les standards de la sécurité web comme les recommandations de la fondation OWASP[1].

C. Cloud

Les faibles capacités de calcul et de stockage des objets connectés impliquent fréquemment l'interfonctionnement de ces derniers avec un cloud (68% des appareils testés par [10]).

L'utilisation du cloud ouvre le système à de nouvelles menaces concernant les communications(III-1), la gestion d'identité(III-2) et le stockage(III-5). D'après [6], 50% des applications mobiles IoT ne chiffrent pas leurs communications vers le cloud, internet ou le réseau local. Il est alors facile d'effectuer sur cette fonctionnalité une attaque *man-in-the-middle*. De plus, un système ayant absolument besoin du cloud pour fonctionner est sujet à des attaques par déni de service comme l'attaque sur Amazon Key [11]. Le coût des attaques sur un tel système est faible et offre un gain important.

Les risques présentés peuvent être réduits en utilisant de la cryptographie pour protéger les canaux de communication et en prévoyant une solution locale assurant la continuité du service en cas de perte de connexion.

D. Wireless

La communication sans fil est omniprésente dans les objets connectés, que ce soit avec ZigBee ou encore via Wi-Fi (support dans 58% des appareils testés par [10]).

L'ajout de communications sans fil auprès d'un système introduit des menaces sur les canaux de communications(III-1), la gestion d'identité(III-2) et le stockage des clés de sécurité(III-5). Les attaques sur ces communications sont variées mais l'attaque *man-in-the-middle* reste la plus fréquente et facile à mettre en œuvre. En 2013, Vidgren et al. [12] proposent une attaque de ce type offrant ainsi la possibilité de récupérer la clé utilisée par le protocole radio ZigBee. Plus récemment, en 2017, Vanhoef et Piessens [13] ont proposé une attaque sur le protocole WPA2 permettant à l'attaquant de déchiffrer les communications. Le gain de cette catégorie d'attaques reste limité: l'attaquant peut écouter toutes les communications, mais, sans l'exploitation de vulnérabilités supplémentaires, il ne dispose pas du contrôle de l'appareil.

Il est possible de prévenir ces attaques en utilisant le paramètre "High Security level" du protocole pour l'attaque sur ZigBee et en mettant à jour le système pour l'attaque sur le protocole WPA2. L'utilisation de plusieurs protocoles de communications offre potentiellement à l'attaquant autant d'accès au système, il est ainsi recommandé de limiter leur nombre.

E. Firmware Update

La mise à jour du *firmware* est une fonctionnalité primordiale dans les objets connectés. Une fois l'objet

[1] https://www.owasp.org

déployé, il est important de permettre une mise à jour de l'appareil à distance.

Malgré la nécessité de cette fonctionnalité, cette dernière introduit de nouvelles menaces sur les communications(III-1), la sécurité embarquée(III-4), le stockage(III-5) et des menaces d'ordre physique(III-3). Il est important de toutes les prendre en compte. D'après HP [6], 60% des appareils analysés ne chiffrent pas leurs données lors du téléchargement d'une mise à jour. Il est alors facile de mettre à jour le firmware avec une version modifiée de ce dernier en utilisant une attaque *man-in-the-middle*. C'est le cas de l'attaque présentée par Barcena et Wueest [10]. Le gain de l'attaquant est alors fort puisqu'il bénéficie ensuite d'un contrôle total sur l'appareil.

Le chiffrement des communications ainsi que la vérification des signatures complexifient la mise en place d'une telle attaque. La présence d'un *secure boot* peut également participer à la prévention de ce type d'attaque en empêchant le système de démarrer si l'intégrité du *firmware* n'est pas vérifiée.

F. Applications mobiles

Dans leur papier Barcena et Wueest [10] montrent que 84% des objets connectés étudiés peuvent interagir avec une application mobile. Ces applications servent principalement à communiquer avec l'objet, le paramétrer ou le commander.

L'utilisation d'une application mobile introduit des menaces sur les communications(III-1), la gestion d'identité(III-2) le stockage(III-5) et d'autres relatives aux attaques physiques(III-3) (*reverse engineering* ou injection de fautes). Un attaquant qui arrive à compromettre une application mobile liée à un objet connecté est en mesure de le contrôler. Il existe des attaques facilement réalisables permettant de modifier le code source de l'application comme le démontre Torano [14] lors d'une attaque sur la poupée My Friend Cayla.

Afin de compliquer le *reverse engineering* effectué lors de cette attaque, il est possible d'utiliser des solutions d'*obfuscation* d'application. Il est également possible de mettre en place des procédures de vérification d'intégrité de l'application avant toute utilisation.

V. Notre méthodologie

Un objet IoT regroupe plusieurs fonctionnalités dont certaines sont essentielles au fonctionnement du service offert. Lorsqu'une fonctionnalité est ajoutée, il est primordial de s'interroger sur sa nécessité puisque son ajout augmente les vecteurs d'attaques sur la solution.

Nous proposons d'accompagner les concepteurs afin qu'ils choisissent les fonctionnalités en leur détaillant les menaces qu'elles peuvent entraîner et en leur donnant les méthodes de sécurisation disponibles pour prévenir ces menaces. Si le coût de l'ensemble (fonctionnalité + sa sécurisation) est plus important que son apport, il est préférable de ne pas l'ajouter. De la sorte, les concepteurs peuvent évaluer le coût de développement d'une solution tout en laissant la possibilité d'introduire de nouvelles fonctionnalités ultérieurement. Cette méthodologie bénéficie pareillement à l'utilisateur avec une sécurité du produit accrue et permet ainsi d'accroître le taux d'acceptation à grande échelle des solutions IoT [15].

VI. Conclusion et perspectives

Dans ce document, les principales fonctionnalités des objets connectés ont été identifiées et rapprochées d'une taxonomie des menaces. Nous avons proposé une méthodologie de contrôle des menaces basée sur le concept de *security by design*.

Le contrôle des fonctionnalités proposé introduit la nécessité d'une sécurité adaptée aux fonctionnalités mises en œuvre pour les cas d'usage variés de l'IoT.

Les travaux futurs s'inscrivent dans cet axe de recherche. Ils porteront sur la recherche d'une sécurisation adaptative servant au plus près les besoins de sécurisation des objets connectés.

References

[1] Gartner, "Gartner says 4.9 billion connected "things" will be in use in 2015," 2014, [accessed 28-December-2017]. [Online]. Available: https://www.gartner.com/newsroom/id/2905717

[2] B. Schneier, "Lessons from the dyn ddos attack," 2016, [accessed 3-December-2017]. [Online]. Available: https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html

[3] B. Herzberg, D. Bekerman, and I. Zeifman, "Breaking down mirai: An iot ddos botnet analysis," 2016, [accessed 29-December-2017]. [Online]. Available: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

[4] B. Krebs, "Target hackers broke in via hvac company," 2014, [accessed 29-December-2017]. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[5] S. Faux, "La sécurité à l'ère des objets connectés: comment s'y prendre ?" in *Workshop "Sécurité des Objets Connectés"*, 2017.

[6] HP, "Hp study reveals 70 percent of internet of things devices vulnerable to attack," 2014, [accessed 20-December-2017]. [Online]. Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

[7] UE, "Règlement général sur la protection des données," 2016, [accessed 6-December-2017]. [Online]. Available: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

[8] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot)," *Recent Trends in Network Security and Applications*, pp. 420–429, 2010.

[9] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "Internet of things: a definition & taxonomy," in *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*. IEEE, 2015, pp. 72–77.

[10] M. B. Barcena and C. Wueest, "Insecurity in the internet of things," *Security Response, Symantec*, 2015.

[11] B. Caudill, "Amazon key security: Cloudcam subject to disruption attacks," 2017, [accessed 29-December-2017]. [Online]. Available: https://rhinosecuritylabs.com/internet-of-things/amazon-key-security-cloudcam-disruption-attacks/

[12] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, "Security threats in zigbee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. IEEE, 2013, pp. 5132–5138.

[13] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *Proceedings of the ACM Conference on Computer and Communications Security, Dallas, TX, USA*, vol. 30, 2017.

[14] C. Torano, "Iot for kids: Cayla doll exploit," 2017, [accessed 29-December-2017]. [Online]. Available: http://thecyberacademy.org/wp-content/uploads/2017/06/CHERYL_TORANO.pdf

[15] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.