Communiquer en BLE : Les pièges à éviter !

Alexis Duque @alexis0duque
Fabien Grenier @fabgrenier
@Rtone_Dev2M

Qui sommes nous ?

Fabien GRENIER

@fabgrenier
RTONE

Responsable de l'équipe Cloud&Mobile

Développeur Java/Web full stack

"Le handball c'est la vie."

Alexis DUQUE

@alexis0duque
RTONE

Tech lead soft embarqué

(vrai) Développeur full stack

"Nan, la course à pied c'est mieux."

Qui sommes nous ?

Fondé en 2007 par 3 ingénieurs

Expert en conception d'objets connectés

3 équipes hard, soft embarqué et Cloud&Mobile

Projets B2C et B2B

De la Startup aux grands groupes

Accompagnement complet du CdC à l'industrialisation

Just Dev It !

Roadmap

- Bluetooth Low Energy ?
- Quelles différences avec le Bluetooth ?
- Pourquoi tant de difficultés ?
- Le BLE en Actions !

Bluetooth Low Energy

2010 : Bluetooth Core Specification v4.0 for low power device

Mais ne remplace pas le Bluetooth : à ne pas mettre à toutes les sauces !

Spécificités

Faible bande passante : ~50 kbps

Faible latence (~10ms) et protocole “non connecté”

Chip radio presque toujours OFF

Très petits paquets : MTU de 20 octets

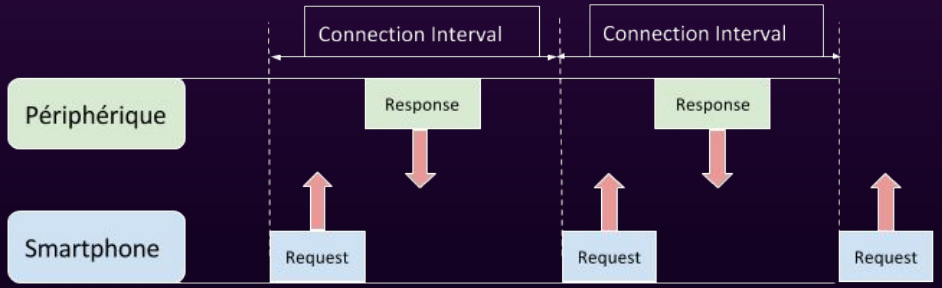
Vocabulaire

Connection Interval

Supervision Timeout

Slave Latency

Advertising Interval



Vocabulaire

Master

Client

Centrale

Scanner

Initiateur

Vocabulaire

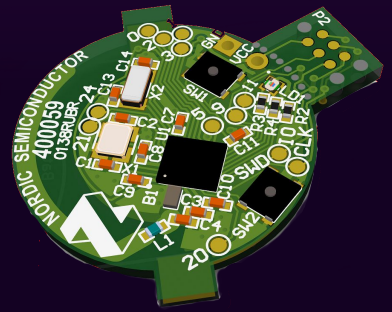
Slave

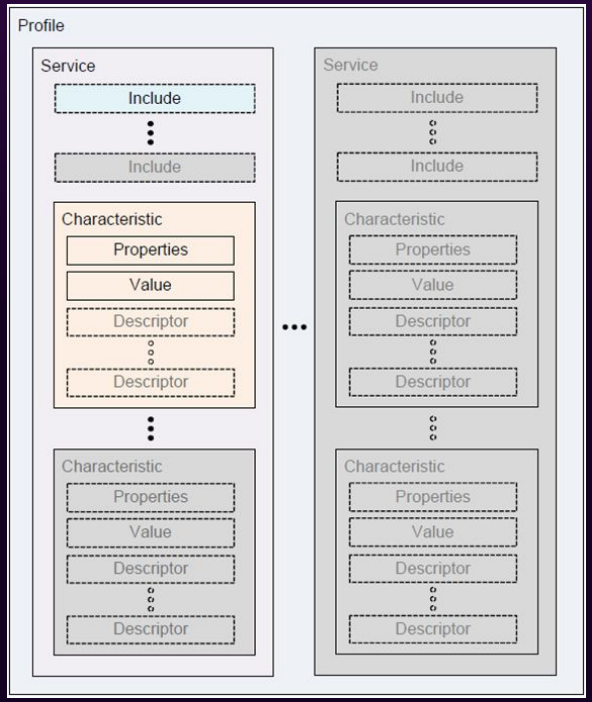
Périphérique

Advertiser

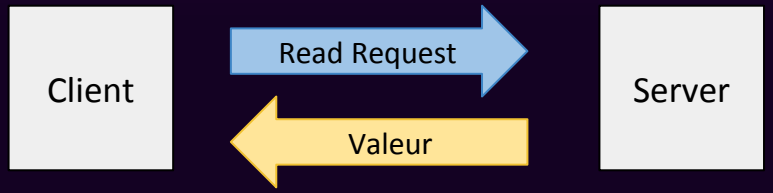
GATT

Serveur

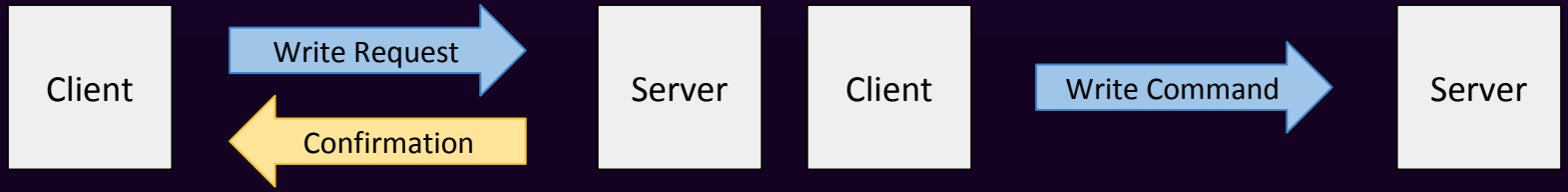




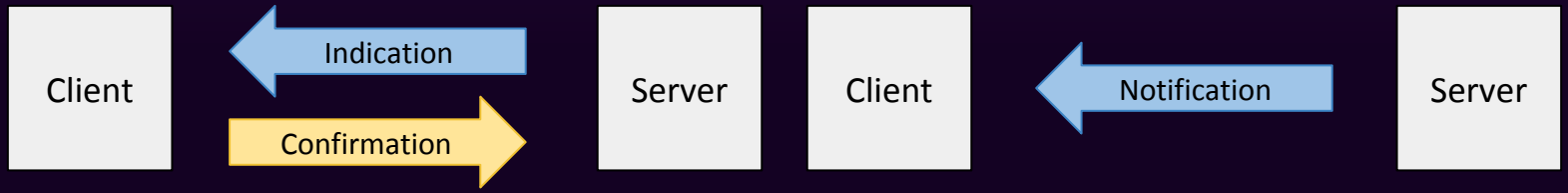
Parler à son objet



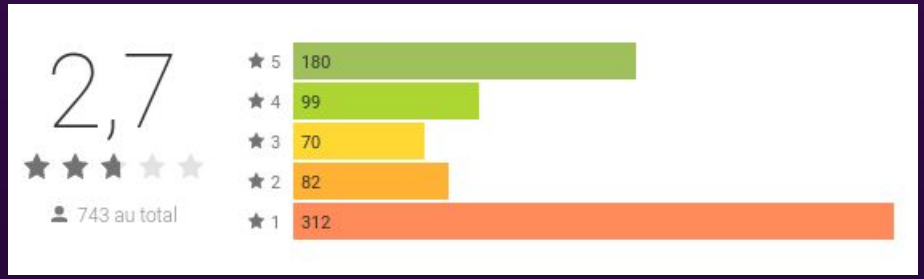
Parler à son objet



Parler à son objet



Un problème

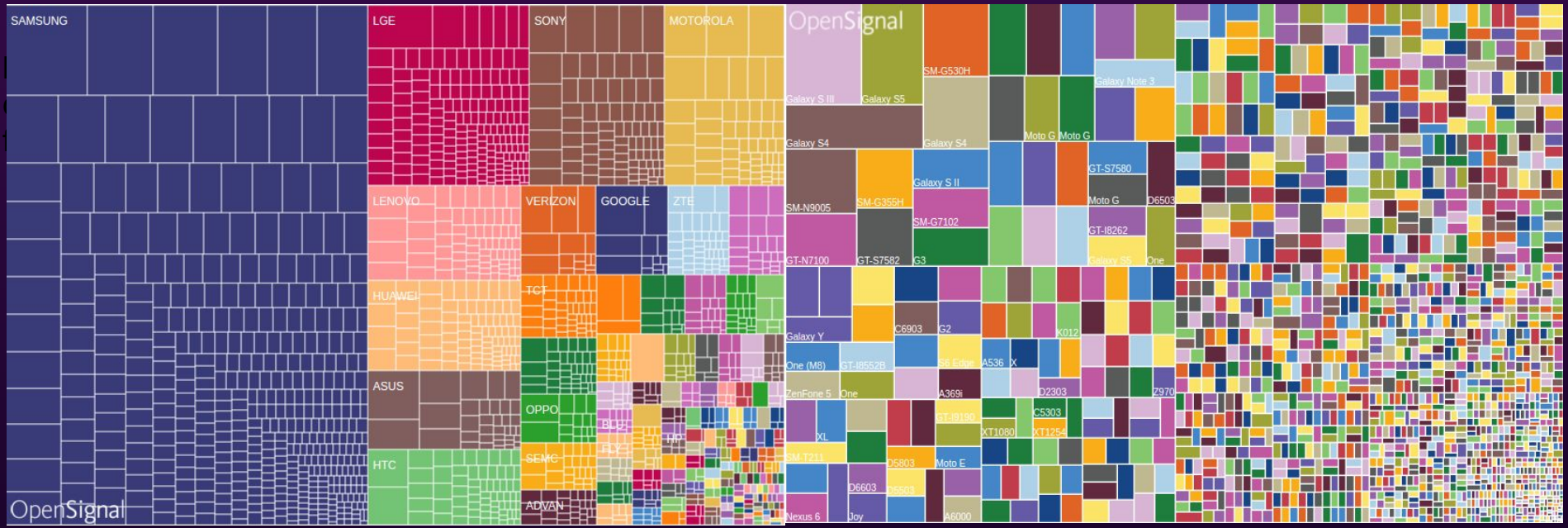

2,7
743 au total
5 180
4 99
3 70
2 82
1 312


27 mars 2016
Je ne arrive pas à me connecter avec mon gsm qu est ce qu il faut faire car au bluetooth je vois la c mais impossible
S 31 mars 2016
Essayez d'aller dans mon compte sur l'application et revalidez le modèle de cookeo, il devrait (parfois au bout de plusieurs essais) vous proposer le process d'association. Cordialement, L'équipe

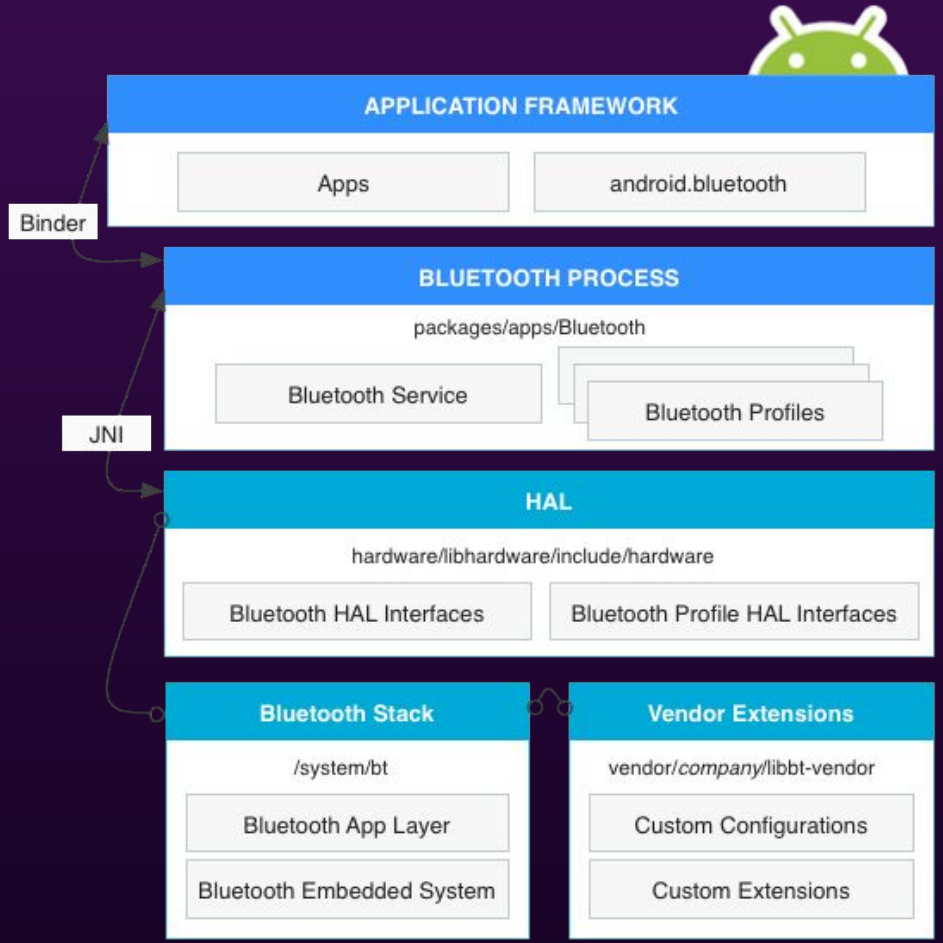

30 mars 2016
Depuis la maj la conextion bleutooth ne marche plus sur S4 association avec bleu conect refuse


David L 31 mars 2016
J'ai pu me connecter en Bluetooth une fois.... depuis ce n'est plus possible.... je commence à regretter mon achat...

Un problème



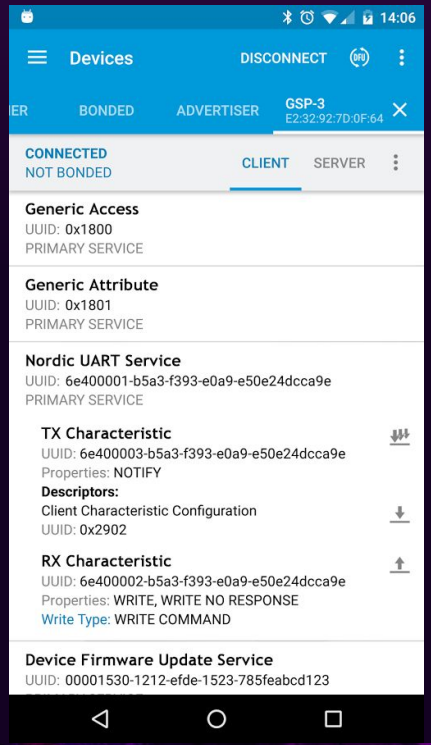
http://opensignal.com/reports/2015/08/android-fragmentation/

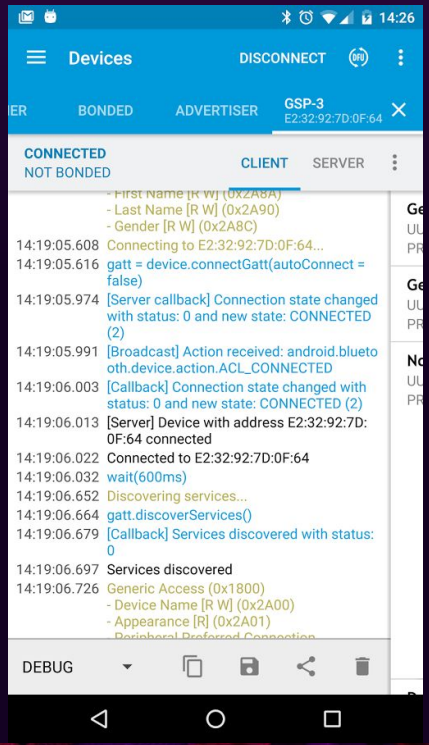

APPLICATION FRAMEWORK
Apps
android.bluetooth
Binder
BLUETOOTH PROCESS
packages/apps/Bluetooth
Bluetooth Service
Bluetooth Profiles
JNI
HAL
hardware/libhardware/include/hardware
Bluetooth HAL Interfaces
Bluetooth Profile HAL Interfaces
Bluetooth Stack
/system/bt
Bluetooth App Layer
Bluetooth Embedded System
Vendor Extensions
vendor/company/libbt-vendor
Custom Configurations
Custom Extensions

Les outils

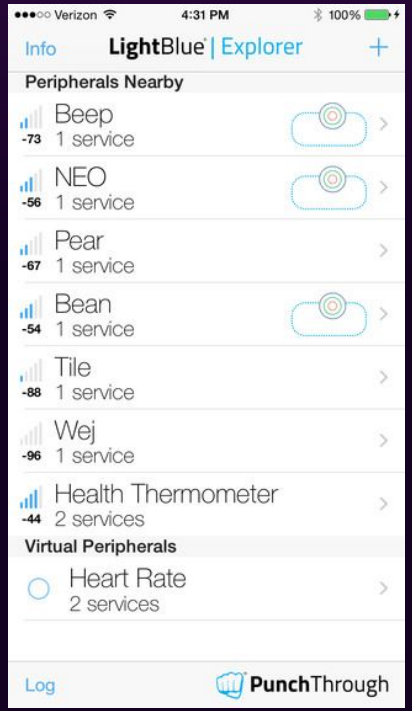
Des Applications

nRF Master Control Panel



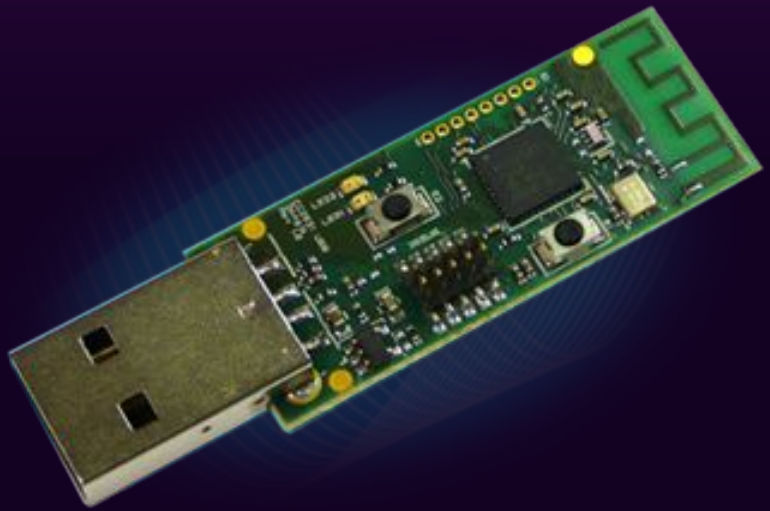


LightBlue



Sniffer BLE

TI CC2540 USB



Ubertooth

Protocole Analyzer

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header				AdvA	AdvData	CRC	RSSI (dBm)	FCS
					Type	TxAdd	RxAdd	PDU-Length					
185	+107495 =19154743	0x25	0x8E89BED6	ADV_IND	0	0	0	17	0x90D7EBB19299	02 01 05 07 02 03 18 02 18 04 18	0xEF5DA8	-57	OK

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header				InitA	AdvA
					Type	TxAdd	RxAdd	PDU-Length		
186	+367 =19155110	0x25	0x8E89BED6	ADV_CONNECT_REQ	5	0	0	34	0x001830EA965F	0x90D7EBB19299

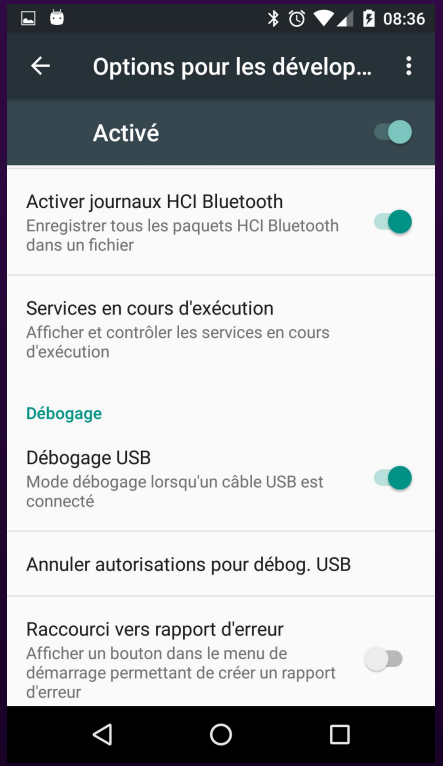
LLData (Part 1)					LLData (Part 2)					CRC	RSSI (dBm)	FCS
AccessAddr	CRCInit	WinSize	WinOffset	Interval	Latency	Timeout	ChM	Hop	SCA			
0x60850A1B	A7 7B 22	02	0x000F	0x0050	0x0000	0x07D0	1F FF FF FF FF	0x09	0x05	0x02DA48	-30	OK

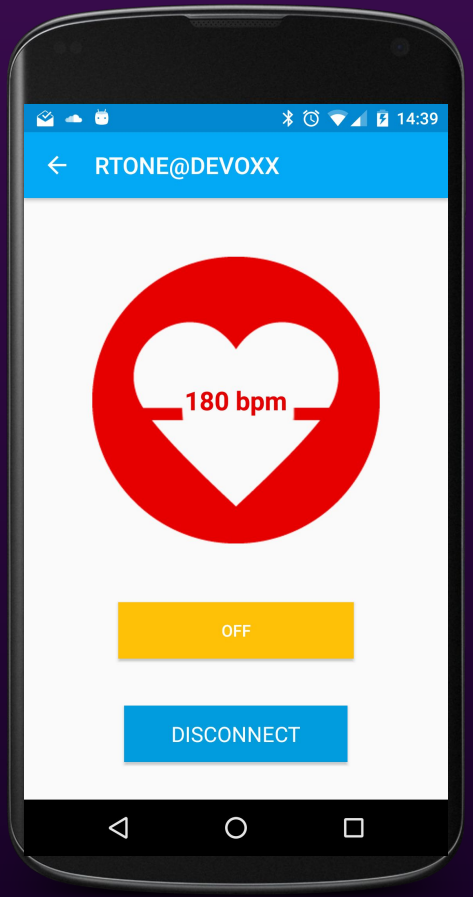
P.nbr.	Time (us)	Channel	Access Address	Data Type	Data Header					CRC	RSSI (dBm)	FCS
					LLID	NESN	SN	MD	PDU-Length			
187	+20891 =19176001	0x09	0x60850A1B	L2CAP-C	1	0	0	0	0	0x133A32	-31	OK

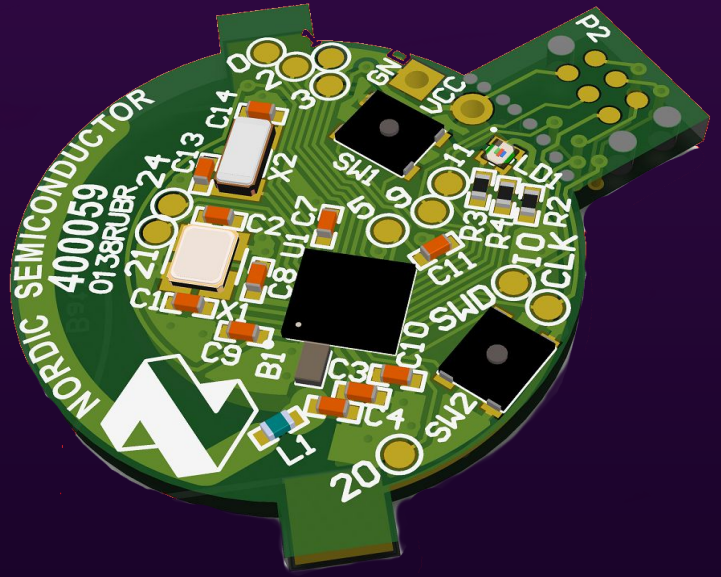
P.nbr.	Time (us)	Channel	Access Address	Data Type	Data Header					CRC	RSSI (dBm)	FCS
					LLID	NESN	SN	MD	PDU-Length			
188	+230 =19176231	0x09	0x60850A1B	L2CAP-C	1	1	0	0	0	0x133CE1	-50	OK

BTSnoop HCI Log

open-bluedroid-log.sh




14:39
RTONE@DEVOXX
180 bpm
OFF
DISCONNECT


NORDIC SEMICONDUCTOR
400059
0138RUBR
SWD
CLK
VCC
GND

Avant de commencer, des rappels ...

Scanner les périphériques à portée

Se connecter utilisant l'adresse MAC ou l'UUID

Explorer les services et caractéristiques disponibles

Sauvegarder les handles, pour les réutiliser !

Ecrire, Lire ou s'abonner aux notifications

Ne pas oublier de (bien) se déconnecter

Live Demo

Step 1 : Permissions

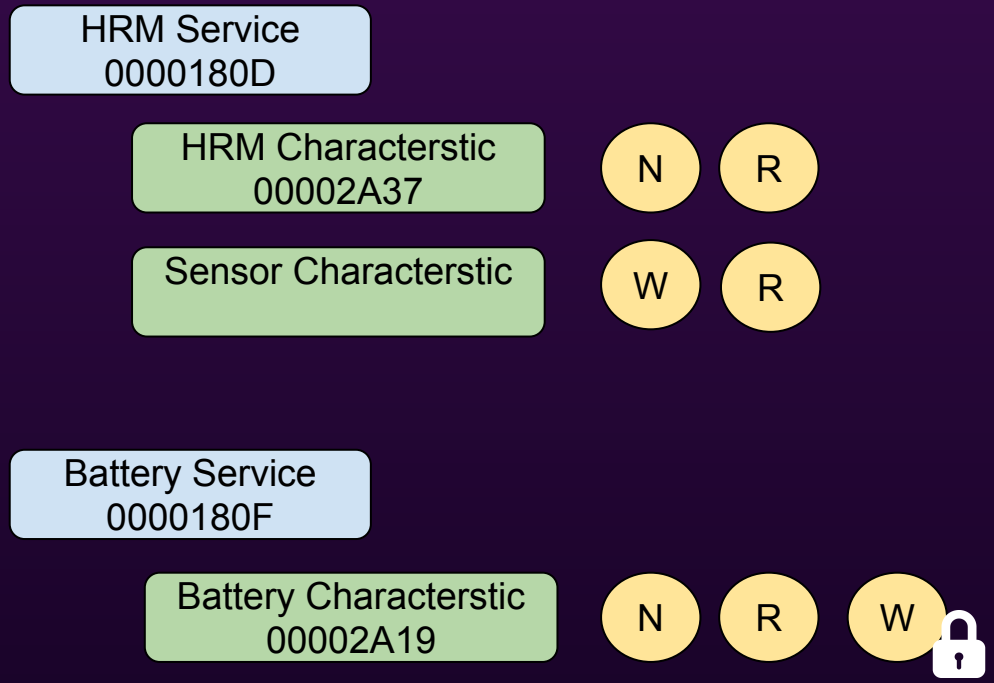
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION

android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN

Step 2 : Découverte des périphériques

Step 3 : Connexion

Step 4 : Inspecter les services



Step 5 : Lecture / Ecriture / Notif.

Step 6 : Déconnexion

Step 7 : Bonding, Chiffrement, MITM


STEVEN SPIELBERG PRESENTS
BACK TO THE FUTURE
PG
A ROBERT ZEMECKIS FILM
OUTATIME

A suivre ...

Bluetooth 4.2

- Bande passante x2.5
- Sécurité renforcée
- Retrocompatibilité

Android N

Web Bluetooth API & Physical Web

Les derniers tips ...

Utiliser un Nexus pour le développement puis tester sur un maximum de marque

Éviter tant que possible le bonding et chiffrement protocolaire, préférer un chiffrement applicatif

cf. https://lacklustre.net/bluetooth/Ryan_Bluetooth_Low_Energy_USENIX_WOOT.pdf

Questions ?

Alexis Duque - alexisd@rtone.fr
Fabien Grenier - fabien@rtone.fr
www.rtone.fr

https://github.com/alexisduque/tia-ble-devoxx16.git

Venez voir notre Quickie sur le VLC !

Des LEDs pour remplacer votre routeur WIFI ?

Par Alexis Duque
Vendredi 12:25 - 12:40
Salle Neuilly 253