HAL
open science

IoT & Privacy - Comment assurer la confidentialité sur les réseaux sans fil ? L'exemple du BLE

Mathieu Cunche, Alexandre Ratel

To cite this version:

Mathieu Cunche, Alexandre Ratel. IoT & Privacy - Comment assurer la confidentialité sur les réseaux sans fil ? L'exemple du BLE. [Rapport Technique] INSA Lyon; SPIE ICS. 2020. hal-03020342

HAL Id: hal-03020342

https://inria.hal.science/hal-03020342v1

Submitted on 3 Jan 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SPIE

Chaire IoT
SPIE - INSA Lyon

IOT & PRIVACY

COMMENT ASSURER LA CONFIDENTIALITÉ SUR LES RÉSEAUX SANS FIL ? L'EXEMPLE DU BLE

Bluetooth Low Energy
Wifi
Anonymization
Randomization
Security

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON
citi lab

SOMMAIRE

Édito de Mathieu Cunche et Alexandre Ratel 03

CHAPITRE 1
Traçage physique via les signaux radio 04

CHAPITRE 2
Mécanismes antitraçage dans le BLE : *address randomization* 06

CHAPITRE 3
Limites et perspectives de la protection 07

Chaire IoT SPIE - INSA Lyon en chiffres 10

À propos 11

ÉDITO

IoT & Privacy : comment assurer la confidentialité sur les réseaux sans fil ?

Le Bluetooth Low Energy (BLE) est une variante *Low Energy* de la technologie Bluetooth qui a été introduite par la version 4.0 du standard Bluetooth en 2010.
Comme son nom l'indique, le BLE se distingue de la version classique du Bluetooth par une consommation plus faible en énergie. En effet, le BLE implémente un mode de transmission à plus faible débit qui permet de diminuer la consommation énergétique. De par sa faible consommation, cette technologie est intégrée dans des systèmes contraints par les ressources énergétiques.
Durant l'année 2017, plus de 2 milliards d'appareils équipés de la technologie BLE ont été distribués.
La technologie BLE se retrouve dans un grand nombre d'objets connectés qui couvrent la plupart des domaines de l'IoT.
En particulier, elle équipe de nombreux objets qui nous accompagnent dans notre vie quotidienne : les smartphones, tablettes et ordinateurs, des accessoires tels que les écouteurs connectés, bracelets et smartwatches, ou encore la domotique (ampoules, interrupteurs, etc).
Grâce au Bluetooth Low Energy, deux appareils BLE, un maître et un esclave, peuvent établir une connexion pour échanger des données. Lorsqu'il n'est pas connecté, un esclave se trouve en mode *advertising* et va annoncer sa présence en émettant périodiquement des messages appelés *advertisement packets*. Il devient ainsi détectable et identifiable par tout appareil maître qui se trouve à portée.
Dans le cadre de la Chaire SPIE – INSA Lyon, nous travaillons à la détection et à la capture du trafic sans fil pour analyser les menaces de fuites d'informations sur la vie privée de l'utilisateur.
Ce cahier illustre ces propriétés au travers du BLE, et les différents mécanismes préventifs exposés peuvent, pour certains, se transposer dans différents protocoles IoT.

MATHIEU CUNCHE,
Maître de conférences, INSA Lyon

ALEXANDRE RATEL,
Architecte IoT et collaboration, SPIE ICS

MATHIEU CUNCHE,
est Maître de conférences au laboratoire CITI de l'INSA Lyon et affilié à l'équipe projet Inria PRIVATICS. Ses domaines de recherche comprennent la protection de la vie privée, la sécurité, les réseaux sans fil, l'internet des objets et les systèmes mobiles. Il s'intéresse en particulier aux problèmes liés au traçage dans le monde physique rendu possible par la prolifération d'objets communicants.

ALEXANDRE RATEL,
34 ans, ingénieur diplômé de l'ENSEA à Cergy-Pontoise, spécialité télécommunications et réseaux. Il intègre SPIE ICS en 2006 en tant qu'apprenti référent technique puis évolue en interne jusqu'à son poste actuel d'architecte IoT et collaboration. Passionné de nouvelles technologies, il aime le partager.

CHAPITRE 1

TRAÇAGE PHYSIQUE VIA LES SIGNAUX RADIO

L'usage des objets connectés est parfois accompagné par des menaces sur la vie privée qu'ils peuvent induire. On soupçonne ainsi capteurs domotiques, bracelets connectés et assistants vocaux d'éroder notre espace intime en collectant et transmettant des données à destination d'acteurs tels que les GAFAM. Cependant, les risques liés aux données captées par ces objets ne sont pas les seuls auxquels s'exposent les utilisateurs d'objets connectés.

Les usages sont légion : pour les loisirs, montres connectées ou dédiées au sport ; en santé, tensiomètres ou glucomètres ; dans l'industrie, capteurs de température, de torsion, de consommation, et bien d'autres encore, sans parler des jouets de nos enfants. La plupart des grands constructeurs ont depuis longtemps sauté le pas.
Cisco embarque nativement la technologie dans toutes ses bornes Wi-Fi Meraki. Il devient alors possible de géolocaliser précisément du matériel (*asset tracking*). HPE Aruba propose des *beacons* à placer à des endroits stratégiques pour déclencher du contenu interactif sur smartphone.
Apple a développé iBeacon, sa propre implémentation basée sur le BLE, qui offre de nombreuses possibilités à tous les développeurs d'applications iPhone.

Identification et traçage dans le monde physique

L'avènement des objets communicants (en radio) s'accompagne de la possibilité d'observer les personnes en se basant sur les signaux émis par leurs objets. En effet, dès qu'ils sont activés, ces objets transmettent des signaux radio qui incluent souvent un identifiant. Celui-ci permet de déterminer l'objet et donc son porteur, l'exposant ainsi à un traçage dans le monde physique.
Dans le cas du BLE, les appareils découvrables transmettent des signaux *(advertisement packets)* dès qu'ils sont allumés et, cela, même s'ils ne sont pas connectés à un autre appareil. Un appareil BLE se trouvant dans cette configuration diffuse ainsi plusieurs fois par minute des messages incluant un identifiant unique. Collecter les identifiants présents dans les messages peut se faire par une simple écoute passive des canaux de transmission.

Techniquement, une simple interface Bluetooth pilotée par des outils logiciels en libre accès permet de collecter ces signaux et d'en extraire les identifiants. Un dispositif de captation de données BLE peut ainsi être construit pour moins de 10 euros. On peut même observer les informations correspondant à ces signaux depuis son appareil mobile (par exemple, avec l'application *RaMBLE* sous Android).
De plus, les identifiants présents dans ces messages ne sont pas chiffrés et sont ainsi exposés à la « vue » de tous. Ces identifiants sont diffusés en clair, en partie car ils sont nécessaires dans le cadre d'échanges qui se font avant ou hors du cadre de l'établissement d'une connexion sécurisée entre les appareils.
Le traçage des personnes via les signaux radio émis par leurs appareils n'existe pas qu'en théorie. Cette pratique est utilisée par certains acteurs qui ont mis au point des systèmes de traçage capables de détecter les personnes et de tracer leurs déplacements. De tels systèmes sont exploités par des acteurs privés, afin de fournir des statistiques sur la fréquentation de lieux tels que des enseignes commerciales, des centres commerciaux ou des aéroports. D'autres acteurs proposent d'utiliser ces systèmes pour *profiler* les personnes et proposer des publicités ciblées dans le monde physique (sur des panneaux d'affichage dynamique).

D'un point de vue radio, la technologie BLE travaille sur un ensemble de 40 canaux présents au sein de la bande ISM de 2,4 GHz. L'échange d'informations se fait via la transmission d'informations au sein de messages radio appelés paquets qui contiennent, entre autres, l'adresse de l'appareil destinataire *(device address)* ainsi que d'éventuelles données.

Ces cas d'application à vocation commerciale démontrent la faisabilité de tels systèmes qui permettraient de mettre en œuvre une surveillance globale des personnes et constitueraient ainsi une menace pour les libertés individuelles.
Ce traçage s'apparente à une collecte de données personnelles qui s'effectue en général sans consentement ni information des personnes. Même si des protections légales et/ou réglementaires telles que la RGPD sont vouées à préserver les utilisateurs contre un traçage illégitime, il convient de proposer également des solutions techniques pour limiter l'exposition de données à la source.

« Dans le cadre de ma thèse, j'étudie les problèmes de vie privée liés à l'utilisation des technologies radio dans l'internet des objets. Plus particulièrement, mes recherches se concentrent sur la technologie Bluetooth dans les versions 4.0 et supérieures. »

GUILLAUME CELOSIA,
doctorant au laboratoire CITI, INSA Lyon

CHAPITRE 2

MÉCANISMES ANTITRAÇAGE DANS LE BLE : ADDRESS RANDOMIZATION

Afin de protéger les utilisateurs, l'apparition du BLE a été accompagnée par une technique antitraçage spécifiée dans la version 4.0 du standard Bluetooth. « LE Privacy » est le nom de cette fonctionnalité qui permet de substituer les identifiants d'appareil, auparavant statiques, par des identifiants temporaires changeant régulièrement pour une valeur aléatoire. L'identifiant présent dans les messages n'est ainsi plus utilisable pour tracer les utilisateurs sur le long terme. Un utilisateur détecté à un instant *t* sous un identifiant *i* réapparaîtra sous une nouvelle identité un peu plus tard. Les identifiants temporaires sont créés avec un générateur aléatoire cryptographique qui rend les valeurs imprédictibles. Il est donc impossible de faire le lien entre deux identités distinctes d'un appareil.

Zoom sur la fonctionnalité LE Privacy

Avec la fonctionnalité LE Privacy, les appareils BLE ont ainsi la possibilité d'utiliser 4 types d'adresses :

- *Public* : identifiant unique et permanent alloué par le constructeur à chaque appareil. Aussi appelé adresse MAC.
- *Random Static* : identifiant aléatoire mais qui n'a pas vocation à être changé régulièrement.
- *Private Non-Resolvable* : identifiant aléatoire et temporaire pouvant changer à n'importe quel moment.
- *Private Resolvable* : identifiant aléatoire et temporaire pouvant changer à n'importe quel moment. Cet identifiant peut être reconnu (*resolved*) par des appareils avec qui il partage une clé secrète (échangée lors de l'appairage initial).

Pour les adresses de type *Private*, le standard recommande un renouvellement de la valeur de l'adresse, au moins toutes les 15 minutes.

La fonctionnalité LE Privacy est aujourd'hui présente dans nombre de produits, en particulier les objets portables tels que les smartphones, écouteurs et bracelets. Des travaux récents[1] menés dans le cadre de la Chaire IoT suggèrent qu'une part significative (plus de la moitié) des appareils BLE en circulation utilise une adresse aléatoire temporaire.

(1) G. Celosia and M. Cunche, "Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism" In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. ACM, 2019.

CHAPITRE 3

LIMITES ET PERSPECTIVES DE LA PROTECTION

La protection offerte par les adresses temporaires et aléatoires n'est pas inconditionnelle. Celle-ci peut en effet être mise en défaut par d'autres éléments liés à l'implémentation et à l'utilisation du BLE.
Tous les constructeurs n'utilisent pas le mécanisme d'adresses aléatoires, ou l'utilisent incorrectement. Certains fabricants continuent de recourir à des adresses permanentes (Samsung, Bose, Logitech) ou utilisent la même adresse temporaire pour une très longue durée (plusieurs jours). D'autres, enfin, choisissent des adresses qui ne sont pas totalement aléatoires.
De plus, il existe d'autres vecteurs d'attaque liés au contenu des messages. En effet, les éléments présents dans les messages peuvent être adaptés au besoin des applications. Il est même possible d'y intégrer des données dans un format libre au sein des structures qualifiées de *manufacturer specific.*

Quelles sources pour les attaques ?

Les attaques trouvent leur source dans les éléments inclus dans le corps des messages et peuvent induire plusieurs types de problèmes. Il est possible de les regrouper en trois catégories.

Des identifiants présents dans le corps des messages *(voir figure 1)*

Ces identifiants peuvent être trivialement utilisés afin de suivre l'attaquant. On les trouve par exemple sous la forme d'UUID ou d'identifiants propres aux applications des constructeurs.

Des compteurs présents dans le corps des messages *(voir figure 2)*

Des compteurs peuvent être intégrés aux messages afin de les identifier et de les distinguer, la valeur de ce compteur augmentant de 1 à chaque nouveau message. Si le compteur poursuit sa progression normale lors d'un changement d'adresse, la continuité de la séquence de valeurs permet de relier entre elles les deux adresses successives d'un appareil.

Une empreinte technique unique

Le contenu des messages dépend de l'application, des choix de l'implémenteur ainsi que de l'état de l'appareil. Cela a pour conséquence d'induire une grande diversité d'un appareil à un autre. Si ce contenu est suffisamment unique, il peut être utilisé pour constituer un identifiant propre à l'appareil qui permettra de le distinguer et de le tracer. Dans le cadre de la Chaire IoT, plusieurs failles de ce type ont pu être mises en évidence[1], en particulier au sein d'appareils d'Apple, Fitbit ou Microsoft.

(1) G. Celosia and M. Cunche, "Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism" In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. ACM, 2019.
G. Celosia and M. Cunche, «Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile.» In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things. ACM, 2019.
G. Celosia and M. Cunche, "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols" In Proceedings on Privacy Enhancing Technologies, vol. 2020, (to appear).

Perspectives

Même si les spécifications du BLE fournissent des instructions et des recommandations sur l'utilisation de l'*address randomization*, elles ignorent certains aspects qui peuvent mener à des failles. Il est donc nécessaire d'enrichir ces spécifications à la lumière des différentes attaques qui ont été mises en évidence. Dans le cadre de la Chaire IoT, plusieurs ensembles de recommandations ont été proposés.
Le problème du traçage affecte potentiellement toutes les technologies sans fil. Le principe d'adresse temporaire a ainsi été décliné dans des technologies telles que le Wi-Fi et le standard véhiculaire 802.11p. Les failles discutées ici peuvent s'appliquer à un large spectre de standards. Ainsi, les pistes de réflexion décrites dans ce document pourront servir à anticiper ces problèmes dès la conception des prochains standards. Au-delà des standards, ces problématiques devront être prises en compte lors des phases de conception et d'intégration. Au même titre que la sécurité, la protection de la vie privée devra faire partie intégrante du cahier des charges et bénéficier de ressources en conséquence.

Figure 1 → **Un appareil BLE change d'adresse, mais un autre identifiant statique est inclus dans le message et permet ainsi de lier les deux adresses**

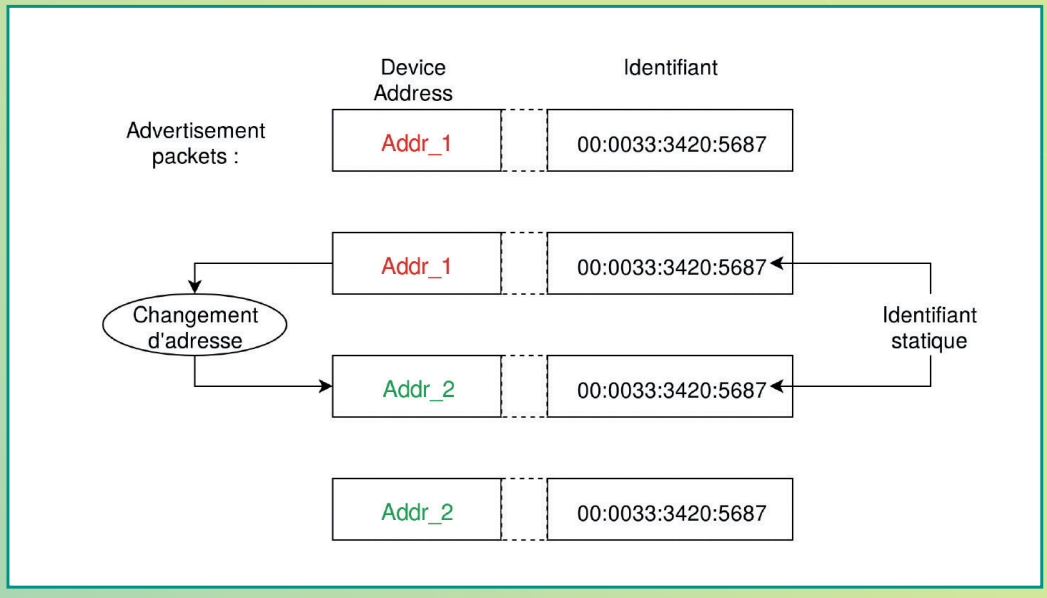
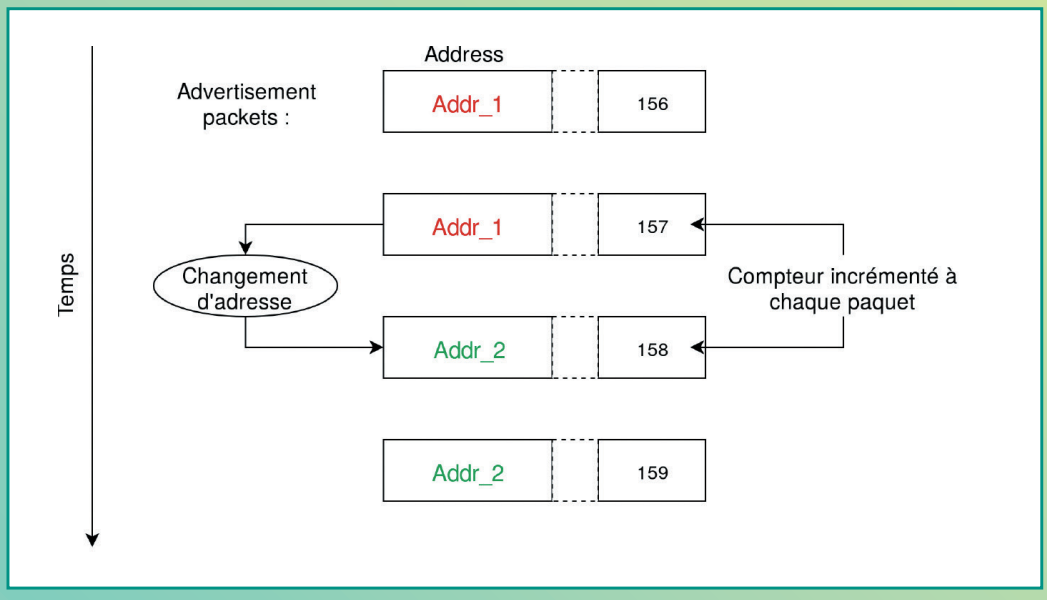
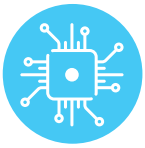


Figure 2 → **Un appareil BLE change d'adresse, mais un compteur est inclus dans le message et la progression linéaire de ce compteur permet de relier les deux adresses**



Une Chaire IoT pour IMAGINER LES USAGES DE DEMAIN

4 axes de recherche



Déploiement de masse et logiciels embarqués pour l'IoT

Sécurisation et respect de la vie privée

Architecture de réseaux cognitifs

Objets connectés : low energy, zero battery

01 juillet 2016 : signature officielle de la Chaire IoT

1 partenariat

SPIE et INSA Lyon, porté par la Fondation INSA Lyon

1 écosystème de partenaires

ADIRA, BOSCH, CA3B, EGIS, FFSTAR, IRT SystemX, Métropole Grand Lyon, MINALOGIC, RTONE, SIDD, SITIV, Visioglobe

3 ans de production et de transmission

20 publications
(18 conférences, 1 journal, 1 thèse)

38 missions,
dont 1 mobilité longue à Princeton

3 plateformes
- LoRa (2 antennes gateways)
- YOUPI (20 nœuds gateway/Edge IoT, 1 cloud)
- UrPolSens (12 capteurs de qualité de l'air)

1 plateforme exploratoire : SCENE
(prévision 5 capteurs parking, 20 capteurs QVT, 2 clouds)

1 école d'hiver européenne IoT
avec 30 participants

9 recrutements au sein de la Chaire
(7 doctorants, 1 ingénieur, 1 stagiaire)

28 diplômés INSA Lyon recrutés chez SPIE,
10 apprentis et 21 stagiaires depuis 2016

À PROPOS...

... de SPIE ICS

Filiale de services numériques de SPIE France, SPIE ICS est spécialisée dans les services liés aux infrastructures ICT, depuis l'environnement utilisateurs jusqu'au data center. Sa vocation est de « co-construire » avec ses clients ETI et grands comptes des services innovants adaptés à leurs métiers, pour accompagner la transformation digitale et simplifier l'expérience du numérique.

... de SPIE France

SPIE France filiale du groupe SPIE, est un acteur majeur de la transition énergétique et numérique. Ses cinq filiales interviennent sur quatre marchés stratégiques : e-fficient Buildings, Smart City, Energies et Smart Industry.

... de SPIE

SPIE est le leader européen indépendant des services multitechniques dans les domaines de l'énergie et des communications.

www.spie.com
@spieicsfrance
@spiegroup

... de l'INSA Lyon

L'INSA Lyon est l'une des plus Grandes Écoles d'ingénieurs françaises. Pluridisciplinaire, internationale, elle forme en cinq ans des ingénieurs pluricompétents, humanistes, innovants et dotés d'un esprit entrepreneurial. Premier des INSA, créé en 1957 avec une ambition d'ouverture sociale, l'INSA Lyon diplôme plus de 1000 ingénieurs par an dans 9 spécialités, et délivre environ 150 doctorats par an et une centaine de mastères. L'INSA Lyon est, avec 770 enseignants, enseignants-chercheurs et chercheurs et 23 laboratoires, un pôle de recherche internationalement reconnu.

www.insa-lyon.fr
@insadelyon

... du laboratoire CITI

Le CITI, Centre of Innovation in Telecommunications and Integration of Service, est un laboratoire académique associé à l'INSA Lyon et à l'INRIA. Ses domaines de recherche relèvent des sciences du traitement de l'information, des réseaux et des communications pour adresser les problèmes liés au développement de l'internet des objets.
Ces réseaux planétaires d'objets fournissent un continuum numérique pour lequel le laboratoire CITI propose des architectures hétérogènes de communication sans fil incluant la mobilité, différents protocoles d'accès, des systèmes embarqués autonomes, des services distribués ubiquitaires et adaptables.

www.citi-lab.fr
@citi_lab

www.spie-ics.com

SPIE ICS

148, avenue Pierre Brossolette
92247 MALAKOFF Cedex
Tél. : +33 (0)1 41 46 41 46
Fax : +33 (0)1 41 46 41 47

INSA Lyon

20, avenue Albert-Einstein
69100 VILLEURBANNE
Tél. : + 33 (0)4 72 43 83 83
Fax : + 33 (0)4 72 43 85 00

Conception-Réalisation : MotàMeaux

SPIE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

citi lab