Protection de la Vie Privée dans les Communications Sans Fil de l'Internet des Objets (IoT)

Guillaume Celosia
Univ Lyon, INSA Lyon, Inria, CITI
F-69621 Villeurbanne, France
guillaume.celosia@inria.fr

Mathieu Cunche
Univ Lyon, INSA Lyon, Inria, CITI
F-69621 Villeurbanne, France
mathieu.cunche@inria.fr

***Résumé*—Avec l'avènement de l'Internet des Objets, l'informatique embarquée dématérialisera les connexions filaires au profit des communications sans fil et le contrôle humain en faveur de machines connectées. Malgré les bénéfices apportés par l'IoT, ces objets connectés peuvent mettre en péril nos vies privées. Au sein des communications radio de l'IoT, le contenu et les métadonnées peuvent être une source de données personnelles. Si le contenu des communications peut être protégé par des mécanismes de chiffrement, les métadonnées (adresses source/destination, taille et fréquence des messages) sont disponibles en clair. Avec le développement de la radio logicielle et des outils de hacking radio, l'accès à ces données va être facilité permettant de mettre à mal la vie privée des utilisateurs. Ainsi, de nouveaux types d'attaques, reposant sur l'exploitation des communications radio de l'IoT, vont faire leur apparition. Nous présentons trois classes d'attaques basées sur les communications radio afin d'obtenir des données personnelles : le traçage physique, l'inférence d'activité et les attaques par inventaire.**

Mots-clés : Internet des Objets, Vie privée, Sécurité, Communication sans fil, Traçage physique, Inférence d'activité, Attaques par inventaire

I. Introduction

L'Internet des Objets est un concept innovant destiné à nous assister dans nos tâches quotidiennes. Se servir de l'informatique embarquée afin de contrôler notre environnement, tel est l'objectif principal de l'IoT apportant également des dangers pour nos vies privées. Introduites avec le développement de l'IoT, le traçage physique, l'inférence d'activité ainsi que les attaques par inventaire sont des nouvelles formes d'attaques. Administrées par le biais des communications sans-fil, ces attaques mettent en péril la protection de nos données personnelles. Quelles soient en clair ou chiffrées, nos données échangées contiennent des métadonnées permettant de nous profiler [1]. Le travail récent de Geneiatakis et al. [4] a montré que l'espionnage est devenu un nouveau jeu auquel n'importe qui, avec des connaissances basiques en informatique, peut prendre part.

A l'heure actuelle où la donnée est une ressource convoitée, l'expérimentation d'autres types de collectes discrètes n'a plus de limites. Avec l'avènement du concept IoT, d'ici 2020 [2], les objets connectés vont considérablement se populariser, multipliant avec eux le nombre de communications radio et l'exposition de nos données au grand air.

Bien que la plupart des mécanismes de sécurité actuels permettent de protéger le contenu des échanges sans fil, il a été démontré [1] qu'ils ne sont plus suffisants pour préserver nos données personnelles des écoutes indiscrètes. De plus, les outils de hacking radio [10] se démocratisent et sont désormais à la portée de tous.

Dans ce papier, nous réalisons un rapide état des lieux sur les menaces vis-à-vis de la vie privée des utilisateurs engendrées par l'IoT. Ainsi, nous tenons à sensibiliser le grand public aux pratiques diverses que peuvent actuellement mener n'importe quelle personne et qui permettent d'inférer une pléthore d'informations concernant nos vies privées.

Nous présentons trois principales menaces sur la vie privée associées aux métadonnées des communications radio de l'IoT :

- Traçage physique : attaque fondée sur la collecte de données de présence et de mobilité dans le monde physique à partir des signaux émis par les objets accompagnant les personnes.
- Inférence d'activité : attaque permettant de déterminer l'activité d'un individu à partir de l'observation des échanges de données de ses périphériques sans fil.
- Attaques par inventaire : attaques basées sur l'inventaire des objets possédés par un individu permettant d'établir son profil complet.

Le papier sera organisé de la manière suivante : la section II décrit le principe du traçage physique. Les sections III et IV présenteront respectivement l'inférence d'activité et les attaques par inventaire. La démocratisation des outils de hacking radio sera discutée dans la section V et la section VI conclura ce papier.

II. Traçage physique

Bien souvent, le traçage physique est associé au traçage GPS du fait que les données de géolocalisation servent à construire les traces de mobilité d'un individu. Cependant, il faut savoir que ce type d'attaque ne tire pas uniquement parti

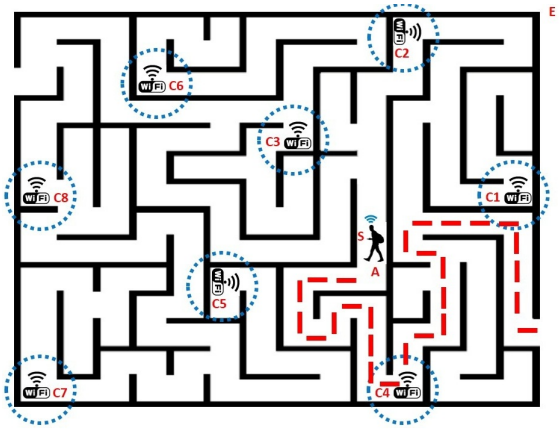

FIGURE 1. Principe du traçage physique

d'un système GPS solitaire mais peut être étendu à d'autres technologies non filaires.

Le traçage physique est donc basé sur la collecte de données permettant de suivre un utilisateur sur son trajet dans le monde réel. Les résultats de cette attaque, généralement réalisée en temps réel, dépendent de la précision des systèmes environnementaux déployés. Par conséquent, le traçage physique, dont l'objectif principal est de suivre une personne dans le monde réel, est définit comme étant une attaque qui porte atteinte à la vie privée.

Introduit de manière sous-jacente, le traçage physique repose sur les communications sans fil. Toute technologie sans fil telles que le Wi-Fi [9] ou le Bluetooth [6] est alors susceptible d'y contribuer. Le seul prérequis à cette attaque est de pouvoir identifier, de manière unique, un objet détenu par la personne ciblée. Cet identifiant unique peut être une adresse MAC [3], un numéro de série [7] ou toute autre information discernable.

Actuellement, les périphériques sans fil implémentent des mécanismes de détection automatique des services environnants. De ce fait, ils émettent continuellement des signaux afin de pouvoir communiquer avec l'environnement. Lorsqu'ils font l'objet d'une collecte malintentionnée, ces signaux traités permettent le suivi des personnes dans le monde réel.

Afin de comprendre le principe de fonctionnement de cette attaque, nous allons succinctement en décrire un scénario représenté à la figure 1.

Soit $\mathcal{A}$, un agent qui se meut dans un environnement $\mathcal{E}$ avec son smartphone $\mathcal{S}$ dont le Wi-Fi est activé. Des capteurs $\mathcal{C}_x$ sont installés dans $\mathcal{E}$ et permettent de capturer les signaux Wi-Fi émanant des périphériques à proximité. De ce fait, à chaque fois que $\mathcal{A}$ se déplacera conjointement avec $\mathcal{S}$, $\mathcal{E}$ sera en mesure de le détecter. Ainsi, $\mathcal{E}$ tracera, au fur et à mesure, le trajet emprunté par $\mathcal{A}$ en fonction des données qu'il collecte.

III. INFÉRENCE D'ACTIVITÉ

L'inférence d'activité fait partie des nouvelles menaces pour nos vies privées introduite avec le développement de l'Internet des Objets. Également basée sur les caractéristiques des ondes radio, cette attaque permet à quiconque, possédant des connaissances basiques en informatiques, de pouvoir inférer l'activité d'un individu en collectant les signaux générés par les objets connectés que celui-ci possède [11].

L'efficacité de cette attaque repose principalement sur la diversité des signaux qui existe. Par exemple, une télécommande pour télévision connectée émettra un signal différent de celui d'une télécommande pour enceinte connectée. En observant respectivement ces deux émissions de signaux, l'attaquant pourra alors inférer de sa cible qu'elle est probablement en train de regarder la télévision ou qu'elle est en train d'écouter de la musique.

Utilisée à d'autres fins, l'inférence d'activité permet de révéler les habitudes de consommations des utilisateurs [5]. Ainsi, en analysant les données collectées, cette attaque permet de dresser un portrait-robot d'une personne ciblée en discernant ses centres d'intérêt particuliers pouvant être les précurseurs d'autres types d'attaque comme le phishing ou le démarchage téléphonique.

IV. ATTAQUES PAR INVENTAIRE

Avec la multiplication des champs d'applications des objets connectés les utilisateurs vont s'entourer d'appareils correspondant à un nombre croissant de cas d'utilisation. La nature des objets en possession d'une personne pourrait alors servir de base pour inférer des informations personnelles [13]. Par exemple, la présence d'un glucomètre pourrait révéler qu'une personne souffre de diabète. En dressant un inventaire des objets associés à une personne, un attaquant pourrait alors dériver un certain nombre d'informations personnelles.

Ainsi, nous risquons d'assister à l'émergence d'attaques par inventaire qui consistent à établir une liste des objets connectés associés à un individu afin d'inférer des caractéristiques propres à celui-ci. Ce type d'attaque va être facilité par l'utilisation des technologies sans fil dans l'IoT qui vont permettre à un attaquant passif de collecter des données. En effet, les signaux générés par les objets sont porteurs d'identifiants révélant la nature de l'objet. Par exemple, une montre GPS Bluetooth connectée va diffuser un identifiant explicite "TomTom GPS Watch". D'autres caractéristiques des communications radio, telles que la taille et la fréquence des paquets, peuvent être exploitées pour déterminer le type de l'objet [1].

Une fois l'inventaire des objets établi, la seconde étape de l'attaque consiste à en dériver un profil de la personne. Certains objets peuvent être associés à des usages particuliers qui peuvent divulguer des centres d'intérêts (sport, musique, ...) ou des problèmes de santé. Également, la valeur des objets peut révéler un certain niveau de vie. Le tableau I présente une liste non exhaustive d'inférences d'informations personnelles possibles.

En plus de l'inférence de données personnelles, l'établissement d'un inventaire dévoile les produits en possession de la personne. Ces données peuvent être exploitées par des campagnes de publicité ciblées. Nous pourrions, par exemple, proposer à un utilisateur un produit complétant les objets déjà

TABLE I
LISTE D'INFORMATIONS PERSONNELLES POUVANT ÊTRE INFÉRÉES À PARTIR D'OBJETS CONNECTÉS.

Type d'objet connecté	Information personnelle inférée
Glucomètre	Diabète
Tensiomètre	Maladie cardiovasculaire
Inhalateur	Problèmes respiratoires
Pacemaker	Maladie cardiaque
Capteur intestinal	Problèmes gastro-intestinaux
Pèse personne	Surveillance pondérale
Casque de relaxation	Stress
Casque de moto, de vélo	Moto, Vélo
Couche, biberon, berceau	Enfant en bas âge
Jouet pour enfant	Enfant
Raquette	Sport de raquette
Distributeur de croquettes	Animal (chien, chat)
Machine à café	Buveur de café
Cave à vin	Amateur de vin
Gramophone	Amateur de musique

en sa possession, ou alors adapter la campagne en fonction des marques des objets équipés par la personne.

V. DÉMOCRATISATION DES OUTILS DE HACKING RADIO

Depuis toujours, les communications radio sont difficilement abordables du fait que le matériel nécessaire pour les expérimentations soit onéreux et principalement destiné aux professionnels. La non disponibilité sur le marché grand public de celui-ci permet d'obtenir une pseudo-sécurité par l'obscurité des données transitant dans les airs. Habituellement, ce type de sécurité opérant par l'obscurité est référencée comme l'une des pires pratiques observable en sécurité informatique.

Actuellement, l'évolution des technologies a permis de doter la population de matériel modeste permettant de comprendre les mécanismes des communications sans fil [12]. Le constant développement de la radio logicielle permet désormais à n'importe qui de pouvoir déclencher des attaques ne nécessitant pas de grandes connaissances dans ce domaine.

Avec la démocratisation des outils de hacking radio, des enjeux plus importants quant à la sécurisation des communications sans fil sont constatés [14]. L'Internet des Objets, composé majoritairement d'objets connectés sans fil, doit alors prendre en compte le fait que les attaquants de demain disposent de tous les outils nécessaires afin de mettre à mal les infrastructures qui seront déployées.

Bien que ce matériel soit facilement acquérable, l'impact des attaques montées n'en est pas moins négligeable [8]. Du traçage physique, des attaques par inventaire en passant par l'inférence d'activité, nos libertés ainsi que nos vies privées seront entachées si des futurs travaux ne s'axent pas sur la protection de celles-ci.

VI. CONCLUSION

Avec l'avènement de l'Internet des Objets, les connexions non filaires vont considérablement s'accroître entraînant une hyper-connectivité mondiale. Conjointement au déploiement des objets connectés et aux échanges de données transitant par les airs, des enjeux se discernent quant à la protection de nos vies privées. La démocratisation des outils de hacking radio permet actuellement à n'importe qui de monter des attaques conséquentes avec des moyens modestes. De ce fait, les objets connectés doivent se doter de nouveaux mécanismes de sécurité robustes. Dans ce papier, nous avons passé en revue trois types d'attaque agissant sur nos données personnelles. L'augmentation des risques proportionnellement au déploiement massif des infrastructures IoT connectées est une raison pour considérer sérieusement ces menaces dans le développement des nouvelles technologies et des standards. Ces attaques seront inévitables si les acteurs du milieu ne joignent pas leurs forces pour les combattre. Dans nos travaux futurs, nous mettrons en pratique chacune des attaques présentées dans ce papier et nous en proposerons des contremesures.

REMERCIEMENTS

Ce travail est supporté par la chaire IoT SPIE ICS-INSA Lyon.

RÉFÉRENCES

[1] Noah Apthorpe, Dillon Reisman, and Nick Feamster. A Smart Home is No Castle : Privacy Vulnerabilities of Encrypted IoT Traffic. *arXiv preprint arXiv :1705.06805*, 2017.

[2] Alex Blanter and Mark Holman. Internet of things 2020 : a glimpse into the future. *Available at Kearney https ://www. atkearney. com/documents/4634214/6398631/AT+ Kearney_Internet+ of+ Things*, 2020, 2016.

[3] Mathieu Cunche. I know your mac address : Targeted tracking of individual using wi-fi. *Journal of Computer Virology and Hacking Techniques*, 10(4) :219–227, 2014.

[4] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. Security and privacy issues for an iot based smart home. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on*, pages 1292–1297. IEEE, 2017.

[5] Bin Guo, Zhiwen Yu, Xingshe Zhou, and Daqing Zhang. Opportunistic iot : Exploring the social side of the internet of things. In *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on*, pages 925–929. IEEE, 2012.

[6] Simon Hay and Robert Harle. Bluetooth tracking without discoverability. In *International Symposium on Location-and Context-Awareness*, pages 120–137. Springer, 2009.

[7] Ari Juels. Rfid security and privacy : A research survey. *IEEE journal on selected areas in communications*, 24(2) :381–394, 2006.

[8] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot : Mirai and other botnets. *Computer*, 50(7) :80–84, 2017.

[9] Célestin Matte and Mathieu Cunche. Wombat : An experimental wi-fi tracking system. In *8e édition de l'Atelier sur la Protection de la Vie Privée (APVP)*, 2017.

[10] Michael Roche. Wireless hacking tools. *Washington University in St. Louis*, 2007.

[11] Vijay Srinivasan, John Stankovic, and Kamin Whitehouse. Protecting Your Daily In-home Activity Information from a Wireless Snooping Attack. In *Proceedings of the 10th International Conference on Ubiquitous Computing*, UbiComp '08, pages 202–211, New York, NY, USA, 2008. ACM.

[12] MB Sruthi, M Abirami, Akhil Manikkoth, R Gandhiraj, and KP Soman. Low cost digital transceiver design for software defined radio using rtl-sdr. In *Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on*, pages 852–855. IEEE, 2013.

[13] Chunlai Wang. Object identification techniques and the application in iot. *Advances in Media Technology*, page 9, 2013.

[14] Rolf H Weber. Internet of things–new security and privacy challenges. *Computer law & security review*, 26(1) :23–30, 2010.