

CRESITT INDUSTRIE
Centre de Ressources
Technologiques en Électronique

CRT  centre de
ressources
technologiques



Hacking Évaluation Cybersécurité



Le CRT CRESITT est soutenu par :



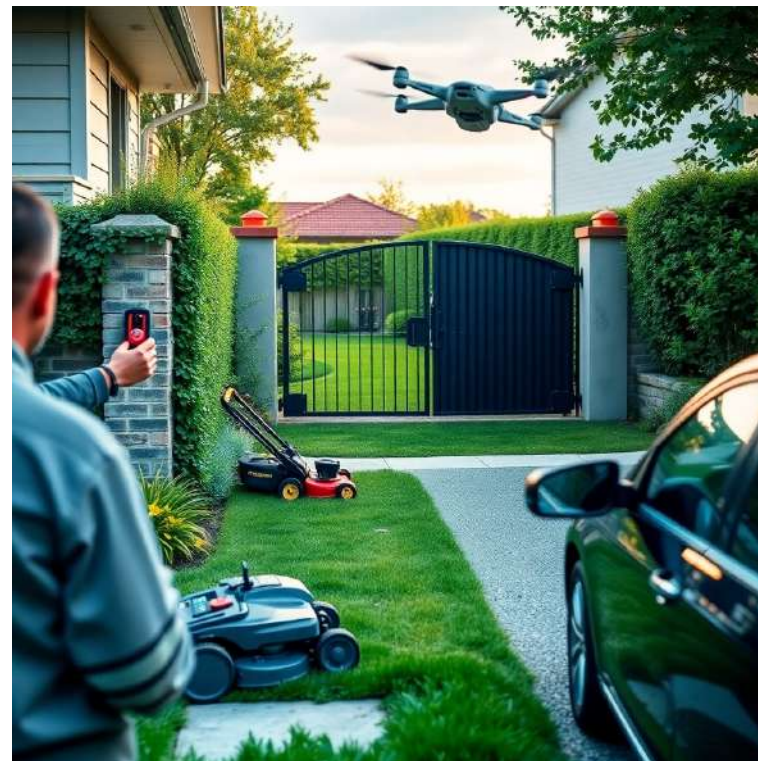
Cofinancé par
l'Union européenne



L'action de diffusion technologique est cofinancée par l'Union européenne.
L'Europe s'engage en région Centre-Val de Loire avec le Fonds européen de développement régional.



Src : <https://www.manutan.be>



Src : <https://muryou-aigazou.com/fr>

- Soutenu par l'État via l'Agence Nationale de la Recherche : France 2030
- Rôle :
 - Renforcer la formation et la sensibilisation à la cybersécurité en région Centre-Val de Loire
- Actions autour du sujet de l'hygiène numérique:
 - Formation de formateurs (BTS, Bac Pro Ciel, Ingénieurs CNRS)
 - Médiation auprès des collèges et lycées
 - **Travaux de Recherche en Cybersécurité sur les failles des objets connectés (collaboration CRESITT Industrie)**
 - Développement d'une plate-forme de gestion de crise et de compétitions CTF
- Membres

- Hacks :
 - Protocole utilisé
 - Infrarouge : Télécommandes
 - RFID : Badge
 - Ondes radios
 - 433Mhz : Capteur de pression de roue de voiture
 - 869Mhz : Alarme incendie
 - 2.4Ghz : Prise commandée / Capteurs



- Boîte noire :
 - Vérification des informations sérigraphiées
 - Récupération des descriptions et manuel d'utilisation
 - Vérification chez les fabricants des informations disponibles
 - Vérification en labo des communications mises en œuvre
 - Mise en situation
 - Capture des échanges
 - Analyses
 - Attaques par différentes méthodes





Appareils testés

- Horloge murale
- Lampe musicale Bluetooth



Capture et rejeu des signaux

Capture

Matériel utilisé :

- Télécommande infrarouge
- Oscilloscope
 - Lecroy Wavesurfer 104Xs

Système Hacking



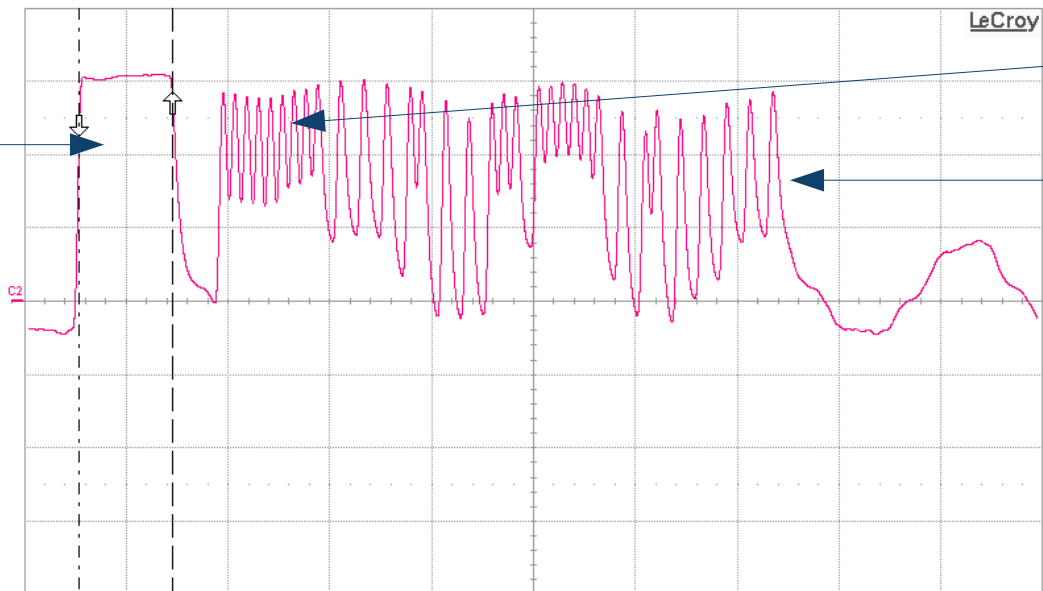
CC2541DK-RC
kit Texas Instrument



Capture du signal analogique aux bornes de la led IR de la télécommande Texas Instrument

Ampoule : appui bouton rouge de sa télécommande

Absence de modulation

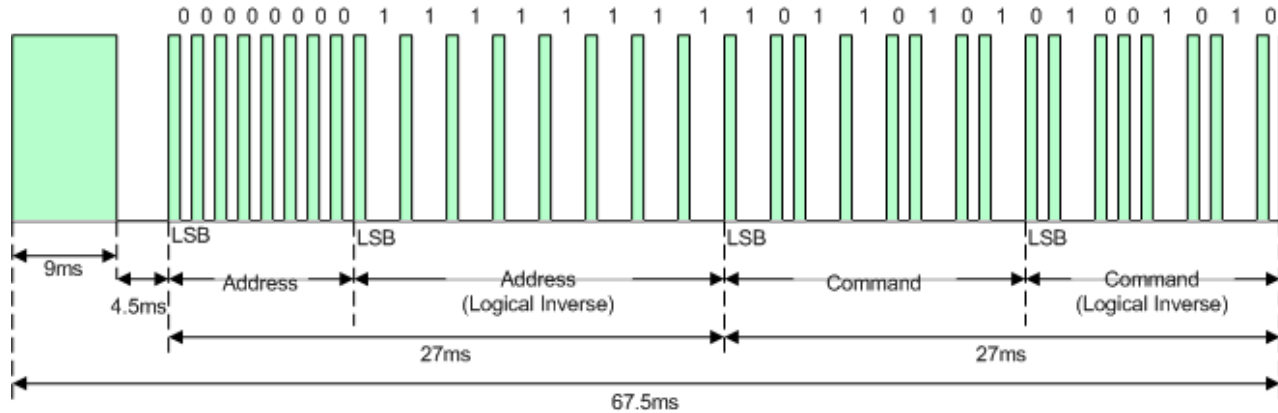


Modulation + signal

Modulation sans signal

C2 F BWL DCIM
200 mV/div
0.00 mV ofst
L 453.43 mV
T 569.75 mV
Δy 116.32 mV

Tbase -44.8 ms Déclench C2:AC
10.0 ms/div Arrêter 234 mV
10.0 kS 100 kS/s Edge Positive
X1= 170 μs ΔX= 9.16 ms
X2= 9.33 ms 1/ΔX= 109.2 Hz



Exemple de trame du protocole NEC (version 1)

Corrélation des signaux – Forme et timing identique

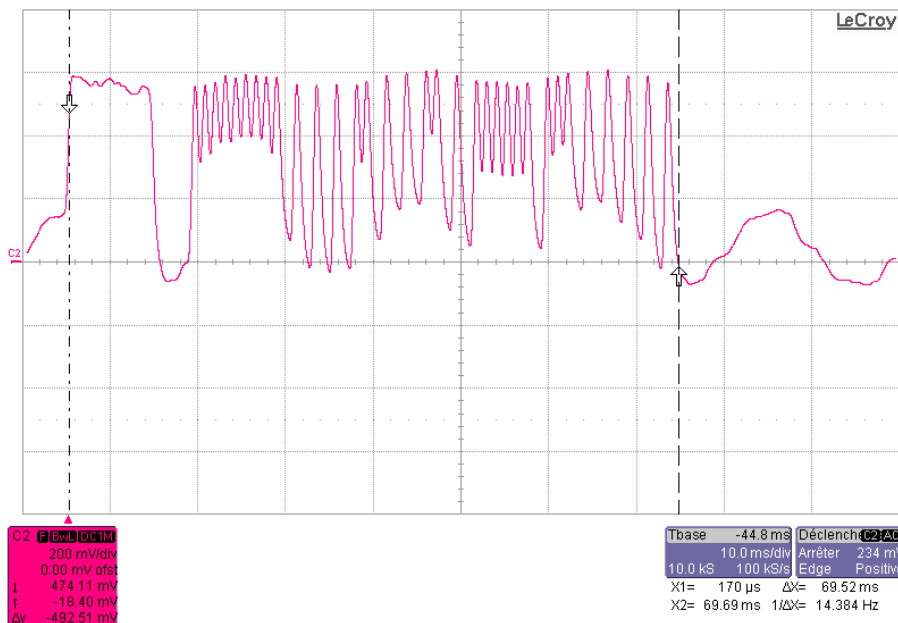
Code identifié : protocole NEC version 2 (LSB)

9ms => 9.16ms

27ms => adresse 26.36ms et commande 27.35ms

67.5ms => 67.63ms

Période de répétition donnée à 109ms et mesurée à 109ms



Bouton bleu

Décodage :

bouton rouge : 0000 0000 1111 0111 0010 0000 1101 1111 soit en hexa adresse=0xEF00 cmd=0xFB04
 bouton vert : 0000 0000 1111 0111 1010 0000 0101 1111 soit en hexa adresse=0xEF00 cmd=0xFC05
 bouton bleu : 0000 0000 1111 0111 0110 0000 1001 1111 soit en hexa adresse=0xEF00 cmd=0xF906
 bouton V+ : 0000 0000 1111 0111 0110 1000 1001 0111 soit en hexa adresse=0xEF00 cmd=0xF916
 bouton V- : 0000 0000 1111 0111 0010 1000 1101 0011 soit en hexa adresse=0xEF00 cmd=0xFB14

Systèmes Infrarouge



Protocole et codes identifiés

Génération possible des signaux

Commande possible des objets

Possibilité d'éblouir le capteur pour empêcher la réception

Système Hacking



CC2541DK-RC
kit Texas Instrument

Systèmes Infrarouge



Système Hacking



Enregistrer le signal infrarouge

Rejeu du signal

Capteur de pression de pneu TPMS

(Tire Pressure Monitoring
System)



*(Équipement obligatoire depuis juillet
2024 pour certains types de véhicules)*

- Réception des trames émises par le capteur
 - Application rtl_433
 - Support de 277 protocoles sur le 433Mhz
 - TPMS (schrader, renault, citroën...)
 - Honda car key
 - Sensor Lacross
 - Wireless Door Bell
 - ...
- Utilisation du HackRF One et de l'application Universal Radio Hacker
 - Analyse spectrale
 - Enregistrement des trames
 - Analyse et rejeu des trames

Système Hacking



HackRF One
+ rtl_433
+ urh
+ sources rtl_433

```

kali@kali:~$ cat /dev/ttyUSB0
Fichier Actions Éditer Vue Aide
model : Aearth-324Spider type : TPMS id : 2615a292
Flags : 51 Pressure : 1 kPa Temperature: -44 C status : 98 Integrity : CHECKSUM
-----
time : 2025-04-29 10:23:08
model : Renault type : TPMS id : 873d97
Flags : 31 pressure_kPa: 41.2 kPa temperature_C: 21 C Integrity : CRC
-----
time : 2025-04-29 10:23:08
model : Renault type : TPMS id : 873d97
Flags : 31 pressure_kPa: 41.2 kPa temperature_C: 21 C Integrity : CRC
-----
time : 2025-04-29 10:23:09
model : Renault type : TPMS id : 873d97
Flags : 31 pressure_kPa: 41.2 kPa temperature_C: 21 C Integrity : CRC
-----
time : 2025-04-29 10:23:09
model : Renault type : TPMS id : 873d97
Flags : 31 pressure_kPa: 41.2 kPa temperature_C: 21 C Integrity : CRC
-----
time : 2025-04-29 10:23:10
model : Renault type : TPMS id : 873d97
Flags : 31 pressure_kPa: 41.2 kPa temperature_C: 21 C Integrity : CRC
-----
time : 2025-04-29 10:23:10
model : Renault type : TPMS id : 873d97
Flags : 31 pressure_kPa: 41.2 kPa temperature_C: 21 C Integrity : CRC
-----
time : 2025-04-29 10:23:11
model : Renault type : TPMS id : 873d97
Flags : 31 pressure_kPa: 42.0 kPa temperature_C: 21 C Integrity : CRC
-----
time : 2025-04-29 10:23:11
model : Renault type : TPMS id : 873d97
Flags : 31 pressure_kPa: 42.0 kPa temperature_C: 21 C Integrity : CRC
-----
time : 2025-04-29 10:23:12
model : Renault type : TPMS id : 38
Flags : 31 pressure_kPa: 19.0 C Humidity : 39 % Integrity : CHECKSUM
Channel : 1 Battery : 1
-----
time : 2025-04-29 10:23:12
model : Renault type : TPMS id : 4d930056
Flags : 31 pressure_kPa: 205.0 kPa Temperature: 86.0 F Integrity : CHECKSUM
Pressure : 205.0 kPa Temperature: 86.0 F flags : 4d930056 ID : 838251
-----
time : 2025-04-29 10:23:13
model : Renault type : TPMS id : ab09d8
Flags : 31 pressure_kPa: 268.5 kPa temperature_C: 22 C Integrity : CRC
-----
time : 2025-04-29 10:23:14
model : Renault type : TPMS id : ab09d8
Flags : 31 pressure_kPa: 268.5 kPa temperature_C: 22 C Integrity : CRC
  
```

```

time : 2025-04-29 09:31:19
model : Hyundai-VDO type : TPMS id : 11e29251
state : 38 flags : 0 repetition: 1 pressure : 23 kPa temp : 162 C maybe_battery: 241 Integrity : CRC
-----
time : 2025-04-29 09:33:10
model : Truck type : TPMS id : 611e2925
wheel : 16 Pressure : 286 kPa Temperature: 9 C State? : 2 Flags? : 1 Integrity : CHECKSUM
-----
time : 2025-04-29 09:51:02
model : Toyota type : TPMS id : f1e617de
status : 128 pressure_PSI: 36.500 temperature_C: 21.000 Integrity : CRC
-----
time : 2025-04-29 09:52:32
model : Hyundai-VDO type : TPMS id : 11e29251
state : 38 flags : 0 repetition: 1 pressure : 12 kPa temp : 184 C maybe_battery: 191 Integrity : CRC
-----
time : 2025-04-29 09:53:35
model : Citroen type : TPMS id : 11e29251
state : 26 flags : 0 repeat : 1 Pressure : 7 kPa Temperature: 187 C maybe_battery: 70 Integrity : CHECKSUM
-----
time : 2025-04-29 09:53:44
model : Truck type : TPMS id : 411e2925
wheel : 16 Pressure : 286 kPa Temperature: 253 C State? : 2 Flags? : 1 Integrity : CHECKSUM
-----
time : 2025-04-29 09:53:44
model : Citroen type : TPMS id : 11e29251
state : 24 flags : 0 repeat : 1 Pressure : 29 kPa Temperature: 189 C maybe_battery: 219 Integrity : CHECKSUM
-----
time : 2025-04-29 09:55:17
model : Truck type : TPMS id : 611e2925
wheel : 16 Pressure : 415 kPa Temperature: 55 C State? : 2 Flags? : 1 Integrity : CHECKSUM
-----
time : 2025-04-29 09:56:54
model : Abarth-124Spider type : TPMS id : 2611e292
flags : 51 Pressure : 1 kPa Temperature: -45 C status : 251 Integrity : CHECKSUM
-----
time : 2025-04-29 09:56:58
model : Citroen type : TPMS id : 11e29251
state : 26 flags : 0 repeat : 1 Pressure : 7 kPa Temperature: 205 C maybe_battery: 166 Integrity : CHECKSUM
-----
time : 2025-04-29 09:57:08
model : Ford type : TPMS id : 2411e292
Pressure : 20.25 PSI Temperature: -55.0 C Moving : 0 Learn : 0 code : 510106 unknown : 00 unknown_3 : 2 Integrity : CHECKSUM
  
```

```

time : 2025-04-30 12:27:41
model : Froove-Security
Channel : 3 State : OFF Unit : 3 Group : 0
-----
time : 2025-04-30 12:27:41
model : Hexa-Security House Code: 9424898
Channel : 3 State : OFF Unit : 3 Group : 0
-----
time : 2025-04-30 12:27:41
model : KlikAanKlikUit-Switch
Unit : 0 Group Call: No id : 9424898 Command : Off Dim : No Dim Value : 0
-----
time : 2025-04-30 12:27:41
model : Froove-Security
Channel : 3 State : OFF Unit : 3 Group : 0
-----
time : 2025-04-30 12:27:41
model : Hexa-Security House Code: 9424898
Channel : 3 State : OFF Unit : 3 Group : 0
-----
time : 2025-04-30 12:27:41
model : KlikAanKlikUit-Switch
Unit : 0 Group Call: No id : 9424898 Command : Off Dim : No Dim Value : 0
-----
time : 2025-04-30 12:27:41
model : KlikAanKlikUit-Switch
Unit : 0 Group Call: No id : 9424898 Command : Off Dim : No Dim Value : 0
-----
time : 2025-04-30 12:27:41
model : Froove-Security
Channel : 3 State : OFF Unit : 3 Group : 0
-----
time : 2025-04-30 12:27:41
model : Froove-Security
Channel : 3 State : OFF Unit : 3 Group : 0
-----
time : 2025-04-30 12:27:41
model : Froove-Security
Channel : 3 State : OFF Unit : 3 Group : 0
-----
time : 2025-04-30 12:27:41
model : Hexa-Security House Code: 9424898
Channel : 3 State : OFF Unit : 3 Group : 0
-----
time : 2025-04-30 12:27:41
model : Hexa-Security House Code: 9424898
Channel : 3 State : OFF Unit : 3 Group : 0

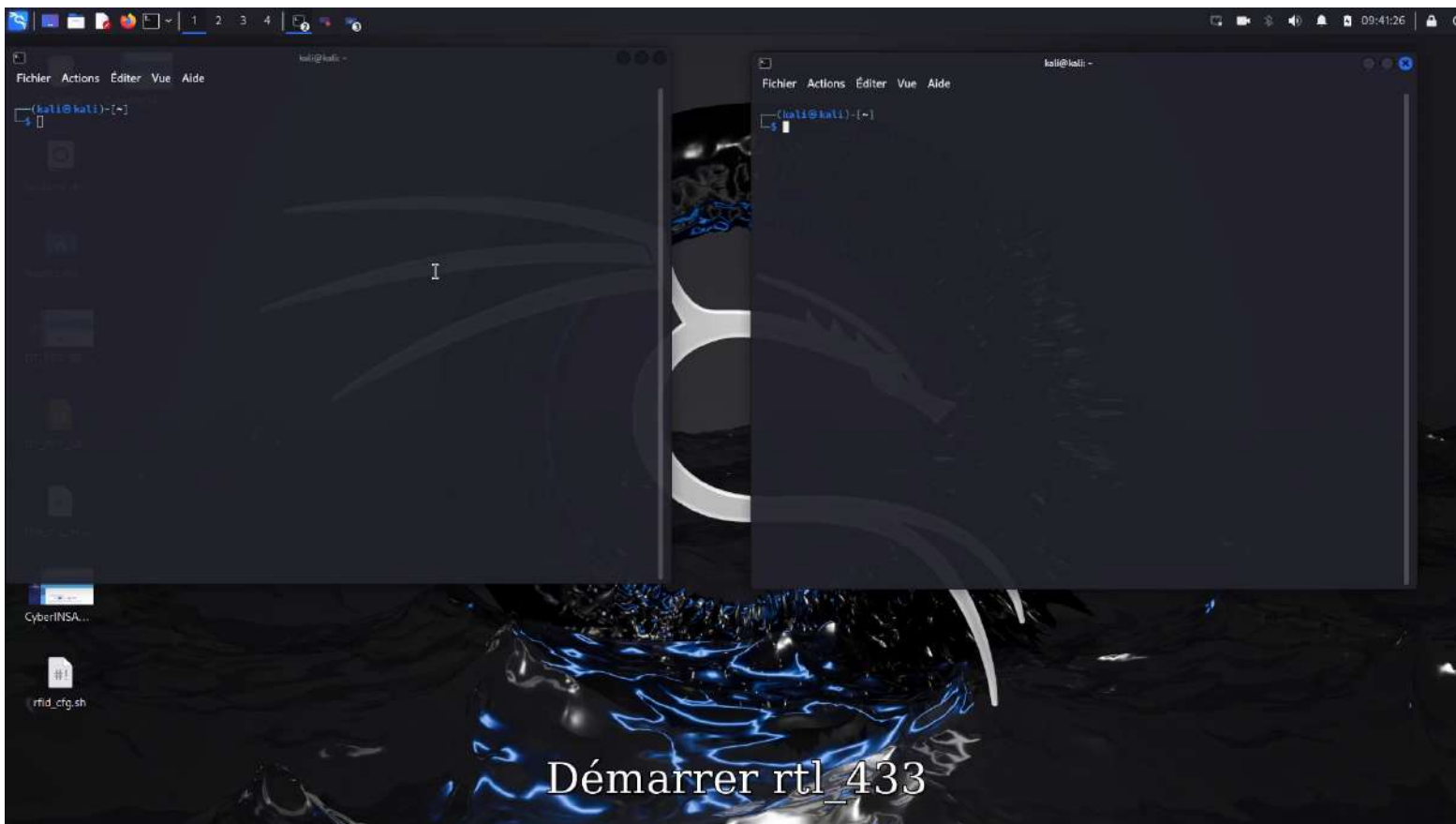
```

Télécommande ?

KlikAanKlik
Uit

Commutateur
On/OFF





Détecteur incendie

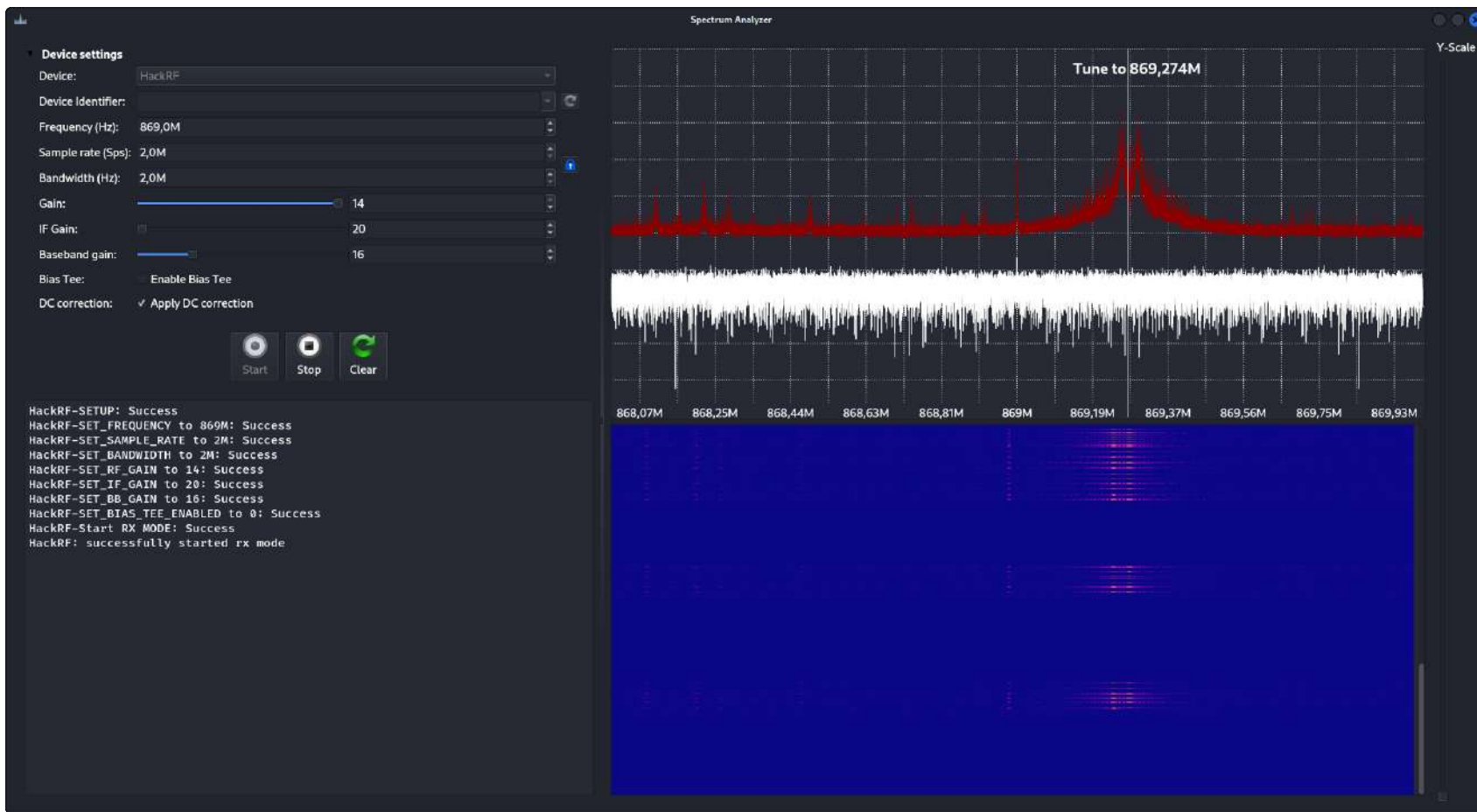


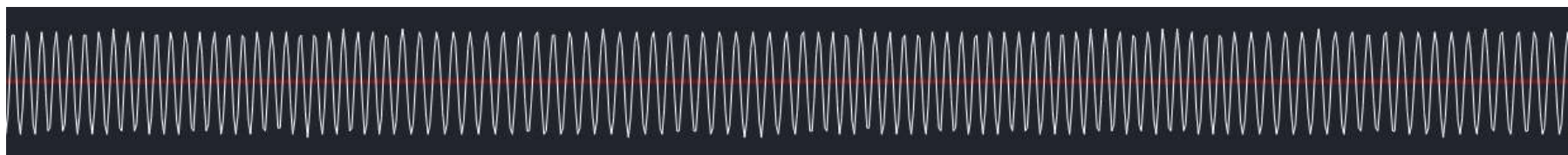
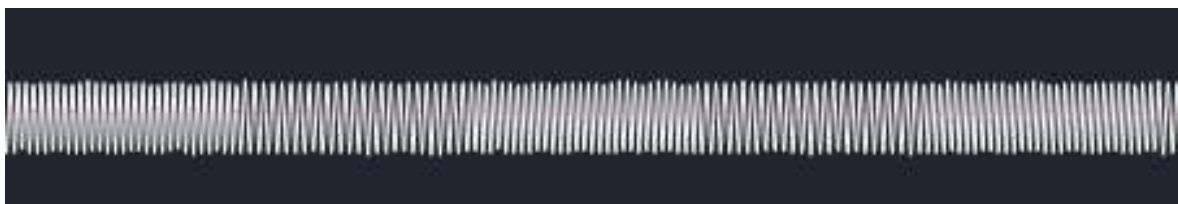
- **Fréquences :**
 - Bluetooth, Wi-Fi, 869Mhz : passerelle
 - 869Mhz : détecteurs
- Déploiement des détecteurs seuls
- Mise en réseau (appairage) des 3 capteurs
- Observation fréquence d'émission
- Capture et rejeu (869Mhz)

Système Hacking

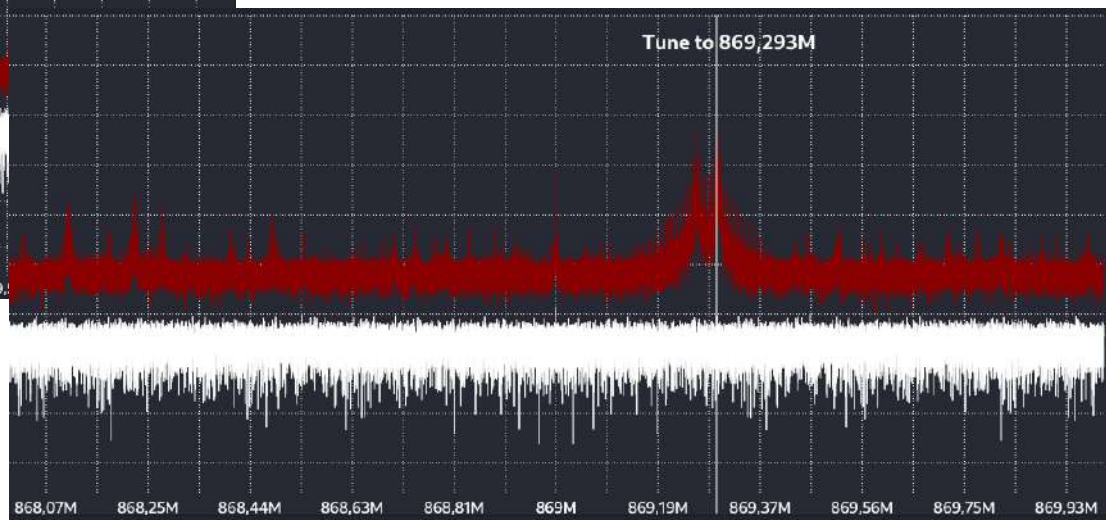
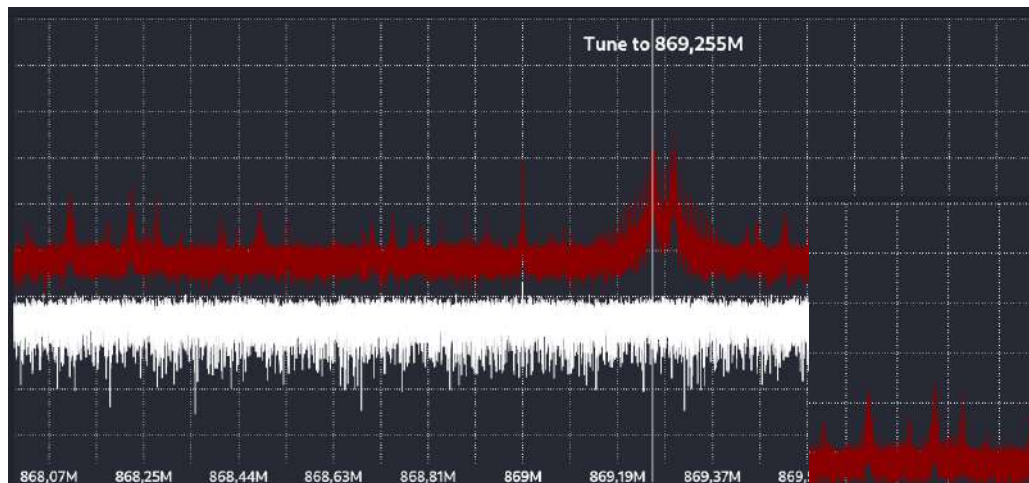


USRP B210
+ Universal Radio
Hacker (urh)





**Modulation de
fréquence**



**Modulation de
fréquence : 254Khz et
295Khz**

	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
23	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
24	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
25	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
26	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
27	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
28	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
29	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
30	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
31	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
32	1	6	2	6	0	9	8	a	5	e	5	7	8	7	a	6	8	0	0												
33	1	6	2	6	0	9	8	a	5	e	5	7	e	8	2	f	0	0	0												
34	1	6	2	6	0	9	8	a	5	e	5	7	e	8	2	f	0	0	0												
35	1	6	2	6	0	9	8	a	5	e	5	7	8	5	a	8	8	0	0												
36	1	6	2	6	0	9	8	a	5	e	5	7	8	5	a	8	8	0	0												
37	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

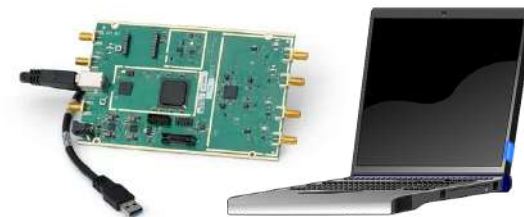
37 trames – Seules les 5 dernières transmettent de l'information

La dernière trame est beaucoup plus longue et seuls les 10 derniers bytes différent de 0x05

Détecteur incendie



Système Hacking



USRP B210
+ urh

Le rejeu des trames enregistrées permet de déclencher l'alarme

Système ZigBee



- Acquisition des trames ZigBee
- Déchiffrement des trames
- Rejeu
- Spoofing
 - Côté passerelle
 - Côté capteurs / actionneur

Système Hacking



**HackRF One
+ gnu Radio
+ wireshark
+ scripts python**

WIRESHARK

 python™



+  **GNU Radio**
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Réception ZigBee - Capture .cap

Analyse trame
récupération payload

Modification,
reconstruction et
chiffrement du payload

Mise en forme 802.15.4
Émission ZigBee

No.	Time	Source	Destination	Protocol	Length	Info
18	38.546929	0x0000	0xfa83	ZigBee	54	Data, Dst: 0xfa83, Src: 0x0000
19	38.547360			IEEE 802.15.4	5	Ack
20	38.573661	0xfa83	0x0000	ZigBee	82	Data, Dst: 0x0000, Src: 0xfa83
21	38.574160			IEEE 802.15.4	5	Ack

```

▶ Frame 18: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▶ IEEE 802.15.4 Data, Dst: 0xfa83, Src: 0x0000
▼ ZigBee Network Layer Data, Dst: 0xfa83, Src: 0x0000
  ▶ Frame Control Field: 0x0248, Frame Type: Data, Discover Route: Enable, Security Data
    Destination: 0xfa83
    Source: 0x0000
    Radius: 30
    Sequence Number: 205
    [Extended Source: TexasIns_00:2e:1e:8b:d7 (00:12:4b:00:2e:1e:8b:d7)]
    [Origin: 1]
  ▼ ZigBee Security Header
    ▶ Security Control Field: 0x28, Key Id: Network Key, Extended Nonce
      Frame Counter: 23359
      Extended Source: TexasIns_00:2e:1e:8b:d7 (00:12:4b:00:2e:1e:8b:d7)
      Key Sequence Number: 0
      Message Integrity Code: 5f7b7e77
    ▶ [Expert Info (Warning/Undecoded): Encrypted Payload]
  ▼ Data (17 bytes)
    Data: 2f4309fc33994c498050fa298f7b47917d
    [Length: 17]
  
```

```

0000 61 80 c0 52 1a 83 fa 00 00 40 02 83 fa 00 00 1e  a b . . . H . . . .
0010 cd 28 3f 5b 00 00 d7 8b 1e 2e 00 4b 12 00 09  2 (? [ . . . . . K . . .
0020 43 90 7c 33 99 4c 49 80 50 fa 29 8f 7b 47 91 7d  c 3 - I T P . ) ( G .
0030 5f 7b 7e 77 f0 fb                                [ - W .
  
```

Trames déchiffrées

Clef par défaut fabricant de puces non modifiée !!!!

Trames chiffrées

No.	Time	Source	Destination	Protocol	Length	Info
18	38.546029	0x0000	0xfa83	ZigBee HA	54	ZCL: Read Attributes, Seq: 91
19	38.547360			IEEE 802.15.4	5	Ack
20	38.573661	0xfa83	0x0000	ZigBee HA	82	ZCL: Read Attributes Response, Seq: 01
21	38.574160			IEEE 802.15.4	5	Ack

```

▶ Frame 18: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▶ IEEE 802.15.4 Data, Dst: 0xfa83, Src: 0x0000
▶ ZigBee Network Layer Data, Dst: 0xfa83, Src: 0x0000
- ZigBee Application Support Layer Data, Dst Endpt: 1, Src Endpt: 1
  ▶ Frame Control Field: Data (0x00)
    Destination Endpoint: 1
    Cluster: Electrical Measurement (0x0b04)
    Profile: Home Automation (0x0104)
    Source Endpoint: 1
    Counter: 127
  ▼ ZigBee Cluster Library Frame, Command: Read Attributes, Seq: 91
    ▶ Frame Control Field: Profile-wide (0x10)
      Sequence Number: 91
      Command: Read Attributes (0x00)
      Attribute: RMS Voltage (0x0505)
      Attribute: RMS Current (0x0508)
      Attribute: Active Power (0x050b)
  
```

```

0000 60 01 04 0b 04 01 01 7f 40 5b 00 05 05 00 05 0b  10 5b 00 05 05 00 05 0b
0010 05
  
```

No.	Time	Source	Destination	Protocol	Length	Info
18	38.546929	0x0000	0xfa83	ZigBee	54	Data, Dst: 0xfa83, Src: 0x0000
19	38.547360			IEEE 802.15.4	5	Ack
20	38.573661	0xfa83	0x0000	ZigBee	82	Data, Dst: 0x0000, Src: 0xfa83
21	38.574100			IEEE 802.15.4	5	Ack

```

▶ Frame 20: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
▶ IEEE 802.15.4 Data, Dst: 0x0000, Src: 0xfa83
▼ ZigBee Network Layer Data, Dst: 0x0000, Src: 0xfa83
  ▶ Frame Control Field: 0x1a48, Frame Type: Data, Discover Route: Enable, Security, Destination, Extended Source Data
    Destination: 0x0000
    Source: 0xfa83
    Radius: 38
    Sequence Number: 39
    Destination: TexasIns_00:2e:1e:8b:d7 (00:12:4b:00:2e:1e:8b:d7)
    Extended Source: IeeeRegi_2b:60:05:7a:37 (70:b3:d5:2b:00:05:7a:37)
  ▼ ZigBee Security Header
    ▶ Security Control Field: 0x28, Key Id: Network Key, Extended Nonce
      Frame Counter: 18797
      Extended Source: IeeeRegi_2b:60:05:7a:37 (70:b3:d5:2b:00:05:7a:37)
      Key Sequence Number: 0
      Message Integrity Code: 2b328280
    ▶ [Expert Info (Warning/Undecoded): Encrypted Payload]
  ▼ Data (29 bytes)
    Data: 6681bba2eea7f0901475a71c40f9a5e9ea943d96b60aea5...
    [Length: 29]
  
```

6600	61 88 c2 62 1a 00 00 83 fa 48 1a 00 00 83 fa 1e	a . b H
6610	27 d7 8b 1e 2e 00 4b 12 00 37 7a 05 60 2b d5 b3	f K . . 7z
6620	70 28 55 4d 00 00 37 7a 05 60 2b d5 b3 70 00 80	p (UM . . 7z p f
6630	81 6b a2 ee a7 10 96 14 79 a7 1c 40 15 a5 89 ea	o u
6640	84 3d 90 0b 89 ae a9 e7 fc 7a 07 95 2b 32 82 80	o z +2+ .
6650	1a 7c	

Trames déchiffrées

Clef par défaut fabricant de puces non modifiée !!!!

Trames chiffrées

No.	Time	Source	Destination	Protocol	Length	Info
18	38.546929	0x0000	0xfa83	ZigBee HA	54	ZCL: Read Attributes, Seq: 91
19	38.547360			IEEE 802...	5	Ack
20	38.573661	0xfa83	0x0000	ZigBee HA	82	ZCL: Read Attributes Response, Seq: 91
21	38.574100			IEEE 802...	5	Ack

```

▶ Frame 20: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
▶ IEEE 802.15.4 Data, Dst: 0x0000, Src: 0xfa83
▶ ZigBee Network Layer Data, Dst: 0x0000, Src: 0xfa83
▼ ZigBee Application Support Layer Data, Dst Endpt: 1, Src Endpt: 1
  ▶ Frame Control Field: Data (0x40)
    Destination Endpoint: 1
    Cluster: Electrical Measurement (0x0b04)
    Profile: Home Automation (0x0104)
    Source Endpoint: 1
    Counter: 86
  - ZigBee Cluster Library Frame, Command: Read Attributes Response, Seq: 91
    ▶ Frame Control Field: Profile-wide (0x18)
      Sequence Number: 91
      Command: Read Attributes Response (0x01)
    ▶ Status Record, UInt16: 230
    ▶ Status Record, UInt16: 11
    ▶ Status Record, UInt16: 0
  
```

0900	49 01 04 0b 04 01 01 56 18 50 01 05 05 00 21 26	0 V [.
0910	30 08 05 00 21 0b 00 0b 05 09 21 00 00

Exemple : smart plug : ordre on

Trame sniffée :

61 88 c6 62 1a 83 fa 00 00 48 02 83 fa 00 00 1e cb 28 3d 5b 00 00 d7 8b 1e 2e 00 4b 12 00 00 4e 14 45 42 f6 b6 06 85 ee 85 87 b4 b9 6f 8b 10 15

61 88 c6 62 1a 83 fa 00 00 : entête protocole 802.15.4

48 02 83 fa 00 00 1e cb : NWK Header

28 3d 5b 00 00 d7 8b 1e 2e 00 4b 12 00 00 : NWK Aux Header

4e 14 45 42 f6 b6 06 85 ee 85 87 : Payload chiffré

b4 b9 6f 8b : MIC (Message Integrity Control) chiffré

10 15 : CRC

Payload déchiffré :

00 01 06 00 04 01 01 7e 01 5a 01 : Payload déchiffré (Application Support Layer (APS))

00 : type data

01 : destination endpoint 1

06 00 : cluster on/off

04 01 : home automation

01 : source endpoint 1

7e : compteur

01 : cluster specific

5a : numéro de séquence

01 : commande on

Modification pour envoi d'un ordre issu du HackRF

numéro de séquence 802.15.4 : 0xc6 => 0xd2

destination : 0xfa83 => 0x0000

source : 0x0000 => 0x3332

compteur de frame : 0x3d5b0000 => 0x3da00000

numéro de séquence Zigbee : 0xcb => 0xd0

payload chiffré : 4e 14 45 42 f6 b6 06 85 ee 85 87 => 8B 33 38 2C 30 24 F5 21 9F 80

B3

implique nouveau MIC : 0x84B69D2B

implique nouveau CRC : 0x6006

Nouvel ordre

61 88 d2 62 1a 00 00 33 32 48 02 83 fa 00 00 1e d0 28 3d a0 00 00 d7 8b 1e 2e 00 4b 12 00 00 8B 33 38 2C 30 24 F5 21 9F 80 B3 84 B6 9D 2B 60 06

Exemple : smart plug : ordre on

Trame sniffée :

61 88 c6 62 1a 83 fa 00 00 48 02 83 fa 00 00 1e cb 28 3d 5b 00 00 d7 8b 1e 2e 00 4b 12 00 00 4e 14 45 42 f6 b6 06 85 ee 85 87 b4 b9 6f 8b 10 15

61 88 c6 62 1a 83 fa 00 00 : entête protocole 802.15.4

48 02 83 fa 00 00 1e cb : NWK Header

28 3d 5b 00 00 d7 8b 1e 2e 00 4b 12 00 00 : NWK Aux Header

4e 14 45 42 f6 b6 06 85 ee 85 87 : Payload chiffré

b4 b9 6f 8b : MIC (Message Integrity Control) chiffré

10 15 : CRC

Payload déchiffré :

00 01 06 00 04 01 01 7e 01 5a 01 : Payload déchiffré (Application Support Layer (APS))

00 : type data

01 : destination endpoint 1

06 00 : cluster on/off

04 01 : home automation

01 : source endpoint 1

7e : compteur

01 : cluster specific

5a : numéro de séquence

01 : commande on

Modification pour envoi d'un ordre issu du HackRF

numéro de séquence 802.15.4 : 0xc6 => 0xd2

destination : 0xfa83 => 0x0000

source : 0x0000 => 0x3332

compteur de frame : 0x3d5b0000 => 0x3da00000

numéro de séquence Zigbee : 0xcb => 0xd0

payload chiffré : 4e 14 45 42 f6 b6 06 85 ee 85 87 => 8B 33 38 2C 30 24 F5 21 9F 80

implicite nouveau MIC : 0x84B69D2B

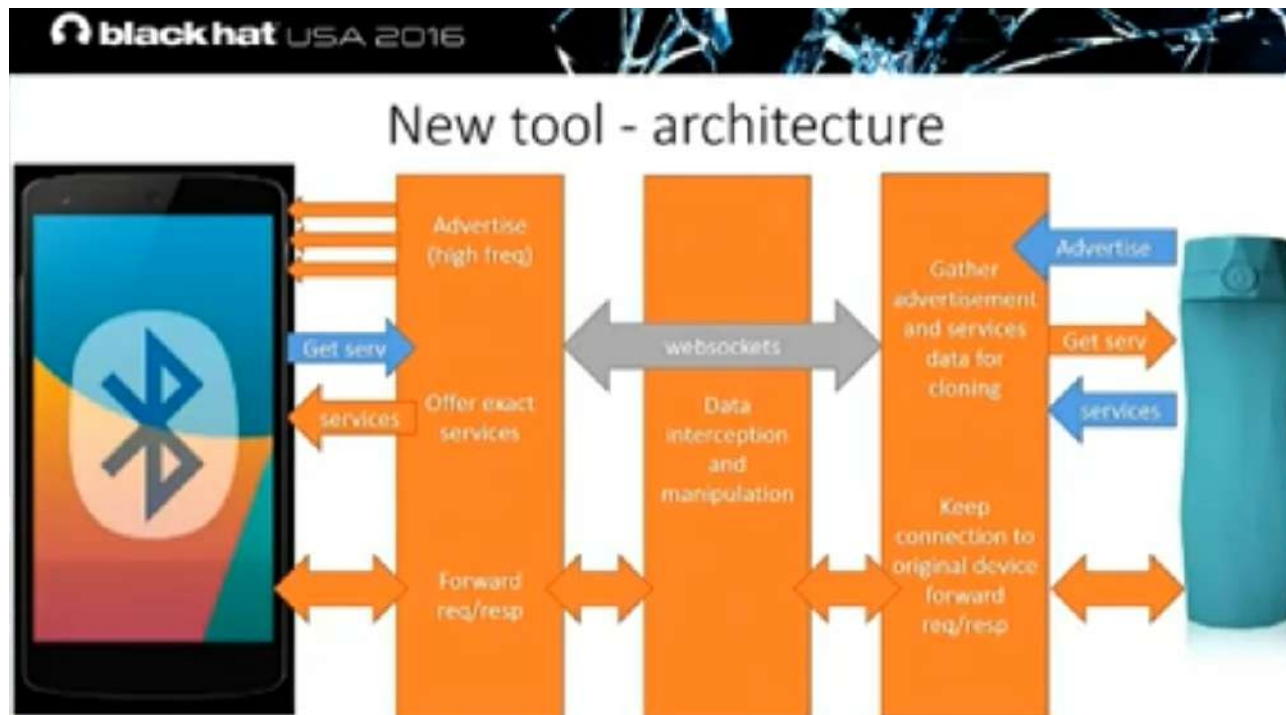
implicite nouveau CRC : 0x6006

B3

Nouvel ordre

61 88 d2 62 1a 00 00 33 32 48 02 83 fa 00 00 1e d0 28 3d a0 00 00 d7 8b 1e 2e 00 4b 12 00 00 8B 33 38 2C 30 24 F5 21 9F 80 B3 84 B6 9D 2B 60 06

Hack bluetooth Man In The Middle live sur le stand CRESITT



Mécanisme du MITM de gattacker présenté par Slawomir Jasek

- Conclusion
 - Solutions infrarouges simple à reproduire
 - Solutions radios
 - Clefs de chiffrement doivent être
 - Modifiables et modifiées
 - Uniques par élément
 - Robustes
 - Mettre en place des détections d'anomalies, remonter l'information, refuser la connexion, la valeur...
 - Se conformer au Cyber Resilience Act et aux normes cyber EN 18031, EN 303 645, NF EN/IEC 62443, NF EN/IEC 61508, NIST SP800-53...

- Création de Capture the Flag (CTF) orientés sécurité IoT
 - 10 challenges
- Création d'un « escape game »
 - Réutilisant une partie des challenges
- Conférence, démos... en lien avec la sécurité IoT