Identification de l'adresse physique de dispositifs radio Bluetooth BR/EDR par radio logicielle

Usage actuel du Bluetooth (état de l'art)

La technologie Bluetooth s'est installée comme une référence pour les usages de connectivité radio : elle est utilisée mondialement par des milliards d'équipements communicants variés (téléphones mobiles, ordinateurs portables, casques sans-fil, systèmes audio de voiture, …) pour des applications en courte portée pouvant nécessiter des débits assez élevés comme le transfert de voix et/ou de données (appels vocaux, streaming audio, échange de fichiers, partage de connexion, …).
Les informations échangées via la forme d'onde Bluetooth sont potentiellement sensibles (données personnelles telles que carnet d'adresse, historique des appels, SMS, appels audio, …) et les spécifications Bluetooth sont censées garantir la confidentialité de ces informations, ainsi que la confidentialité de localisation des utilisateurs, et ce au travers de différents mécanismes de sécurité : chiffrement des données, mais aussi protection de la forme d'onde au niveau de la couche physique : étalement de spectre par sauts de fréquence, blanchiment, masquage de l'adresse physique (BD_ADDR) des participants, …

Positionnement du problème: failles de sécurité existantes

Plusieurs failles de sécurité et attaques potentielles ont cependant été publiées concernant la forme d'onde Bluetooth. Parmi elles, plusieurs études (cf. [R1] et [R3]) montrent qu'il est possible de dévoiler l'adresse physique d'un équipement Bluetooth (pourtant réputée secrète), ouvrant la voie à des usages malicieux tels que par exemple la localisation ou le pistage d'un (ou plusieurs) équipement(s) Bluetooth.
De plus, les modules de radio logicielle (SDR) large bande, désormais disponibles à bas coût et permettant de numériser instantanément l'ensemble de la bande Bluetooth (d'une largeur totale d'environ 80 MHz), mettent à mal les techniques de sauts de fréquence (FHSS) censées garantir la sécurité de la forme d'onde Bluetooth. Ces modules large bande permettent également de suivre en parallèle différentes communications au travers de plusieurs pico-réseaux Bluetooth.

Motivation et périmètre de l'étude

La présente publication vise à présenter deux techniques d'identification (*Fingerprinting*) d'utilisateur(s) Bluetooth par désanonymisation de leur adresse physique (BD_ADDR), information pourtant considérée secrète pour un tiers non-autorisé et donc immunisée contre les attaques de suivi.
Associé à la récupération complémentaire de la valeur d'horloge du pico-réseau Bluetooth (autre information réputée secrète), on montre qu'il est pourtant possible de dévoiler le motif pseudo-aléatoire de sauts de fréquence généré par l'algorithme d'EVF et utilisé par la forme d'onde radio Bluetooth.

L'article présente également les bénéfices d'utiliser un module de radio logicielle (SDR) à large bande capable de numériser l'ensemble de la bande Bluetooth en accélérant significativement l'identification potentielle de certains utilisateurs de différents pico-réseaux colocalisés.

La présente étude se limite au Bluetooth classique, c'est-à-dire aux modes BR (*Basic Rate*) et EDR (*Enhanced Data Rate*) de la forme d'onde Bluetooth qui permettent d'atteindre les plus hauts débits et pour lesquels les spécifications n'évoluent plus depuis plusieurs années : les failles existantes risquent donc de perdurer.
La variante *Bluetooth Low Energy* (BLE), introduite en 2010 dans les spécifications (V4.0), est principalement destinée à démocratiser le Bluetooth à l'Internet des Objets (IoT) avec des limitations en termes de puissance et de débit. Utilisant par spécification un procédé de randomisation de l'adresse physique des équipements, le BLE est hors du périmètre de cette étude.

Protocole Bluetooth Classic (BR/EDR)

Présentation

Bluetooth BR/EDR est un protocole radio faible puissance (quelques mW) courte portée (10 à 100 m) permettant l'établissement d'un pico-réseau ad hoc (sans infrastructure préalable) et des échanges bidirectionnels jusque 3 Mbits/s dans la bande de fréquence ISM à 2.4 GHz.

La forme d'onde Bluetooth BR/EDR[1], dont la dernière version 5.4 a été publiée en 2023, est notamment sécurisée par :

- étalement de spectre par évasion de fréquence (EVF, ou FHSS en anglais) : un nouveau canal est sélectionné pseudo-aléatoirement parmi 79 canaux contigus (d'une largeur de bande unitaire de 1 MHz) à chaque nouveau créneau temporel d'émission/réception appelé *Time Slot* (TS) valant 625 µs, soit une vitesse de 1600 sauts par seconde
- authentification et création d'un secret partagé par chiffrement asymétrique (DH)
- randomisation des données par blanchiment (embrouillement via séquence pseudo-aléatoire)
- chiffrement (optionnel) des données en AES-CCM.

Figure 1 : Pico-réseau Bluetooth

La Figure 1 présente un pico-réseau Bluetooth actif typique interconnectant 2 équipements Bluetooth, chacun disposant :

- d'une valeur d'horloge propre, définie sur 28 bits avec une granularité (LSB) d'un demi TS (soit 312.5 µs) et rebouclant au bout d'un peu plus de 23 heures.
- d'une adresse physique de 48 bits appelée BD_ADDR (équivalent à une adresse MAC pour une carte réseau) permettant son identification unique parmi l'ensemble des équipements Bluetooth produits à travers le monde.

Le format de trame typique d'un paquet de type Bluetooth BR est présenté en Figure 2.

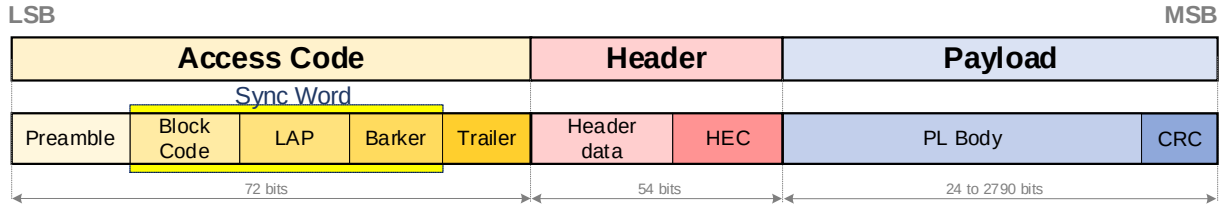

Figure 2 : Format d'un paquet Bluetooth BR

La première portion, appelée code d'accès (*Access Code*), est la même pour tous les paquets transmis dans un même pico-réseau (permettant la ségrégation de multiples pico-réseaux Bluetooth potentiellement colocalisés), et est construit à partir d'une portion de l'adresse BD_ADDR du maître : la portion LAP (présentée sur la Figure 3) qui est transmise en clair au sein du code d'accès.

1 Pour alléger l'écriture, toute référence à Bluetooth dans la suite de ce document fait référence au Bluetooth BR/EDR : comme indiqué en partie introductive, la forme d'onde *Bluetooth Low Energy* (BLE) est hors du périmètre de cette étude.

La 2ème portion appelée entête (*Header*) contient différentes informations (*Header data*) concernant le paquet dont son type (parmi un jeu de messages possibles), une adresse identifiant un membre actif du pico-réseau (comme destinataire ou émetteur du paquet) et un jeu de bits permettant notamment de contrôler l'acquittement ou la demande de retransmission d'un paquet. La partie *Header* contient également des bits de parité (champ HEC) permettant de vérifier l'intégrité de l'entête.
La 3ème et dernière portion temporelle d'un paquet Bluetooth BR/EDR contient la charge utile (*Payload*), c'est-à-dire les données transmises (voix ou données selon les applications) au sein du paquet. Pour la plupart des types de paquet, la présence d'un champ CRC permet de contrôler l'intégrité des données. Pour information, les bits de contrôle d'intégrité (HEC pour la partie *Header* et CRC pour la partie *Payload*) sont générés en utilisant des registres à décalage à rétroaction linéaire (LFSR), dont la valeur d'initialisation est égale à une portion (UAP, illustrée en Figure 3) de l'adresse BD_ADDR du maître : il est ainsi possible pour un attaquant d'exploiter les valeurs décodées de HEC et CRC pour remonter à la valeur d'UAP.

Les portions *Header* et *Payload* subissent en outre une étape de blanchiment (w*hitening*) avant transmission : l'ensemble de ces bits sont ainsi multipliés (au sens « ou exclusif ») par une séquence pseudo-aléatoire générée par un LFSR dont la valeur d'initialisation dépend cette fois de 6 bits (CLK_{6-1}) de la valeur d'horloge du maître du pico-réseau. Cette étape de blanchiment permet de randomiser les bits des champs *Header* et *Payload*, et d'éviter l'apparition de certaines longues séries de 0 ou de 1). Le blanchiment participe également à la sécurisation de la communication (contre les écoutes notamment) en compliquant la tâche (par ajout d'un aléa de 6 bits) d'un éventuel attaquant ne connaissant pas la valeur d'horloge du maître. Mais ce procédé peut aisément être surmonté par force brute (FB).

Dans un pico-réseau Bluetooth établi où tous les participants sont synchronisés, l'un d'entre eux assure le rôle de maître tandis que les autres participants sont dénommés esclaves (ou périphériques). Le maître joue un rôle prépondérant au sein du pico-réseau puisqu'il impose :

- sa valeur d'horloge comme heure commune du pico-réseau (appelée CLK)
- une partie de son adresse physique BD_ADDR (portion LAP présente dans l'*Access Code* et portion UAP utilisée dans la construction des champs HEC du *Header* et CRC de la *Payload*) pour taguer l'ensemble des paquets Bluetooth échangés au sein dudit pico-réseau

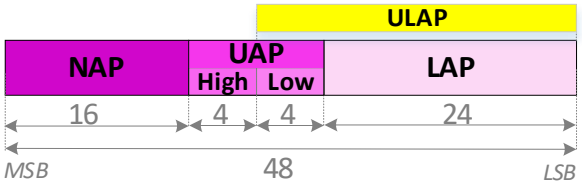

Figure 3 : Format de l'adresse physique BD_ADDR

La Figure 3 illustre le format de l'adresse physique BD_ADDR permettant d'identifier de manière unique chaque équipement Bluetooth. Cette adresse, codée sur 48 bits, reprend la même structure que l'adresse MAC pour la norme Ethernet et est constituée de trois parties :

- La partie basse (LAP) de 3 octets correspond au numéro de série du module Bluetooth affecté par le constructeur.
- La partie médiane (UAP), de taille 1 octet, contient une partie de l'identité du constructeur.
- La partie haute (NAP), composé de 2 octets (dont l'un est égal à 0x00) apporte le complément d'information pour identifier de manière unique le constructeur de l'équipement Bluetooth. Cette portion d'adresse est appelée partie non-significative dans le sens où, contrairement aux parties LAP et UAP, elle n'est pas utilisée par les algorithmes bande de base Bluetooth pour introduire de l'aléa servant à sécuriser la forme d'onde.
  À noter que seule une trentaine de valeurs NAP sont effectivement attribuées, ce qui facilite une recherche exhaustive par force brute dans un contexte de reconstruction complète d'une adresse BD_ADDR.

La Figure 4 suivante présente l'algorithme d'EVF pseudo-aléatoire utilisé en Bluetooth délivrant, TS après TS, la suite des canaux fréquentiels à utiliser pour les transmissions de paquets :

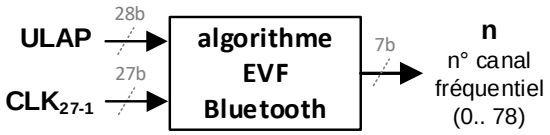

Figure 4 : Interfaces de l'algorithme EVF en Bluetooth

Le pseudo-aléa introduit par cet algorithme est régi par 2 paramètres d'entrée dont les valeurs sont tenues secrètes hors du cercle des participants déjà connectés au pico-réseau (*trusted users*), à savoir :

- la valeur ULAP correspondant à la partie basse (sur 28 bits soit les 4 LSB de l'UAP associés aux 24 bits de LAP) de l'adresse physique BD_ADDR du maître du pico-réseau
- la valeur courante CLK (ou CLK_{27-0}) de l'horloge du pico-réseau Bluetooth (définie sur 28 bits mais avec une entropie réelle de 27 bits, le LSB CLK_0 valant nécessairement 0 pour le maître), cette valeur étant celle de l'horloge du maître du pico-réseau.

Ainsi, si un tiers réussit à découvrir ce jeu de 2 valeurs ULAP et CLK (avec une entropie totale de 55 bits) pour un pico-réseau Bluetooth, alors le schéma pseudo-aléatoire des sauts de fréquence de ce pico-réseau lui est accessible : ce tiers peut alors connaître précisément les instants de changement de TS (ayant connaissance de l'horloge CLK du réseau au ½ TS près) et savoir, pour tout TS, sur quel canal fréquentiel Bluetooth une transmission de paquet est susceptible de se produire au sein du pico-réseau espionné.

Intérêt de l'usage d'un module SDR large bande en interception

Grâce à des ADC très rapides capables d'échantillonner en temps réel des signaux radio à large bande, les modules de radio logicielle (SDR) permettent aujourd'hui de développer de manière souple (logiciel), rapide et peu coûteuse certaines fonctionnalités (filtrage, démodulation, …) qui demandaient auparavant des circuits matériels dédiés à chaque type de signal radio.

Il existe des solutions SDR très peu coûteuses mais à largeur de bande limitée, capables par exemple de démoduler un seul canal Bluetooth à la fois. Même si ces elles permettent d'obtenir certains résultats (cf. [R1] et [R2]), elles ne permettent pas de capturer l'ensemble du spectre Bluetooth en instantané, et n'offre donc pas la capacité de suivre l'ensemble des communications pouvant se dérouler de manière concomitante et possiblement dans plusieurs pico-réseaux Bluetooth en un endroit géographique donné. L'interception de l'ensemble de la bande Bluetooth (79 canaux) permet également de capturer beaucoup plus de paquets en un temps d'acquisition donné, et donc d'identifier certaines informations recherchées beaucoup plus rapidement (facteur 79 par rapport à l'usage d'une solution bande étroite n'utilisant qu'un seul canal typiquement).

Intérêt d'avoir accès à la couche physique Bluetooth

Le développement logiciel additionnel d'une couche physique Bluetooth en réception (Rx) capable de traiter les signaux dans le domaine temps-fréquence, permet d'apporter les bénéfices suivants:

- maîtriser le protocole, et accéder à l'ensemble des messages gérant la sécurité et l'établissement de la connexion (protocole LMP de gestion des liens en Bluetooth par exemple)
- extraire des données du pico-réseau réputées secrètes (comme l'adresse MAC de certains participants, opération appelée *Fingerprinting*, ou encore la valeur d'horloge du pico-réseau), contribuant à dévoiler ensuite le plan de sauts de fréquence utilisé.

Mise en oeuvre n°1 : *Fingerprinting* actif par procédure d'*Inquiry*

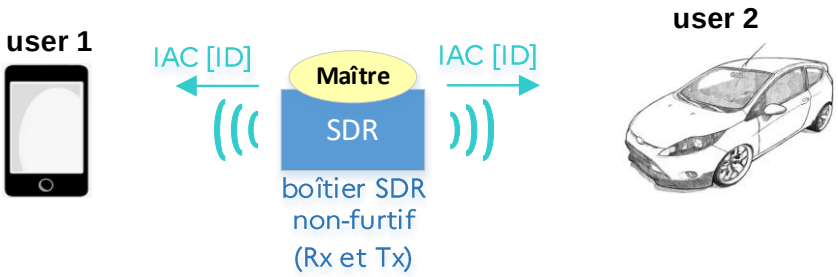

Figure 5 : Boîtier SDR utilisé comme émetteur Bluetooth en mode *General Inquiry*

Avec cette première approche schématisée en Figure 5, il s'agit de récupérer l'adresse MAC (BD_ADDR) d'un dispositif Bluetooth visé (par exemple le smartphone *user 1*) en déroulant la procédure protocolaire de *General Inquiry*, utilisée classiquement par un équipement Bluetooth en phase amont (préalablement à l'établissement d'un pico-réseau) pour découvrir son environnement radio proche.

Un module de radio logicielle (appelé SDR), placé à proximité radio de l'équipement Bluetooth qu'on cherche à identifier (*user 1*), est configuré comme futur maître d'un pico-réseau à établir : à la recherche des participants potentiels à un pico-réseau Bluetooth (car situés à sa portée radio), le boîtier SDR émet une succession (sur différentes fréquences, conformément à l'algorithme d'EVF) de courts messages (tous identiques) de type ID portant un code d'accès générique appelé GIAC dans le cadre de la procédure de *General Inquiry* : il n'est donc dans ce cas pas furtif d'un point de vue radio.

Tout équipement Bluetooth configuré comme « découvrable » (propriété réglable via un paramètre de configuration) recevant correctement ce message GIAC est alors tenu, dans un rôle de futur esclave, de répondre en déclinant en retour son identité complète par envoi d'un message de type *Frequency Hop Synchronization* (FHS), comme illustré sur la Figure 6.

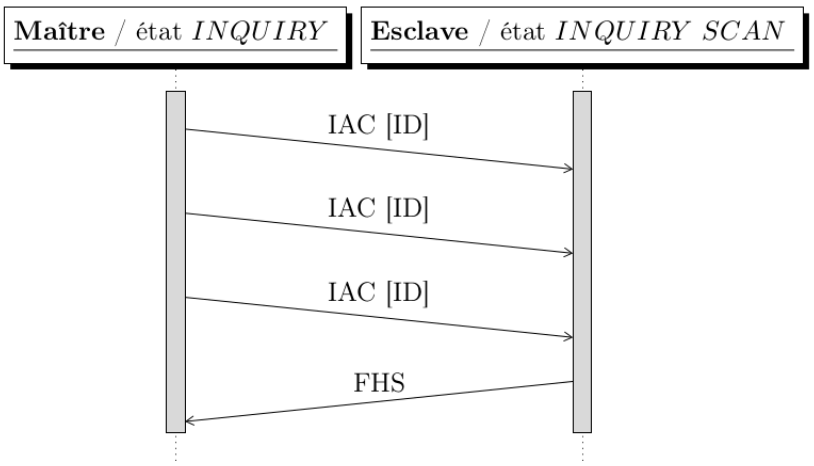

Figure 6 : Procédure de *General Inquiry*

Le message FHS reçu par le maître, dont la partie charge utile est illustrée en Figure 7, contient un grand nombre d'informations sur l'équipement Bluetooth émetteur de ce message, parmi lesquelles son adresse physique BD_ADDR complète sur 6 octets (par concaténation des champs LAP, UAP et NAP comme présentés en Figure 3), objet de la recherche de *Fingerprinting*.
Le message FHS renseigne également sur la valeur d'horloge (cf. champ CLK_{27-2}) courante de l'émetteur du message.

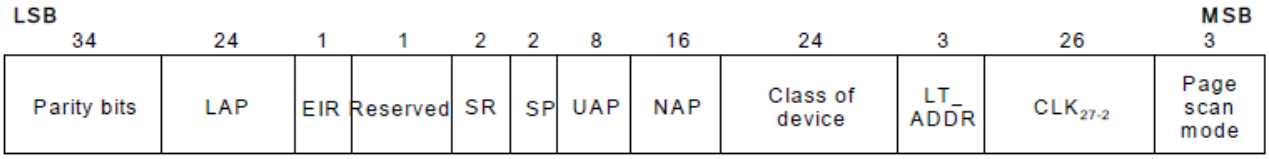

Figure 7 : Format de la charge utile d'un message FHS

Le module SDR jouant le rôle du maître doit ici être capable à la fois d'émettre (envoi de message ID portant un GIAC) et de recevoir (réception de message(s) FHS).

Cette 1ère mise en oeuvre est, certes, simple à réaliser, mais présente cependant plusieurs défauts :

- Elle n'est pas discrète puisque le module SDR interagit ici avec le dispositif Bluetooth qu'on cherche à identifier en lui envoyant une requête : il y a donc trace d'un échange protocolaire et de transmissions radio).

- Elle ne peut fonctionner que sous condition que l'équipement Bluetooth visé soit configuré en mode « découvrable » (d*iscoverable*), sans quoi ce dernier ne répondra pas aux requêtes d'*Inquiry*.

- Enfin, il n'est pas garanti que l'équipement Bluetooth répondant aux requêtes de GIAC soit l'équipement initialement visé : un autre dispositif Bluetooth présent également à proximité radio du module SDR interrogateur (par exemple l'équipement « *user 2* » sur la Figure 5) et défini en mode « découvrable » risque lui aussi de répondre aux requêtes GIAC en envoyant une réponse sous forme de paquet FHS.

Mise en œuvre n°2 : *Fingerprinting* passif par écoute de pico-réseaux actifs

La deuxième méthode présentée dans cette section est plus ambitieuse et vise à surmonter les deux défauts majeurs de la méthode 1, à savoir rester furtif (pas d'émission radio ni interaction protocolaire avec les équipements recherchés) et être capable d'identifier des équipements quand bien même ceux-ci sont définis en mode « non-découvrables », et ce sans avoir à compter sur la capture de paquets FHS.

Présentée en Figure 8, elle consiste à utiliser un boîtier SDR large bande pour capturer et enregistrer de manière passive et donc furtive (pas d'émission radio, boîtier utilisé en Rx uniquement avec capture d'échantillons IQ vers un fichier) des signaux radio émis dans un pico-réseau Bluetooth déjà établi où différents participants synchronisés peuvent échanger des données.

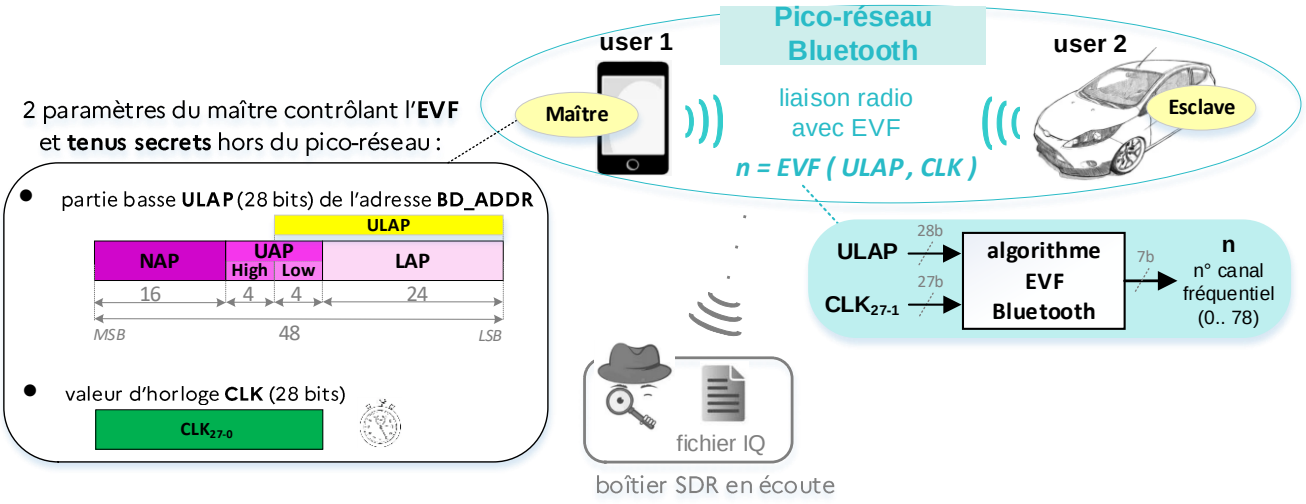

Figure 8 : Écoute passive sur un pico-réseau Bluetooth

Comme schématisé en Figure 9, il est alors possible, à l'aide d'une application de traitement du signal large bande dans l'espace temps-fréquence, d'exploiter les échantillons IQ reçus par une chaîne de démodulation en bande de base, développée à partir des spécifications Bluetooth.

Après différents traitements spécifiques (synchronisation, détection des paquets Bluetooth, opération de déblanchiment par FB, vérification de l'intégrité des parties *Header* et *Payload* par tentatives de décodage en FB des champs HEC et CRC, …), il est possible d'identifier les différents paquets transitant sur l'interface radio puis d'en extraire certaines informations cachées contrôlant l'algorithme EVF générant le motif de sauts de fréquence utilisé en Bluetooth, à savoir l'adresse physique Bluetooth BD_ADDR du maître du pico-réseau ainsi que sa valeur d'horloge, comme décrit plus précisément dans les 2 sous-sections suivantes.

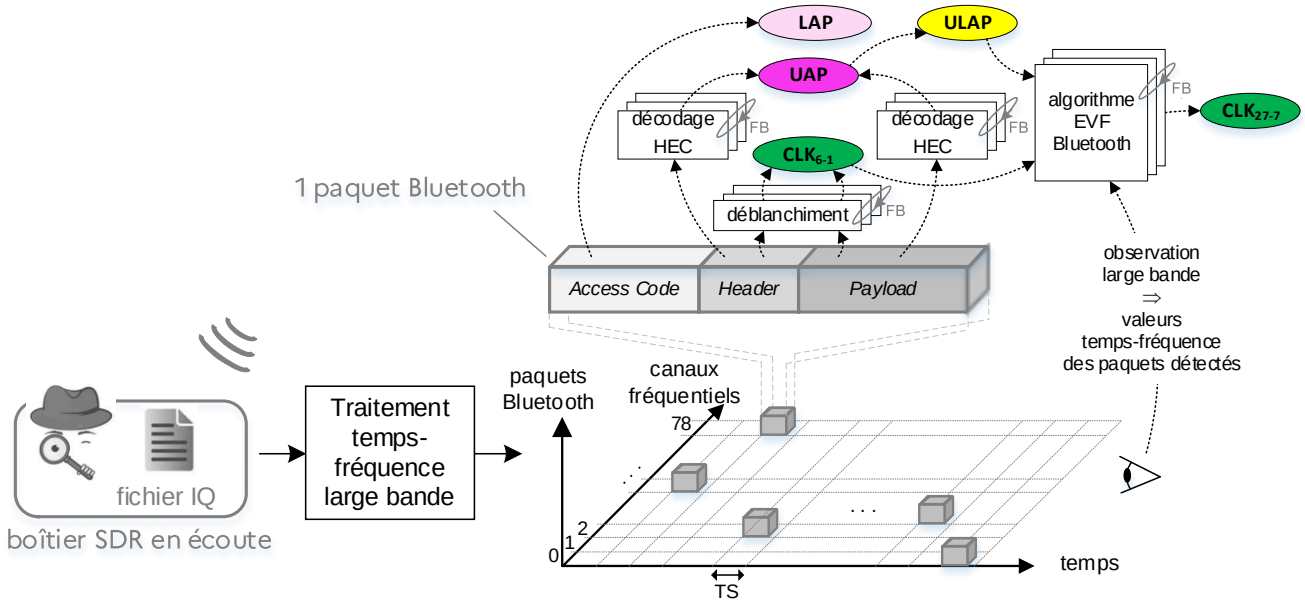

Figure 9 : Traitements large bande basés sur une écoute passive d'un pico-réseau Bluetooth permettant de dévoiler adresse BD_ADDR et horloge du maître, et par conséquent le schéma d'EVF

Challenge n°1 : extraction de l'adresse BD_ADDR (1ère donnée cachée)

Le 1er défi est de réussir à dévoiler l'adresse physique complète (BD_ADDR, de taille 6 octets, cf. Figure 3) du maître du pico-réseau Bluetooth de manière passive.
Ceci est rendu possible par une suite de traitements utilisant les différentes portions temporelles d'un paquet intercepté:

- la partie basse (LAP) de l'adresse BD_ADDR, de taille 24 bits, peut être directement récupérée en clair dans la portion de code d'accès (*Access Code)* transmise systématiquement au début de chaque paquet.

- la partie médiane (UAP), de taille 8 bits, peut être retrouvée car utilisée comme valeur initiale chargée dans les LFSR servant au calcul de détection d'erreur de transmission par ajout de bits de parité au sein des portions *Header* (bits HEC) et *Payload* (bits CRC). Le blanchiment appliqué à l'émission sur ces 2 portions nécessite de procéder côté réception à l'opération duale de déblanchiment, et ce à l'aveugle dans le cas d'une telle écoute, c'est-à-dire sans connaître les 6 bits d'horloge utilisés pour rendre pseudo-aléatoire et secrète cette étape : ceci est aisément surmonté par FB avec calcul et gestion de 2^6 (64) contextes en parallèle, la valeur des 6 bits d'horloge (CLK_{6-1}) menant au bon décodage des champs HEC et CRC étant au passage également révélée à l'issue du déblanchiment.

- la partie haute (NAP) de l'adresse BD_ADDR, enfin, est facilement déduite des valeurs LAP et UAP par une simple table de correspondance.

À noter que par post-traitement de paquets interceptés sur un pico-réseau établi, seule l'adresse MAC du maître peut être dévoilée car seule cette valeur est alors utilisée comme code d'accès unique (appelé CAC) pour tous les paquets échangés sur le pico-réseau, qu'ils transitent du maître vers l'esclave ou dans le sens dual.

En utilisant un module SDR large bande capable de suivre l'ensemble des canaux fréquentiels Bluetooth, on peut de plus identifier plusieurs pico-réseaux Bluetooth en parallèle, et donc potentiellement identifier des dizaines d'équipements Bluetooth (les maîtres de ces différents pico-réseaux) en un temps limité en se plaçant dans des zones assez denses où apparaissent de manière possiblement éphémère des réseaux Bluetooth, comme par exemple près d'un réseau autoroutier (cf. [R3] et échanges Bluetooth entre smartphones et systèmes audio de voitures).

Challenge n°2 : extraction de la valeur d'horloge (2ème donnée cachée)

L'accès au schéma des sauts de fréquence, permettant ensuite de se synchroniser sur les communications Bluetooth au sein d'un pico-réseau établi, est possible sous réserve de relever un 2ème challenge : réussir à dévoiler la valeur complète (28 bits) du signal d'horloge (CLK) du pico-réseau Bluetooth.

Comme dessiné sur la Figure 9, reste à ce stade à déterminer la valeur de 21 bits d'horloge (CLK_{27-7}) puisque le LSB CLK_0 est égal à 0 et que la valeur des 6 bits CLK_{6-1} est connue à l'issue de l'étape de déblanchiment par FB (objet du challenge n°1).

Comme présenté en [R2], ceci peut être réalisé par écoute sur un unique canal fréquentiel (parmi les 79 possibles), suite à interception d'un nombre réduit de paquets Bluetooth (4 typiquement).
Connaissant la portion ULAP d'adresse physique du pico-réseau en écoute (résultat du challenge n°1) et par mesure additionnelle des écarts temporels de réception entre les paquets Bluetooth capturés, un algorithme de recherche exhaustive (par FB donc) balayant l'ensemble des valeurs possibles de bits d'horloge non-encore déterminées (reste 21 bits d'entropie, à savoir CLK_{27-7}) et itérant sur chaque paquet reçu converge rapidement (en 4 itérations typiquement) vers l'unique valeur d'horloge pouvant expliquer la séquence de paquets interceptés sur le canal fréquentiel d'observation choisi et aux instants mesurés. La valeur complète du signal d'horloge (CLK) est alors dévoilée, donnant accès au plan des futurs sauts de fréquence.

La convergence vers une unique valeur d'horloge après un nombre réduit (4 typiquement) de paquets interceptés se justifie par le fait que l'ensemble des 79 canaux Bluetooth disponibles pour un pico-réseau établi sont sélectionnés, par spécification, de manière équiprobable par l'algorithme d'EVF : l'observation, à un instant donné, d'un paquet Bluetooth sur un numéro de canal fréquentiel donné généré par l'algorithme déterministe d'EVF Bluetooth ne peut ainsi s'expliquer que par la configuration à cet instant d'une valeur d'horloge parmi un jeu de valeurs dont le cardinal ne représente qu' 1/79 ème de l'ensemble des valeurs d'horloge possibles.
Ainsi, à chaque allongement de l'observation via la capture d'un nouveau paquet Bluetooth, le nombre de valeurs d'horloges susceptibles d'expliquer l'observation globale générée par l'algorithme d'EVF est divisé par 79 : l'aléa sur la détermination de la valeur d'horloge est donc en moyenne diminué de 6.3 bits[2] à chaque nouveau paquet Bluetooth intercepté. Avec une indétermination restante de 21 bits sur la valeur d'horloge à l'issue du déblanchiment, seules 4 itérations[3] (et donc 4 paquets reçus) se révèlent en général nécessaires pour aboutir à la bonne et unique valeur d'horloge recherchée du pico-réseau Bluetooth étudié.

Dans l'hypothèse où l'on dispose d'une acquisition SDR large bande (comme supposé ici et indiqué sur la Figure 9), le dévoilement de la valeur d'horloge se fait sensiblement de la même manière mais beaucoup plus rapidement : chaque paquet intercepté est désormais tagué avec 2 attributs (n° de TS comme index temporel, et n° de canal Bluetooth comme index fréquentiel), et la recherche par FB de la seule valeur d'horloge capable d'expliquer cette observation large bande aboutit typiquement après captures de 4 paquets Bluetooth.
La différence appréciable étant qu'il suffit d'une acquisition radio 79 fois plus courte (en termes de temps) puisqu'on dispose alors d'une vue large bande sur les 79 canaux, et non plus sur un seul canal comme c'est le cas dans [R2] : l'extraction d'une valeur d'horloge exigeant par exemple une acquisition de 8 secondes en observation mono-canal ne nécessitera qu'environ 100 ms avec une acquisition SDR large bande contenant tous les canaux Bluetooth.

[2] 6.3 (bits) correspondant au logarithme (en base 2) de la valeur 79
[3] À raison d'une diminution d'aléa de 6.3 bits par itération, les 21 bits d'entropie sont réduits à 0 en 4 itérations puisque 4 x 6.3 > 21)

Glossaire

AES	*Advanced Encryption Standard*
BD_ADDR	*Bluetooth Device Address* (adresse physique d'un équipement Bluetooth, communément appellée adresse MAC également, et codée sur 6 octets)
BR	*Basic Rate*
CAC	*Channel Access Code*
CCM	*Counter with Cipher block chaining Message authentication code*
CLK	*Clock* ⇔ valeur d'horloge du pico-réseau Bluetooth
CRC	*Cyclic Redundancy Check*
DH	Diffie-Hellman
EDR	*Enhanced Data Rate*
EVF	Évasion de Fréquence
FB	Force Brute
FHS	*Frequency Hop Synchronization*
FHSS	*Frequency Hopping Spread Spectrum*
Fingerprinting	Identification de l'adresse BD_ADDR (MAC) d'un équipement Bluetooth
GIAC	General IAC (code d'accès de valeur prédéfinie - 0x9E8B33 - servant à appeler l'ensemble des dispositifs Bluetooth en phase d'*Inquiry*)
HEC	*Header Error Check*
IAC	*Inquiry Access Code*
ID	*Identity* (un type de message de contrôle Bluetooth)
IoT	*Internet of Things* (Internet des Objets)
ISM	Industriel, Scientifique et Médical (bande de fréquence)
IQ	Nom des échantillons complexes de signal numérisés par le module SDR, I désignant la voie réelle en phase (*In phase*) et Q la voie imaginaire en quadrature (*Quadrature Phase*). Le fichier IQ apparaissant sur les Figure 8 et Figure 9 contient l'ensemble des échantillons IQ numérisés par le boîtier SDR.
LAP	*Lower Address Part* (portion de poids faible d'une adresse BD_ADDR)
LFSR	*Linear Feedback Shift Register*
LMP	*Link Manager Protocol*
MAC	*Media Access Control*
n°	numéro
NAP	*Non-significant Address Part* (portion de poids fort d'une adresse BD_ADDR)
PL	*Payload*
Rx	Réception
SDR	*Software Defined Radio* <=> radio logicielle
TS	*Time Slot*
Tx	Transmission
UAP	*Upper Address Part* (portion centrale d'une adresse BD_ADDR)
ULAP	UAP (*Least Significant Byte*) + LAP

Références bibliographiques

[R1] D. Spill & A. Bittau, 2007 : "*Bluesniff : Eve meets Alice and Bluetooth*"

[R2] A. Tabassam & S. Heiss, 2008 : "*Bluetooth Clock Recovery and Hop Sequence Synchronization Using Software Defined Radios*"

[R3] M. Cominelli et al., 2020 : "*Even Black Cats Cannot Stay Hidden in the Dark: Full-band De-anonymization of Bluetooth Classic Devices*"