APSYS .Lab

Spark the future. Craft tomorrow.

LAAS CNRS

EXPLOITING WIRELESS KEYBOARDS FOR FUN AND PROFIT

TOULOUSE HACKING CONVENTION - 11 JUIN 2021

Romain CAYRE

rcayre@laas.fr / romain.cayre@airbus.com

AN **AIRBUS** COMPANY

CONTEXTE DE CES TRAVAUX

- Ancien étudiant de **l'INSA Toulouse** (spécialité **Informatique et Réseaux**) et **TLS-SEC**

- **Thèse CIFRE** au **LAAS-CNRS** (**équipe TSF**)**,** co-encadrée par **Apsys.Lab, démarrée le 14 janvier 2019**

- Encadrants: Vincent NICOMETTE, Guillaume AURIOL, Mohamed KAÂNICHE
- Encadrant(e) industriel: Géraldine MARCONATO

PLAN DE LA PRÉSENTATION

- Introduction et état de l'art offensif
- Erreurs de conception courantes
- Analyse en boîte noire d'un clavier sans fil
- Scénarios d'attaque complexes

INTRODUCTION ET ÉTAT DE L'ART OFFENSIF

POURQUOI S'INTÉRESSER AUX CLAVIERS SANS FIL ?

- Équipements très **communs** et **critiques en terme de sécurité**
  - Transmission d'informations sensibles
  - Exécution de code à distance
  - Peu pris en compte d'un point de vue défensif

- Technologies généralement **propriétaires**
  - Protocoles peu ou pas documentés, sécurité par l'obscurité
  - Mauvaise compréhension des risques associés
  - Généralement difficiles, voire impossibles à mettre à jour

- **Intérêt pédagogique** sur la sécurité des protocoles sans fil
  - Une longue liste d'erreurs de conception plus ou moins critiques …
  - … parfaite démonstration de tout ce qu'il ne faut pas faire quand on conçoit un protocole

TROIS GRANDES CATÉGORIES DE PROTOCOLES

Protocoles propriétaires (27MHz)

- Premiers claviers et souris sans fil proposés historiquement
- Fabricants divers (Microsoft, Logitech,...)
- Choix de conception exotiques

Bluetooth / BLE

- De plus en plus courants
- Basés sur des protocoles connus, offrant une sécurité convenable si correctement utilisés (ex: HID over GATT)
- Probablement le choix le plus sûr à l'heure actuelle !

Protocoles propriétaires (2.4GHz)

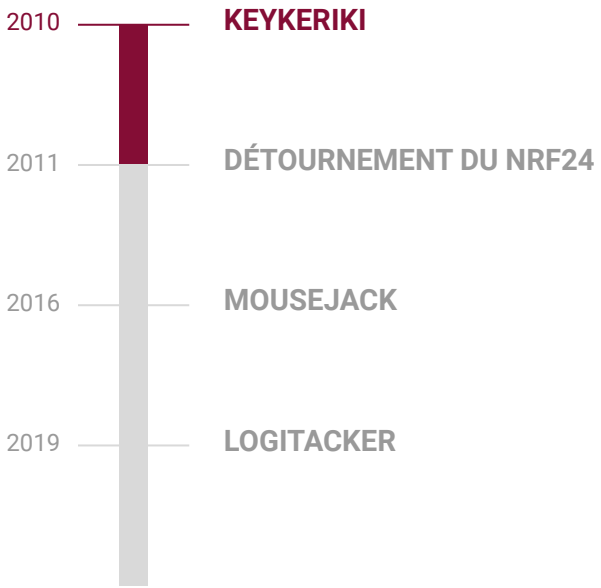
- Très majoritaires à l'heure actuelle
- Utilisé par de très nombreux fabricants (Logitech, Microsoft, HP, Amazon Basics...)
- Sécurité par l'obscurité, graves erreurs de conception

On se concentre ici sur l'analyse et le détournement des protocoles propriétaires, d'un point de vue offensif

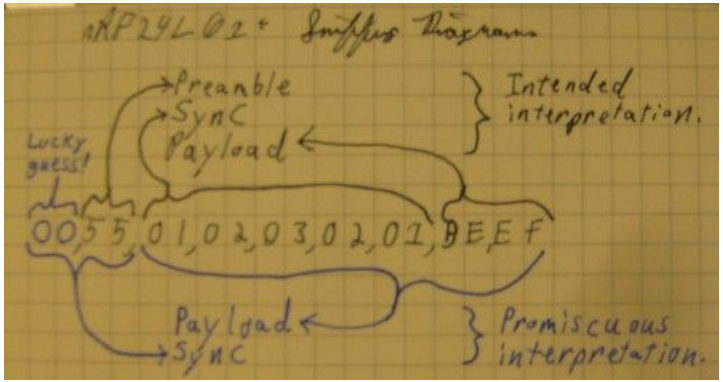
ÉTAT DE L'ART OFFENSIF

KEYKERIKI (T. Shroeber et M. Moser)

- **Premiers travaux orientés sécurité** sur ce type d'équipements
- **Rétro-ingénierie** des protocoles propriétaires de **Microsoft** et **Logitech** (27MHz en v1, 2.4GHz en v2)
- Principalement orienté sur **l'écoute passive**: implémentation de **keyloggers sans fil**
- Nécessite le développement d'un **matériel spécialisé**

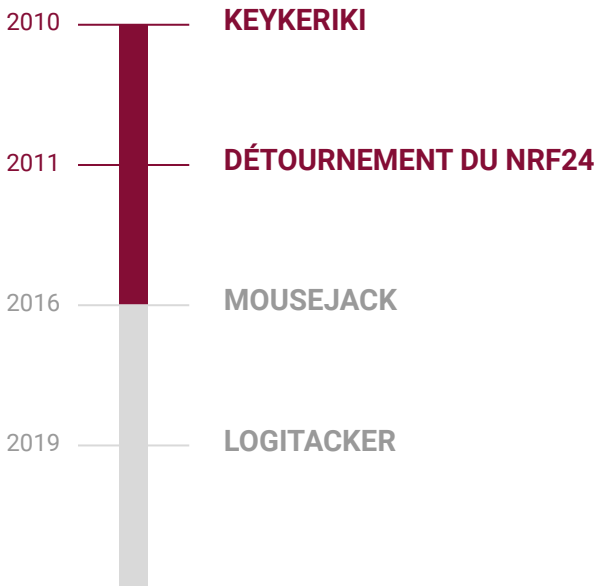


ÉTAT DE L'ART OFFENSIF



DÉTOURNEMENT DU NRF24 (T. Goodspeed)

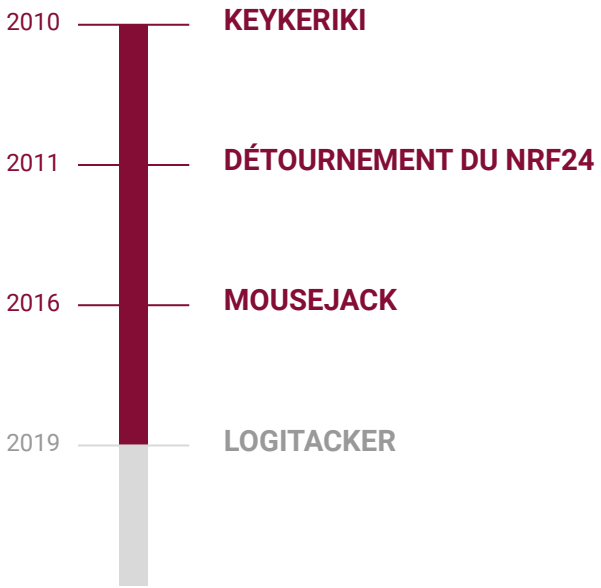
- Billet de blog de T. Goodspeed: **Promiscuity is the nRF24L01+'s Duty**
- Démontre une **vulnérabilité de la puce nRF24** (Nordic SemiConductors) permettant de la détourner pour la doter d'un **mode "promiscuous"**
- **Contribution importante**, ayant considérablement facilité l'analyse des protocoles et les recherches ultérieures



ÉTAT DE L'ART OFFENSIF

MOUSEJACK (M. Newlin)

- Présentation de **vulnérabilités potentiellement critiques**, touchant de nombreux fabricants (Microsoft, Logitech, HP, Amazon, …)
- **Attaques actives et passives:** Écoute passive, injections de frappes chiffrées ou non, appairage forcé, dénis de services …
- **Pas d'exploits diffusés**, mais diffusion d'un **firmware expérimental pour le nRF24** permettant d'interagir avec les protocoles concernés



ÉTAT DE L'ART OFFENSIF

LOGITACKER (M. Mengs)

- Nouvelles vulnérabilités critiques, visant le protocole **Logitech Unifying**
- **Rétro-ingénierie du processus d'appairage:** Récupération de la clé AES lors de l'appairage
- **Nouvelles stratégies d'injection**: contourne les patchs de Logitech destinés à empêcher les vulnérabilités MouseJack
- Développement d'un **firmware offensif** pour nRF52840

2010 — **KEYKERIKI**

2011 — **DÉTOURNEMENT DU NRF24**

2016 — **MOUSEJACK**

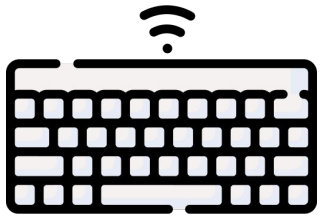
2019 — **LOGITACKER**

ERREURS DE CONCEPTION COURANTES

SÉCURITÉ PAR L'OBSCURITÉ - APPAIRAGE LOGITECH

Comment s'entendre sur une clé de chiffrement AES lors de la phase d'appairage ?

- Un échange de clés Diffie Hellman ? trop facile !
- On va plutôt transmettre les valeurs en clair, échanger quelques octets et faire des XOR un peu aléatoires



Pairing request (phase 1)

Wireless Product ID du clavier

Pairing response (phase 1)

Wireless Product ID du dongle

Pairing request (phase 2)

Valeur aléatoire du clavier

Pairing response (phase 2)

Valeur aléatoire du dongle

SÉCURITÉ PAR L'OBSCURITÉ - APPAIRAGE LOGITECH

Comment s'entendre sur une clé de chiffrement AES lors de la phase d'appairage ?

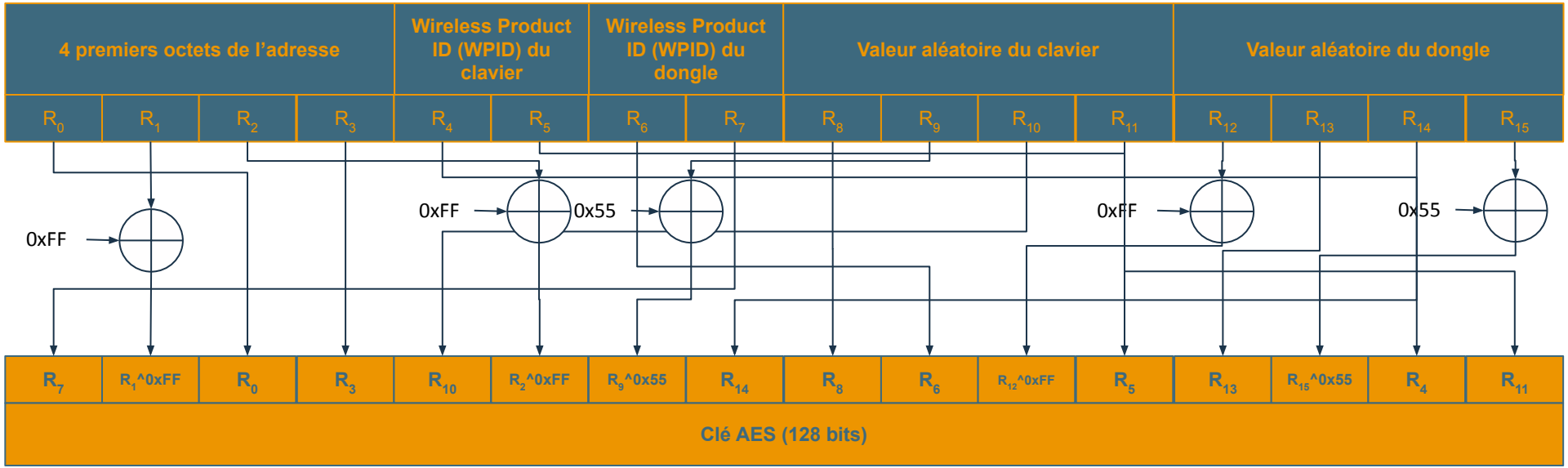
- Un échange de clés Diffie Hellman ? trop facile !
- On va plutôt transmettre les valeurs en clair, échanger quelques octets et faire des XOR un peu aléatoires

4 premiers octets de l'adresse				Wireless Product ID (WPID) du clavier		Wireless Product ID (WPID) du dongle		Valeur aléatoire du clavier				Valeur aléatoire du dongle			
R_0	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}	R_{11}	R_{12}	R_{13}	R_{14}	R_{15}

SÉCURITÉ PAR L'OBSCURITÉ - APPAIRAGE LOGITECH

Comment s'entendre sur une clé de chiffrement AES lors de la phase d'appairage ?

- Un échange de clés Diffie Hellman ? trop facile !
- On va plutôt transmettre les valeurs en clair, échanger quelques octets et faire des XOR un peu aléatoires



SÉCURITÉ PAR L'OBSCURITÉ - CHAMP KEYCODE DU PROTOCOLE MOSART

Protocole "Mosart"

- Protocole propriétaire utilisé par de **très** nombreux fabricants (HP, Anker, Lenxington, EagleTek …)
- Rétro-ingénierie du protocole par Marc Newlin pour ses recherches sur MouseJack
- Aucun nom identifié du protocole, mais un `lsusb` lorsque le dongle est branché renvoie la sortie suivante:

```
Bus 001 Device 009: ID 062a:4101 MosArt Semiconductor Corp. Wireless Keyboard/Mouse
```

- Aucun mécanisme de sécurité efficace (ni possibilité d'en implémenter):
  - pas de chiffrement
  - pas de "personnalisation" du protocole par les fabricants
  - repose principalement sur de la sécurité par l'obscurité

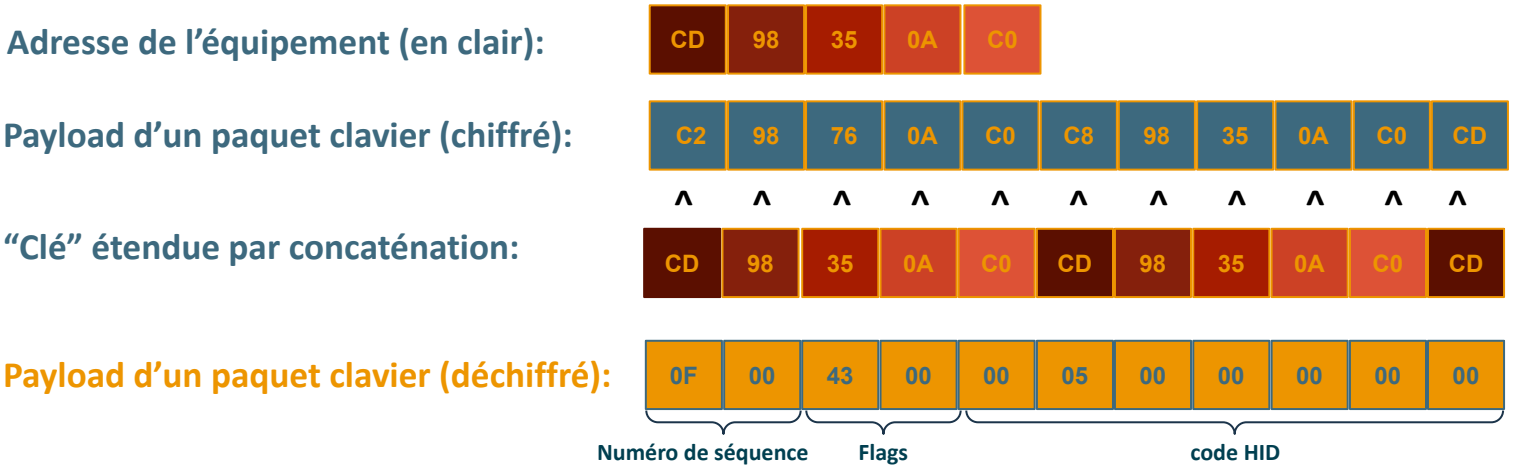
SÉCURITÉ PAR L'OBSCURITÉ - CHAMP KEYCODE DU PROTOCOLE MOSART

- Les trames correspondantes aux frappes claviers contiennent un champ "keycode" indiquant la touche utilisée
- Format **non standard**: il faut établir le mapping entre la valeur du *keycode* et la touche correspondante

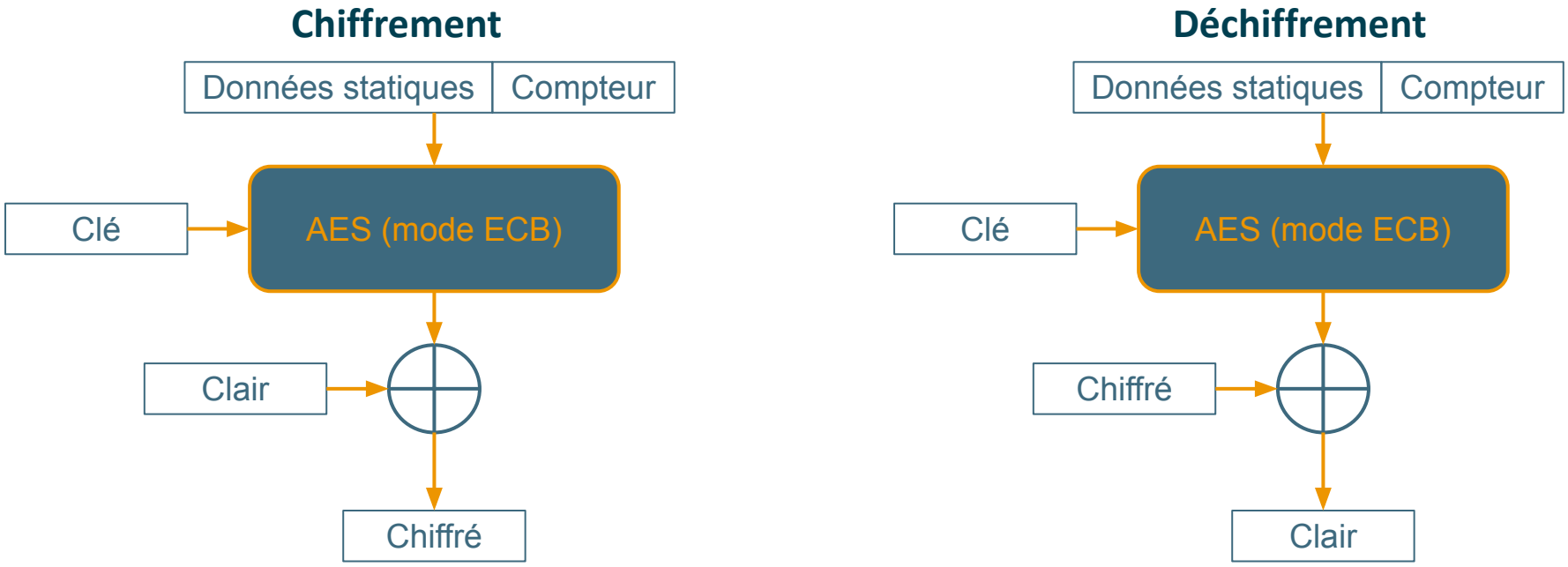
- **Approche par bruteforce:** 255 valeurs à tester
  - on émet un paquet contenant la valeur n dans le champ *KeyCode*
  - on monitore les entrées pour identifier le code HID correspondant HID_n
  - on enregistre la correspondance n ↔ HID_n
  - on refait l'opération avec la valeur n+1, etc ...

CHIFFREMENT FAIBLE - “CHIFFREMENT” MADE IN MICROSOFT

- Les trames correspondant aux frappes claviers sont “chiffrées” avec un chiffrement basé sur l’opération XOR
- Pas besoin d’échange de clés: utilisons l’adresse (qui transite en clair au début de chaque trame) !



CHIFFREMENT FAIBLE - MAUVAISE UTILISATION D'AES: LE CAS LOGITECH



Format d'une trame : Enc(Clair,Compteur,Clé) | Compteur

CHIFFREMENT FAIBLE - MAUVAISE UTILISATION D'AES: LE CAS LOGITECH

Format d'une trame : | Enc(Clair,Compteur,Clé) | Compteur |

Les messages clairs sont parfaitement connus :

- suite de 5 octets, représentant le code HID d'une touche
  ex : 0x00 0x04 0x00 0x00 0x00 pour la touche 'A'
- Chaque pression de touche est suivie d'une touche "relâchée"
  ex: 0x00 0x00 0x00 0x00 0x00

Écoute de deux trames consécutives:

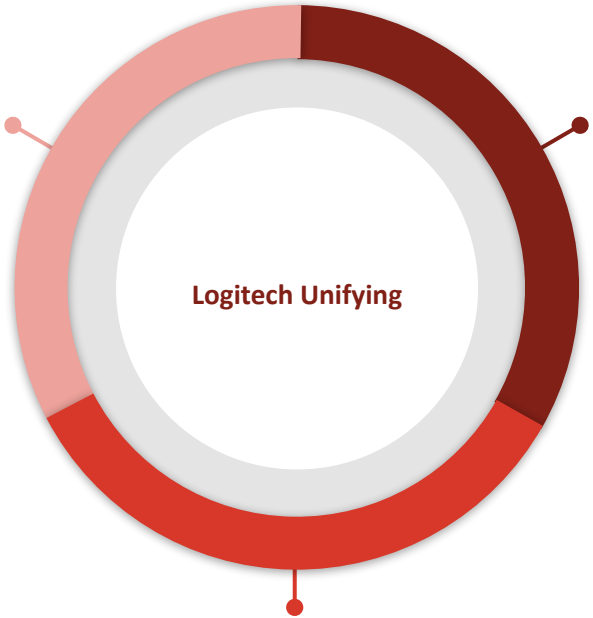
Enc(0x00 0x04 0x00 0x00 0x00,12345,K)	12345	'A' key press
Enc(0x00 0x00 0x00 0x00 0x00,12346,K)	12346	Key release

Injection de deux trames consécutives:

x	12346	'B' key press
Enc(0x00 0x00 0x00 0x00 0x00,12346,K)	12346	Key release

Avec x = Enc(0x00 0x00 0x00 0x00 0x00,12346,K) ^ 0x00 0x05 0x00 0x00 0x00

FAIBLESSE STRUCTURELLE - L'ALGORITHME DE CHANNEL HOPPING DE LOGITECH



DONGLE

Le dongle saute de fréquence en fréquence s'il ne reçoit pas de trames de type KeepAlive

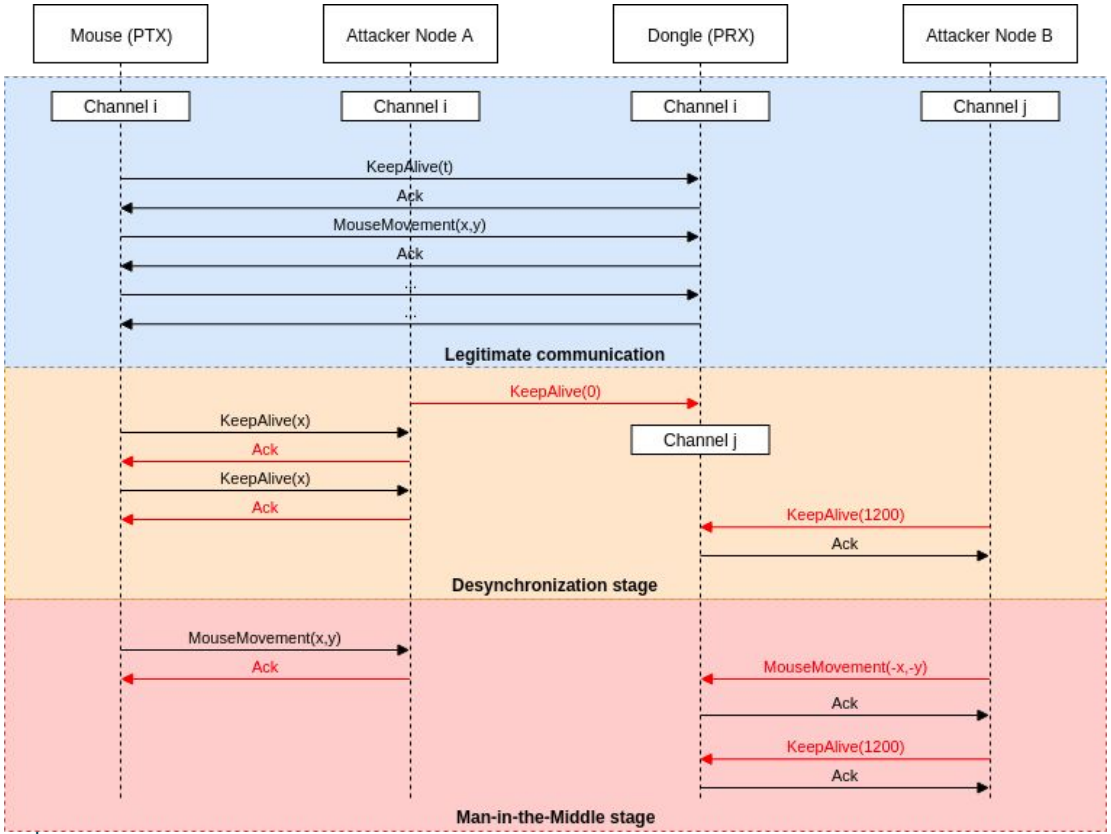
SOURIS / CLAVIER

L'équipement saute de fréquence en fréquence si l'une de ses trames n'est pas acquittée

SAUT DE FRÉQUENCE "PARESSEUX"

L'algorithme tente de maximiser le temps passé sur un canal fixe

FAIBLESSE STRUCTURELLE - L'ALGORITHME DE CHANNEL HOPPING DE LOGITECH



ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - CIBLE

Notre cible: un mini-clavier/touchpad sans fil

- Utilise un protocole propriétaire dans la bande 2.4 GHz
- Principalement destiné à un usage nomade
- Vendu sous plusieurs marques différentes, mais le fabricant d'origine est facilement identifiable (via lsusb par exemple)
- Toutes les vulnérabilités présentées ici ont été remontées au fabricant il y a plusieurs mois…

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - OUTIL MATÉRIEL

Équipement SDR:**HackRF one (Great Scott Gadgets)**

- Radio logicielle *half duplex*, couvrant de 1MHz à 6GHz (parfait pour la bande de fréquence visée)
- Compatible avec la plupart des outils logiciels, bien documenté

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - FRÉQUENCE

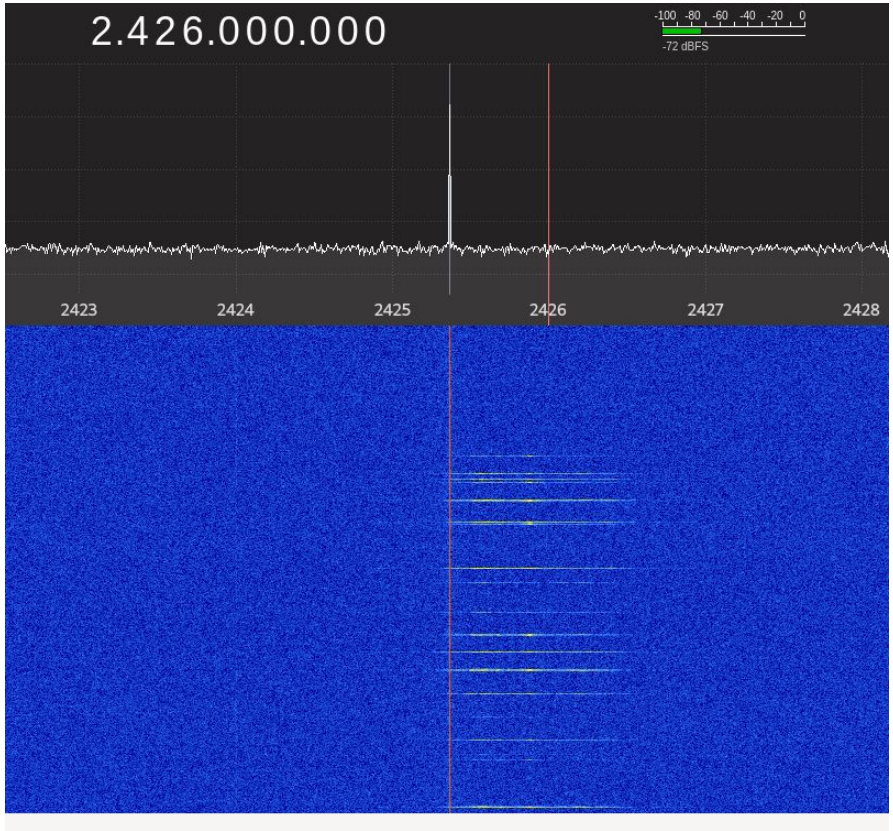
Identification de la fréquence centrale

Outil: GQRX

Méthodologie:

- générer de l'activité sur l'équipement (appui sur des touches, mouvements de souris …)
- parcourir la bande jusqu'à identifier la fréquence centrale utilisée (ici 2426 MHz)
- identifier si le signal est intermittent: cela peut indiquer un algorithme de saut de fréquence

Note: la bande 2.4-2.5GHz étant généralement très bruitée, cette analyse peut être laborieuse ...



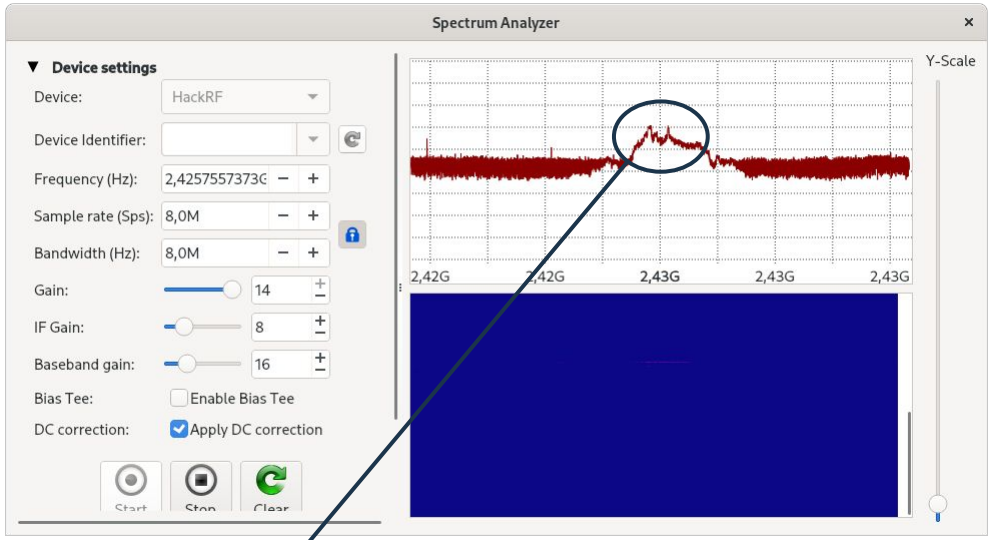
ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - MODULATION

Identification de la modulation

Outil: Universal Radio Hacker (URH)

Méthodologie:

- Utiliser l'analyseur de spectre pour obtenir le profil fréquentiel du signal



2 pics fréquentiels: très caractéristique d'une 2-FSK

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - MODULATION

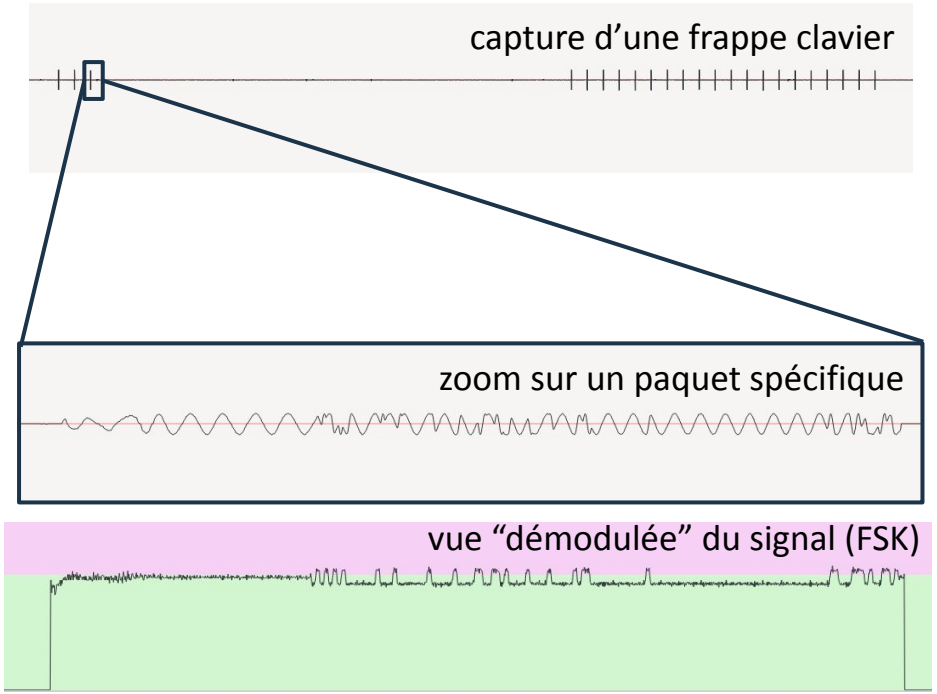
Identification de la modulation

Outil: Universal Radio Hacker (URH)

Méthodologie:

- Utiliser l'analyseur de spectre pour obtenir le profil fréquentiel du signal
- Enregistrer un signal correspondant à une frappe clavier et examiner son profil temporel
- Dans cette bande de fréquences, on trouve généralement des modulations de phase (BPSK/QPSK) ou de fréquence (GFSK)

-> on a très probablement affaire à une GFSK ici



2 fréquences alternées: très caractéristique d'une 2-FSK

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - DÉBIT DE DONNÉES

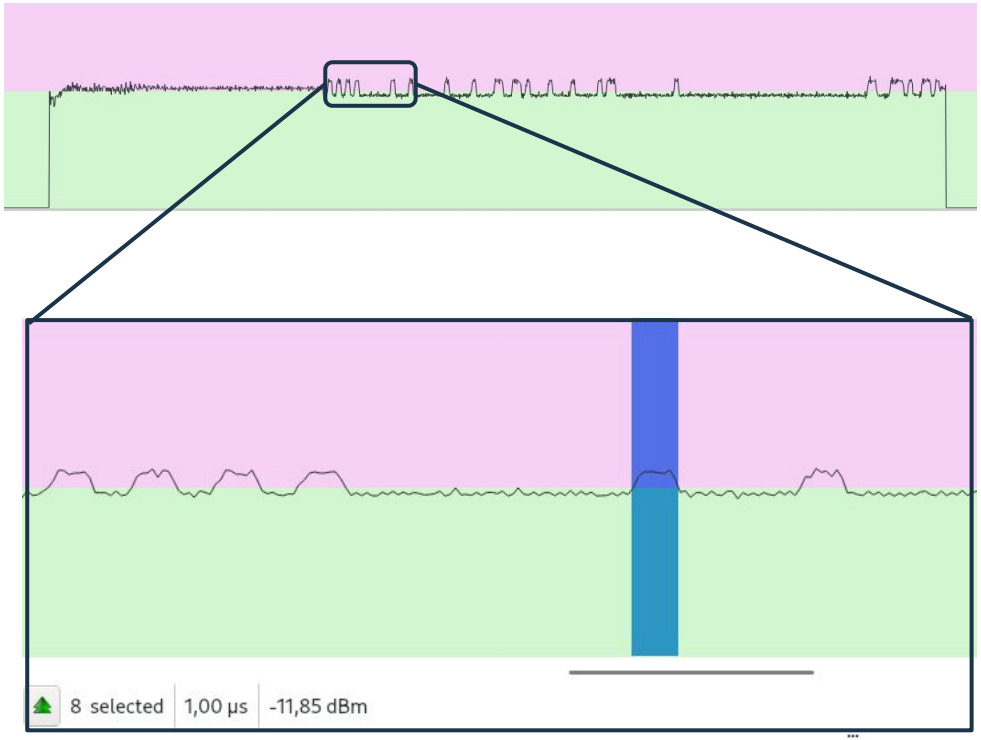
Identification du débit de données

Outil: Universal Radio Hacker (URH)

Méthodologie:

- On a réalisé notre capture à 8Msps: on doit déterminer combien d' échantillons sont utilisés pour coder un bit
- On sélectionne sur la vue "démodulée" l'impulsion correspondant à un 1 ou à un 0 la plus courte possible, on zoome et compte le nombre de symboles correspondants

8 samples/bit à 8MSps ⇔ 1Mbit/s



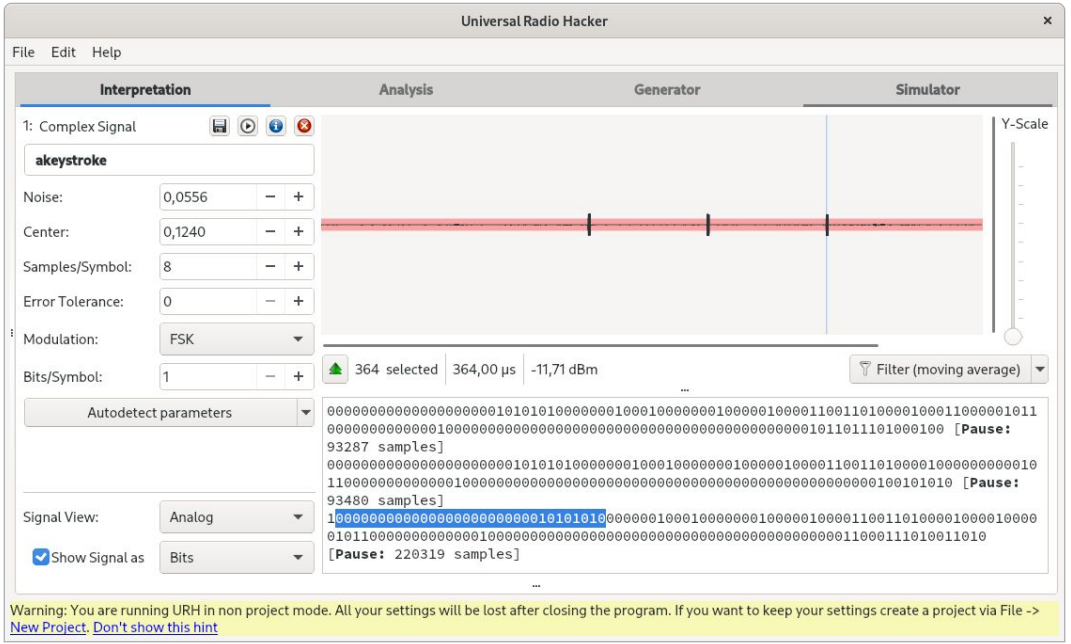
ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - PRÉAMBULE

Identification du débit de données

Outil: Universal Radio Hacker (URH)

Méthodologie:

- On modifie les paramètres Noise / Center jusqu'à obtenir une série de séquences binaires stables
- On identifie le motif de début de paquet
- Motif très caractéristique d'un préambule: 3 octets à zéro suivis d'une série de bits alternés sur 1 octet (0x000000AA)



ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - OUTIL MATÉRIEL

Sniffer radio 2.4GHz: **nRF24**

- Dongle Logitech Unifying / Crazy Radio PA
- Supporte la modulation GFSK à 250kbps, 1Mbps et 2Mbps dans la bande 2.4GHz
- Sélection d'un préambule arbitraire grâce à la vulnérabilité découverte par T. Goodspeed
- Firmware orienté recherche développé par Marc Newlin dans le cadre de ses recherches sur MouseJack: RFStorm

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - COLLECTE DE TRAMES

```python
# initialisation du dongle
dev = nrf24()
# configuration du mode promiscuous à 1Mbps, préambule 0x000000AA, taille 25
dev.enter_promiscuous_mode_generic(rate=RF_RATE_1M,prefix=bytes.fromhex("000000aa"),payload_length=25)
# sélection du canal 26 (soit 2426 MHz)
dev.set_channel(26)

# Boucle infinie d'affichage des paquets reçus
while True:
        p = dev.receive_payload()
        if p is not None and len(p) > 1:
                print(":".join(["{:02x}".format(i) for i in p]))
```

```
00:00:00:aa:02:20:20:86:68:40:0b:00:04:00:00:00:00:00:01:2a:d3:f7:5e:a9:a4:af:7b:56:f6
00:00:00:aa:02:20:20:86:68:46:0b:00:00:00:00:00:00:00:5d:03:7e:af:db:df:fd:2b:5c:ea:54
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:66:68:f5:6f:76:da:5e:fa:fa
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:fe:ec:e9:f6:eb:9f:7a:df:6b
00:00:00:aa:02:20:20:86:68:46:0b:00:00:00:00:00:00:00:5d:03:5f:5c:7f:b5:9d:a2:fb:54:92
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ff:5f:55:1b:6d:26:b4:91:52
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:5f:9e:e6:b7:d6:ef:76:bd:52
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:6f:be:e7:77:fd:ea:ff:55:ac
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ff:af:d6:da:ad:b4:fd:bd:59
00:00:00:aa:02:20:20:86:68:44:0b:00:00:00:00:00:00:00:9b:64:b5:7f:d1:9c:7a:b7:7f:b6:37
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:6f:5d:ca:f3:ff:d3:ab:f2:e3
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ef:f6:6f:9a:f6:b9:df:d6:f7
```

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - ANALYSE DE TRAMES

Préambule

```
00:00:00:aa:02:20:20:86:68:40:0b:00:04:00:00:00:00:00:01:2a:d3:f7:5e:a9:a4:af:7b:56:f6
00:00:00:aa:02:20:20:86:68:46:0b:00:00:00:00:00:00:00:5d:03:7e:af:db:df:fd:2b:5c:ea:54
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:66:68:f5:6f:76:da:5e:fa:fa
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:fe:ec:e9:f6:eb:9f:7a:df:6b
00:00:00:aa:02:20:20:86:68:46:0b:00:00:00:00:00:00:00:5d:03:5f:5c:7f:b5:9d:a2:fb:54:92
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ff:5f:55:1b:6d:26:b4:91:52
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:5f:9e:e6:b7:d6:ef:76:bd:52
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:6f:be:e7:77:fd:ea:ff:55:ac
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ff:af:d6:da:ad:b4:fd:bd:59
00:00:00:aa:02:20:20:86:68:44:0b:00:00:00:00:00:00:00:9b:64:b5:7f:d1:9c:7a:b7:7f:b6:37
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:6f:5d:ca:f3:ff:d3:ab:f2:e3
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ef:f6:6f:9a:f6:b9:df:d6:f7
```

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - ANALYSE DE TRAMES

Préambule

5 octets stables: adresse

```
00:00:00:aa:02:20:20:86:68:40:0b:00:04:00:00:00:00:00:01:2a:d3:f7:5e:a9:a4:af:7b:56:f6
00:00:00:aa:02:20:20:86:68:46:0b:00:00:00:00:00:00:00:5d:03:7e:af:db:df:fd:2b:5c:ea:54
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:66:68:f5:6f:76:da:5e:fa:fa
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:fe:ec:e9:f6:eb:9f:7a:df:6b
00:00:00:aa:02:20:20:86:68:46:0b:00:00:00:00:00:00:00:5d:03:5f:5c:7f:b5:9d:a2:fb:54:92
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ff:5f:55:1b:6d:26:b4:91:52
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:5f:9e:e6:b7:d6:ef:76:bd:52
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:6f:be:e7:77:fd:ea:ff:55:ac
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ff:af:d6:da:ad:b4:fd:bd:59
00:00:00:aa:02:20:20:86:68:44:0b:00:00:00:00:00:00:00:9b:64:b5:7f:d1:9c:7a:b7:7f:b6:37
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:6f:5d:ca:f3:ff:d3:ab:f2:e3
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ef:f6:6f:9a:f6:b9:df:d6:f7
```

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - ANALYSE DE TRAMES

5 octets stables: adresse

Préambule

00:00:00:aa	02:20:20:86:68	40	0b:00:04:00:00:00:00:00:01:2a:d3:f7:5e:a9:a4:af:7b:56:f6
00:00:00:aa	02:20:20:86:68	46	0b:00:00:00:00:00:00:00:5d:03:7e:af:db:df:fd:2b:5c:ea:54
00:00:00:aa	02:20:20:86:68	40	0b:00:00:00:00:00:00:00:07:8b:66:68:f5:6f:76:da:5e:fa:fa
00:00:00:aa	02:20:20:86:68	42	0b:00:00:00:00:00:00:00:c1:ec:fe:ec:e9:f6:eb:9f:7a:df:6b
00:00:00:aa	02:20:20:86:68	46	0b:00:00:00:00:00:00:00:5d:03:5f:5c:7f:b5:9d:a2:fb:54:92
00:00:00:aa	02:20:20:86:68	42	0b:00:00:00:00:00:00:00:c1:ec:ff:5f:55:1b:6d:26:b4:91:52
00:00:00:aa	02:20:20:86:68	40	0b:00:00:00:00:00:00:00:07:8b:5f:9e:e6:b7:d6:ef:76:bd:52
00:00:00:aa	02:20:20:86:68	40	0b:00:00:00:00:00:00:00:07:8b:6f:be:e7:77:fd:ea:ff:55:ac
00:00:00:aa	02:20:20:86:68	42	0b:00:00:00:00:00:00:00:c1:ec:ff:af:d6:da:ad:b4:fd:bd:59
00:00:00:aa	02:20:20:86:68	44	0b:00:00:00:00:00:00:00:9b:64:b5:7f:d1:9c:7a:b7:7f:b6:37
00:00:00:aa	02:20:20:86:68	40	0b:00:00:00:00:00:00:00:07:8b:6f:5d:ca:f3:ff:d3:ab:f2:e3
00:00:00:aa	02:20:20:86:68	42	0b:00:00:00:00:00:00:00:c1:ec:ef:f6:6f:9a:f6:b9:df:d6:f7

valeur stable, inconnue pour les 4 bits de poids fort, valeur variable incrémentée de 2 pour les 4 bits de poids faible: compteur ?

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - ANALYSE DE TRAMES

5 octets stables: adresse

Préambule

valeur stable pour une série de paquets similaires (frappes claviers): indicateur de type de trame ?

00:00:00:aa	02:20:20:86:68	40	0b:00:04:00:00:00:00:00:01:2a:d3:f7:5e:a9:a4:af:7b:56:f6
00:00:00:aa	02:20:20:86:68	46	0b:00:00:00:00:00:00:00:5d:03:7e:af:db:df:fd:2b:5c:ea:54
00:00:00:aa	02:20:20:86:68	40	0b:00:00:00:00:00:00:00:07:8b:66:68:f5:6f:76:da:5e:fa:fa
00:00:00:aa	02:20:20:86:68	42	0b:00:00:00:00:00:00:00:c1:ec:fe:ec:e9:f6:eb:9f:7a:df:6b
00:00:00:aa	02:20:20:86:68	46	0b:00:00:00:00:00:00:00:5d:03:5f:5c:7f:b5:9d:a2:fb:54:92
00:00:00:aa	02:20:20:86:68	42	0b:00:00:00:00:00:00:00:c1:ec:ff:5f:55:1b:6d:26:b4:91:52
00:00:00:aa	02:20:20:86:68	40	0b:00:00:00:00:00:00:00:07:8b:5f:9e:e6:b7:d6:ef:76:bd:52
00:00:00:aa	02:20:20:86:68	40	0b:00:00:00:00:00:00:00:07:8b:6f:be:e7:77:fd:ea:ff:55:ac
00:00:00:aa	02:20:20:86:68	42	0b:00:00:00:00:00:00:00:c1:ec:ff:af:d6:da:ad:b4:fd:bd:59
00:00:00:aa	02:20:20:86:68	44	0b:00:00:00:00:00:00:00:9b:64:b5:7f:d1:9c:7a:b7:7f:b6:37
00:00:00:aa	02:20:20:86:68	40	0b:00:00:00:00:00:00:00:07:8b:6f:5d:ca:f3:ff:d3:ab:f2:e3
00:00:00:aa	02:20:20:86:68	42	0b:00:00:00:00:00:00:00:c1:ec:ef:f6:6f:9a:f6:b9:df:d6:f7

valeur stable, inconnue pour les 4 bits de poids fort, valeur variable incrémentée de 2 pour les 4 bits de poids faible: compteur ?

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - ANALYSE DE TRAMES

Préambule

5 octets stables: adresse

valeur stable pour une série de paquets similaires (frappes claviers): indicateur de type de trame ?

00:00:00:aa:	02:20:20:86:68	40	0b:	00:04:00:00:00:00:00:	01:2a:d3:f7:5e:a9:a4:af:7b:56:f6
00:00:00:aa:	02:20:20:86:68	46	0b:	00:00:00:00:00:00:00:	5d:03:7e:af:db:df:fd:2b:5c:ea:54
00:00:00:aa:	02:20:20:86:68	40	0b:	00:00:00:00:00:00:00:	07:8b:66:68:f5:6f:76:da:5e:fa:fa
00:00:00:aa:	02:20:20:86:68	42	0b:	00:00:00:00:00:00:00:	c1:ec:fe:ec:e9:f6:eb:9f:7a:df:6b
00:00:00:aa:	02:20:20:86:68	46	0b:	00:00:00:00:00:00:00:	5d:03:5f:5c:7f:b5:9d:a2:fb:54:92
00:00:00:aa:	02:20:20:86:68	42	0b:	00:00:00:00:00:00:00:	c1:ec:ff:5f:55:1b:6d:26:b4:91:52
00:00:00:aa:	02:20:20:86:68	40	0b:	00:00:00:00:00:00:00:	07:8b:5f:9e:e6:b7:d6:ef:76:bd:52
00:00:00:aa:	02:20:20:86:68	40	0b:	00:00:00:00:00:00:00:	07:8b:6f:be:e7:77:fd:ea:ff:55:ac
00:00:00:aa:	02:20:20:86:68	42	0b:	00:00:00:00:00:00:00:	c1:ec:ff:af:d6:da:ad:b4:fd:bd:59
00:00:00:aa:	02:20:20:86:68	44	0b:	00:00:00:00:00:00:00:	9b:64:b5:7f:d1:9c:7a:b7:7f:b6:37
00:00:00:aa:	02:20:20:86:68	40	0b:	00:00:00:00:00:00:00:	07:8b:6f:5d:ca:f3:ff:d3:ab:f2:e3
00:00:00:aa:	02:20:20:86:68	42	0b:	00:00:00:00:00:00:00:	c1:ec:ef:f6:6f:9a:f6:b9:df:d6:f7

valeur stable, inconnue pour les 4 bits de poids fort, valeur variable incrémentée de 2 pour les 4 bits de poids faible: compteur ?

7 octets dont le 2ème a une valeur variable (0x04/0x00) et où les autres octets sont à 0: caractéristique d'un code HID (touche A activée / touche A relâchée)

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - ANALYSE DE TRAMES

```
00:00:00:aa:02:20:20:86:68:40:0b:00:04:00:00:00:00:00:01:2a:d3:f7:5e:a9:a4:af:7b:56:f6
00:00:00:aa:02:20:20:86:68:46:0b:00:00:00:00:00:00:00:5d:03:7e:af:db:df:fd:2b:5c:ea:54
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:66:68:f5:6f:76:da:5e:fa:fa
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:fe:ec:e9:f6:eb:9f:7a:df:6b
00:00:00:aa:02:20:20:86:68:46:0b:00:00:00:00:00:00:00:5d:03:5f:5c:7f:b5:9d:a2:fb:54:92
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ff:5f:55:1b:6d:26:b4:91:52
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:5f:9e:e6:b7:d6:ef:76:bd:52
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:6f:be:e7:77:fd:ea:ff:55:ac
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ff:af:d6:da:ad:b4:fd:bd:59
00:00:00:aa:02:20:20:86:68:44:0b:00:00:00:00:00:00:00:9b:64:b5:7f:d1:9c:7a:b7:7f:b6:37
00:00:00:aa:02:20:20:86:68:40:0b:00:00:00:00:00:00:00:07:8b:6f:5d:ca:f3:ff:d3:ab:f2:e3
00:00:00:aa:02:20:20:86:68:42:0b:00:00:00:00:00:00:00:c1:ec:ef:f6:6f:9a:f6:b9:df:d6:f7
```

2 octets variables en fin de paquet, valeurs similaires si le contenu précédent est similaire: très probablement un CRC

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - CRC

Taille du CRC

Échantillons de payloads+CRC

```
$ ./reveng -w 16 -s 420b00000000000000c1ec 400b00000000000000078b 460b00000000000005d03
width=16  poly=0x1021  init=0x8b83  refin=false  refout=false  xorout=0x0000  check=0xbf3e
residue=0x0000  name=(none)
```

```
$ python3 ~/crccheck.py
Payload: 420b00000000000000 / CRC calculé: c1ec / CRC sniffé: c1ec
Payload: 400b00000000000000 / CRC calculé: 078b / CRC sniffé: 078b
Payload: 460b00000000000000 / CRC calculé: 5d03 / CRC sniffé: 5d03
```

ANALYSE EN BOÎTE NOIRE D'UN CLAVIER SANS FIL - ATTAQUES

Keylogger

- Sniffer les trames dont le champ type est égal à 0x0b (frappe clavier)
- Extraire le code HID du payload
- Afficher la correspondance code HID / touche utilisée

Injection de frappes clavier

- Sniffer des trames pour récupérer l'adresse
- Forger une séquence de paquets de type frappes claviers (0x0b) correspondant aux touches à déclencher

SCÉNARIOS D'ATTAQUE COMPLEXES

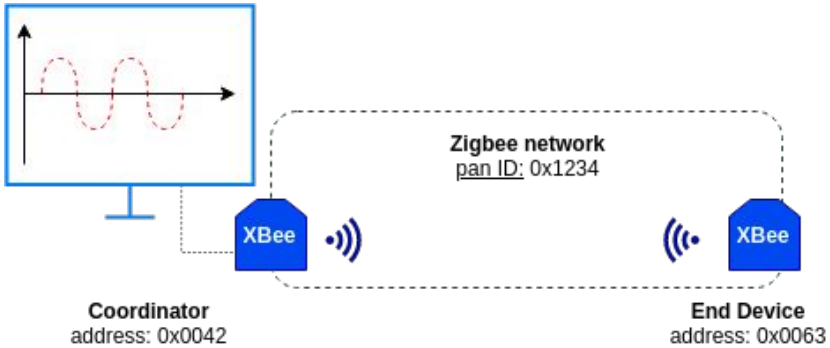
SCÉNARIOS D'ATTAQUE COMPLEXES - CLAVIER DE BANQUE RANDOMISÉ

Objectif: attaquer un formulaire de connexion de banque en ligne avec clavier randomisé (récupération de l'identifiant et du mot de passe)

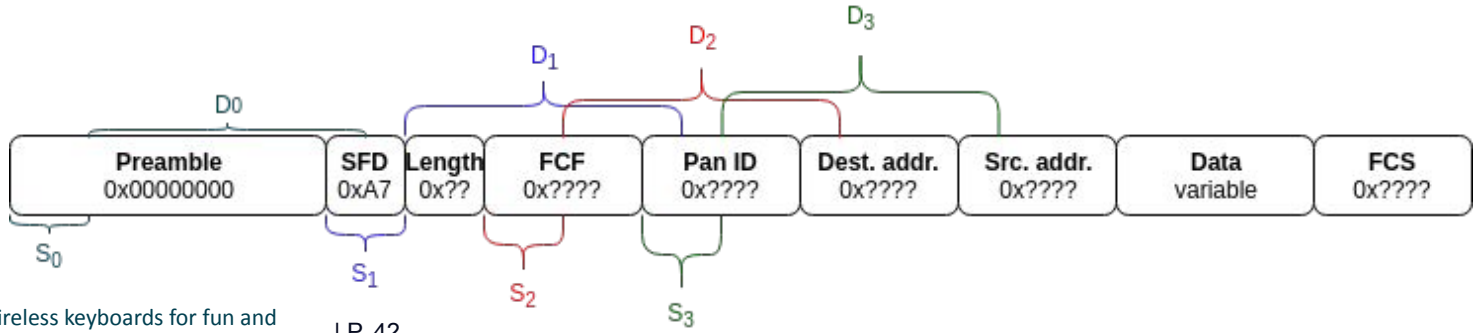
- La victime et l'attaquant sont connectés au même réseau local (ex: point d'accès gratuit)
- La victime se connecte à son compte en ligne en utilisant une souris sans fil Logitech

SCÉNARIOS D'ATTAQUE COMPLEXES - COLLECTE D'INFORMATION ZIGBEE

<u>Objectif:</u> collecter des informations sur les réseaux Zigbee environnants



- L'attaquant a compromis un ordinateur au sein d'une entreprise équipé d'un dongle Logitech Unifying
- Exploitation d'une variante de l'attaque WazaBee: permet d'établir une équivalence entre une modulation O-QPSK (Zigbee) et une modulation GFSK à 2Mbit/s (BLE, ESB)



CONCLUSION

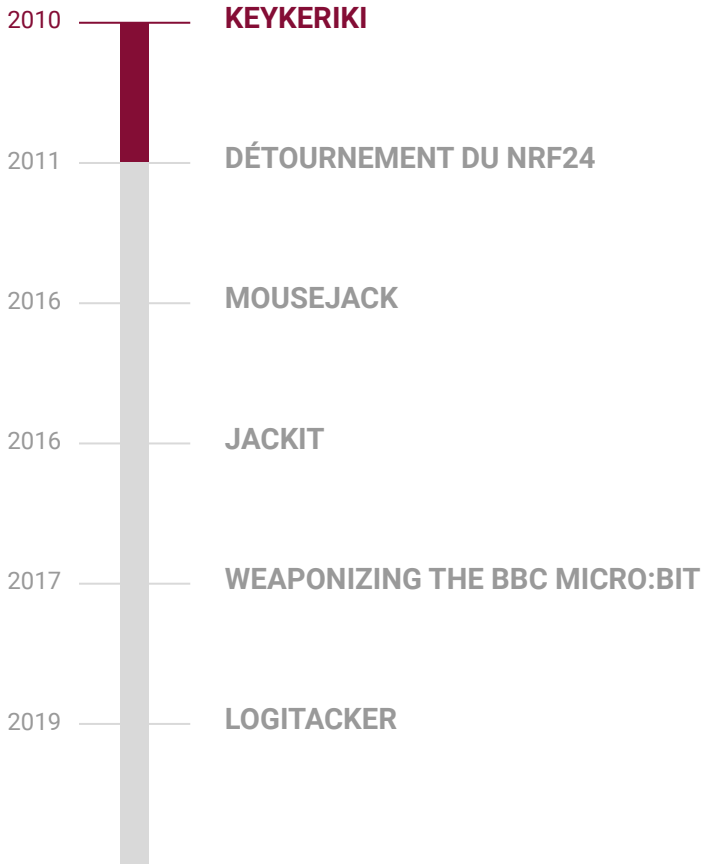
- Équipements critiques au niveau de la **vie privée** et de la **sécurité**
- Protocoles **propriétaires** reposant sur la **sécurité par l'obscurité**
- Peu ou pas de **chiffrement,** Faiblesses **structurelles**
- **Nouvelles menaces:** attaques via des équipements mobiles (smartphone, objets connectés)
- **Nouvelles stratégies défensives**

Merci pour votre attention !

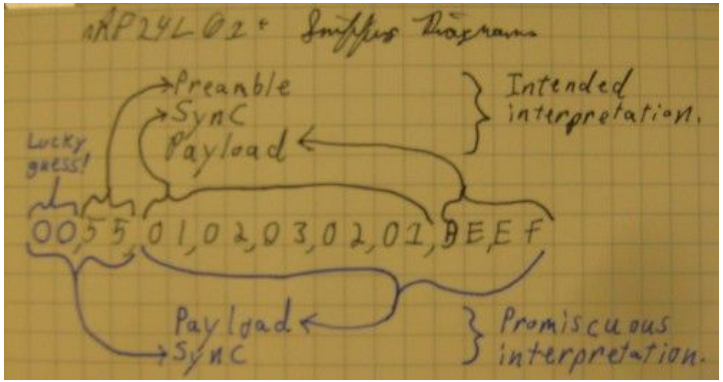
ÉTAT DE L'ART OFFENSIF

KEYKERIKI (T. Shroeber et M. Moser)

- **Premiers travaux orientés sécurité** sur ce type d'équipements
- **Rétro-ingénierie** des protocoles propriétaires de **Microsoft** et **Logitech** (27MHz en v1, 2.4GHz en v2)
- Principalement orienté sur **l'écoute passive**: implémentation de **keyloggers sans fil**
- Nécessite le développement d'un **matériel spécialisé**



ÉTAT DE L'ART OFFENSIF



DÉTOURNEMENT DU NRF24 (T. Goodspeed)

- Billet de blog de T. Goodspeed: **Promiscuity is the nRF24L01+'s Duty**
- Démontre une **vulnérabilité de la puce nRF24** (Nordic SemiConductors) permettant de la détourner pour la doter d'un **mode "promiscuous"**
- **Contribution importante**, ayant considérablement facilité l'analyse des protocoles et les recherches ultérieures

2010 — **KEYKERIKI**

2011 — **DÉTOURNEMENT DU NRF24**

2016 — MOUSEJACK

2016 — JACKIT

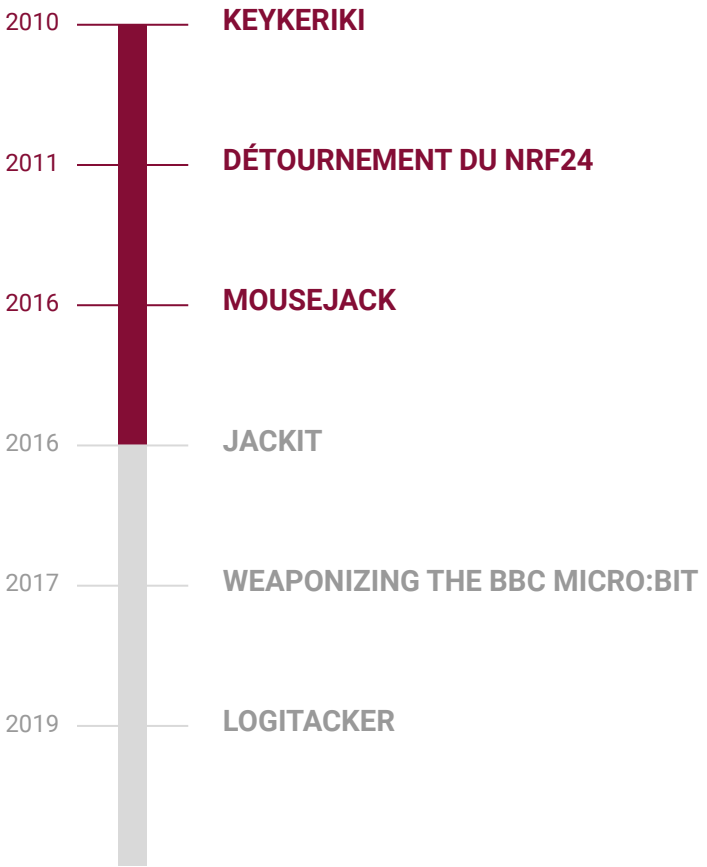
2017 — WEAPONIZING THE BBC MICRO:BIT

2019 — LOGITACKER

ÉTAT DE L'ART OFFENSIF

MOUSEJACK (M. Newlin)

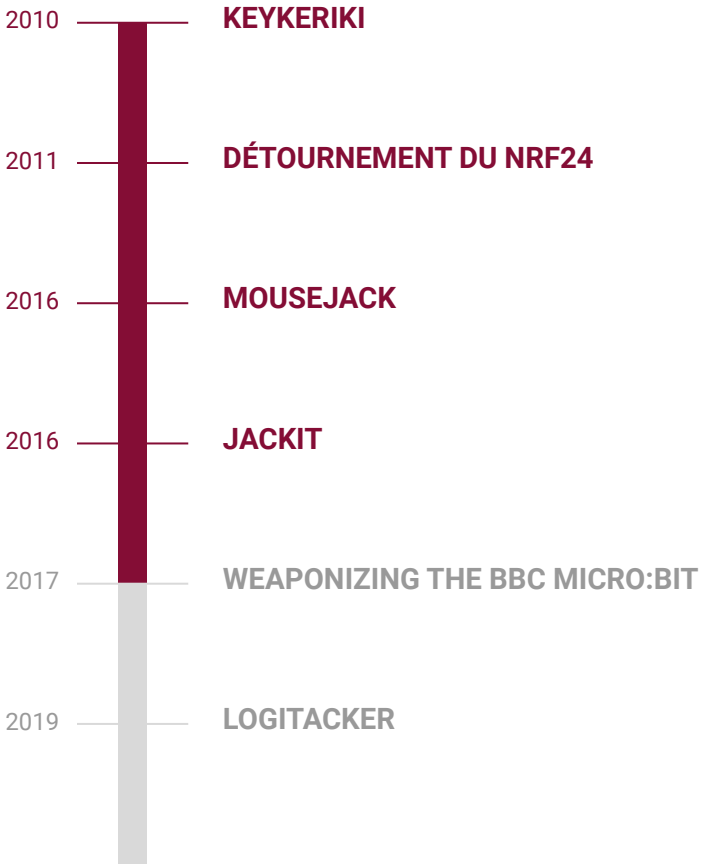
- Présentation de **vulnérabilités potentiellement critiques**, touchant de nombreux fabricants (Microsoft, Logitech, HP, Amazon, …)
- **Attaques actives et passives:** Écoute passive, injections de frappes chiffrées ou non, appairage forcé, dénis de services …
- **Pas d'exploits diffusés**, mais diffusion d'un **firmware expérimental pour le nRF24** permettant d'interagir avec les protocoles concernés



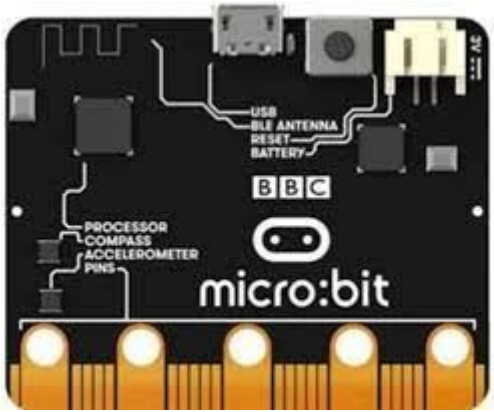
ÉTAT DE L'ART OFFENSIF

JACKIT (InsecurityOfThings)

- **Implémentation partielle** des vulnérabilités de **MouseJack**, notamment les **injections de frappes**
- Fournis un **interpréteur de DuckyScript**, permettant de réutiliser les nombreux codes sources développés pour le **RubberDucky**
- **Implémentation open-source**: https://github.com/insecurityofthings/jackit



ÉTAT DE L'ART OFFENSIF



WEAPONIZING THE BBC MICRO:BIT (D. Cauquil)

- Détournement d'une **plateforme pédagogique** pour apprendre le développement embarqué, le **BBC Micro:Bit**
- Basé sur un **nRF51822** de **Nordic SemiConductors**
- Développement d'un **firmware offensif basé sur Micro:Python**
- Facilite l'analyse des **protocoles propriétaires dans la bande 2.4GHz**

2010 — **KEYKERIKI**

2011 — **DÉTOURNEMENT DU NRF24**

2016 — **MOUSEJACK**

2016 — **JACKIT**

2017 — **WEAPONIZING THE BBC MICRO:BIT**

2019 — **LOGITACKER**

ÉTAT DE L'ART OFFENSIF

LOGITACKER (M. Mengs)

- Nouvelles vulnérabilités critiques, visant le protocole **Logitech Unifying**
- **Rétro-ingénierie du processus d'appairage:** Récupération de la clé AES lors de l'appairage
- **Nouvelles stratégies d'injection**: contourne les patchs de Logitech destinés à empêcher les vulnérabilités MouseJack
- Développement d'un **firmware offensif** pour nRF52840

2010 — **KEYKERIKI**

2011 — **DÉTOURNEMENT DU NRF24**

2016 — **MOUSEJACK**

2016 — **JACKIT**

2017 — **WEAPONIZING THE BBC MICRO:BIT**

2019 — **LOGITACKER**