Quelques travaux de recherche dans la cybersécurité de l'IoT…

Guillaume Auriol
INSA Toulouse – LAAS-CNRS

Remerciements!

- Romain Cayre (MC Eurecom)
- Florent Galtier (IR LAAS-CNRS)
- Paul Olivier (Post Doc LAAS-CNRS)

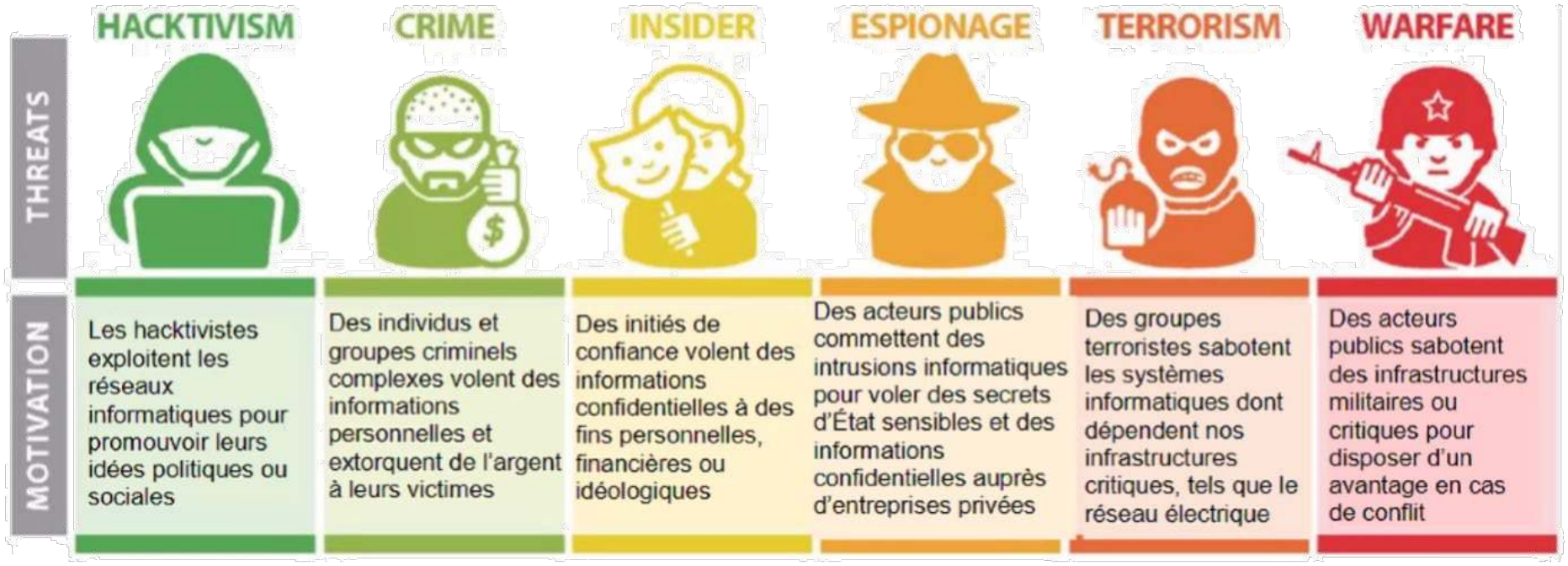
La plus grande part des travaux présentée dans ce support, c’est eux!

Cybersécurité et IoT

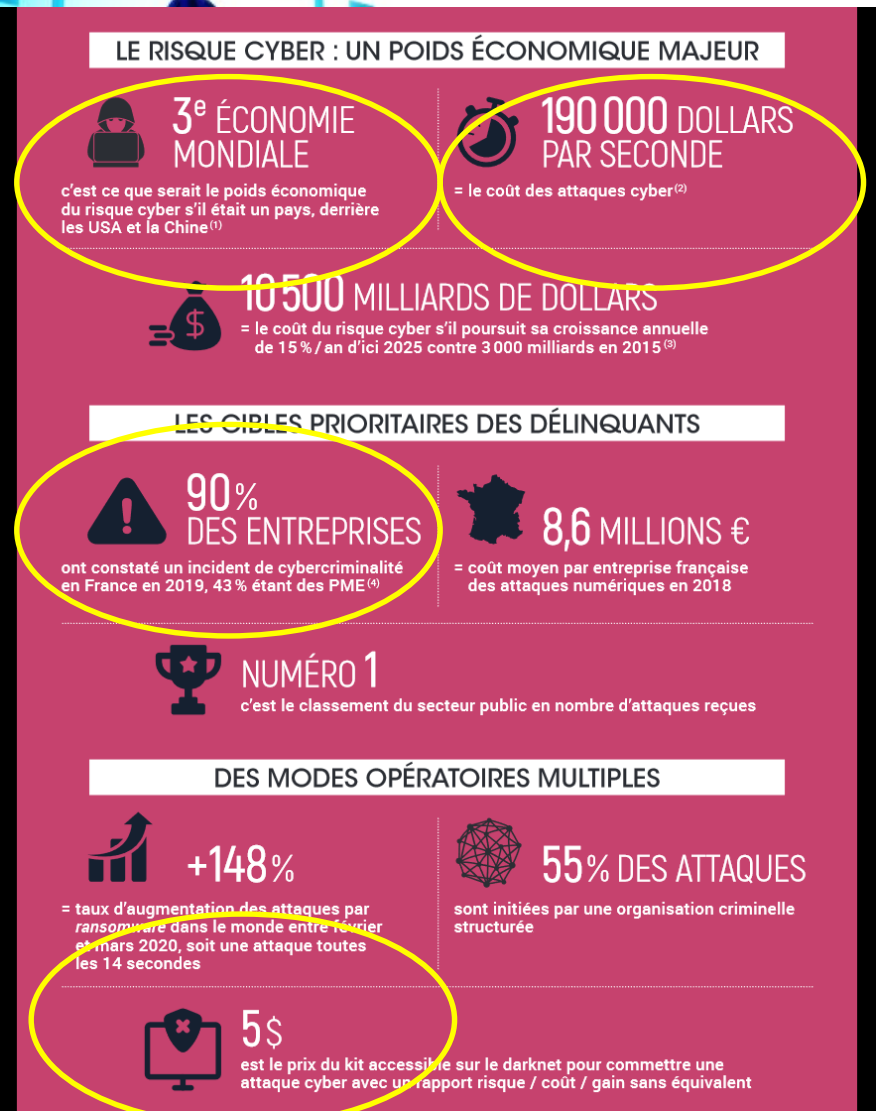
…

ne font pas bon ménage!

Cybersécurité vs. cybercriminalité

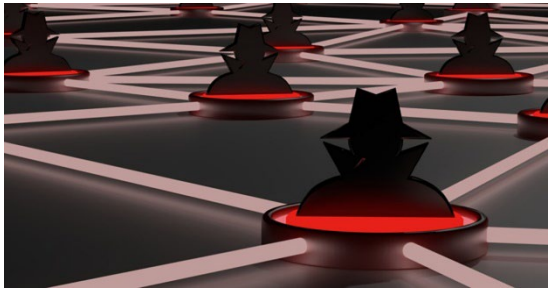


Cybersécurité vs. cybercriminalité



Objets connectés

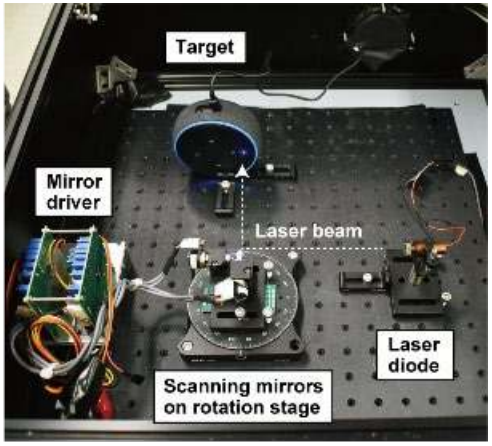
Cybersécurité et Objets connectés



Venezuela juin 2018 : l'attentat aux drones contre Maduro revendiqué par Los Soldados de Franelas

[Wiki] **Mirai** (未来), mot japonais pour « avenir ») est un logiciel malveillant qui transforme des ordinateurs utilisant le système d'exploitation Linux en *bots* contrôlés à distance, formant alors un botnet utilisé notamment pour réaliser des attaques à grande échelle sur les réseaux. Il cible principalement les dispositifs grand public tels que des caméras pilotables à distance ou encore des routeurs pour la maison[1]. Un ou plusieurs botnets Mirai ont été utilisés dans certaines des plus importantes et percutantes attaques en déni de service distribué (DDoS).

Cybersécurité et Objets connectés

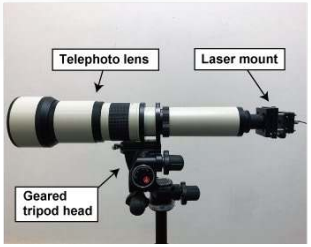


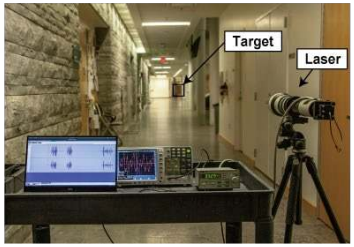
Light Commands:
Laser-Based Audio Injection on Voice-Controllable Systems

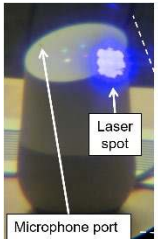
Takeshi Sugawara, **Benjamin Cyr,**
Sara Rampazzi, Daniel Genkin, Kevin Fu

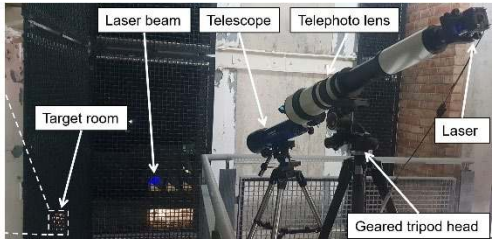
UEC TOKYO

M | CSE COMPUTER SCIENCE AND ENGINEERING UNIVERSITY OF MICHIGAN



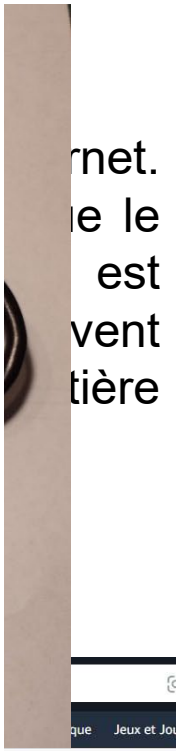


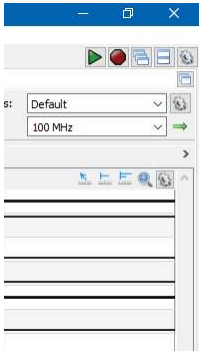




Device	Voice Recognition System	Minimun Laser Power at 30 cm [mW]	Max Distance at 60 mW [m]*	Max Distance at 5 mW [m]**
Google Home	Google Assistant	0.5	50+	110+
Google Home mini	Google Assistant	16	20	-
Google NEST Cam IQ	Google Assistant	9	50+	-
Echo Plus 1st Generation	Amazon Alexa	2.4	50+	110+
Echo Plus 2nd Generation	Amazon Alexa	2.9	50+	50
Echo	Amazon Alexa	25	50+	-
Echo Dot 2nd Generation	Amazon Alexa	7	50+	-
Echo Dot 3rd Generation	Amazon Alexa	9	50+	-
Echo Show 5	Amazon Alexa	17	50+	-
Echo Spot	Amazon Alexa	29	50+	-
Facebook Portal Mini	Alexa + Portal	18	5	-
Fire Cube TV	Amazon Alexa	13	20	-
EchoBee 4	Amazon Alexa	1.7	50+	70
iPhone XR	Siri	21	10	-
iPad 6th Gen	Siri	27	20	-
Samsung Galaxy S9	Google Assistant	60	5	-
Google Pixel 2	Google Assistant	46	5	-

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
0004c790	6f	67	20	69	6e	2c	20	70	6c	65	61	73	65	20	75	73	og in, please us
0004c7a0	65	20	3a	20	75	73	65	72	6e	61	6d	65	2f	70	61	73	e : username/pas
0004c7b0	73	77	6f	72	64	2e	20	44	65	66	61	75	6c	74	20	69	sword. Default i
0004c7c0	73	20	61	64	6d	69	6e	2f	61	64	6d	69	6e	3c	62	72	s admin/admin<br
0004c7d0	3e	00	55	73	65	72	3a	3c	69	6e	70	75	74	20	74	79	>.User:<input ty
0004c7e0	70	65	3d	27	74	65	78	74	27	20	6e	61	6d	65	3d	27	pe='text' name='
0004c7f0	55	53	45	52	4e	41	4d	45	27	20	70	6c	61	63	65	68	USERNAME' placeh
0004c800	6f	6c	64	65	72	3d	27	75	73	65	72	20	6e	61	6d	65	older='user name
0004c810	27	3e	3c	62	72	3e	00	50	61	73	73	77	6f	72	64	3a	'> .Password:
0004c820	3c	69	6e	70	75	74	20	74	79	70	65	3d	27	70	61	73	<input type='pas
0004c830	73	77	6f	72	64	27	20	6e	61	6d	65	3d	27	50	41	53	sword' name='PAS
0004c840	53	57	4f	52	44	27	20	70	6c	61	63	65	68	6f	6c	64	SWORD' placehold
0004c850	65	72	3d	27	70	61	73	73	77	6f	72	64	27	3e	3c	62	er='password'><b
0004c860	72	3e	00	3c	69	6e	70	75	74	20	74	79	70	65	3d	27	r>.<input type='
0004c870	73	75	62	6d	69	74	27	20	6e	61	6d	65	3d	27	53	55	submit' name='SU
0004c880	42	4d	49	54	27	20	76	61	6c	75	65	3d	27	53	75	62	BMIT' value='Sub
0004c890	6d	69	74	27	3e	3c	2f	66	6f	72	6d	3e	3c	70	3e	00	mit'></form> .
0004c8a0	59	6f	75	20	61	6c	73	6f	20	63	61	6e	20	67	6f	20	You also can go
0004c8b0	3c	61	20	68	72	65	66	3d	27	2f	69	6e	6c	69	6e	65	<a href='/inline
0004c8c0	27	3e	68	65	72	65	3c	2f	61	3e	3c	2f	70	3e	3c	2f	'>here </
0004c8d0	62	6f	64	79	3e	3c	2f	68	74	6d	6c	3e	00	30	78	30	body></html>.0x0
0004c8e0	30	00	61	35	37	63	62	63	63	65	36	31	63	37	64	39	0.a57cbcce61c7d9
0004c8f0	30	61	31	39	38	65	33	61	62	39	31	36	39	31	35	30	0a198e3ab9169150
0004c900	31	39	31	62	63	66	30	62	39	32	66	38	32	64	63	30	191bcf0b92f82dc0
0004c910	64	61	37	37	61	31	62	32	64	62	62	38	62	62	63	65	da77a1b2dbb8bbce
0004c920	31	32	00	72	74	70	61	73	73	77	64	00	00	00	00	00	12.rtpasswd.....
0004c930	00	00	61	64	6d	69	6e	00	53	65	6b	72	65	74	50	34	..admin.SekretP4
0004c940	73	35	5f	32	38	46	39	35	41	46	41	00	45	53	50	72	s5_28F95AFA.ESPr
0004c950	65	73	73	6f	31	5f	30	30	31	39	00	00	00	63	82	53	esso1_0019...c,S
0004c960	63	25	64	00	28	1a	14	00	00	00	00	00	00	00	00	00	c%d.(.....
0004c970	00	00	00	50	00	25	73	20	25	75	0a	00	00	70	6d	00	...P.%s %u...pm.
0004c980	00	66	70	6d	00	70	70	00	00	18	fe	34	00	64	65	76	.fpm.pp...þ4.dev
0004c990	00	6d	61	63	00	2c	01	00	f6	f4	f8	f0	f5	f1	f2	f3	.mac.,..öôøðõñòó
0004c9a0	f9	fa	fb	fc	fd	fe	ff	00	f4	f6	f7	f8	f2	f5	f1	f8	ùúûüýþÿ.ôö÷øòõñø
0004c9b0	f3	f9	fa	fb	fc	fd	fe	ff	00	ff	ff	ff	ff	ff	ff	00	óùúûüýþÿ.ÿÿÿÿÿÿ.



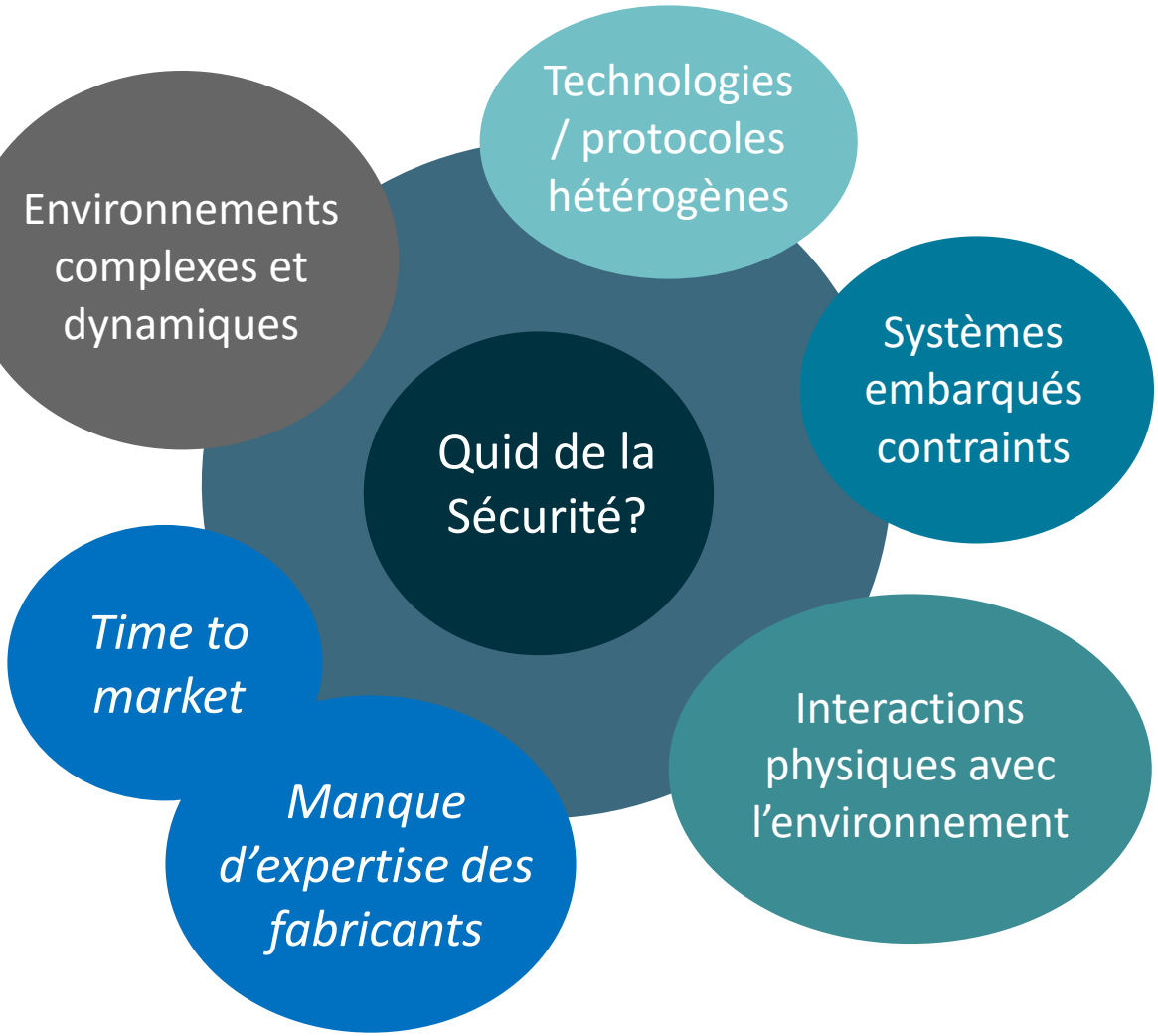


Cybersécurité et IoT

Equipe TSF au LAAS-CNRS

Cybersécurité et Objets connectés

- Contexte et enjeux



Problématiques

- Offensif
  - Identifier et évaluer les nouvelles menaces présentes dans les protocoles de l'IoT
  - Automatiser l'audit des protocoles de l'IoT
- Défensif
  - Concevoir des mécanismes de détection d'intrusion et de remédiation

Doctorants et Post Doc

(cyber IoT)

- 2012 – 2015 : Yann Bachy, LAAS-CNRS, Thalès
  - *« Sécurité des équipements grand public connectés à Internet : évaluation des liens de communication »*
- 2016 – 2020 : Jonathan Roux, LAAS-CNRS
  - *« Détection d'intrusion dans des environnements connectés sans fil par l'analyse de l'activité radio »*
- 2020 – 2023 : Florent Galtier, LAAS-CNRS
  - *« Sécurité des réseaux sans fil à courte et longue portée basée sur des mécanismes de monitoring de la couche physique »*
- 2020 – 2023 : Romain Cayre, LAAS-CNRS, Airbus Protect
  - *« Offensive and defensive approaches for wireless communication protocols security in IoT »*
- 2023 – 2026 : Louis Lolive, IRT Saint Exupéry, projet ANR Cyber Space Simulation (CSS)
  - *« Mécanismes embarqués dans les satellites de détection d'intrusion »*

- 2023-2024 : Paul Olivier, LAAS-CNRS, PEPR Superviz
  - *« Mécanismes embarqués dans l'IoT de détection d'intrusion*

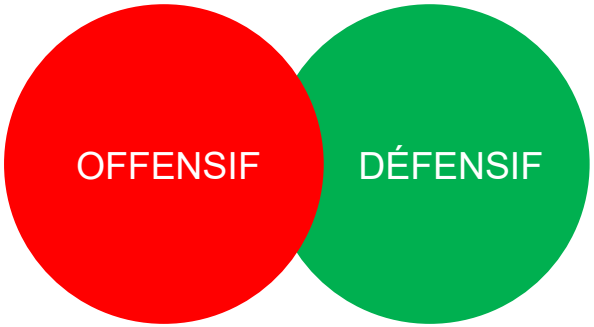
Encadrants : Eric Alata, Guillaume Auriol, Mohamed Kaâniche, Vincent Nicomette

Travaux récents

Framework offensif
pour l'audit des technologies sans fil (Mirage)

Fingerprinting
physique pour l'IoT

Attaques pivot inter-protocolaires
application au BLE et 802.15.4 (WazaBee)



Framework de détection d'intrusion
embarqué dans les contrôleurs Bluetooth (Oasis)

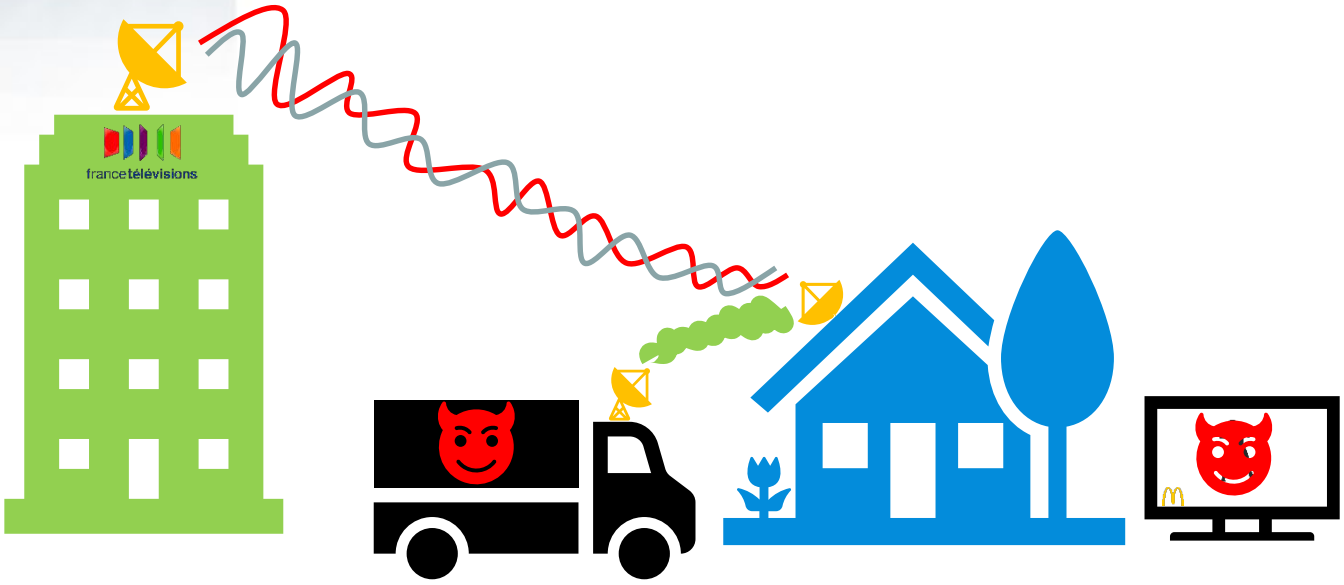
Attaques bas niveau
application à l'injection de trame Bluetooth Low Energy (InjectaBLE)

Quelques travaux de recherche

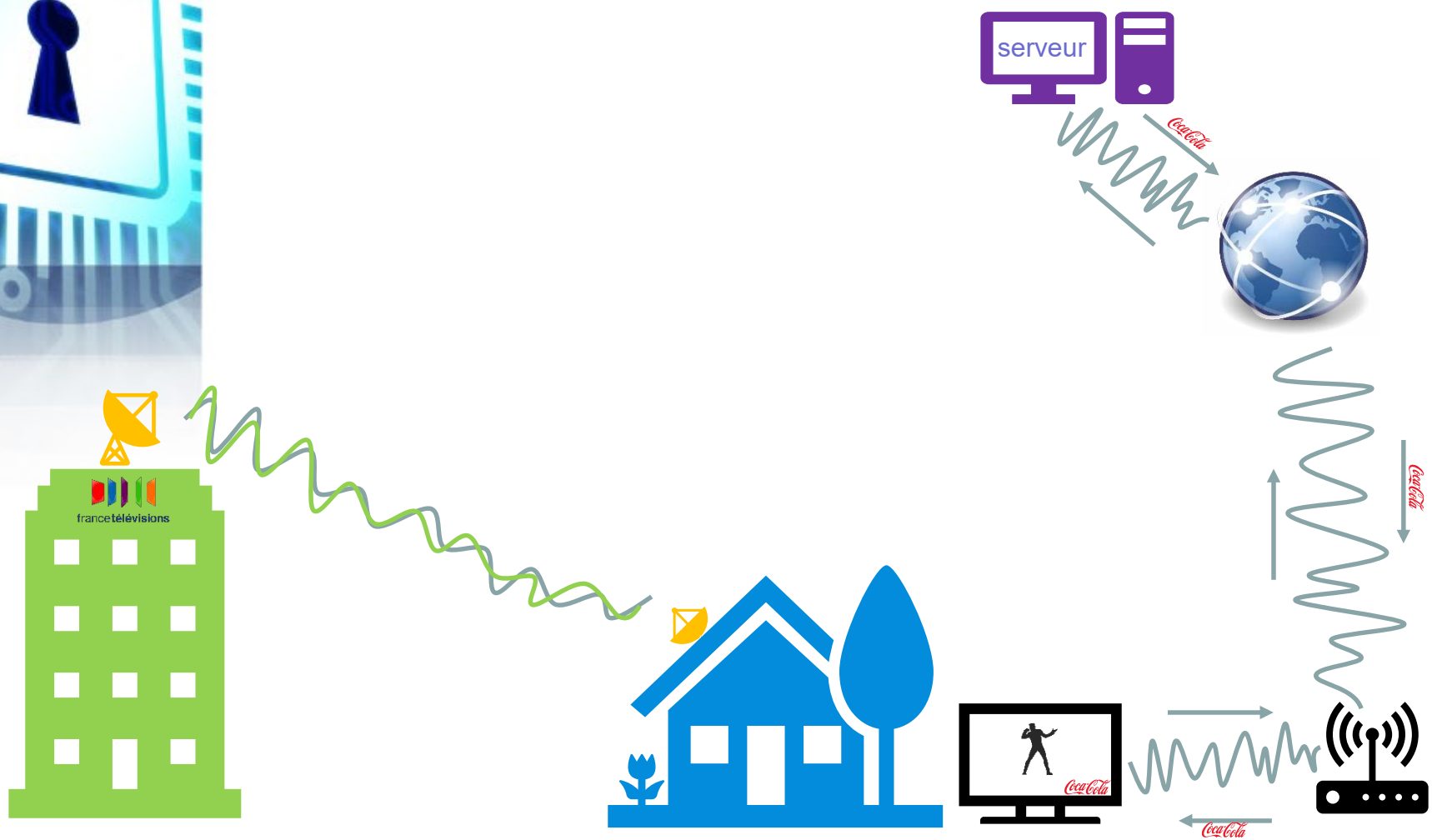
Plan

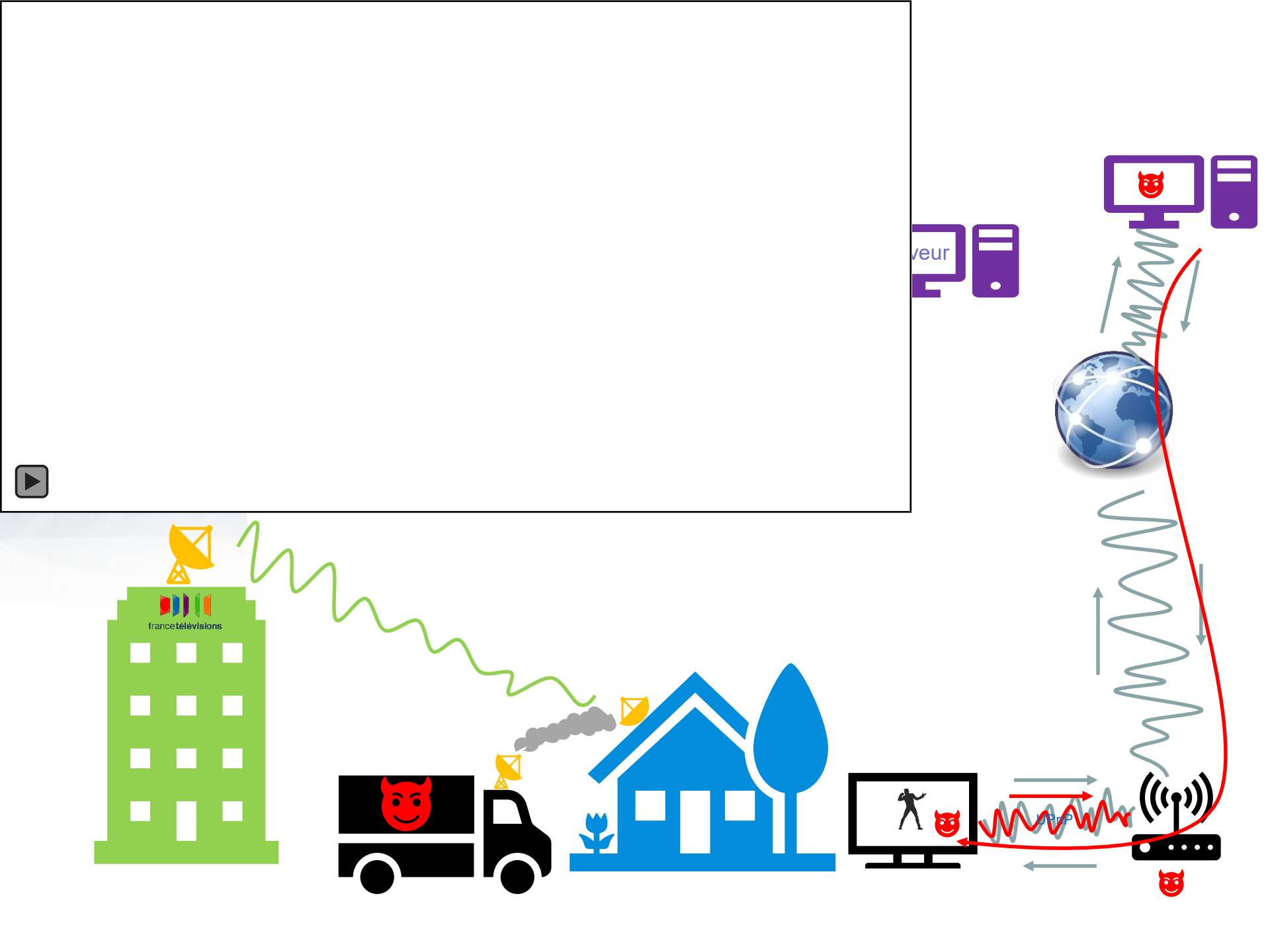
- Vulnérabilités DVB : smart TV
- Mirage, framework offensif pour l'audit des technologies sans fils : clavier et souris sans fils
- Wazabee, attaque cross-protocoles : smart Phone et capteur XBee
- Injectable, exploitation d'une vulnérabilité BLE : ampoule Philips Hue
- Fingerprint, détection de spoofing d'adresses MAC : ampoule Philips Hue et modules XBee

Vulné



Vulnérabilités DVB




veur
francetélévisions
UPnP

Mirage

- Automatiser les audit sécurité dans un environnement IoT
  - Comment générer des attaques réalistes ?
  - Comment simuler le comportement d'un attaquant ?

API unifiée

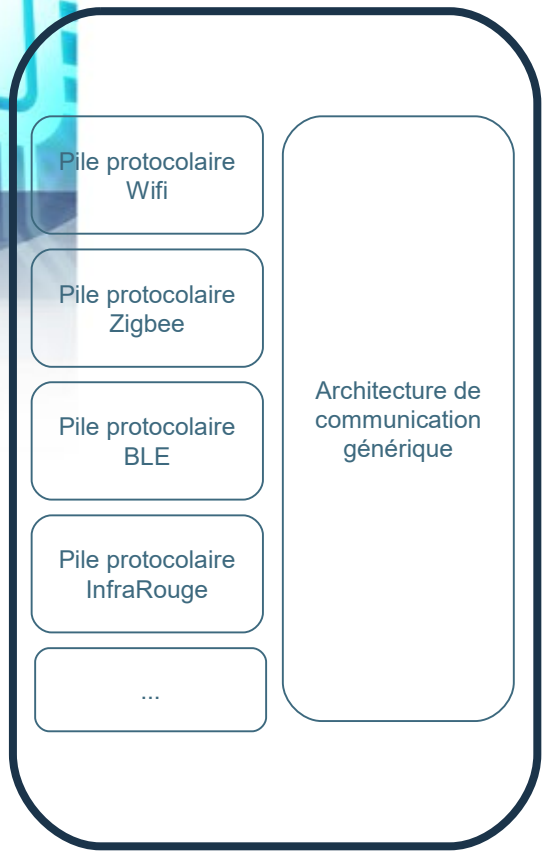
Modularité et réutilisabilité

Généricité

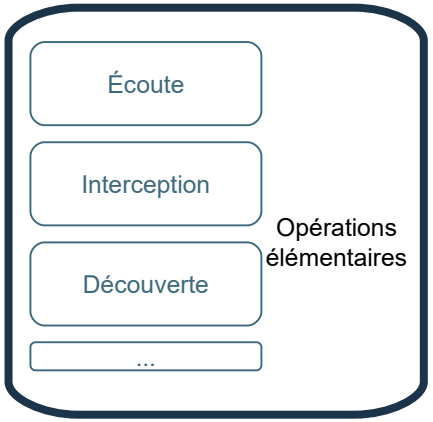
Analyse bas niveau

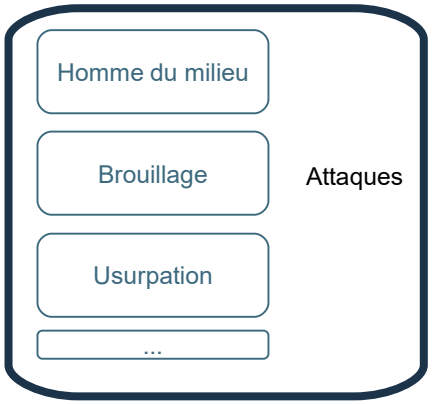
Mirage

- Principe

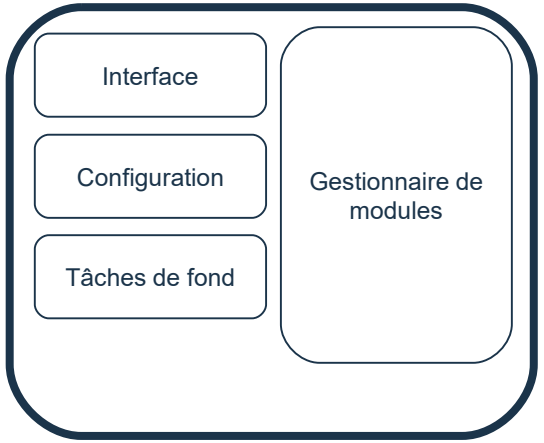


LIBRAIRIES





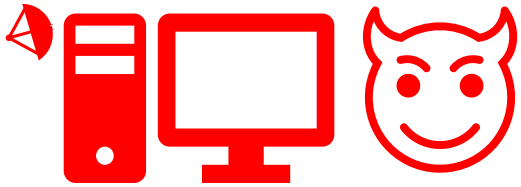
MODULES



SCENARIOS

Mirage

- Capture et injection : claviers et souris connectés



Étape 1
Écouter
→ Capter les mouvement de la souris

Étape 2
Injecter
→ Se faire passer pour le clavier et exfiltrer une image de l'écran

Étape 3
Exploiter
→ Superposer les mouvements de la souris sur l'image de l'écran

Mirage

- Capture et injection : claviers et

Mirage

- Capture et injection : claviers et

Mirage

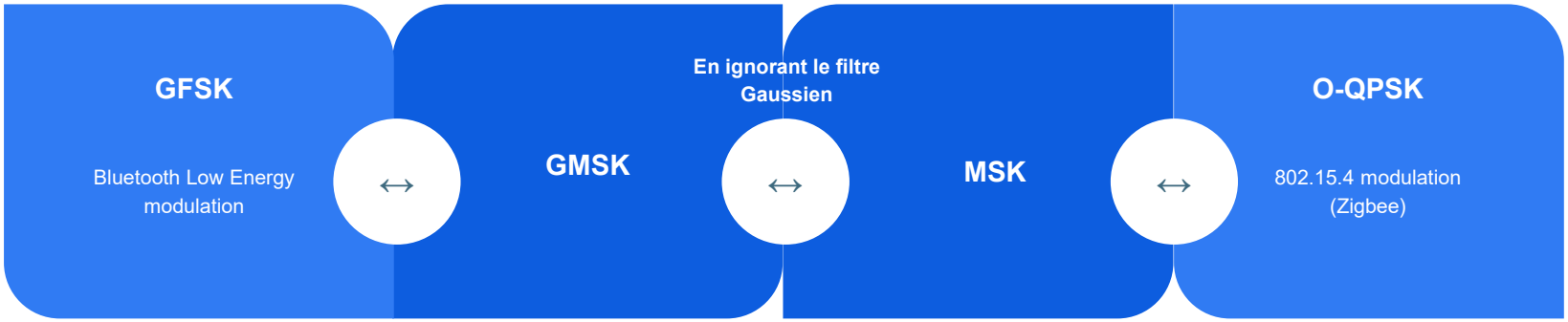
- Capture et injection : claviers et

Wazabee

- Attaques inter protocolaires
  - Faire parler un équipement avec un protocole P’ alors qu’il est fait pour parler avec P
  - …
  - Peu de chance que le protocole P’ soit surveillé

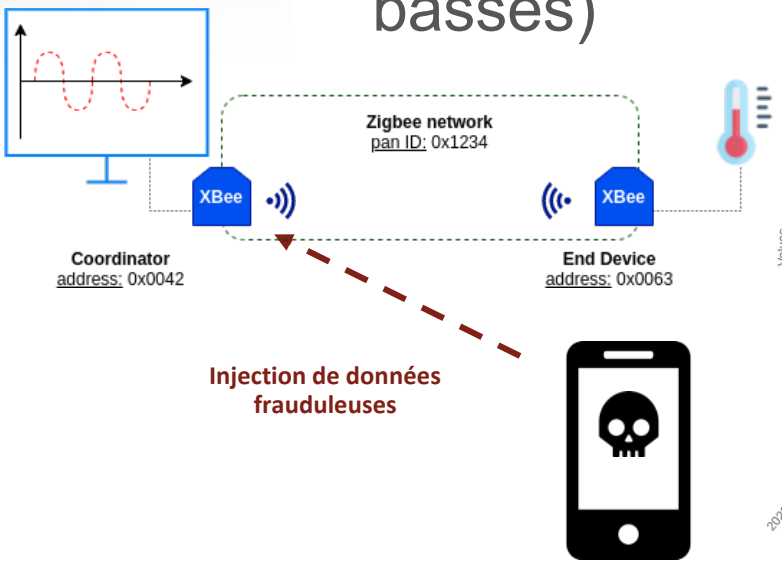
Wazabee

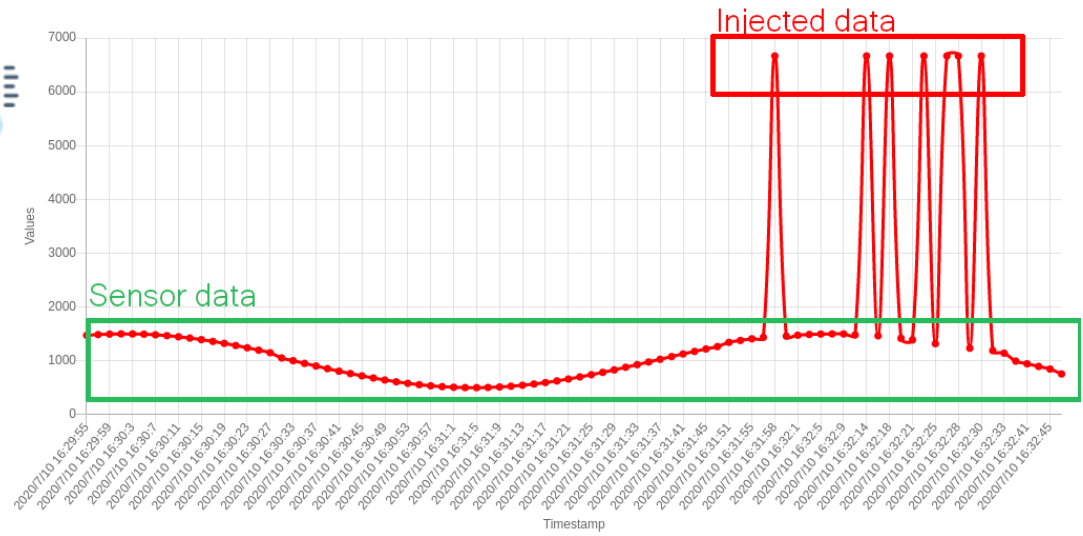
- Bluetooth Low Energy 5.0 → ZigBEE (802.15.4)
  - Exploitation de la proximité entre les modulations GFSK et O-QPSK
  - Modification des mécanismes de contrôle bas niveau (whitening, CRC,…)



Wazabee

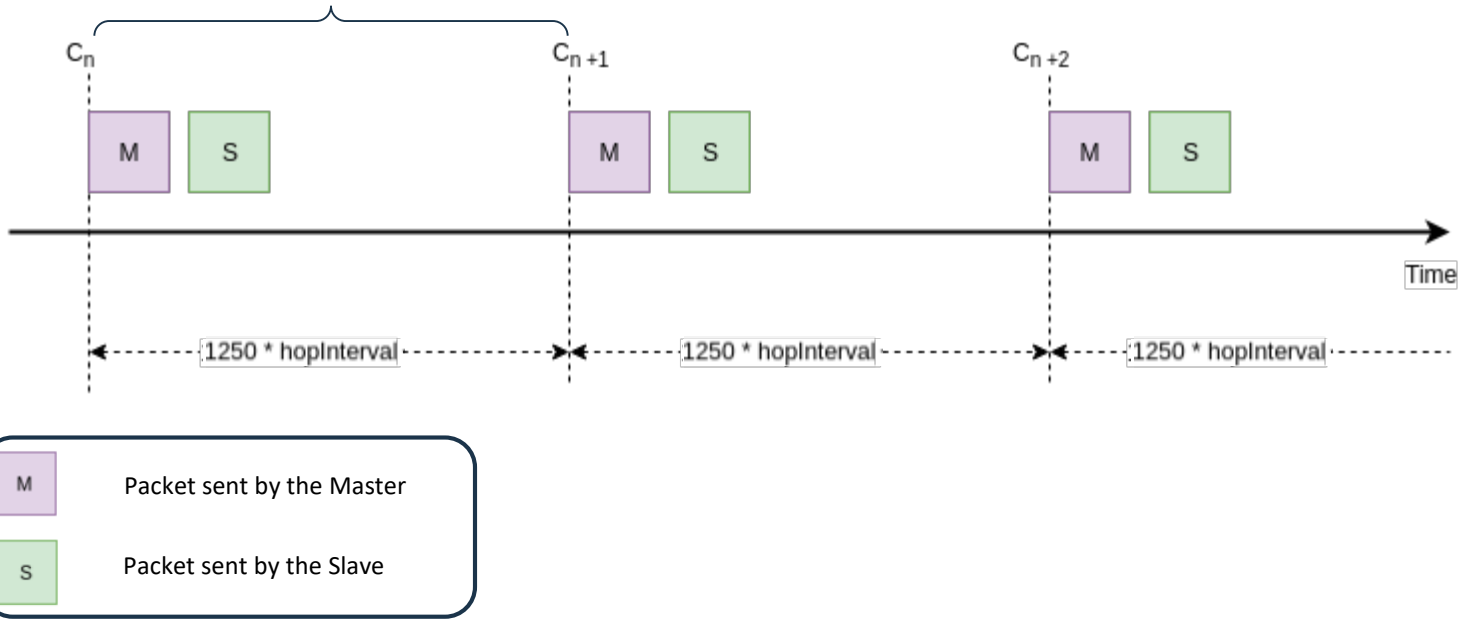
- Implémentation partielle (émission)
- Injection de trames Zigbee à partir d'un smartphone BLE Android (OnePlus 6T)
- Peu de privilèges nécessaires sur le téléphone (pas besoin d'accès aux couches basses)





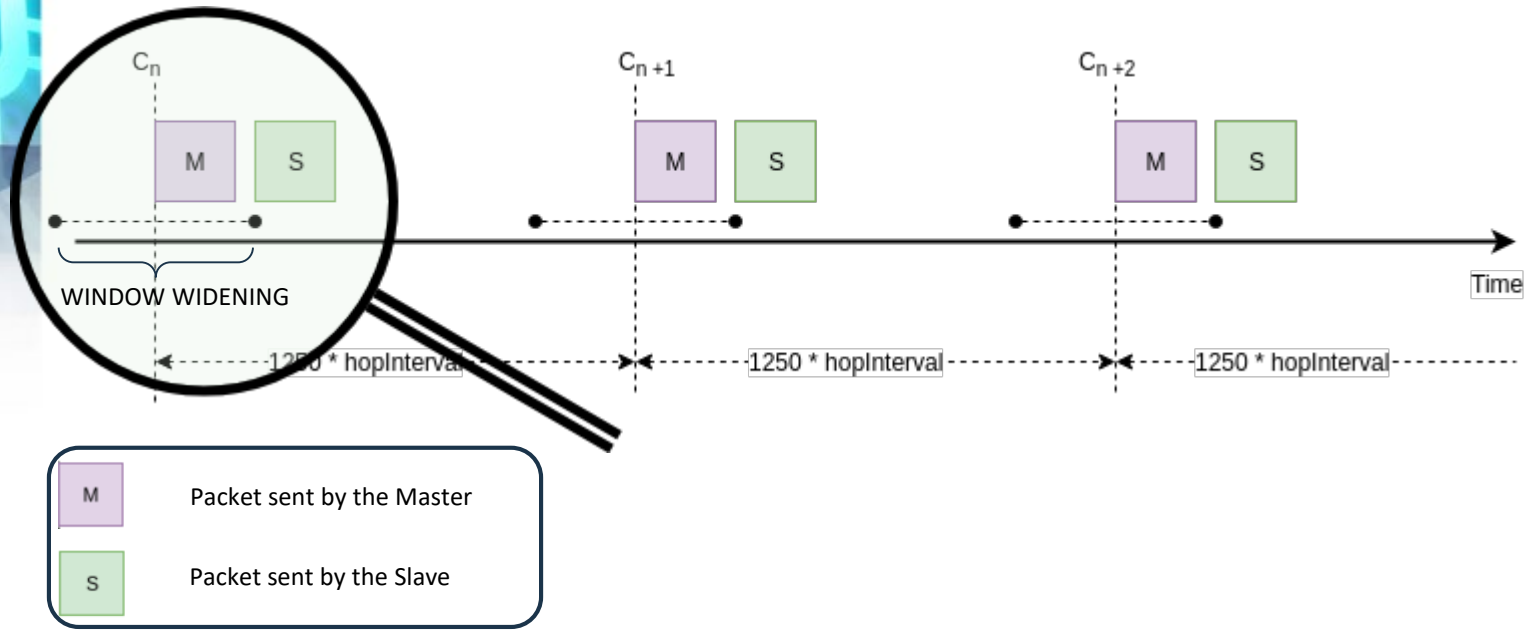
Injectable

- Exploitation d'une vulnérabilité de la norme BLE



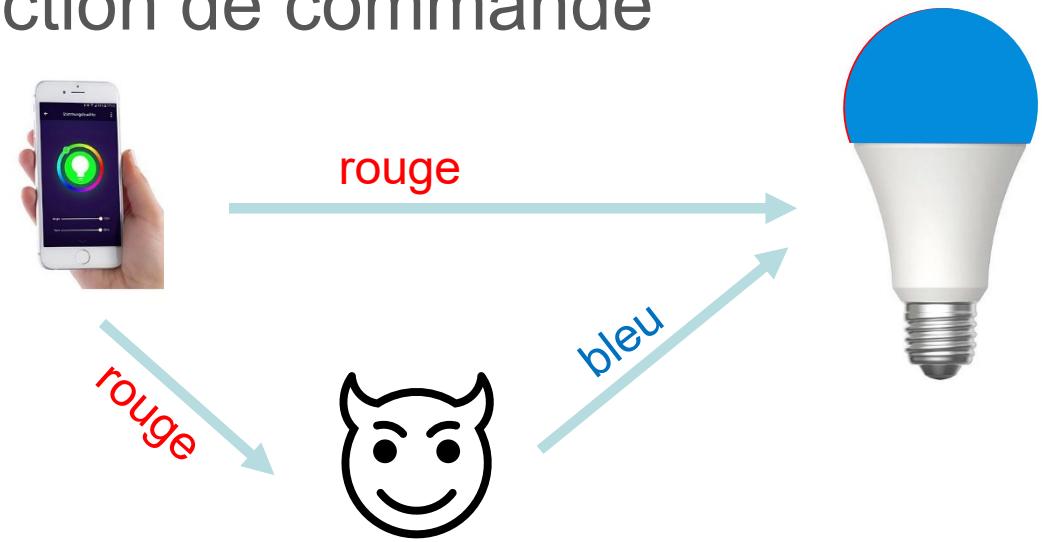
Injectable

- Exploitation d'une vulnérabilité de la norme BLE



Injectable

- Ampoules connectées
  - Injection de commande



  - Attaque MITM

➔ Exfiltration de données en Morse!

BLUETOOTH SECURITY

Security Notice

Bluetooth SIG Statement Regarding the 'InjectaBLE' Vulnerability Report

Researchers at the LAAS-CNRS lab have identified a packet-injection scenario related to unencrypted Bluetooth® LE baseband links that affects Bluetooth Core Specifications versions 4.0 through 5.2. The researchers identified that it is possible for an attacker following communications between Central and Peripheral role devices to successfully inject a crafted packet into the link by spoofing the Central's address during the time between the start of the Peripheral receiving a packet from the Central and the time at which the Central actually transmits during each connection interval. As greater window widening values are applied, for example as the connection interval increases, the chances of a successful packet injection increase.

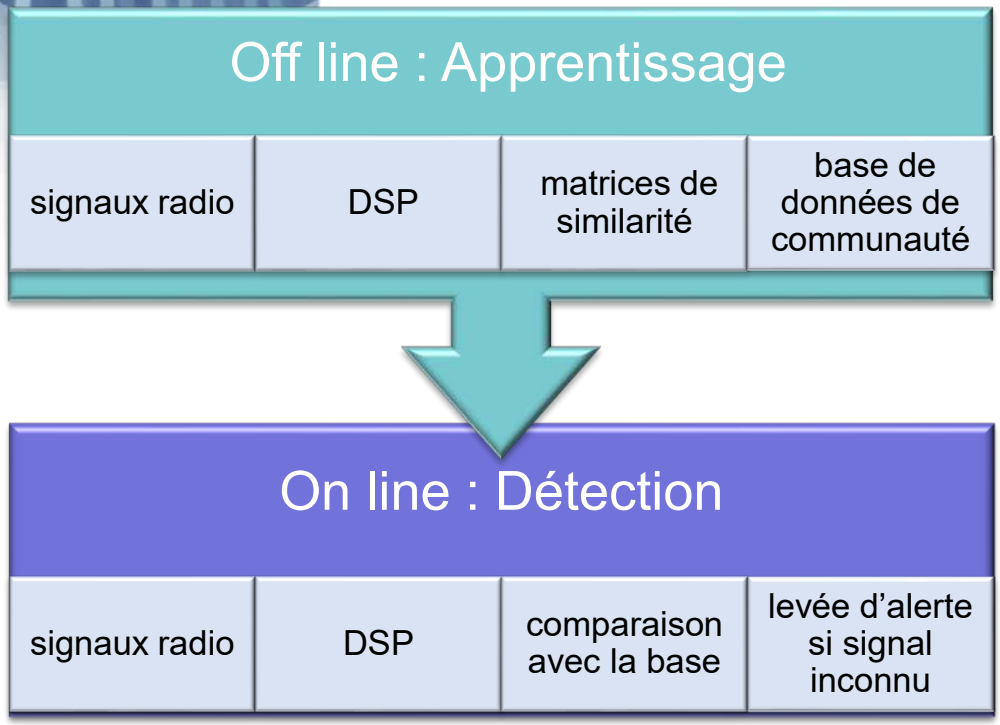
A successful packet injection in a device not establishing or using encryption may permit the attacker to spoof the Central or Peripheral device to the device in the opposing role. It is also possible for crafted packets to be used to transparently place the attacker in a full man-in-the-middle (MITM) position by establishing the attacker as the Central role to the Peripheral with new connection parameters, with the attacker taking over the Peripheral role. This will permit the attacker to modify, suppress or inject any traffic it wishes while the link remains established.

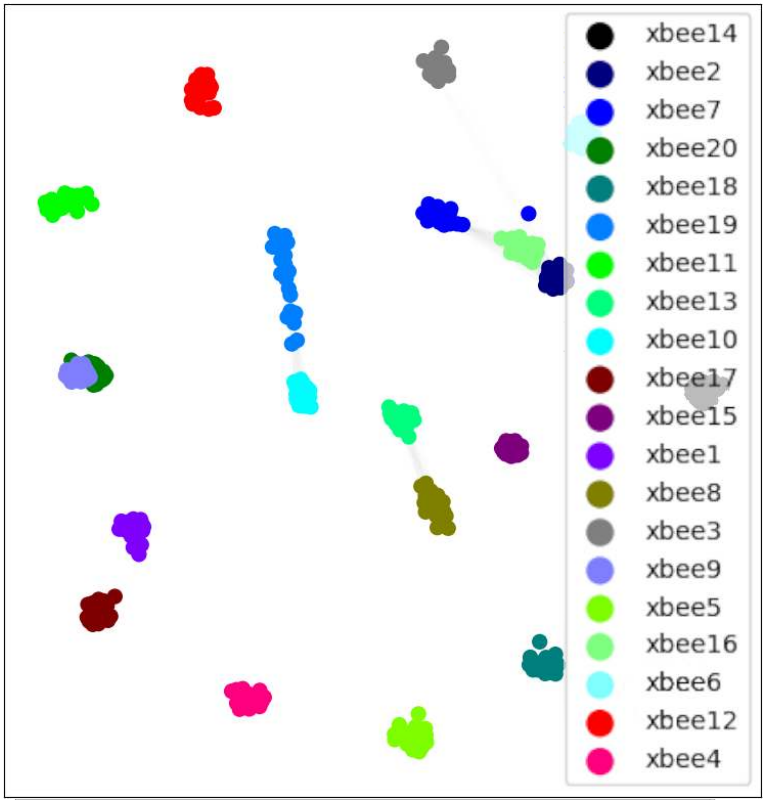
The Bluetooth SIG strongly recommends that implementations verify that they are using encryption in any profile that requires it under specification, and that vendor-specific profile implementations with custom attributes require encryption for both read and write operations on those characteristics by default.

The Bluetooth SIG is also broadly communicating details on this vulnerability and its remedies to our member companies and is encouraging them to rapidly integrate any necessary patches. As always, Bluetooth users should ensure they have installed the latest recommended updates from device and operating system manufacturers.

Fingerprint

- Identification par densité spectrale de puissance (DSP)
  - A l'aide d'équipements SDR low cost



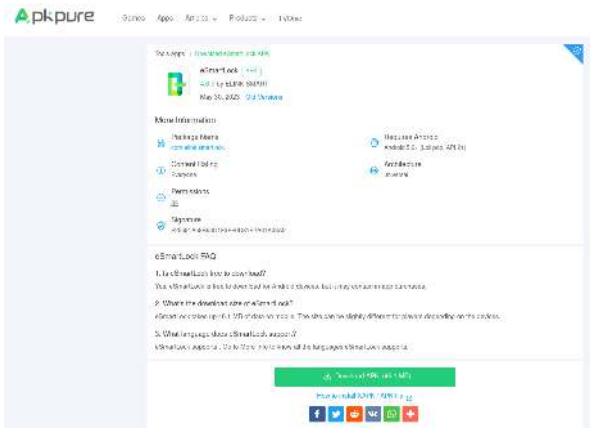


Conclusion

Re merci à R. Cayre, F. Galtier, P. Olivier

Ca s'améliore…

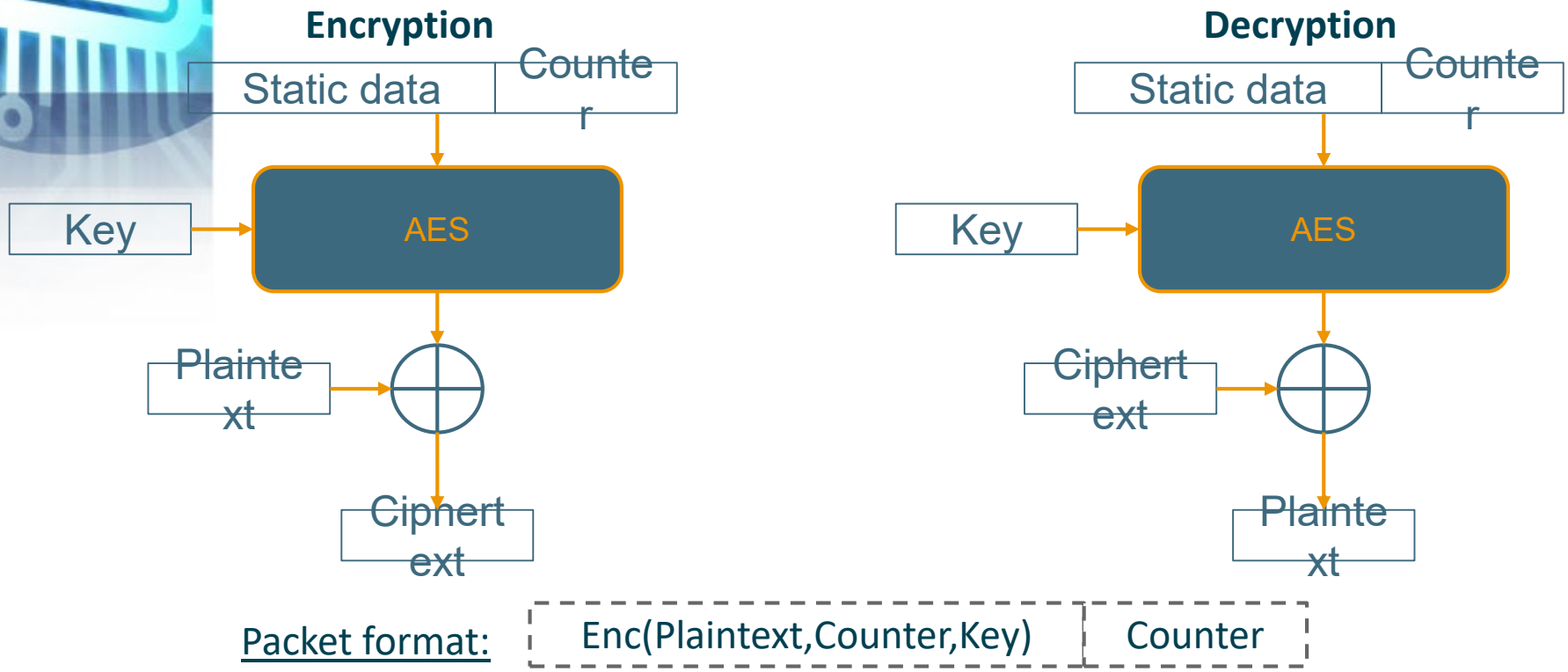
- Mais lentement



Analyse OTA
Reverse engineering de l'application

Ca s'améliore…

- Mais lentement



Ca s'améliore…

- Mais pas vraiment

  - Se faire passer pour l'application pour récupérer les dernières mesures

➔ Pb de Privacy

  - Se faire passer pour l'appareil pour retourner de fausses mesures

➔ Pb !

Questions?

Re merci à R. Cayre, F. Galtier, P. Olivier