BLUETOOTH LOW ENERGY

LES ARCANES D'UN PROTOCOLE ~~TROP~~ AMBITIEUX

Damien Cauquil | RESSI 2019

digital.security

/ME

 Responsable R&D @ Econocom Digital.Security

 Chercheur sécurité Senior

 Hardware hacker (ou presque)

SOMMAIRE

- Origines du protocole
- Bluetooth Low Energy 101
- Maturité du protocole et des usages
- Evolutions et ambitions futures
- Conclusion

ORIGINES DU PROTOCOLE


Bluetooth®
SPECIAL INTEREST GROUP
IoT

BLUETOOTH 4.0

- Introduction de *Bluetooth Smart* en **2010**
- Fait partie intégrante de **Bluetooth 4.0**
- Volonté d'en faire un **protocole majeur** de l'IoT
- Relégation des versions précédentes (Bluetooth *Classic*)

OBJETS À CONNECTER

- Montres
- Appareils médicaux
- Jouets
- Smartphones...

SIMPLIFICATION DU PROTOCOLE BLUETOOTH

Débit quasi identique au *Bluetooth Classic* (1 Mbit/s)
avec une consommation **10 fois moindre**

CONTRAINTES MATÉRIELLES (IOT)

- Faible puissance de calcul
- Source d'énergie limitée (pile, batterie)
- Faible espace de stockage

CONSÉQUENCE

Des choix techniques ont été faits pour **favoriser l'adoption** du protocole par les concepteurs d'objets connectés

... au détriment de la sécurité.

SPÉCIFICATIONS CORE

VERSIONS 4.X ET 5.X

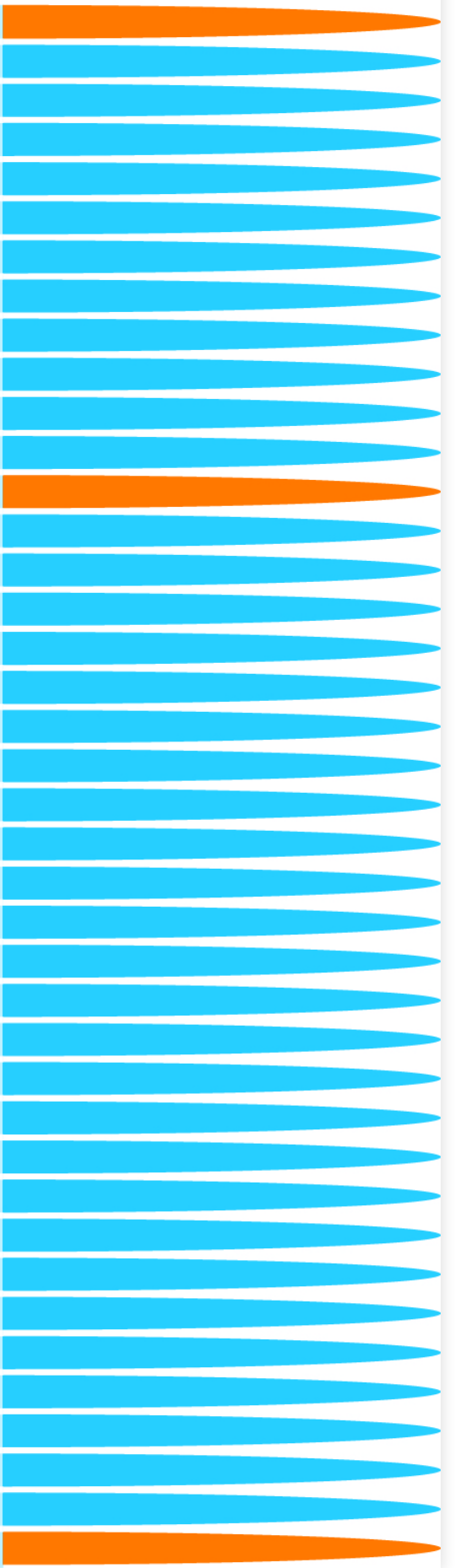
digital.security

CARACTÉRISTIQUES RF

- Utilise la plage de fréquence 2.40 - 2.48 GHz
- Emploie la modulation GFSK
- 40 canaux de 2MHz

digital.security

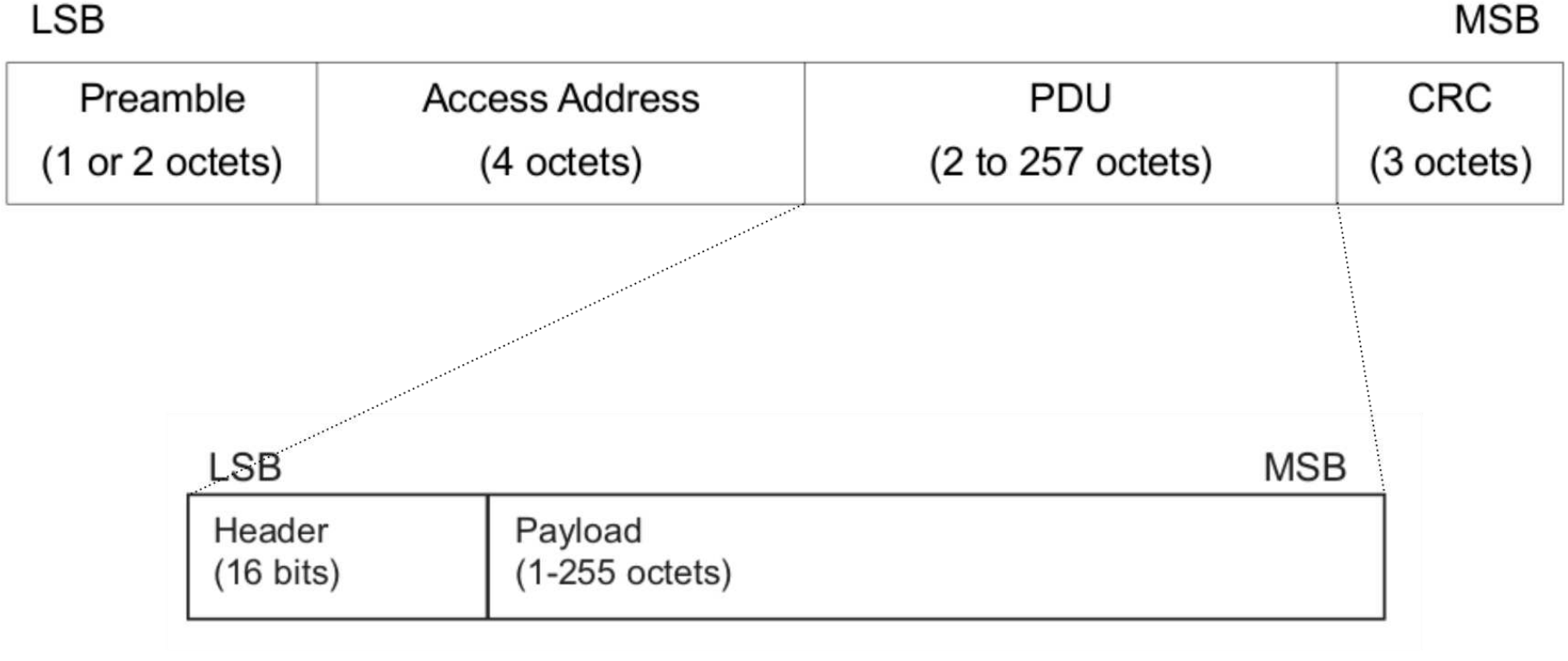
Frequency	LL
2402 MHz	37
2404 MHz	0
2406 MHz	1
2408 MHz	2
2410 MHz	3
2412 MHz	4
2414 MHz	5
2416 MHz	6
2418 MHz	7
2420 MHz	8
2422 MHz	9
2424 MHz	10
2426 MHz	38
2428 MHz	11
2430 MHz	12
2432 MHz	13
2434 MHz	14
2436 MHz	15
2438 MHz	16
2440 MHz	17
2442 MHz	18
2444 MHz	19
2446 MHz	20
2448 MHz	21
2450 MHz	22
2452 MHz	23
2454 MHz	24
2456 MHz	25
2458 MHz	26
2460 MHz	27
2462 MHz	28
2464 MHz	29
2466 MHz	30
2468 MHz	31
2470 MHz	32
2472 MHz	33
2474 MHz	34
2476 MHz	35
2478 MHz	36
2480 MHz	39



PHY LAYERS

- **BLE 4.x**: 1 MBit/s
- **BLE 5**:
  - 2Mbit/s, 1Mbit/s et 125kb/s
  - Coded PHY

FORMAT DE TRAME



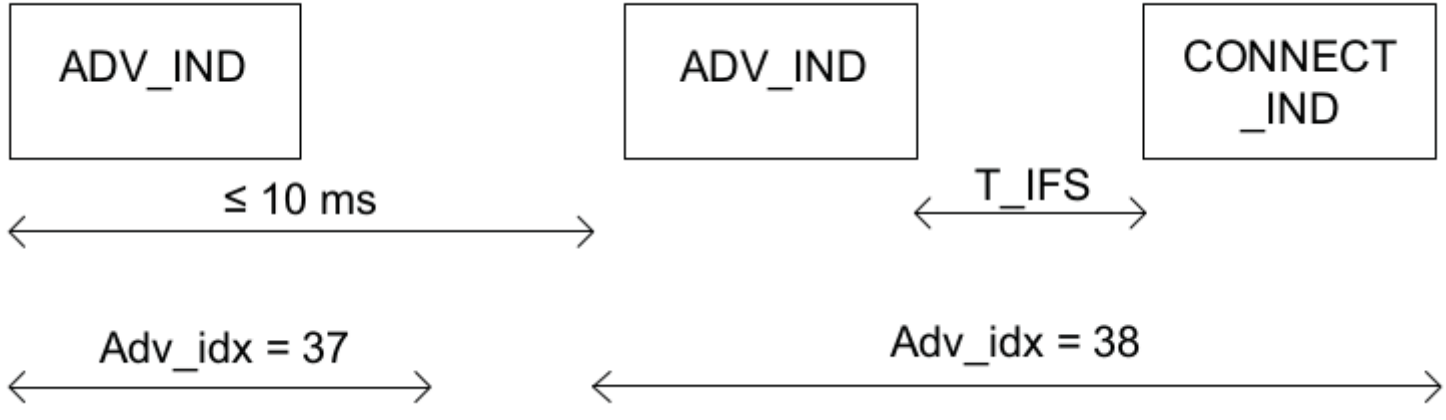
RÔLES DES PÉRIPHÉRIQUES

- **Broadcaster**: le périphérique s'annonce seulement et n'accepte aucune connexion ;
- **Observer**: le périphérique ne détecte que les périphériques qui s'annoncent, et ne crée aucune connexion ;

RÔLES DES PÉRIPHÉRIQUES (SUITE)

- **Peripheral**: le périphérique s'annonce et accepte une (ou plusieurs) connexions ;
- **Central**: le périphérique détecte les périphériques qui s'annoncent et peut creér une ou plusieurs connexions.

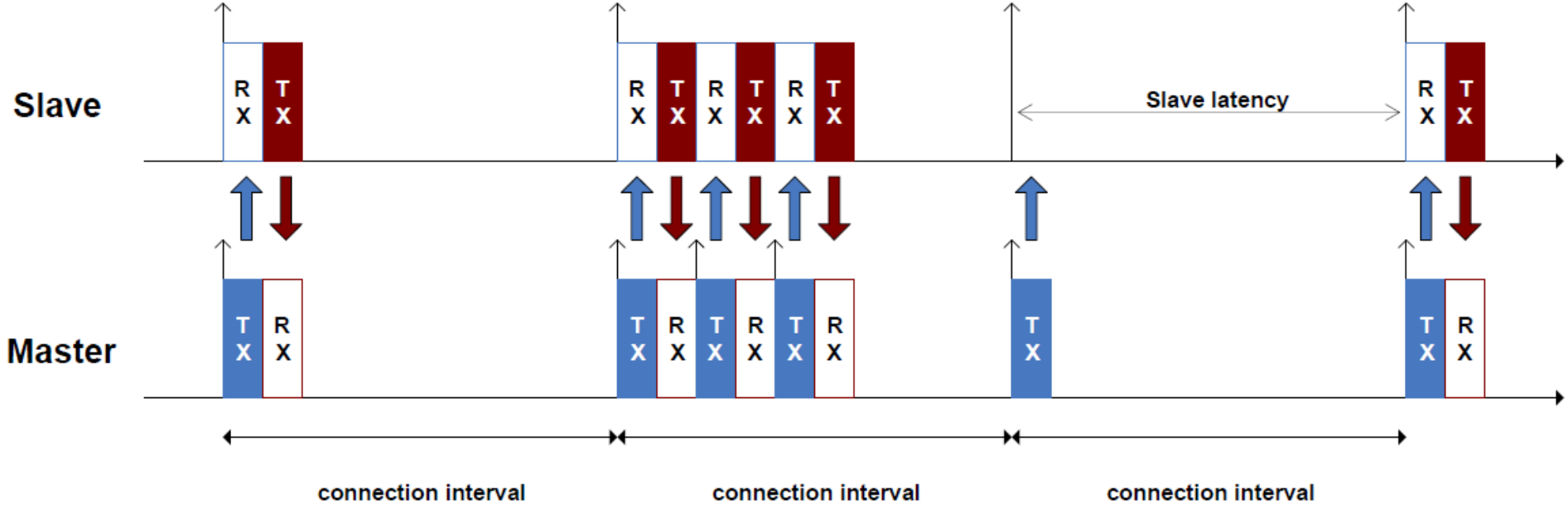
ETABLISSEMENT DE CONNEXION



CONNECT_IND

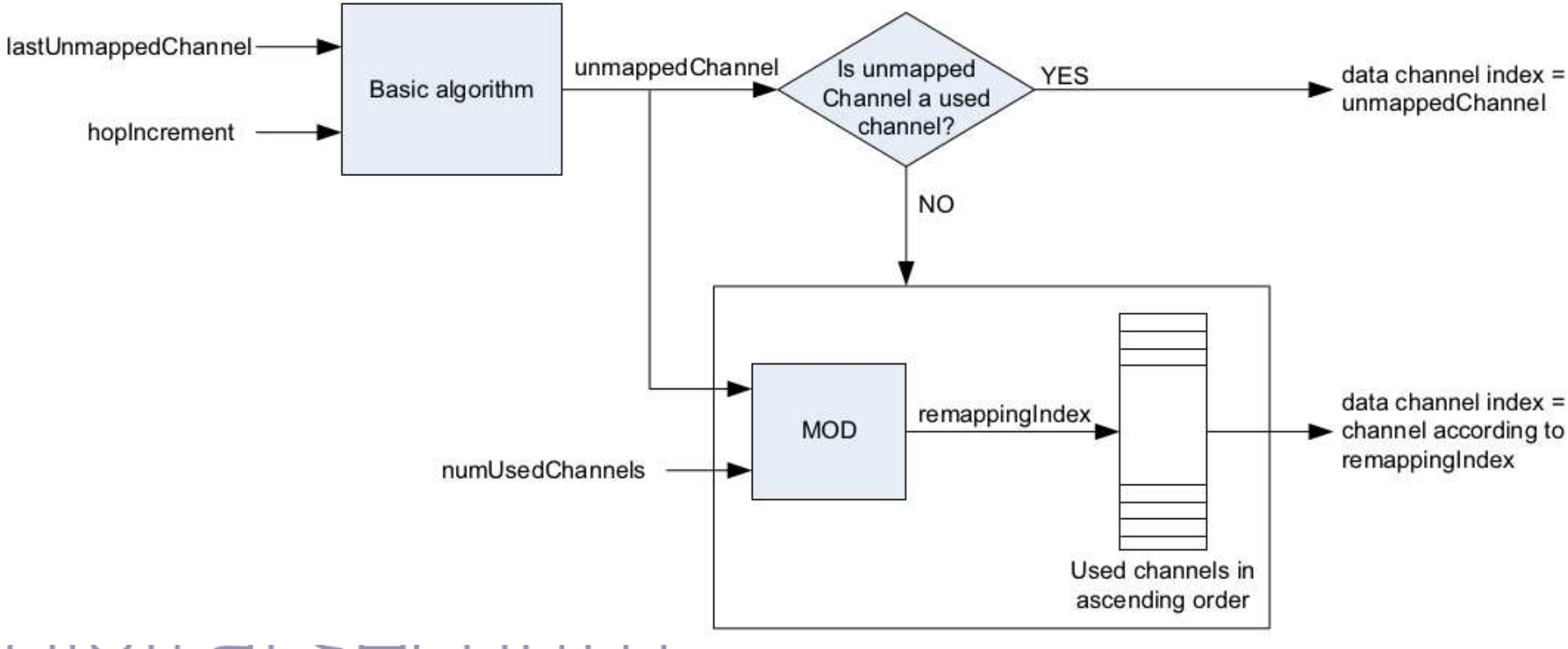
LLData									
AA (4 octets)	CRCInit (3 octets)	WinSize (1 octet)	WinOffset (2 octets)	Interval (2 octets)	Latency (2 octets)	Timeout (2 octets)	ChM (5 octets)	Hop (5 bits)	SCA (3 bits)

MAINTIEN DE LA CONNEXION

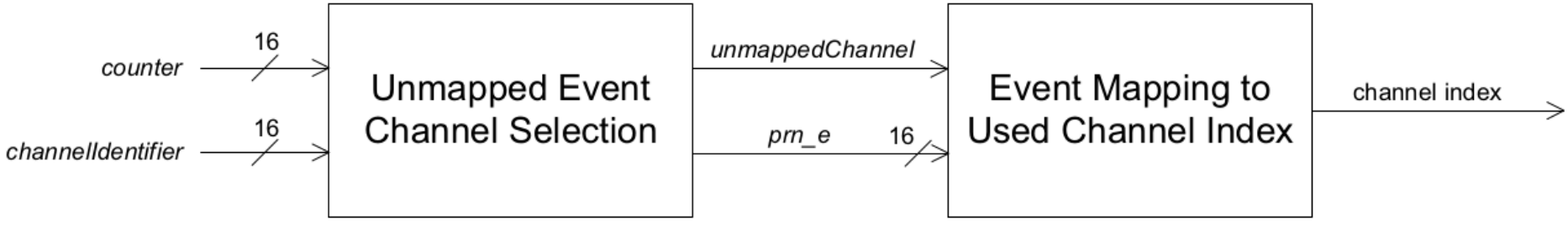


CHANNEL SELECTION ALGORITHM #1

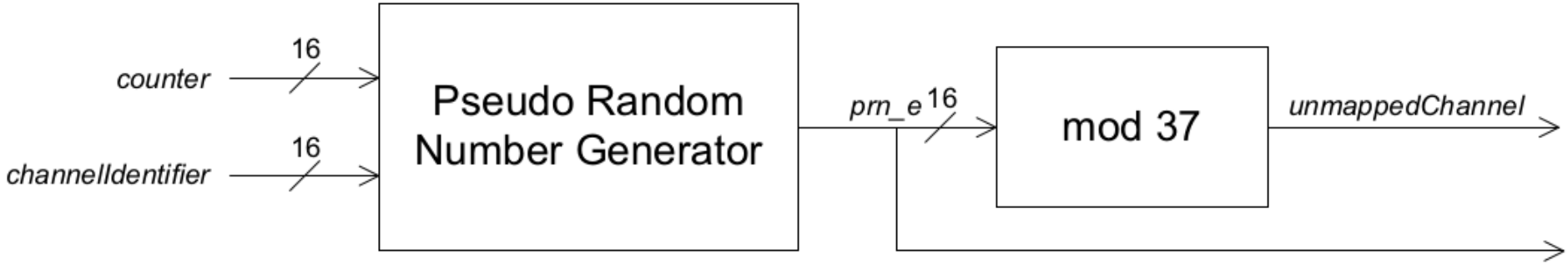
$$C_{n+1}=(C_n + \mathit{hopIncrement}) \text{ Mod } 37$$



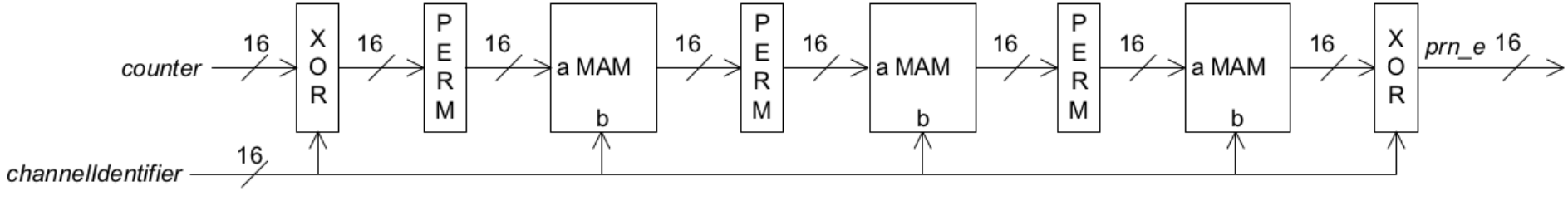
CHANNEL SELECTION ALGORITHM #2



UNMAPPED EVENT CHANNEL SELECTION



CSA#2 PRNG

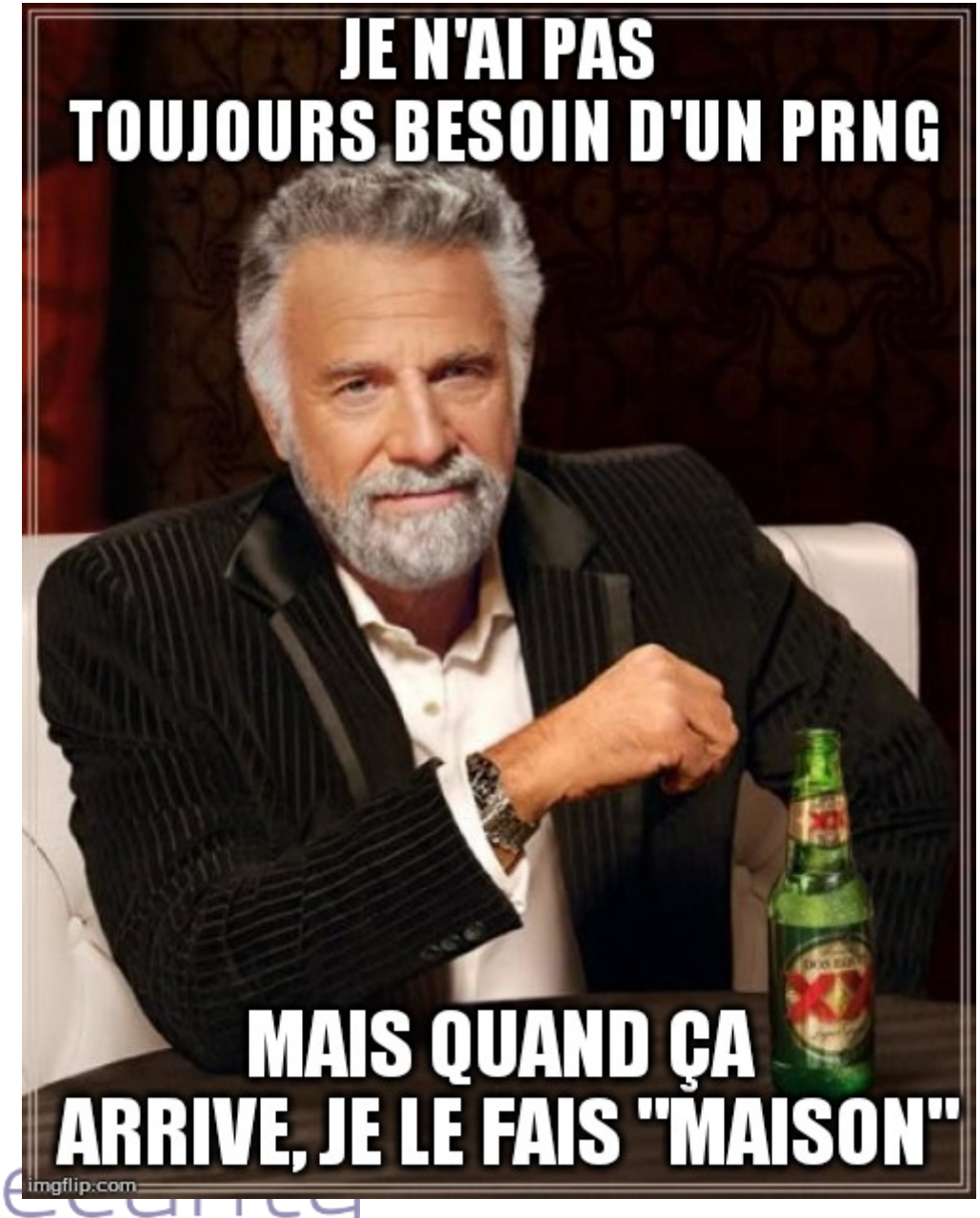


FROM UNMAPPED CHANNEL TO CHANNEL

IMPROVED COEXISTENCE

BLE 4.x a montré **ses faiblesses** en terme de génération de séquence de canaux.

BLE 5 utilise désormais un **PRNG** *maison* pour générer la séquence de canaux.



CHANNEL MAP ET INTERVAL DE SAUT DYNAMIQUES

- Le maître (central) ou l'esclave (peripheral) peuvent renégocier l'**intervalle de saut**

- Le maître (central) peut modifier la *channel map* à tout moment, et indiquer à l'esclave le moment où la bascule se fera

QUID DE LA SÉCURITÉ ?

CONNEXIONS SÉCURISÉES

- **BLE <=4.1**: négociation d'une Short-Term Key (STK) pour sécuriser la communication après échange d'une Temporary Key (TK) via pairing
- **BLE >=4.2**: négociation d'une Long-Term Key (LTK) pour sécuriser les échanges
- BLE 4.2 introduit le support de clés ECDH pour l'échange de la LTK

APPAIRAGE

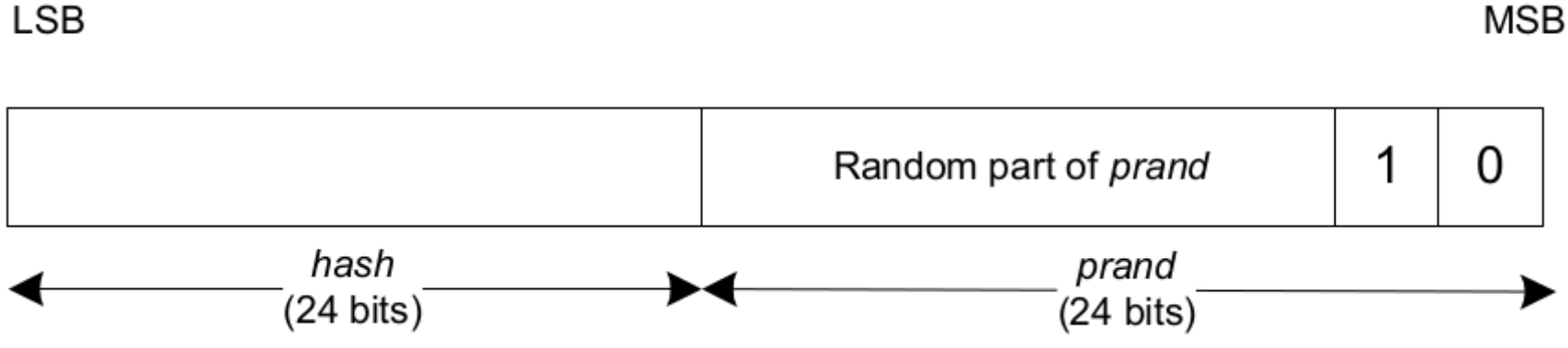
- **JustWorks**: code PIN par défaut (000000)
- **PassKey**: affichage d'un code PIN sur un device, saisie sur le second
- **Comparaison numérique** (>=4.2): affichage d'un code PIN sur les deux devices, et validation utilisateur
- **Out of band**: transmission des données par canal auxiliaire (NFC, QRCode, etc...)

JUSTWORKS, JUSTPWNED

ANONYMISATION DES ADDRESSES BLUETOOTH

- **Adresses privées** résolvables
- **Randomisation à intervalle régulier** des adresses Bluetooth

ADRESSES PRIVÉES RÉSOLVABLES



RANDOMISATION DES ADRESSES

- Les connexions reposent sur une *Access Address* et non sur l'adresse Bluetooth

- Les données d'annonce permettent l'identification d'un périphérique en particulier, notamment grâce au champ *manufacturer*

MATURITÉ DU PROTOCOLE ET DE SES USAGES

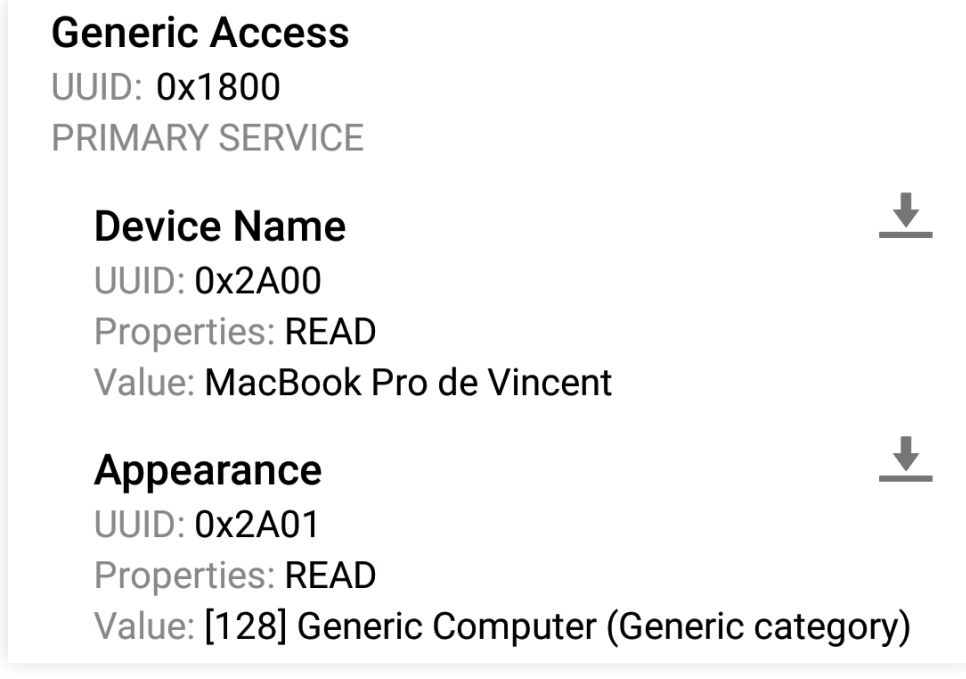
digital.security

MATURITÉ EN TERME DE SÉCURITÉ ?

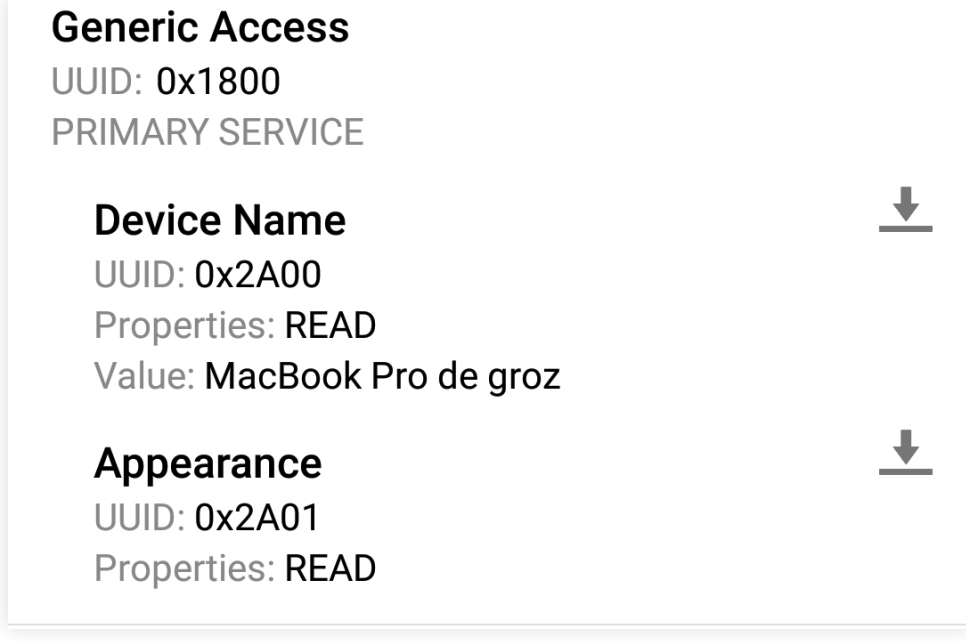
RANDOMISATION DES ADRESSES

- Bonne mesure, mais n'échappe pas au *fingerprinting*
- Les fabricants d'équipements se moquent de la protection de la vie privée

RANDOMISATION DES ADRESSES



RANDOMISATION DES ADRESSES



ECOUTE PASSIVE DES COMMUNICATIONS

- Si on intercepte un *CONNECT_IND* et que la connexion n'est pas chiffrée, c'est plié
- Calculer le *CRCInit* d'une connexion est **trivial**
- Retrouver l'**intervalle de saut** par mesure est facile
- Déduire ensuite l'**incrément de saut** est trivial

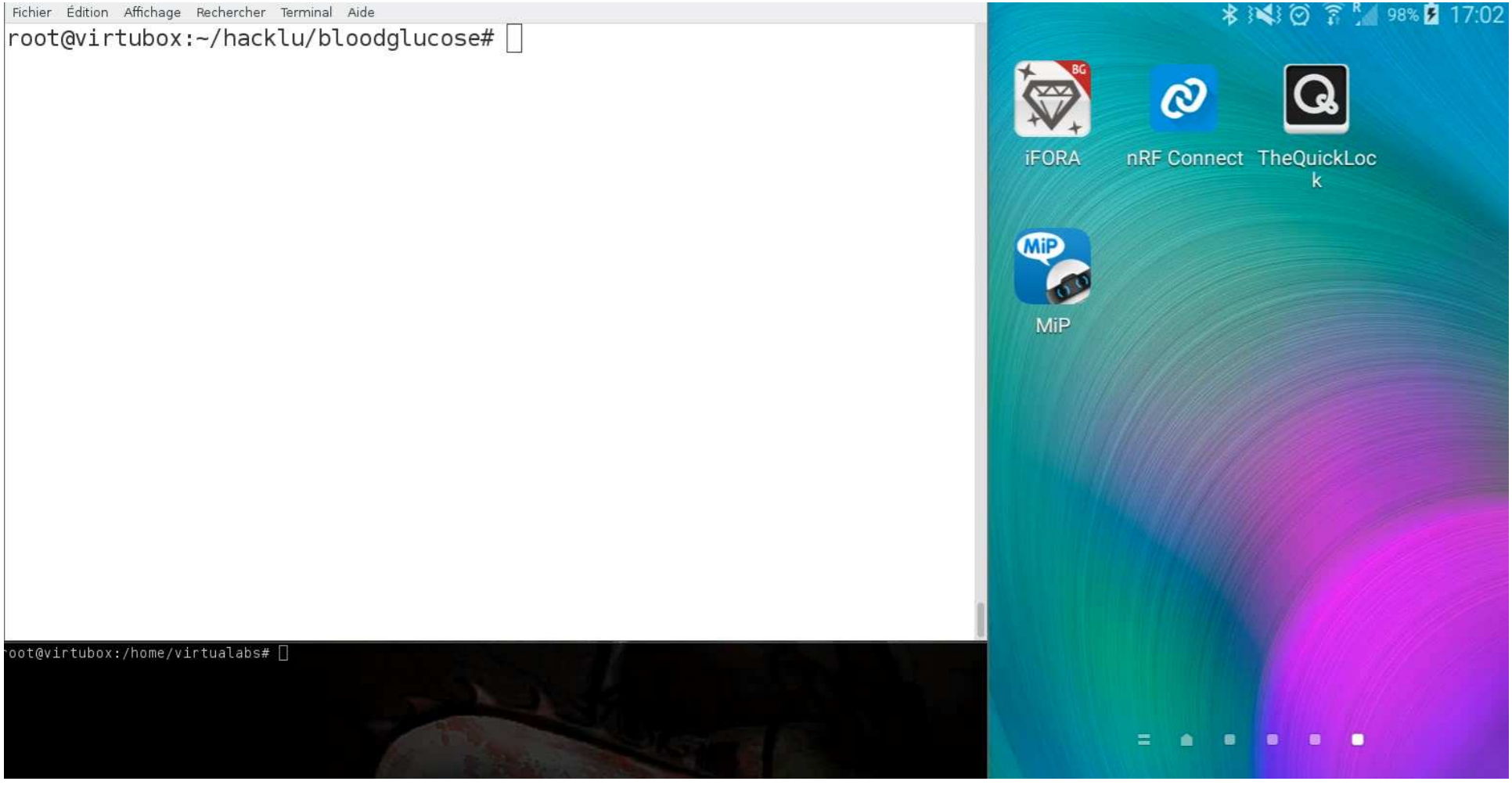
```
virtualabs@virtubox:~/demo$
```

ECOUTE PASSIVE DE COMMUNICATIONS CHIFFRÉES

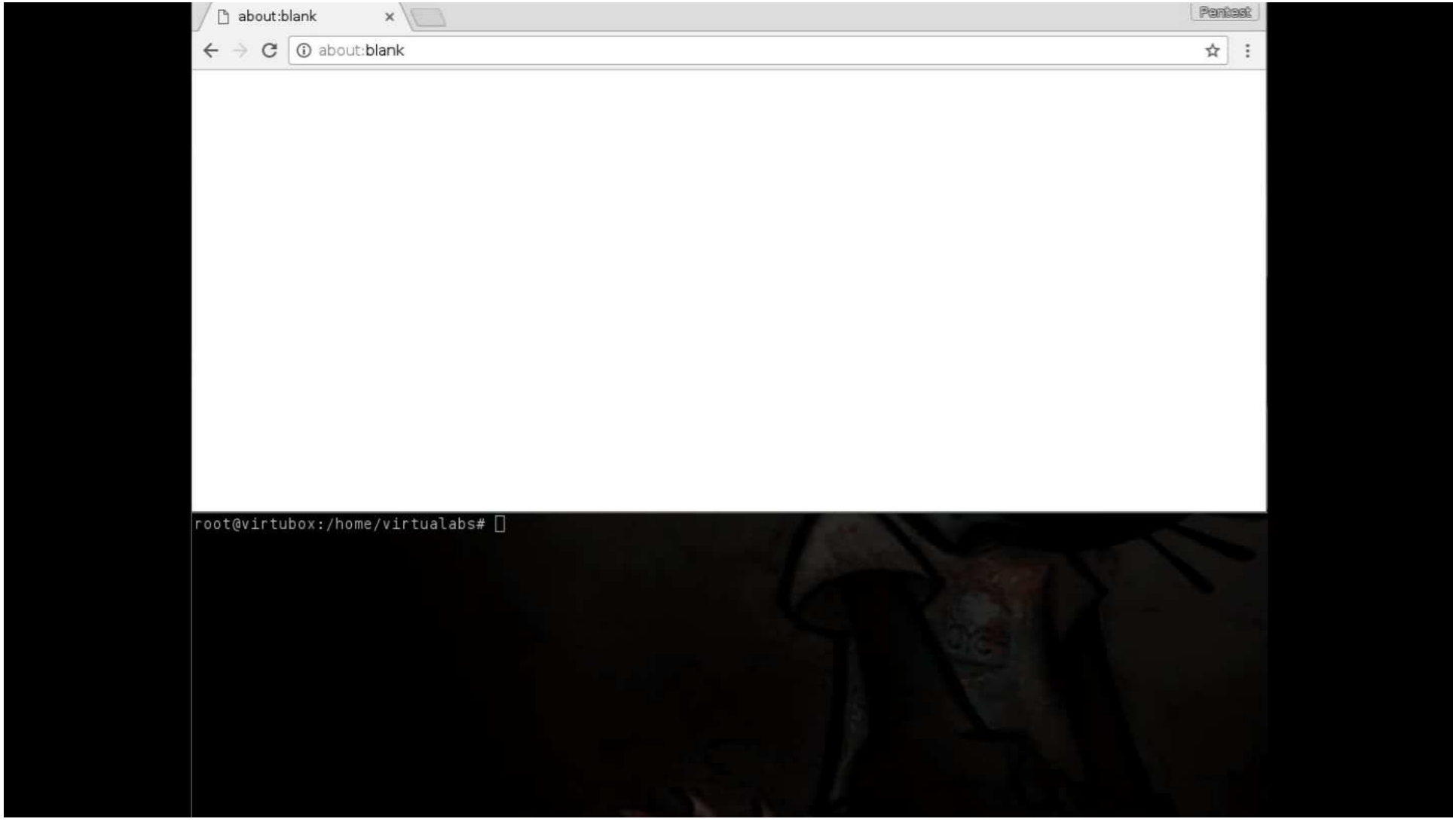
- Interception de l'échange de la Short-Term Key ou de la Long-Term Key si protégée par un code PIN
- Brute-force du code PIN et récupération de la clé
- Déchiffrement des communications

MAN-IN-THE-MIDDLE

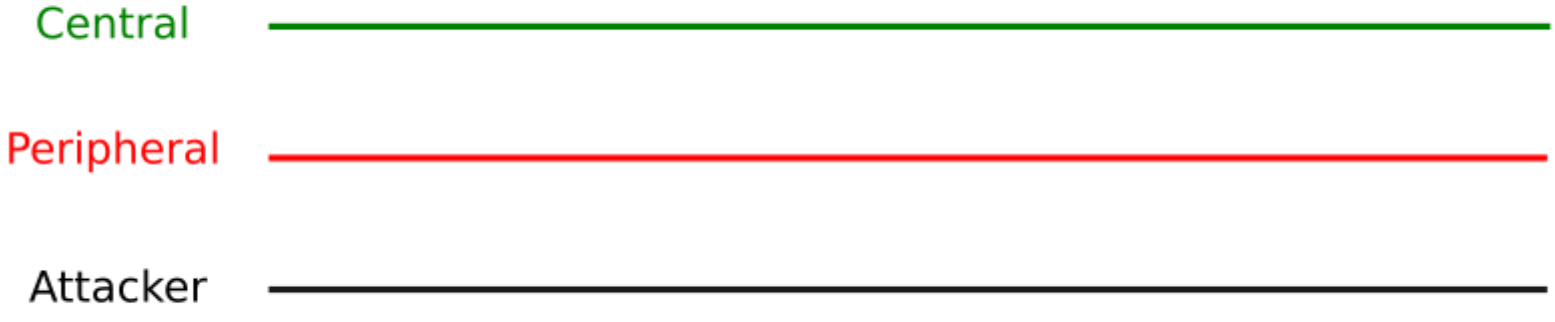
- Absence d'authentification
- Latence du protocole
- Possibilité d'usurper une adresse Bluetooth via un matériel adéquat



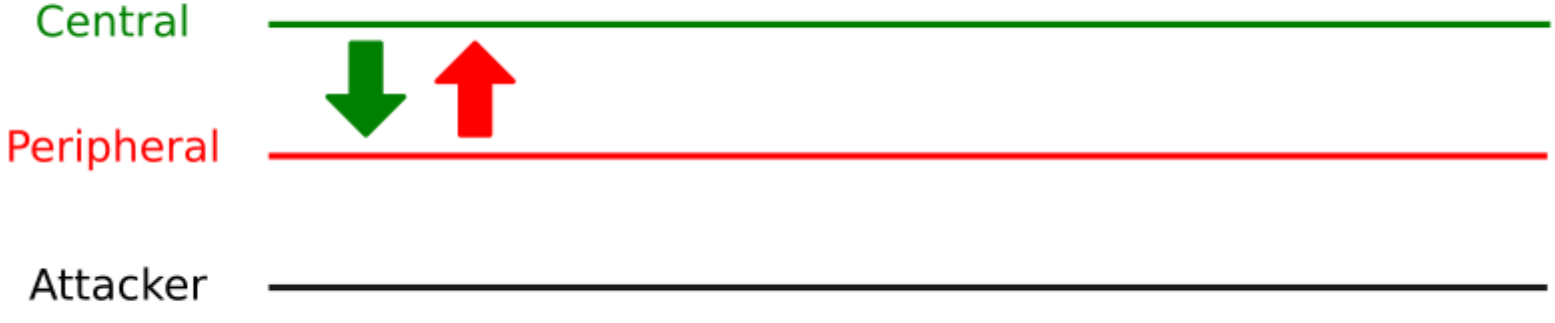
digital.security


about:blank
Pentest
about:blank
root@virtubox:/home/virtualabs#

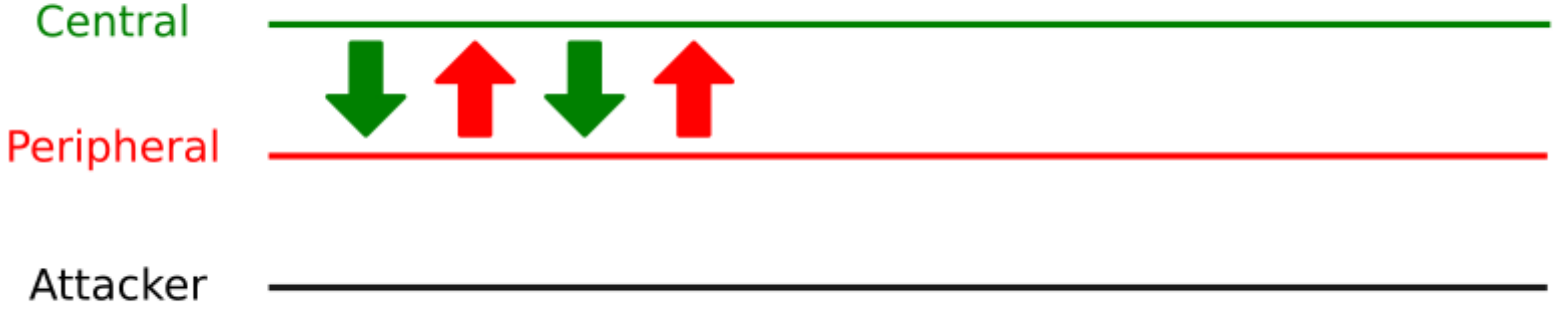
BROUILLAGE RÉACTIF



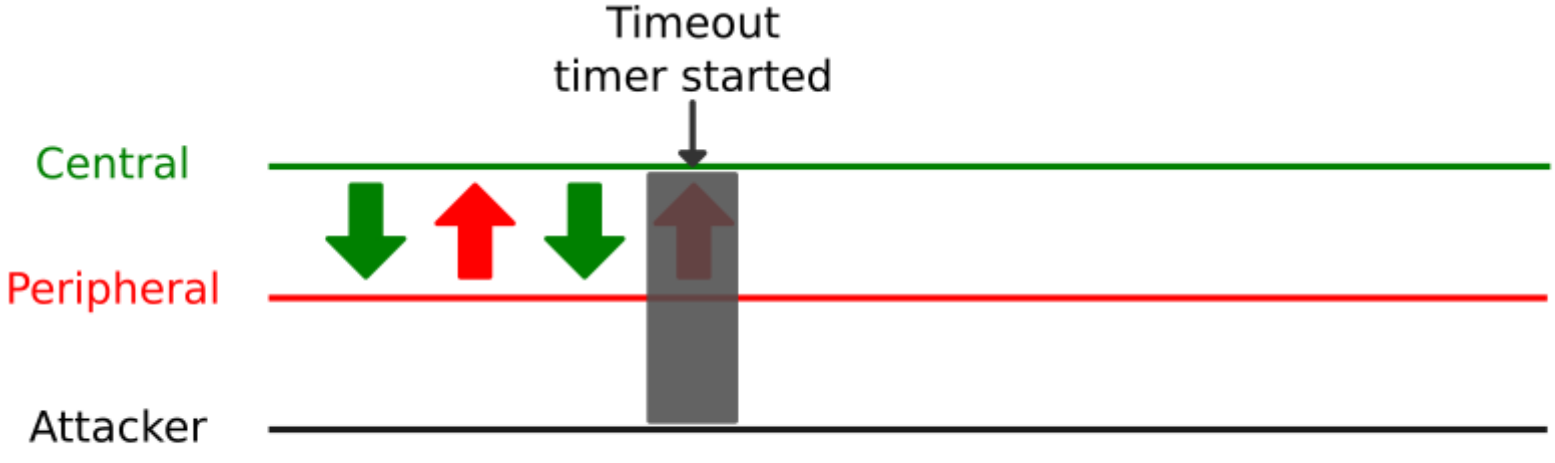
BROUILLAGE RÉACTIF



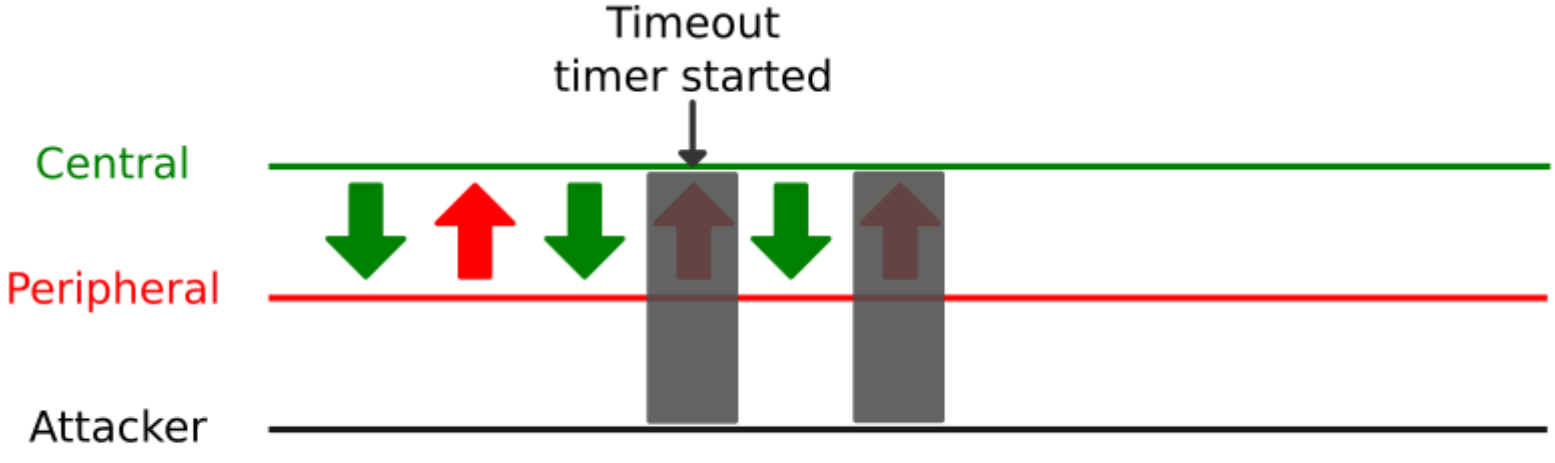
BROUILLAGE RÉACTIF



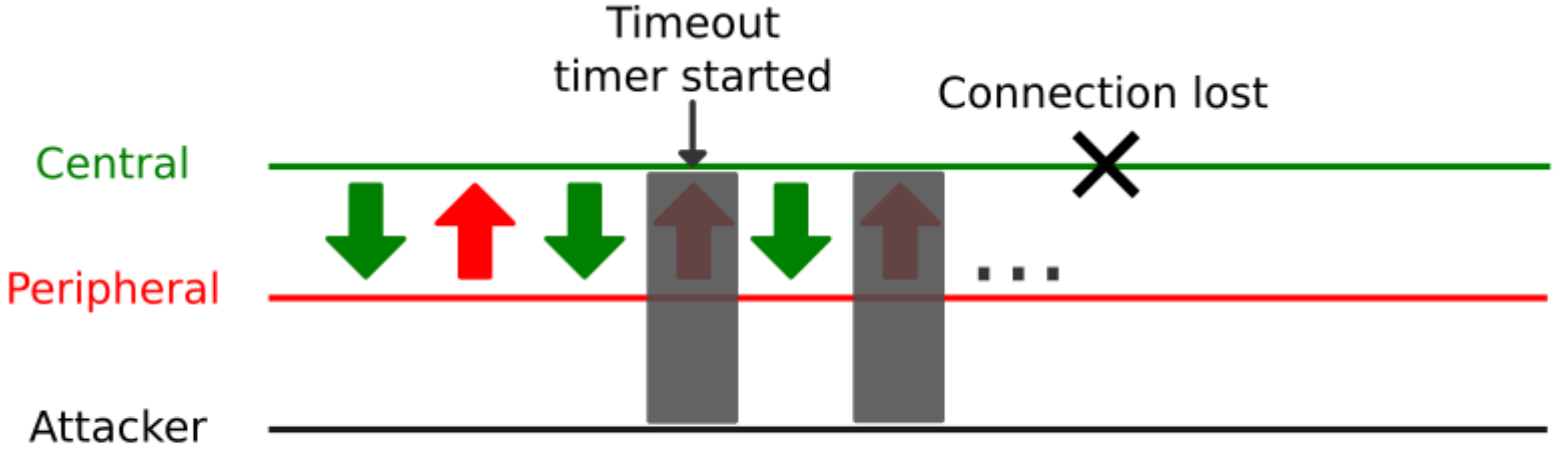
BROUILLAGE RÉACTIF

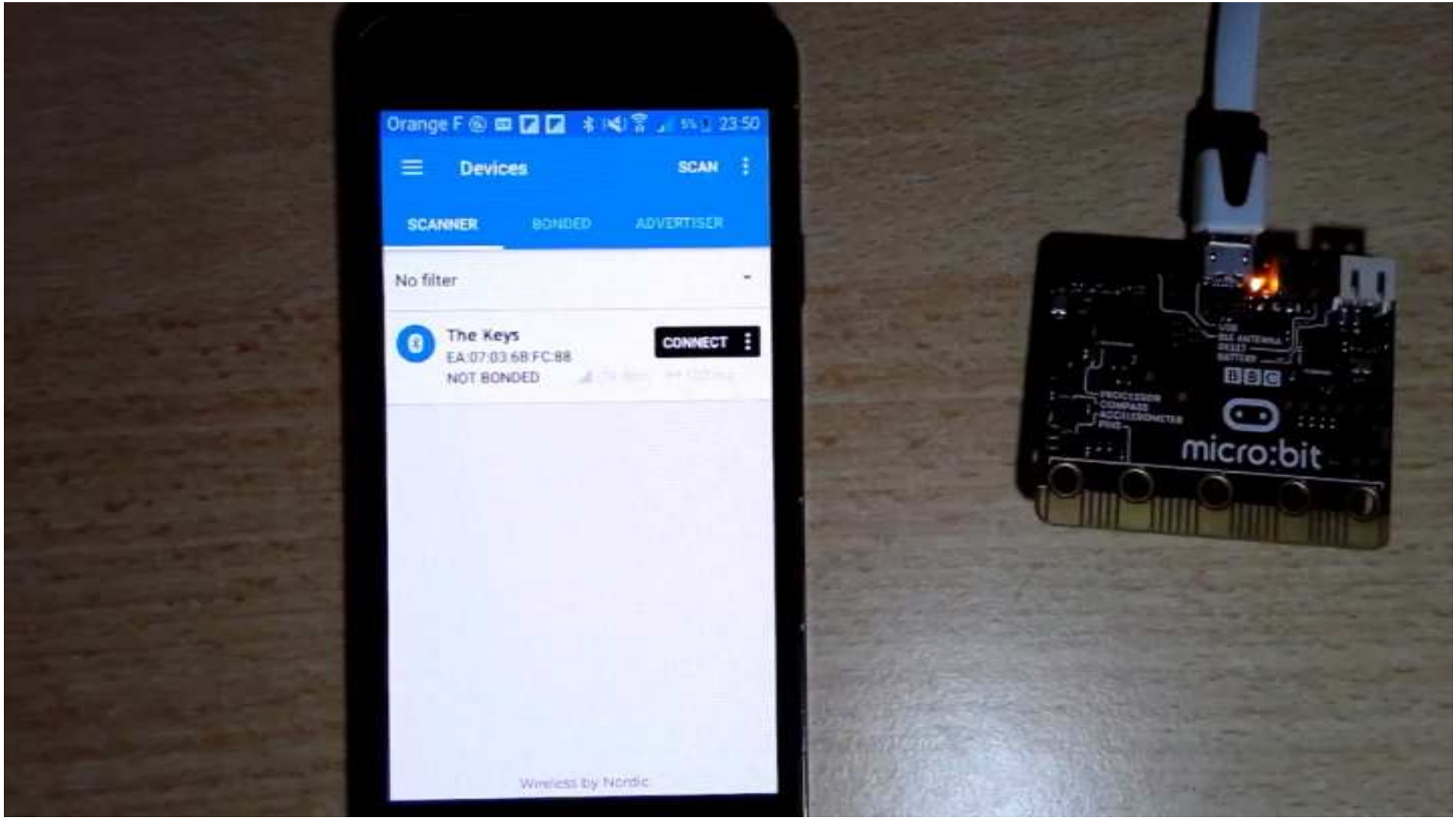


BROUILLAGE RÉACTIF

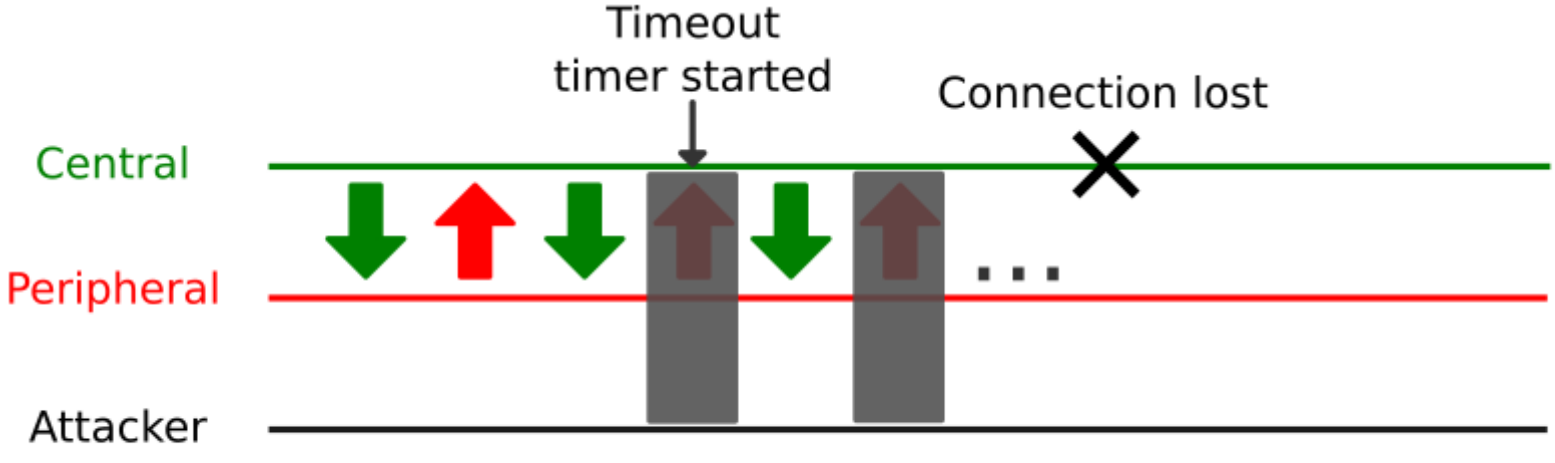


BROUILLAGE RÉACTIF

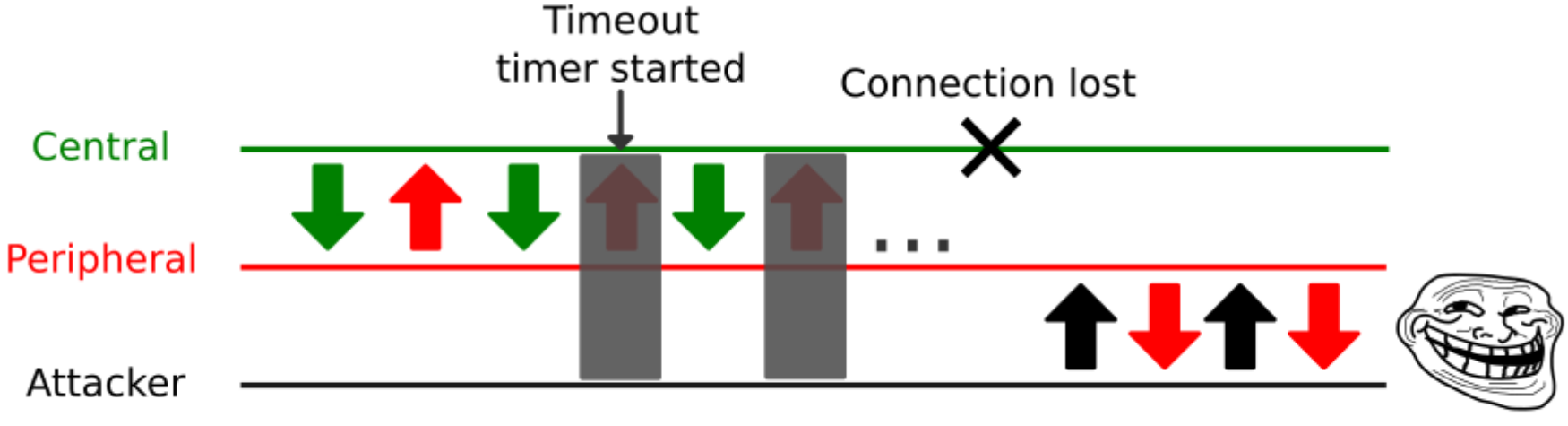


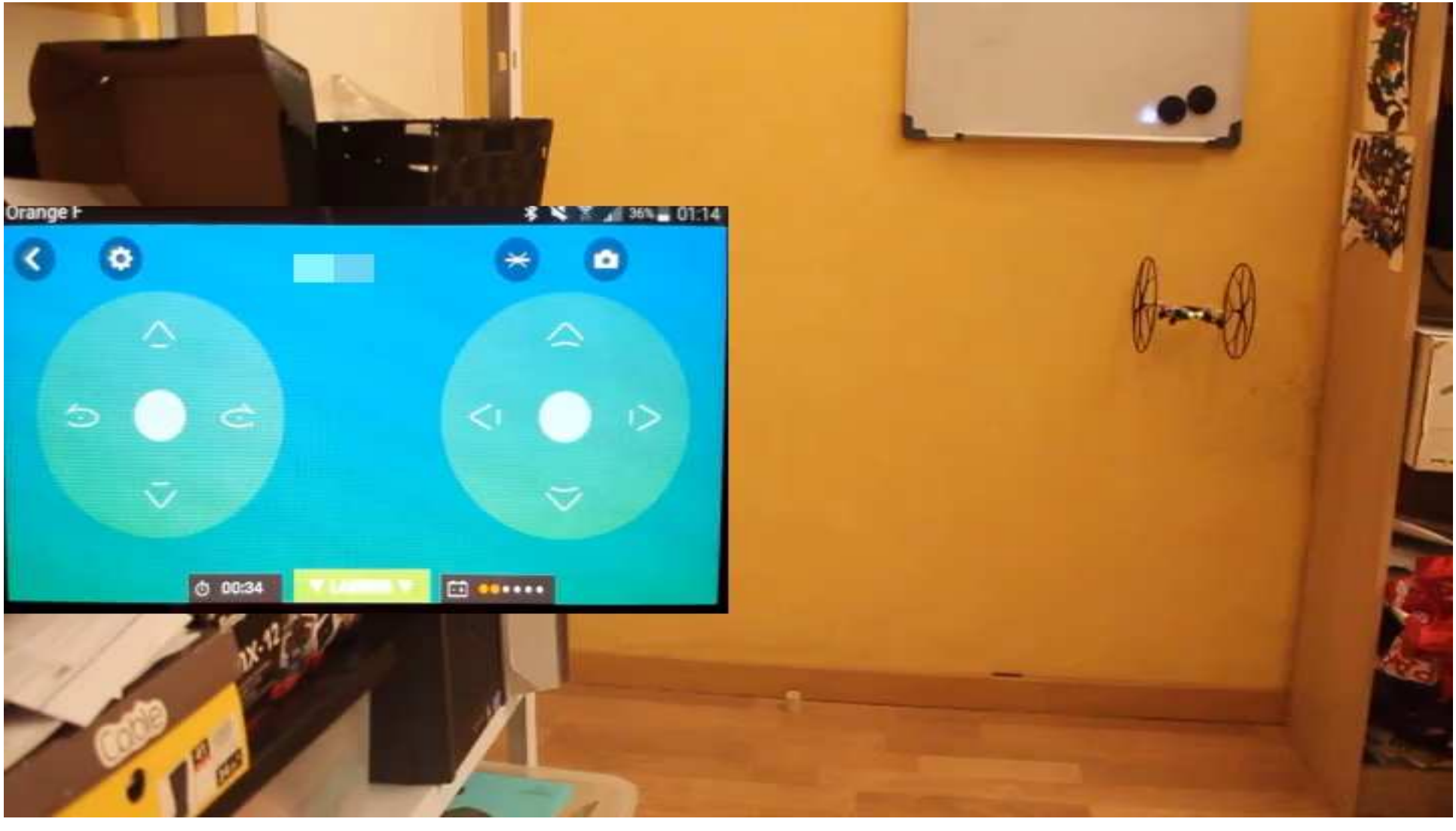

Orange F
23:50
Devices
SCAN
SCANNER
BONDED
ADVERTISER
No filter
The Keys
EA:07:03:6B:FC:88
NOT BONDED
CONNECT
Wireless by Nordic
micro:bit

PRISE DE CONTRÔLE DE CONNEXION



PRISE DE CONTRÔLE DE CONNEXION





digital.security


SAMSUNG
Orange F
11:50
Télécommande
Hush
00:22
NIVEAU MAXIMUM
Boucle
Flotteur
Télécommande traditionnelle
root@virtubox:~/btlejack# ./btlejack -f

MATURITÉ DES USAGES ?

TC

Login

Startups
Apps
Gadgets
Videos
Audio
Extra Crunch NEW

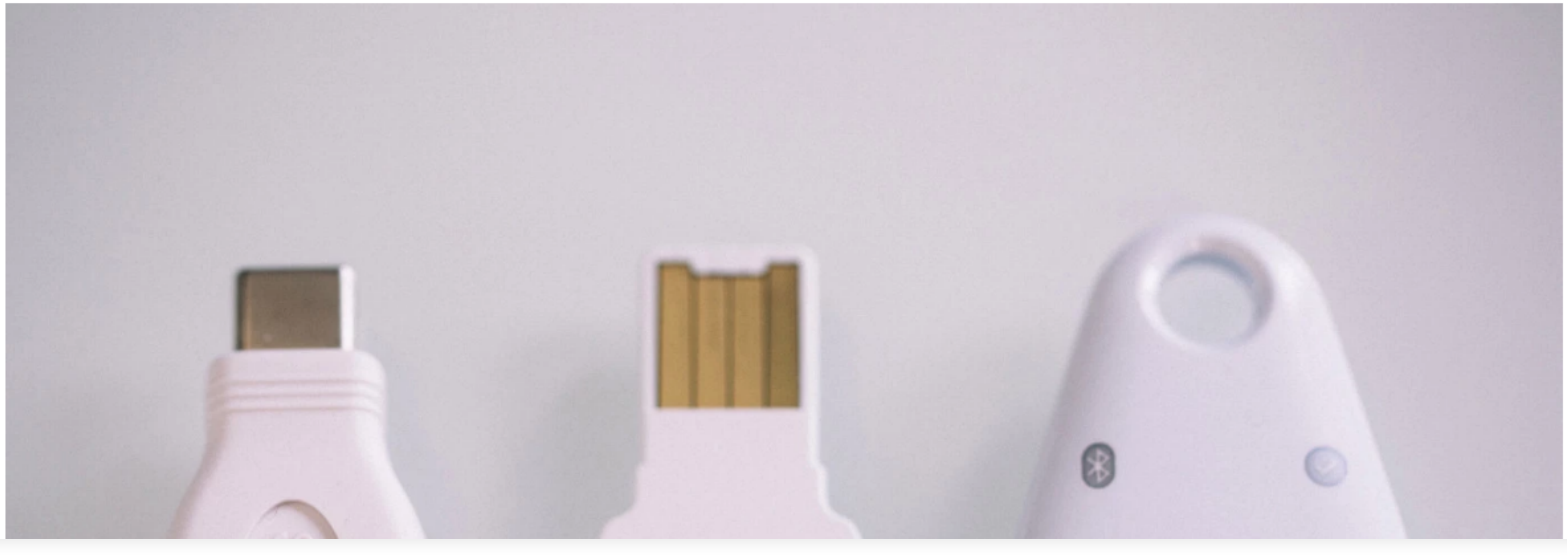
—

Events
Advertise
Crunchbase
More

Google discloses security bug in its Bluetooth Titan Security Keys, offers free replacement

Frederic Lardinois @fredericl / 1 day ago

Comment



SECURITY IS HARD

- Les concepteurs ne veulent pas utiliser les **connexions sécurisées** parce que **ça embête l'utilisateur**
- Ils développent donc des méthodes **alternatives**
- Ces méthodes **exposent les périphériques** à des attaques

TIMELINE DES VERSIONS

- **2010**: version 4.0
- **2013**: version 4.1
- **2014**: version 4.2
- **2016**: version 5
- **2017**: Bluetooth Mesh
- **2019**: Bluetooth 5.1

CONCLUSION

CONCLUSION

- **Protocole immature**, évoluant beaucoup plus vite que ses implémentations
- Fonctions de sécurité **sciemment inutilisées**, bien que certaines soient efficaces
- Sujet à **plusieurs attaques connues** depuis 2013, toujours fonctionnelles
- Volonté d'en faire un protocole utilisable à **longue distance**

USAGES FUTURS DE BLE

- Radiocommande moyenne distance (< 800 m) d'engins/équipements
- Localisation à moyenne distance
- Transfert rapide de données de proximité
- Nouveaux usages dans le domaine médical (hospitalisation de jour, suivi et surveillance)

MERCI DE VOTRE ATTENTION, DES QUESTIONS ?

Contact

damien.cauquil@digital.security

@virtualabs

digital.security