APSYS .Lab

Spark the future. Craft tomorrow.

LAAS CNRS

SÉCURITÉ IOT: DE L'OFFENSIF AU DÉFENSIF

RéSIST, 8 octobre 2019 - TOULOUSE

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

AN **AIRBUS** COMPANY

QUI SUIS JE ?

- Actuellement en **thèse CIFRE** au **LAAS-CNRS,** co-encadrée par **Apsys.Lab**
- Ancien étudiant de **l'INSA Toulouse** et **TLS-SEC**
- Stage de fin d'études au **LAAS-CNRS**, équipe **TSF**
- Développeur de **Mirage**, un **framework offensif** dédié à l'audit des **technologies sans fil** utilisées dans l'IoT

PLAN DE LA PRÉSENTATION

- **Contexte** et **problématique**
- **Architecture** de Mirage
- Etat de l'art **offensif** des **protocoles IoT**
- Démonstration des **modules offensifs** de Mirage
- **Sécurité défensive: enjeux** et **perspectives**

CONTEXTE ET PROBLÉMATIQUE

SÉCURITÉ DES OBJETS CONNECTÉS

Problématiques et enjeux

CONTEXTE INDUSTRIEL: L'INDUSTRIE 4.0

⇒ Augmentation de la **surface d'attaque**, forte **complexité**

PROBLÉMATIQUES

- Comment **détecter et/ou prévenir** des tentatives d'intrusion dans ce type d'environnement ?

- Comment **évaluer l'efficacité d'un système de détection d'intrusion** ?
  - *Comment injecter des attaques ?*
  - *Comment simuler le comportement d'un attaquant ?*

- Comment **analyser et découvrir des vulnérabilités** sur ce type d'équipement ?

CONTEXTE : CONCEPTION D'UN IDS

Collecte des données

Observation d'une utilisation légitime

Apprentissage

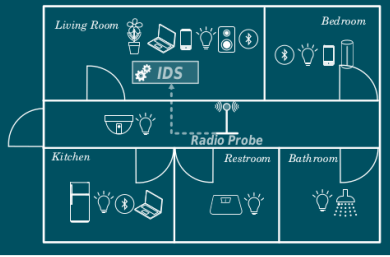
Génération d'un modèle

Détection

Mise à l'épreuve du modèle

Génération de campagnes d'attaques

Stage de fin d'études au LAAS-CNRS

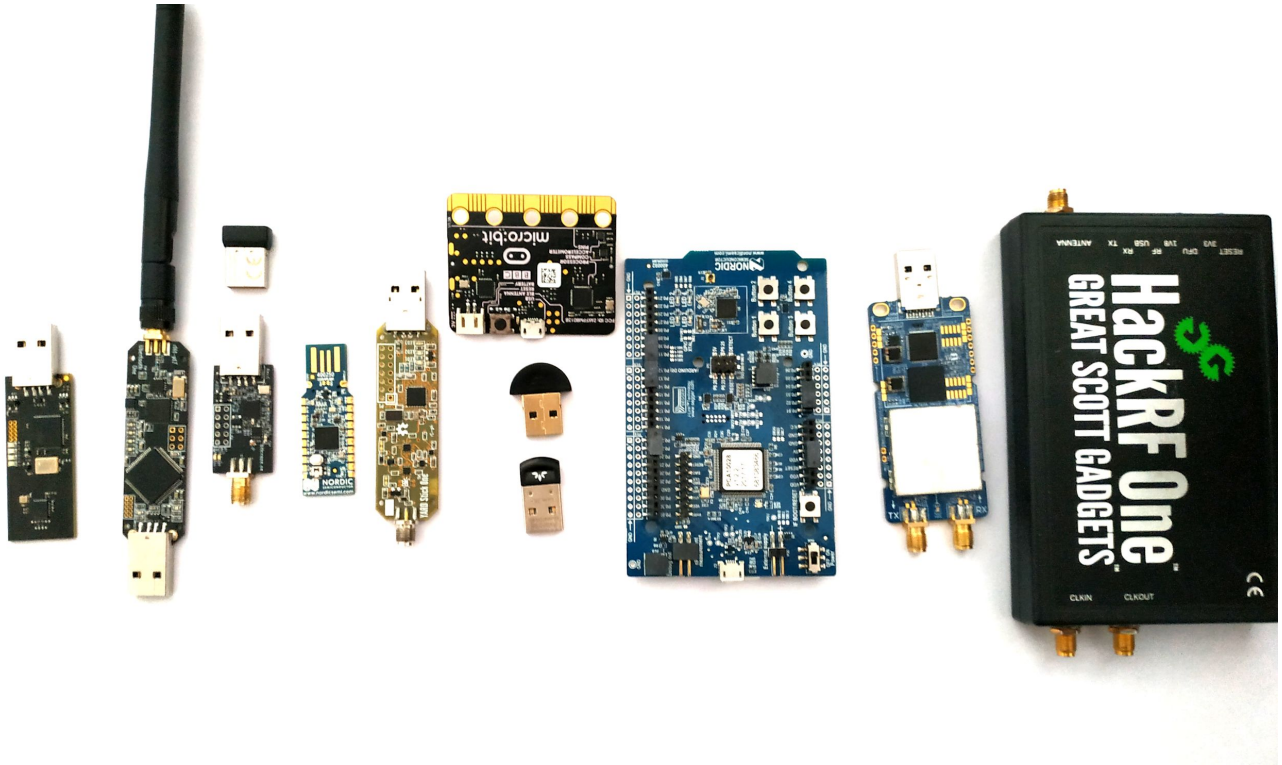


SÉCURITÉ OFFENSIVE - TECHNOLOGIES SANS FIL

Technologies sans fil

- **Hétérogènes**
- **Complexes**
- En pleine **expansion**
- **Peu étudiées**

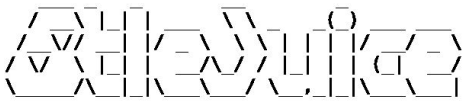
SÉCURITÉ OFFENSIVE - OUTILS MATÉRIELS



Outils matériels

- **Nombreux** et **variés**
- **Peu adaptés** à la sécurité offensive
- **Hétérogènes** (API, fonctionnalités)

SÉCURITÉ OFFENSIVE - OUTILS LOGICIELS



Outils logiciels

- **Nombreux** et **variés**
- **Incompatibles** les uns avec les autres (API, formats, etc.)
- **Usage de librairies haut niveau**, peu adaptées aux enjeux de la sécurité

SÉCURITÉ OFFENSIVE - CONSÉQUENCES

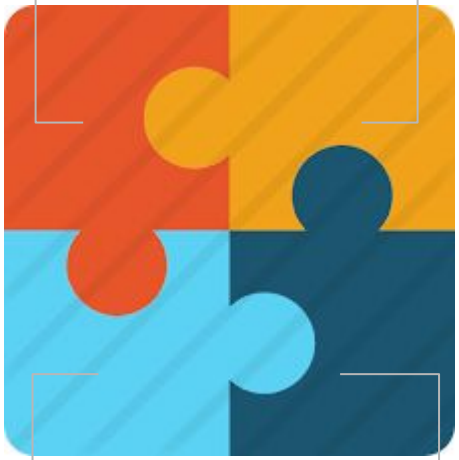
- **Frein au développement** des outils offensifs
- **Limitations** importantes pour **l'automatisation**
- Beaucoup de **développements inutiles** ou **redondants**
- L'analyste doit assimiler de **nombreuses informations techniques** peu pertinentes

ARCHITECTURE DE MIRAGE

PHILOSOPHIE DU FRAMEWORK

Approche unifiée

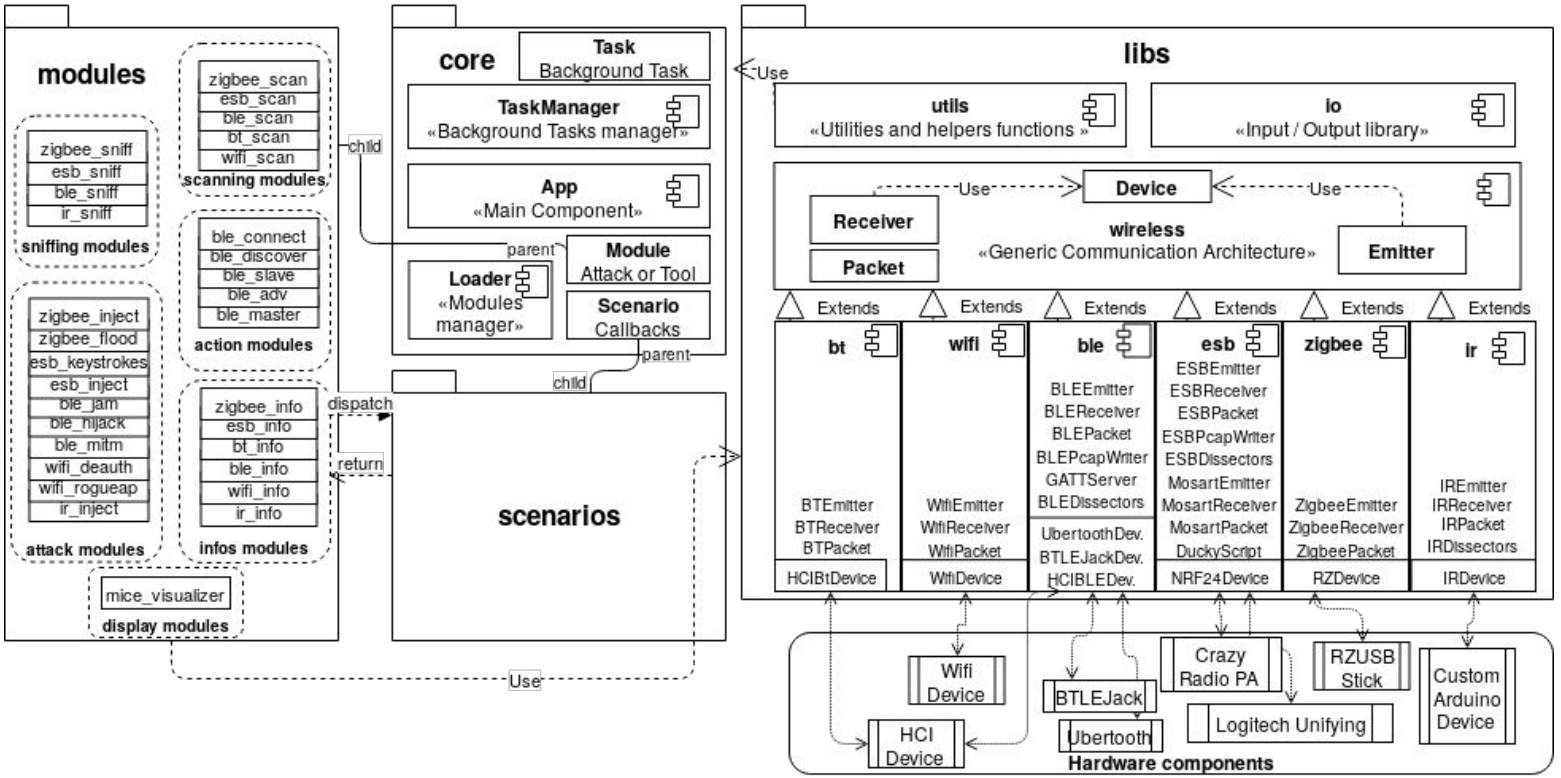
Approche modulaire



Approche générique

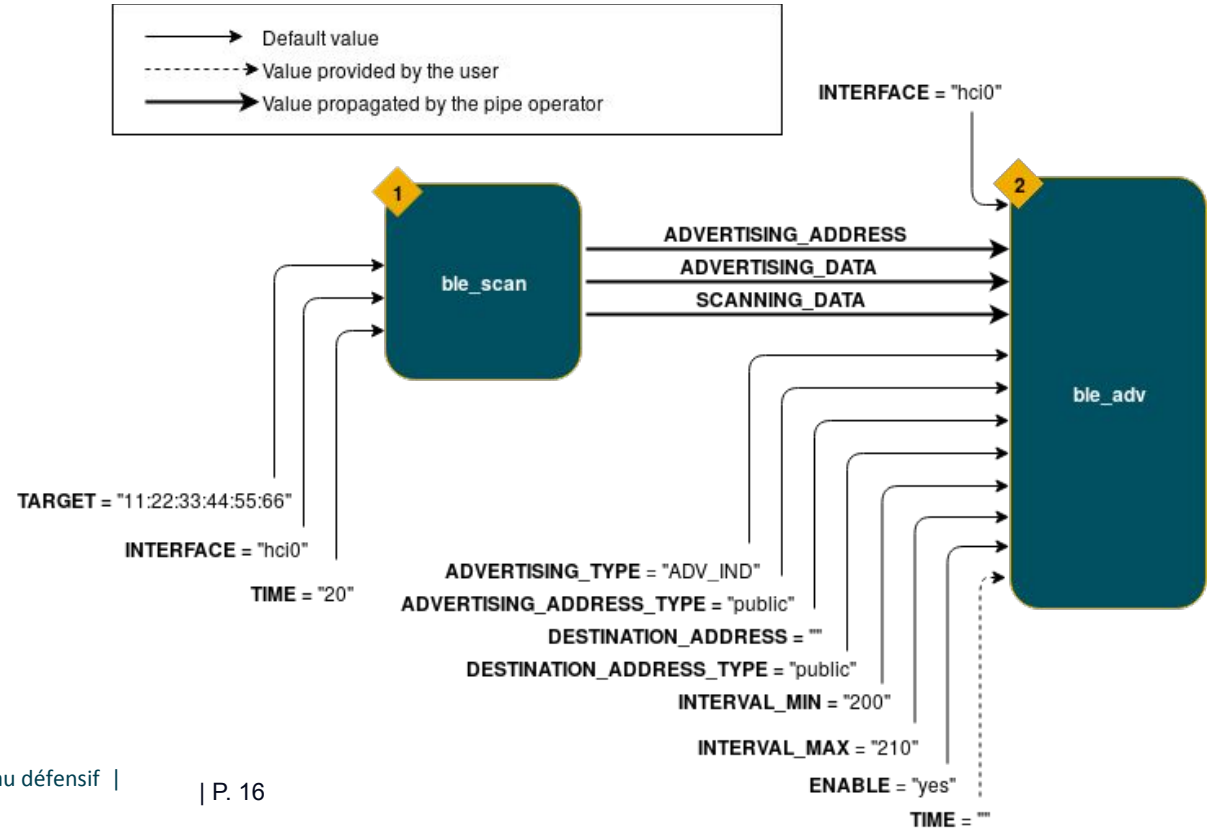
Approche bas niveau

MIRAGE : ARCHITECTURE GLOBALE



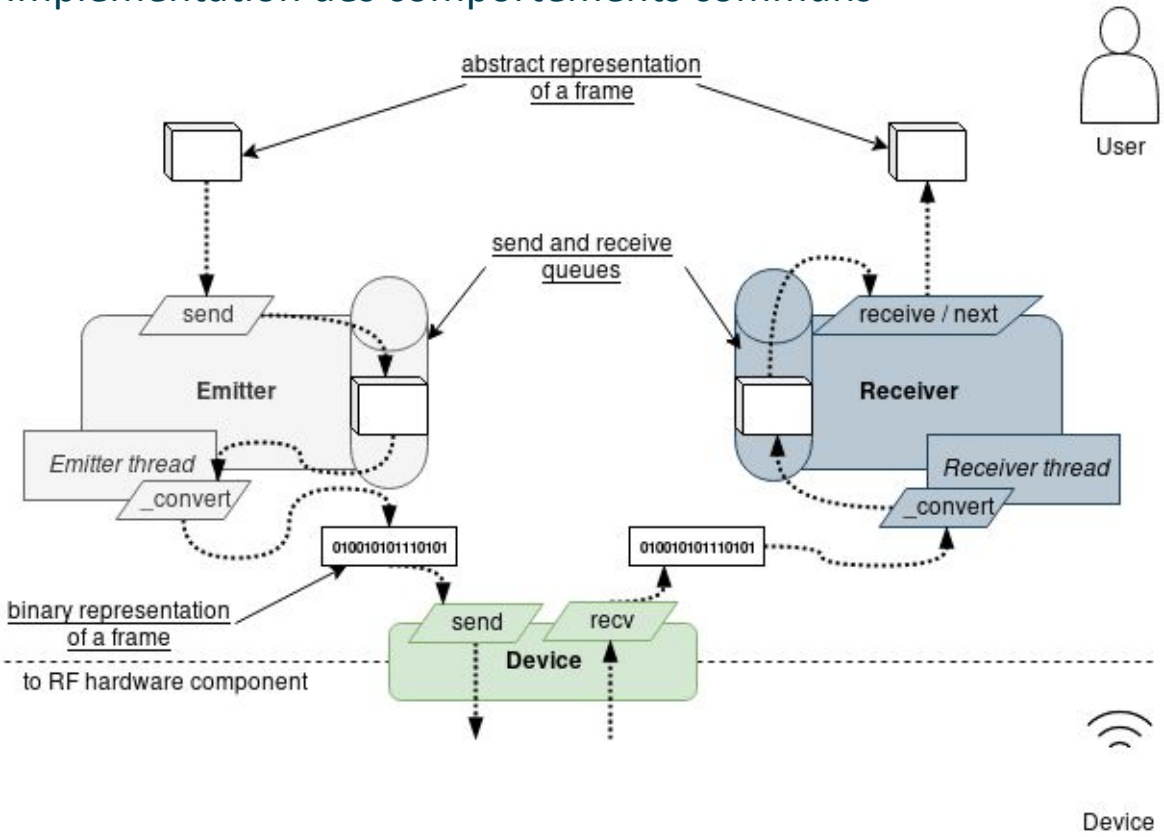
MIRAGE : CHAÎNAGE DE MODULES

```
$ mirage "ble_scan|ble_adv" ble_scan1.TARGET="11:22:33:44:55:66" ble_scan1.TIME="5" ble_adv2.TIME=""
```



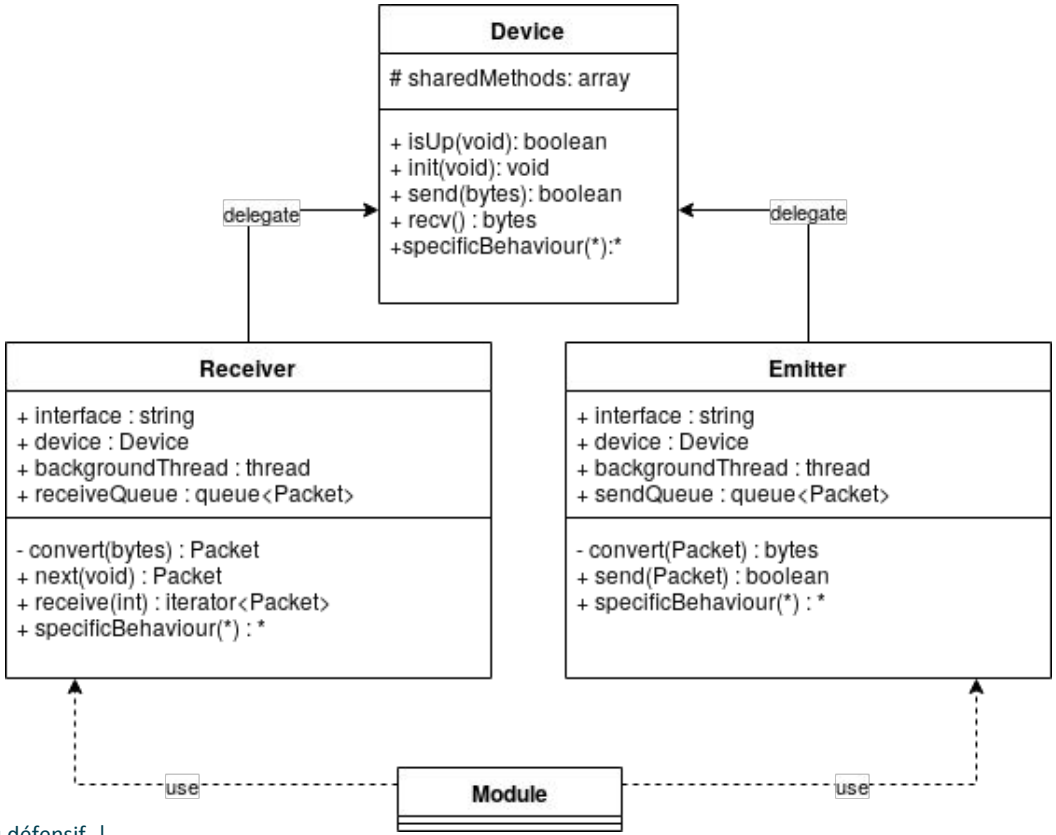
MIRAGE : ARCHITECTURE DE COMMUNICATION GÉNÉRIQUE

Implémentation des comportements communs

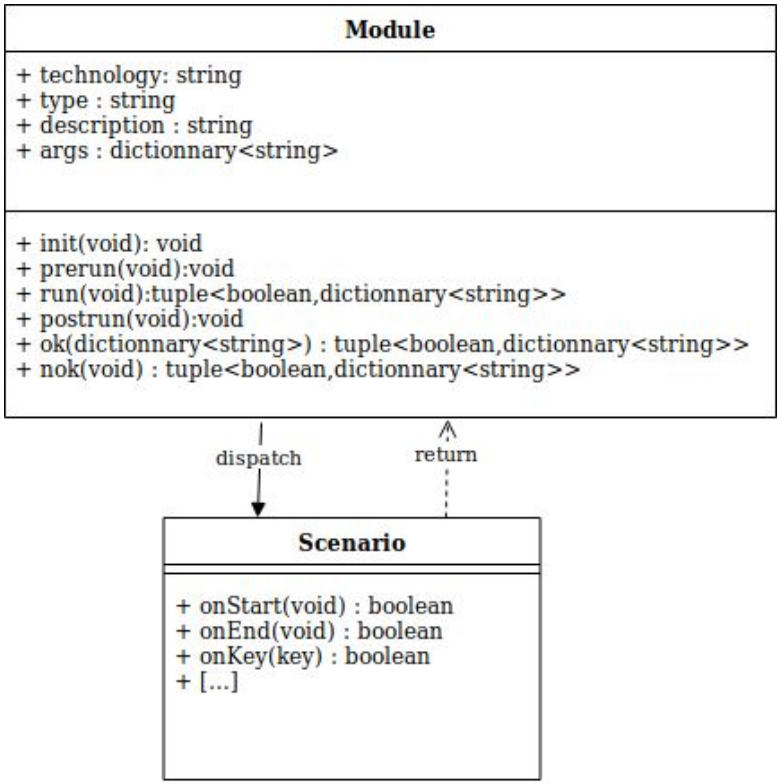


MIRAGE : ARCHITECTURE DE COMMUNICATION GÉNÉRIQUE

Implémentation des comportements spécifiques

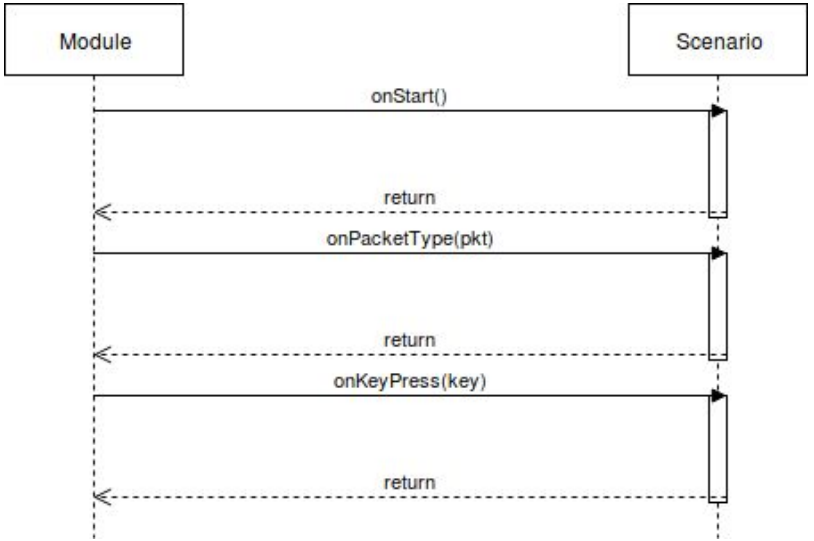


MIRAGE : MODULES ET SCÉNARIOS



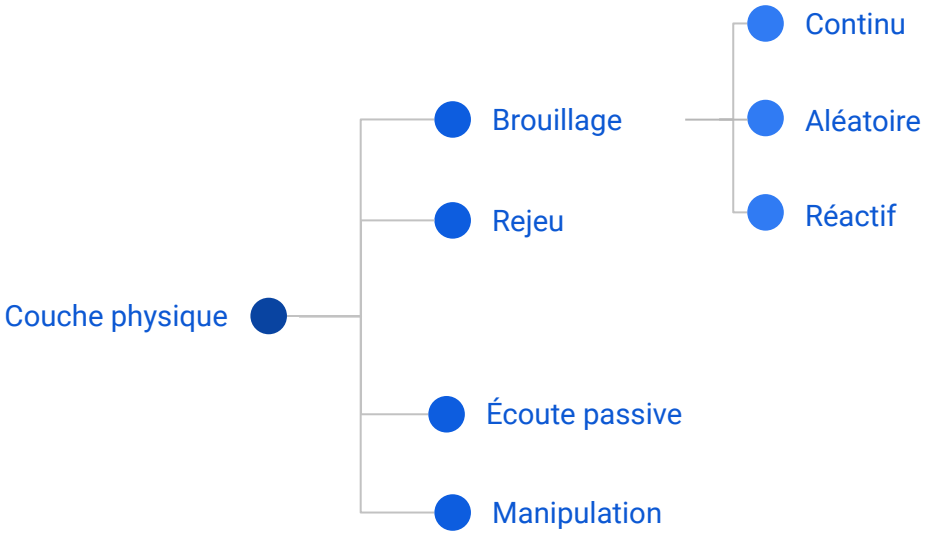
Présentation des modules et scénarios ↑

Mécanismes d'exécution d'un scénario ↓

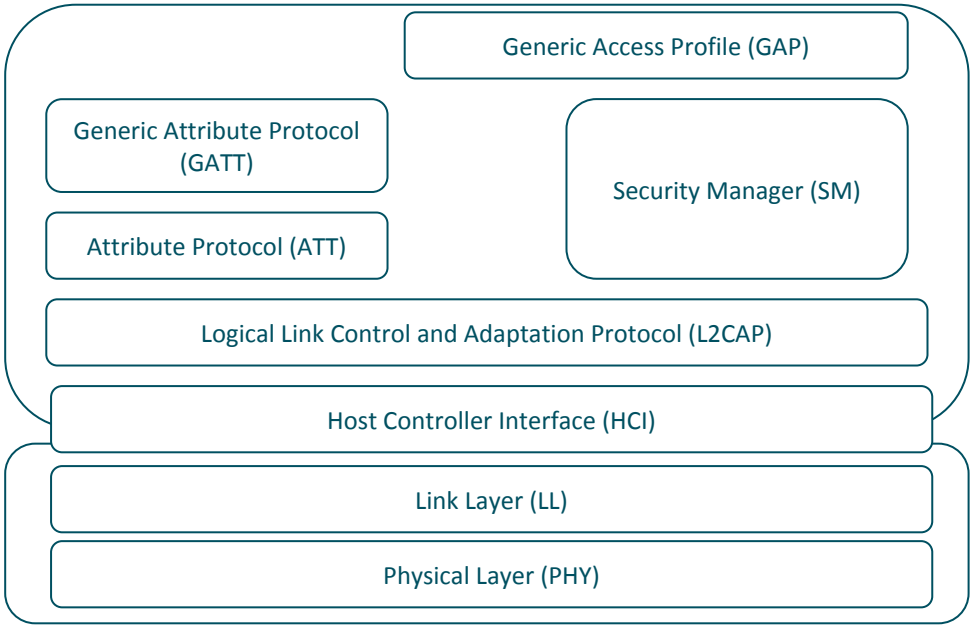


ÉTAT DE L'ART OFFENSIF DES PROTOCOLES IOT

ATTAQUES COMMUNES - COUCHE PHYSIQUE



BLUETOOTH LOW ENERGY - PILE PROTOCOLAIRE



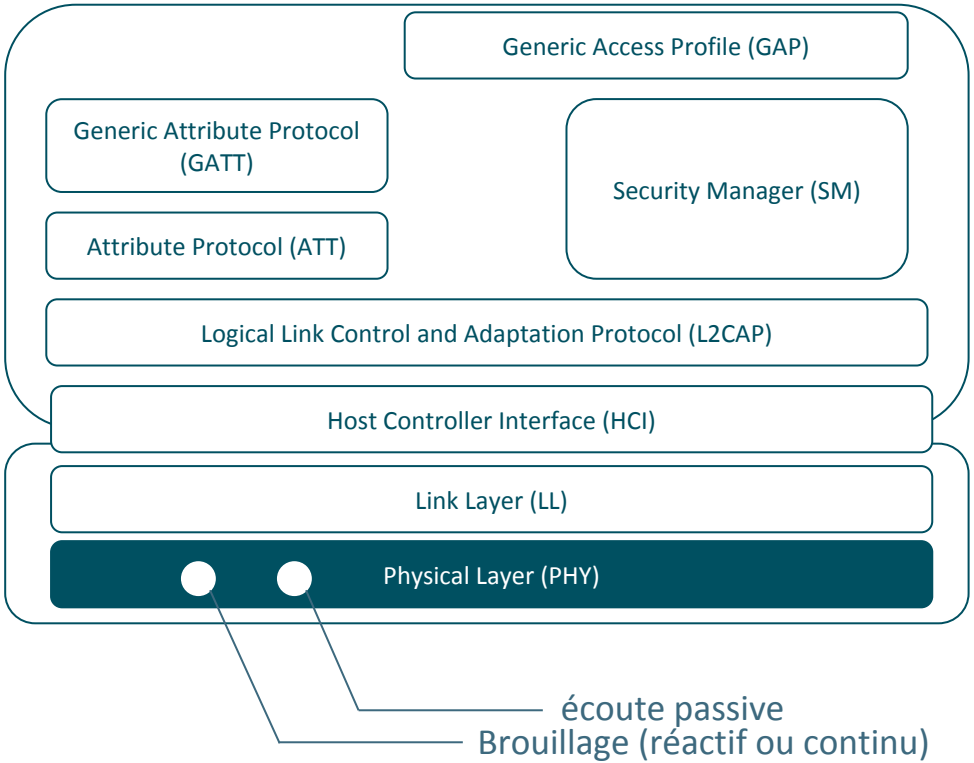
BLE utilise une pile protocolaire composée de deux composants :

- **Controller** (couches basses)
- **Host** (couches hautes)

Ces deux composants communiquent par l'intermédiaire d'une interface nommée **Host Controller Interface** (HCI)

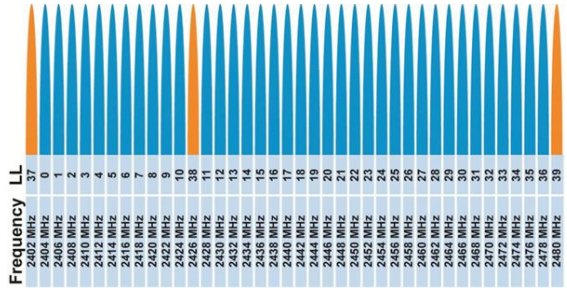
Bluetooth SMART

BLUETOOTH LOW ENERGY - COUCHE PHYSIQUE

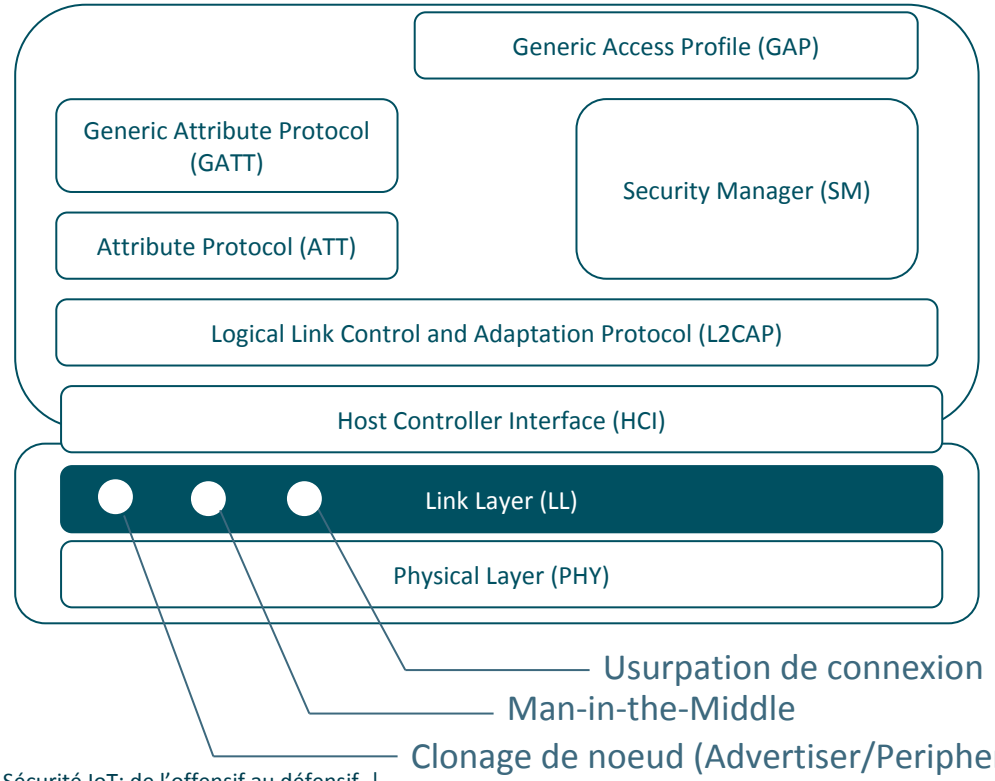


La couche physique repose sur un algorithme **de saut de fréquence linéaire,** rendant les **approches passives complexes.** Deux solutions existent :

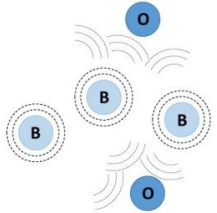
- Observer **le message d'initiation de connexion,** contenant les **paramètres de l'algorithme**
- Récupérer **les paramètres** par l'intermédiaire **d'heuristiques**



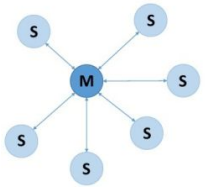
BLUETOOTH LOW ENERGY - COUCHE LIAISON



La couche liaison définit **deux modes** :

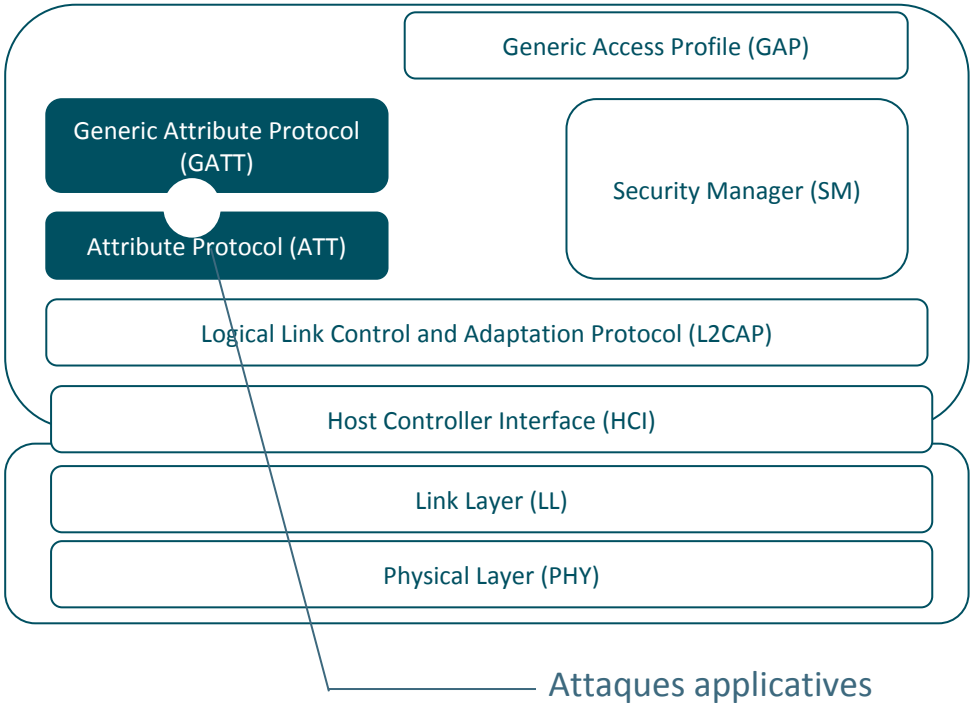


- **Un mode d'*advertising***, comparable à un mécanisme de diffusion de messages en *broadcast*



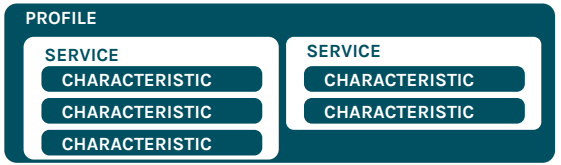
- **Un mode *connecté***, correspondant à une topologie Maître / Esclave (*Master / Slave*)

BLUETOOTH LOW ENERGY - COUCHES APPLICATIVES



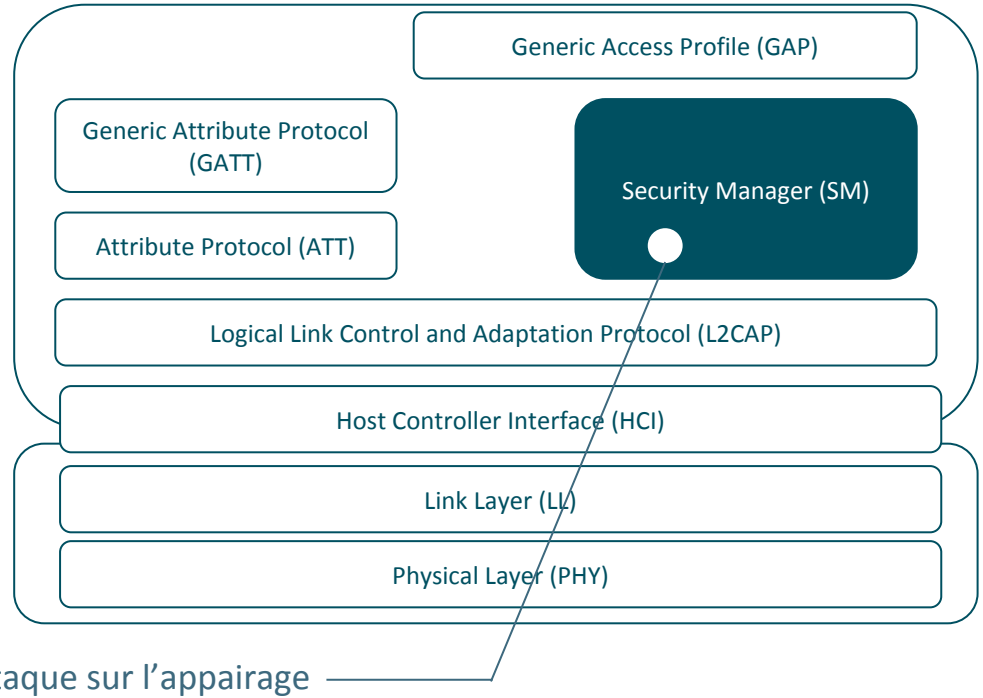
Les couches ATT et GATT sont les couches applicatives principales.

- La **couche ATT** implémente un modèle client serveur. Un serveur ATT peut être considéré comme une base de données **d'attributs**, caractérisés par un identifiant (handle), une valeur et un type.

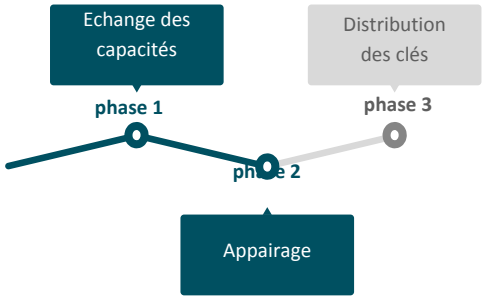


- La **couche GATT** spécialise la couche ATT en distinguant des services primaires et secondaires, contenant des caractéristiques.

BLUETOOTH LOW ENERGY - SÉCURITÉ

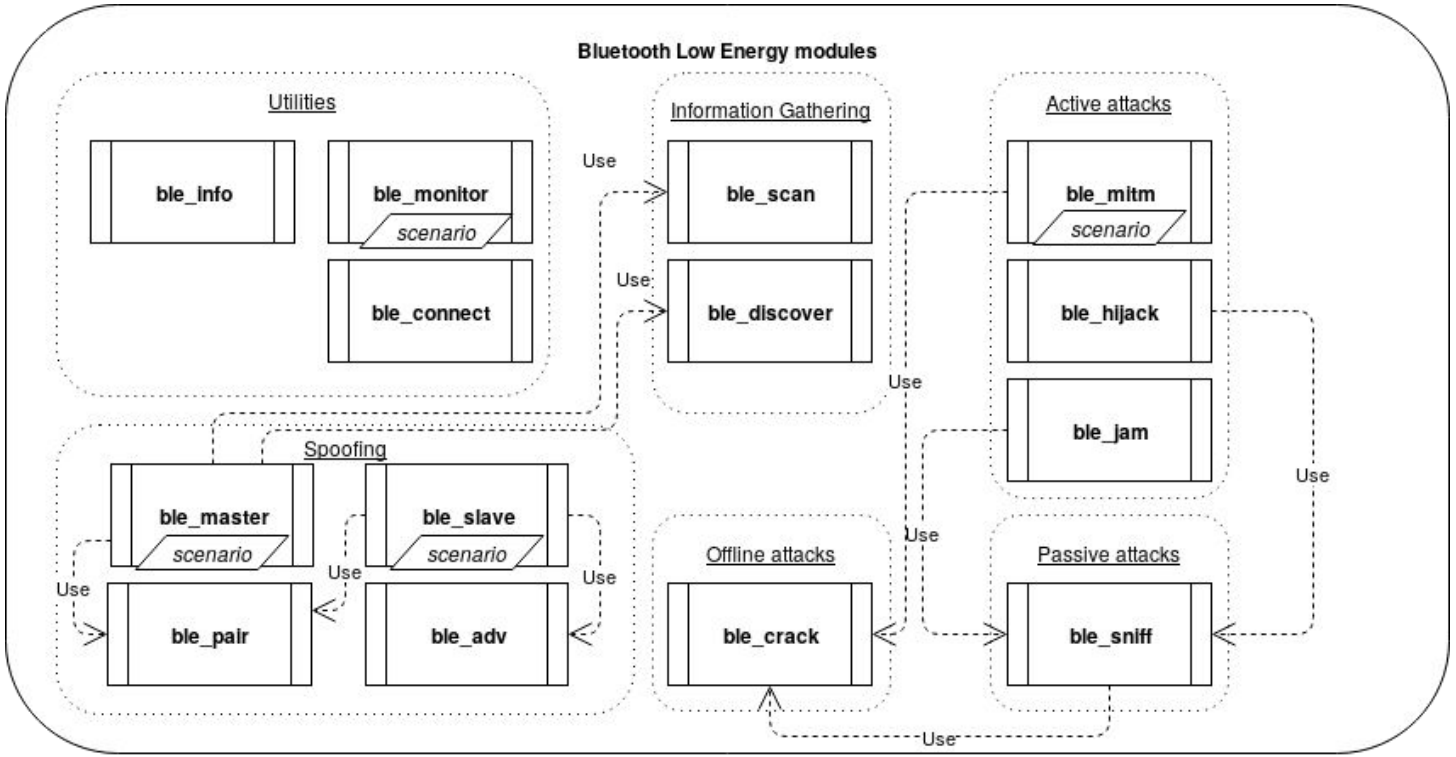


La couche Security Manager gère la sécurité du protocole.

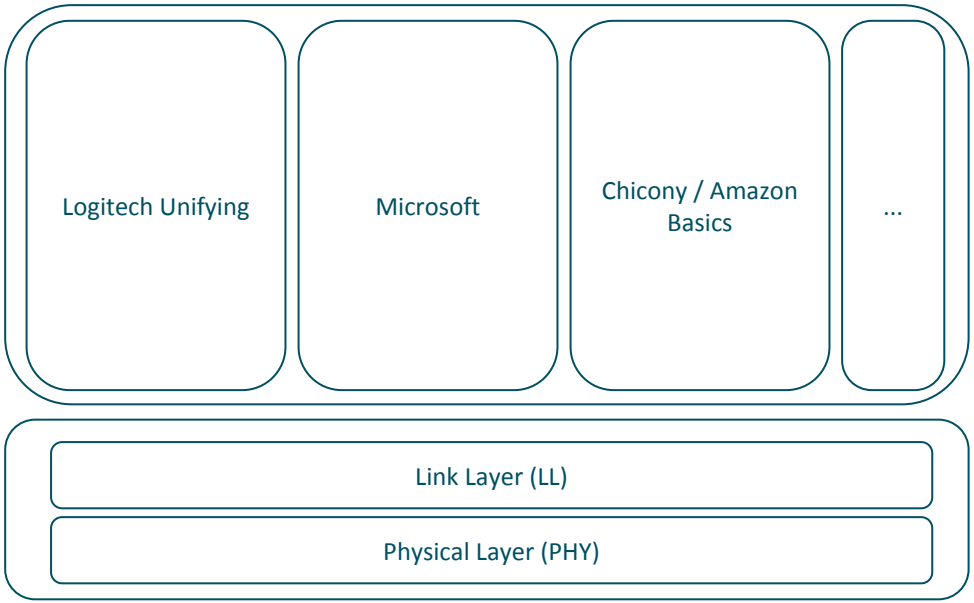


- Elle implémente un **mécanisme d'appairage** permettant de négocier une clé commune à partir d'un code PIN. Les premières versions de ce mécanisme étaient **vulnérables** à une attaque par bruteforce (6 digits …).
- Cette négociation de clé permet de dériver une **Short Term Key**, permettant elle même de chiffrer la distribution de la **Long Term Key**, compromettant la sécurité des communications ultérieures…

MODULES BLE DE MIRAGE - VUE D'ENSEMBLE



ENHANCED SHOCKBURST - PILE PROTOCOLAIRE



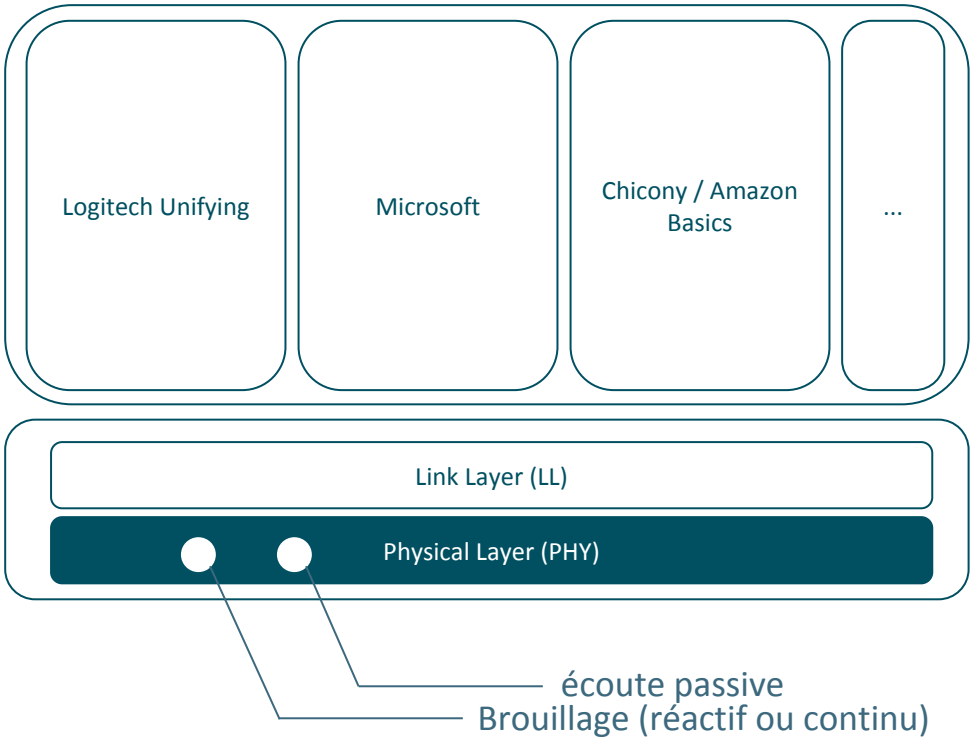
Enhanced ShockBurst est un protocole proposé par **Nordic Semiconductors,** couramment utilisé par les constructeurs de **périphériques d'entrée sans fil:**

- *Souris*
- *Claviers*
- *Pointeurs de présentation*
- *Manettes de jeu*

La spécification définit les **couches physique** et **liaison** du protocole.

Les constructeurs implémentent leur **propres couches applicatives propriétaires** au dessus de ce socle de base.

ENHANCED SHOCKBURST - PILE PROTOCOLAIRE

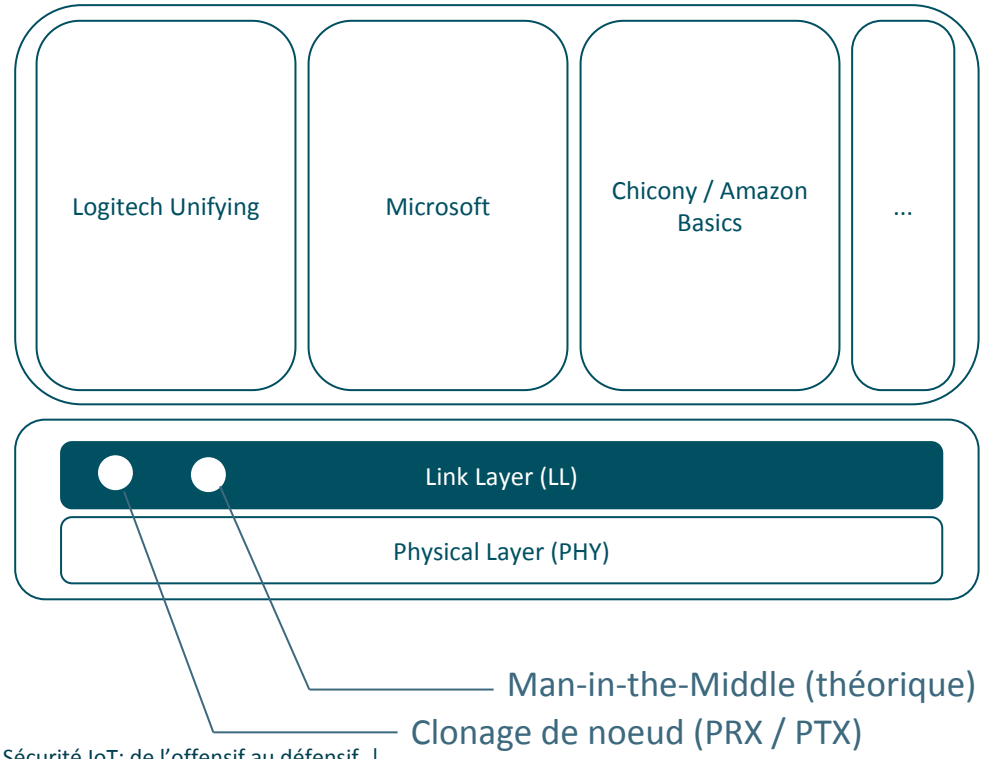


La couche physique repose sur une modulation par déplacement de fréquence (*Gaussian Frequency Shift Keying*).

La bande de fréquences utilisée est **2.4GHz-2.5GHz,** et est divisée en **100 canaux.**

Trois baudrates sont utilisables: **250 KBps, 1MBps et 2MBps.**

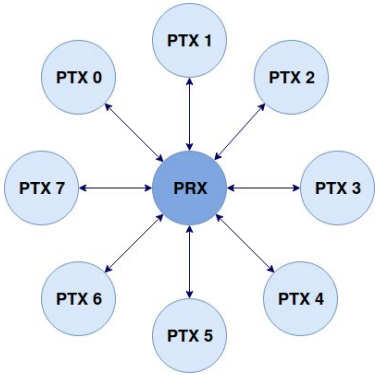
ENHANCED SHOCKBURST - PILE PROTOCOLAIRE



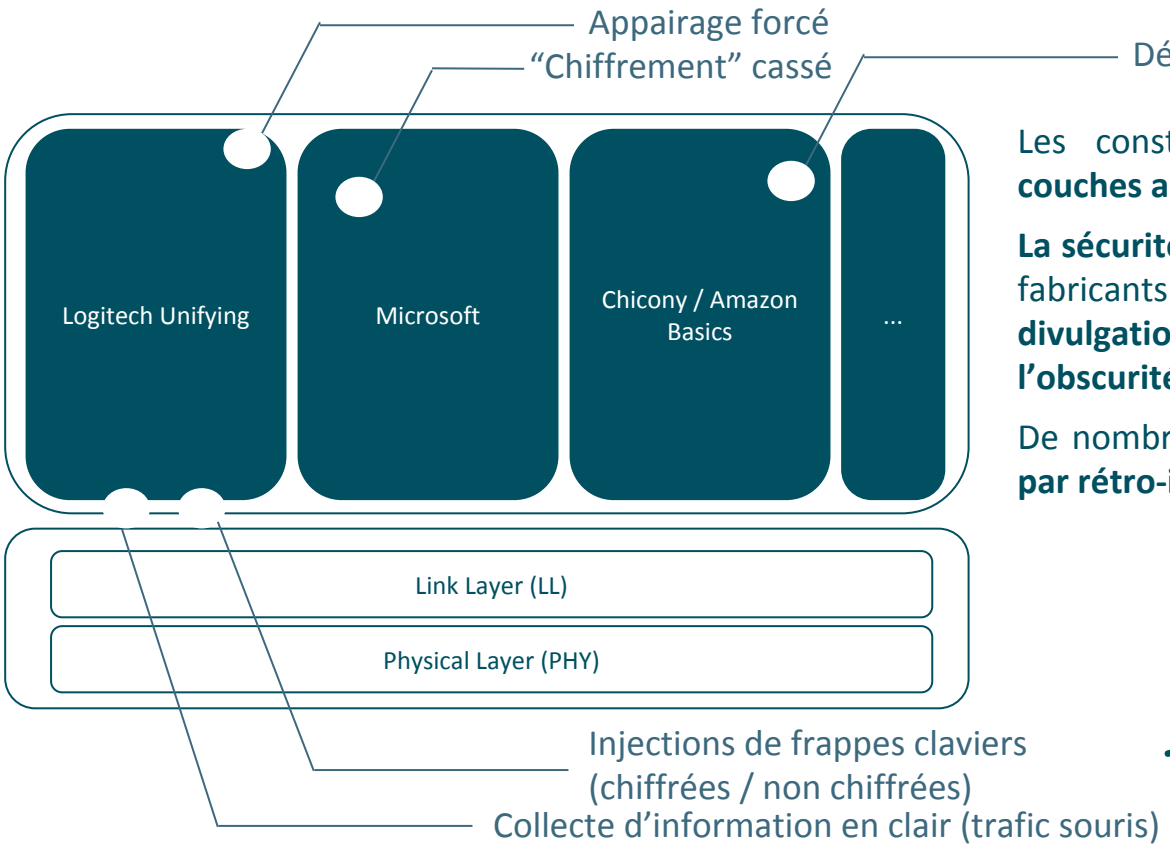
La couche liaison définit deux rôles:

- **PTX** (émetteur): noeud capable d'émettre des trames de données à destination du PRX
- **PRX** (récepteur): noeud capable de recevoir et d'acquitter les trames émises par les PTX

Le protocole utilise une **topologie en étoile**, permettant d'interconnecter un PRX avec huit PTX différents:



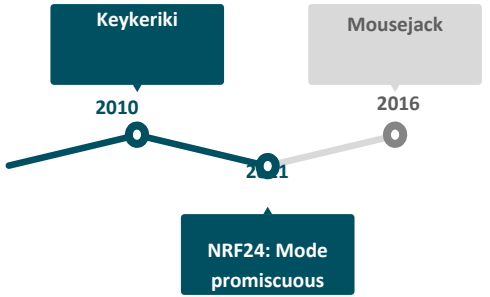
ENHANCED SHOCKBURST - PILE PROTOCOLAIRE



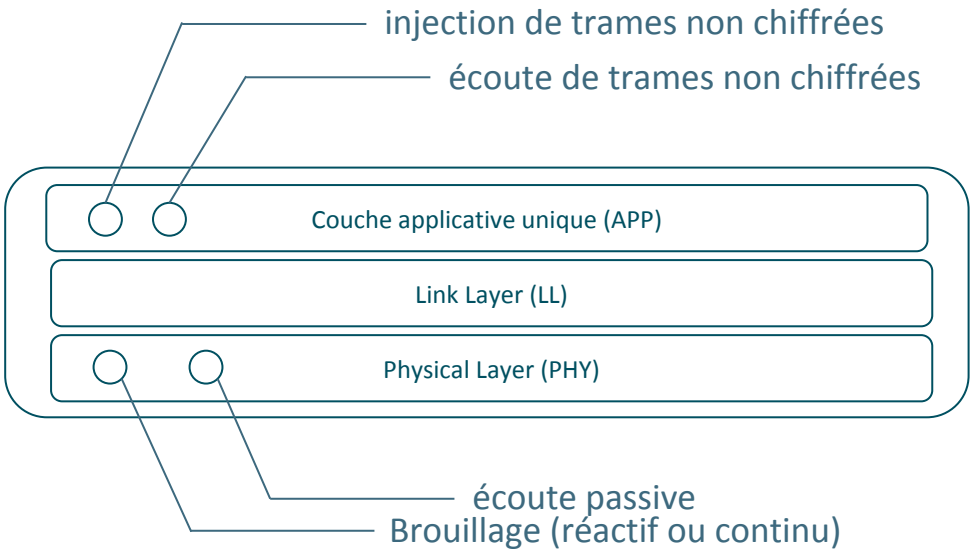
Les constructeurs implémentent leurs **propres couches applicatives propriétaires.**

La sécurité de ces couches est très inégale selon les fabricants et repose principalement sur **la non divulgation des spécifications (sécurité par l’obscurité).**

De nombreuses vulnérabilités **ont été découvertes par rétro-ingénierie ces dernières années:**



MOSART - VUE D'ENSEMBLE



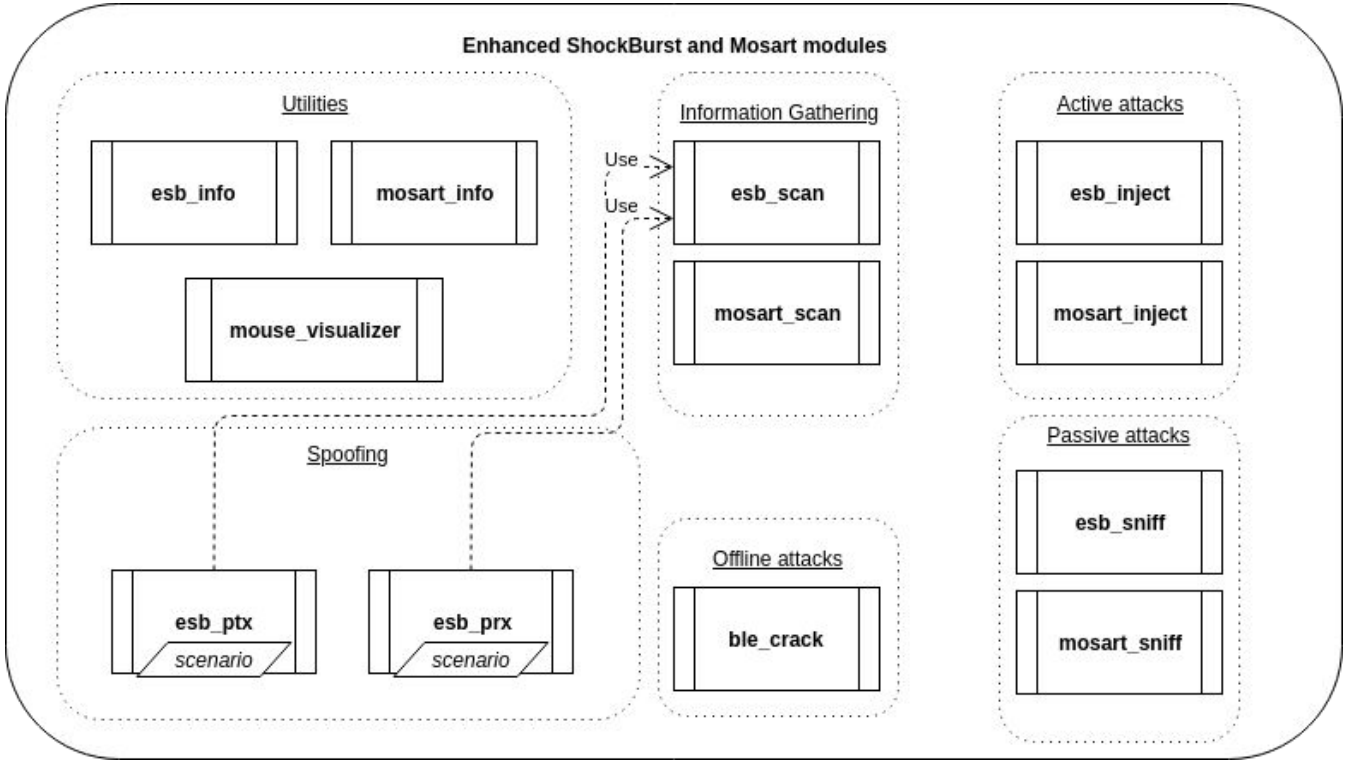
Mosart est un protocole dérivé du ShockBurst**, utilisé par certains constructeurs de périphériques d'entrée sans fil.**

Le protocole propose une **pile protocolaire unique** optimisée pour les périphériques d'entrée sans fil, **non personnalisable** par le constructeur.

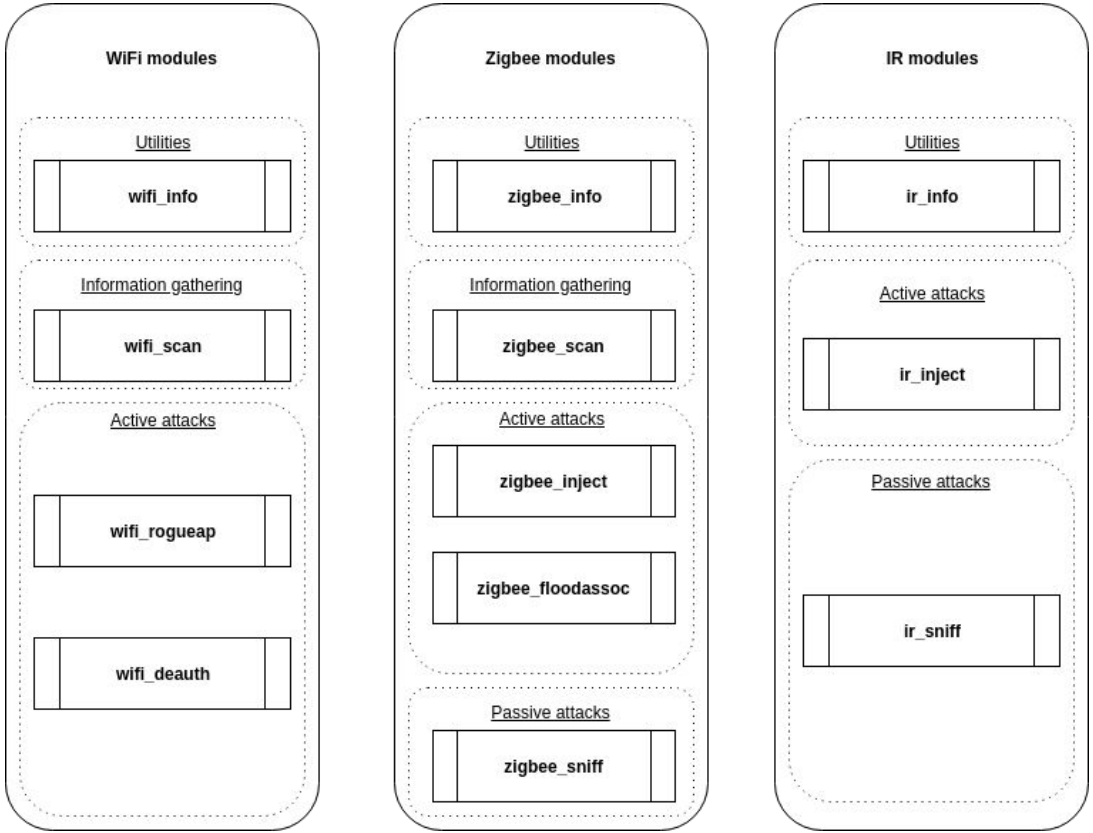
La couche physique est basée sur une modulation GFSK sur la bande 2.4-2.5GHz.

La couche applicative n'intègre aucun mécanisme de chiffrement.

MODULES ESB ET MOSART DE MIRAGE - VUE D'ENSEMBLE



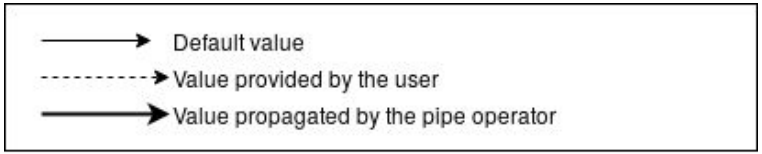
AUTRES PROTOCOLES - VUE D'ENSEMBLE



DÉMONSTRATION DES MODULES OFFENSIFS

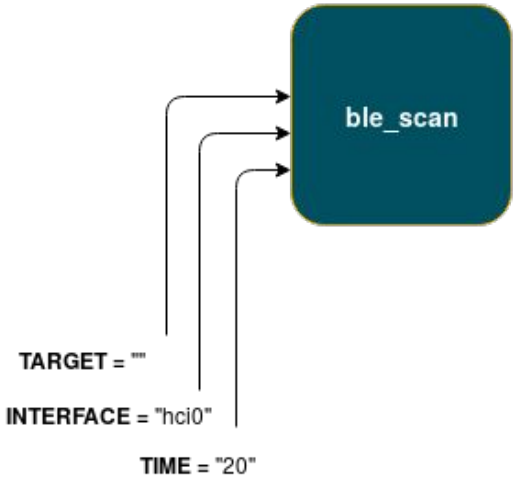
MODULES - COLLECTE D'INFORMATIONS / BLE_SCAN

- Module de **collecte d'information (mode *advertising*)**
- **Scan de l'environnement** : permet d'identifier l'adresse BD de l'équipement cible
- Mécanisme de **filtrage basique** par adresse

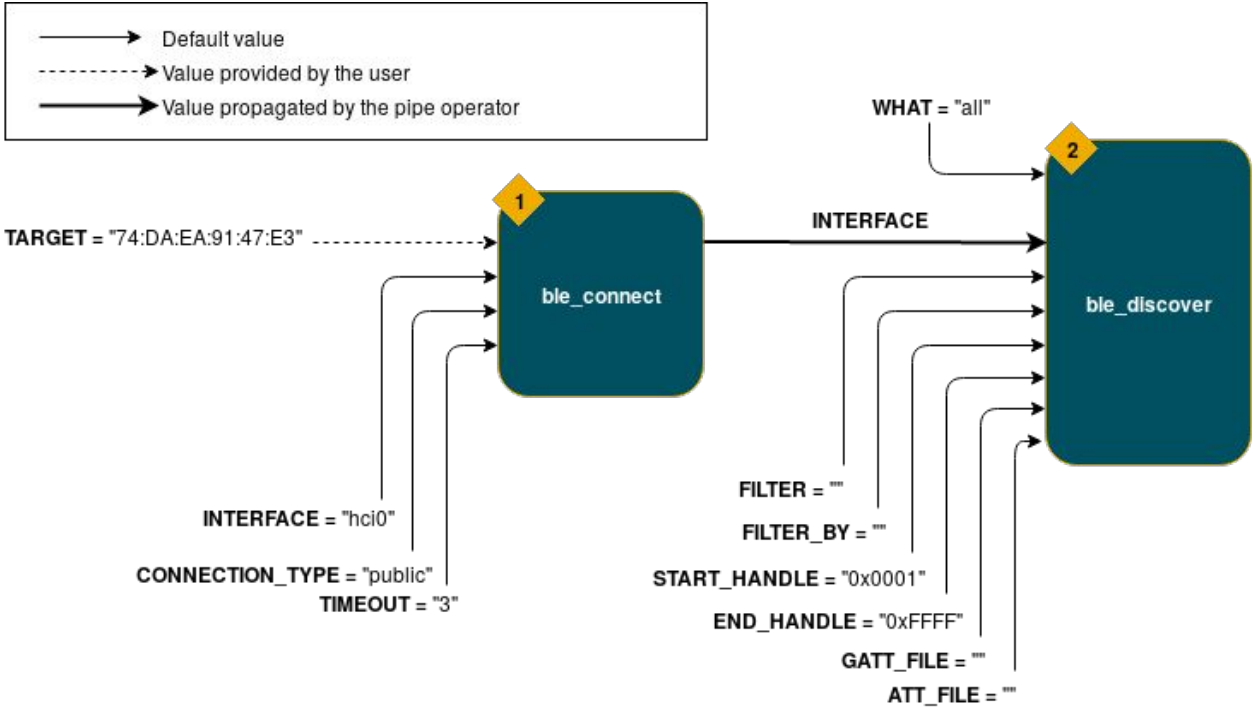



```
$ sudo ./mirage.py ble_scan
[INFO] Module ble_scan loaded !
[SUCCESS] HCI Device (hci0) successfully instanciated !

Devices found
 BD Address          | Name              | Company                  |
 74:DA:EA:91:47:E3   | Lampe de bureau   | Texas Instruments Inc.   |
```

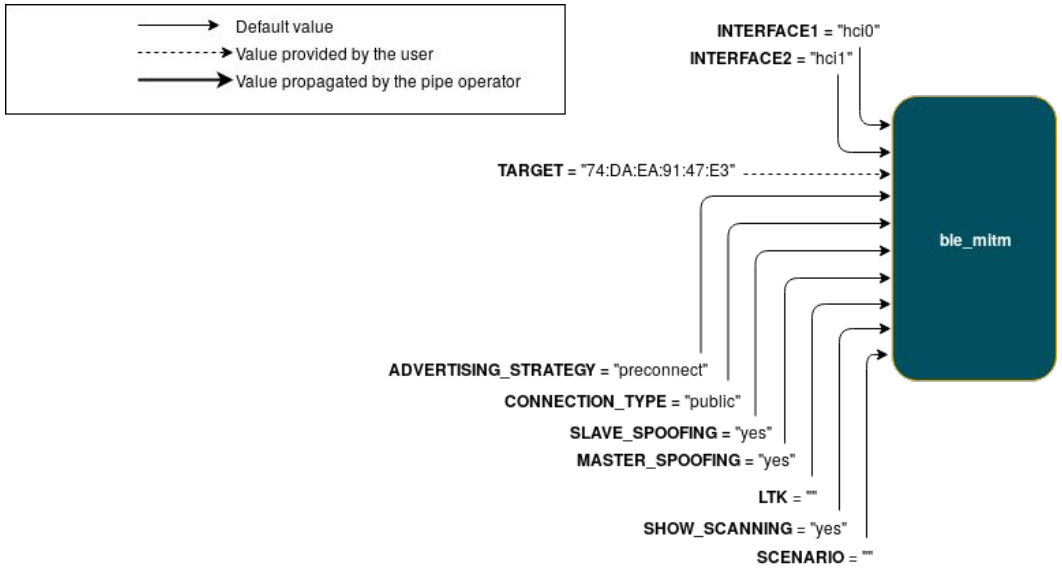


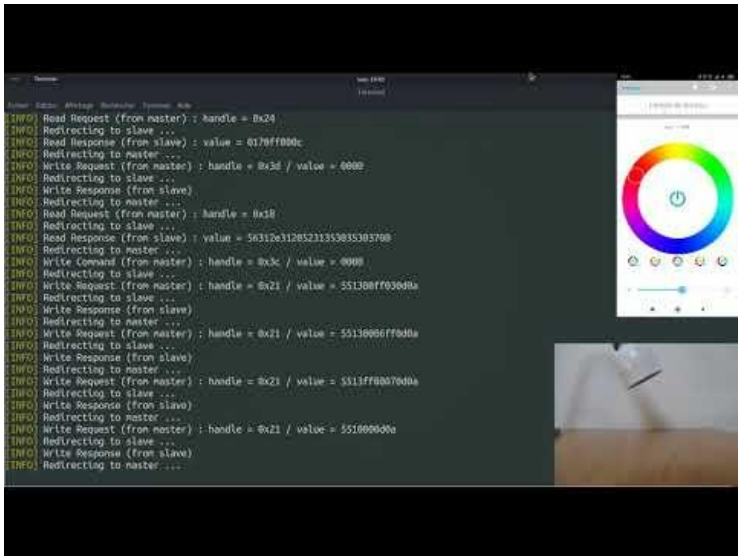
MODULES - COLLECTE D'INFORMATIONS / BLE_DISCOVER



- Module de **collecte d'information (mode *connecté*)**
- **Dump du serveur ATT/GATT** : permet d'identifier les services et les caractéristiques d'un objet connecté
- Mécanisme de **filtrage basique** par type et valeur
- **Exportation** des données au format .CFG

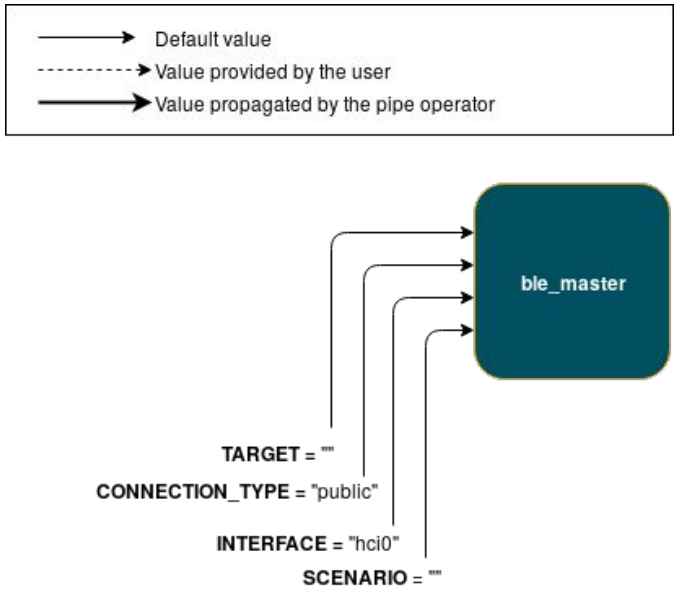
MODULES - ATTAQUE ACTIVE / BLE_MITM

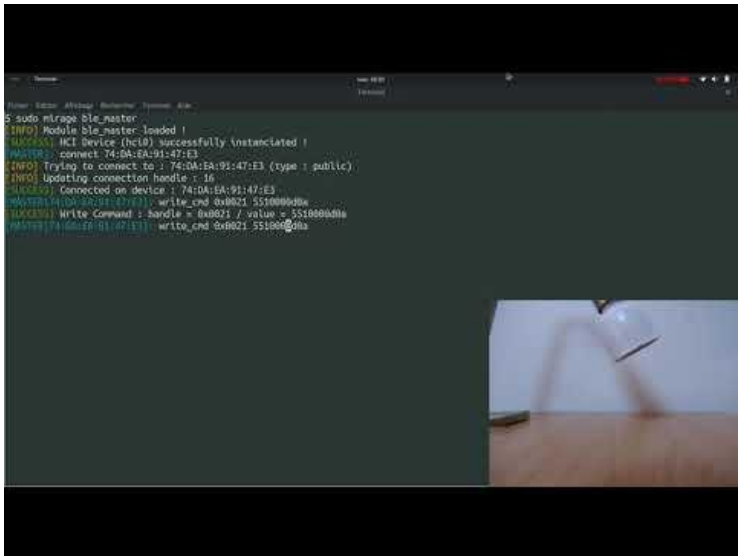




- Module d'**attaque active,** personnalisable via les **scénarios**
- implémente les **stratégies d'attaque** de *BTLEJuice* et *GATTacker*
- **Résout les problématiques** liées à l'usage de bibliothèques haut niveau
- **Gestion des mécanismes d'appairage :** crack de la *Temporary Key*
- **Gestion du chiffrement**

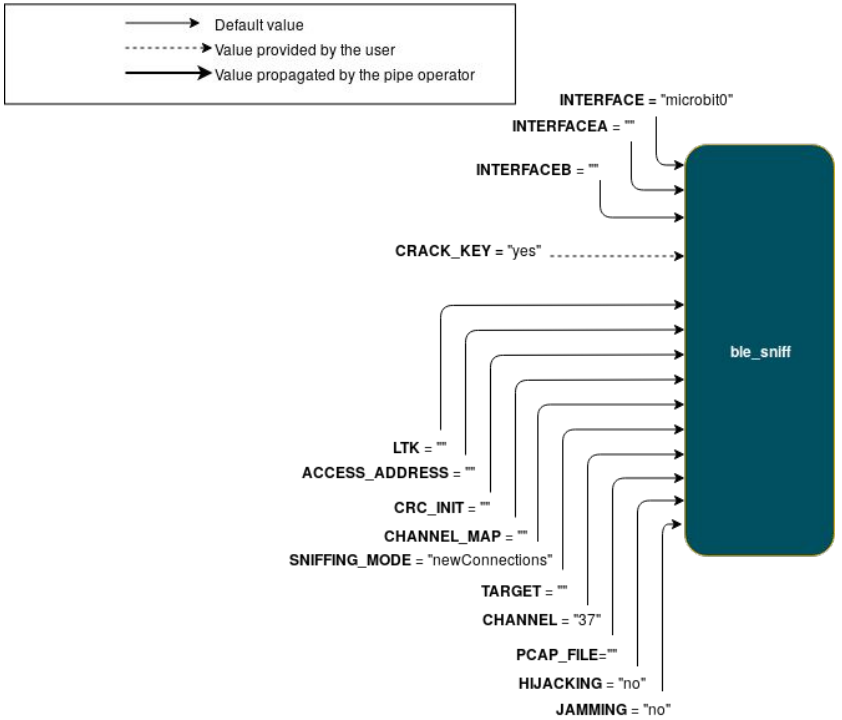
MODULES - ATTAQUE ACTIVE / BLE_MASTER

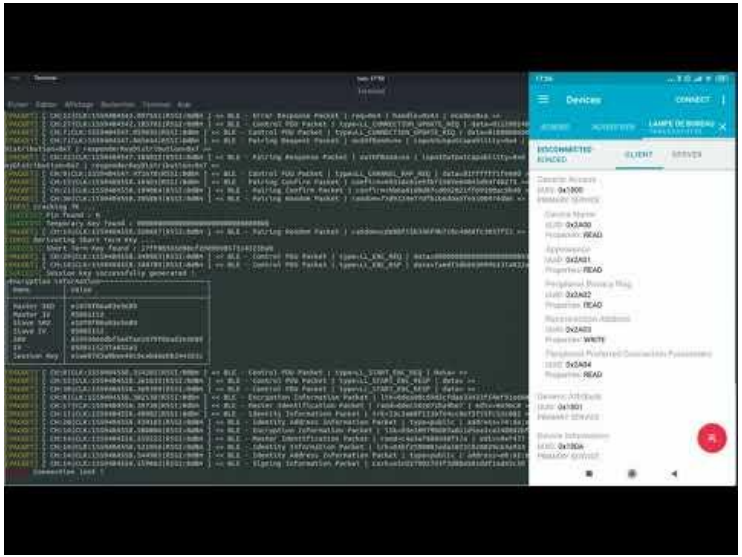




- Module d'**attaque active / simulation d'équipement**
- implémente le comportement d'un équipement **master**
- **Utilisable en mode CLI** et **personnalisable** via les scénarios
- Peut être utilisé **seul** ou **dans une exécution chaînée**

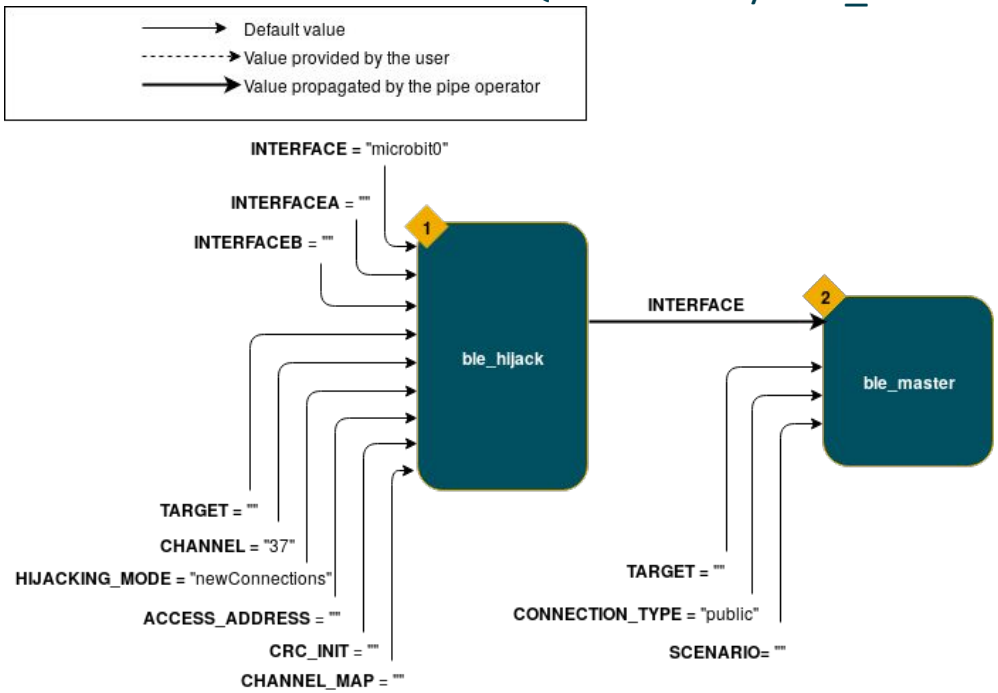
MODULES - ATTAQUE PASSIVE / BLE_SNIFF

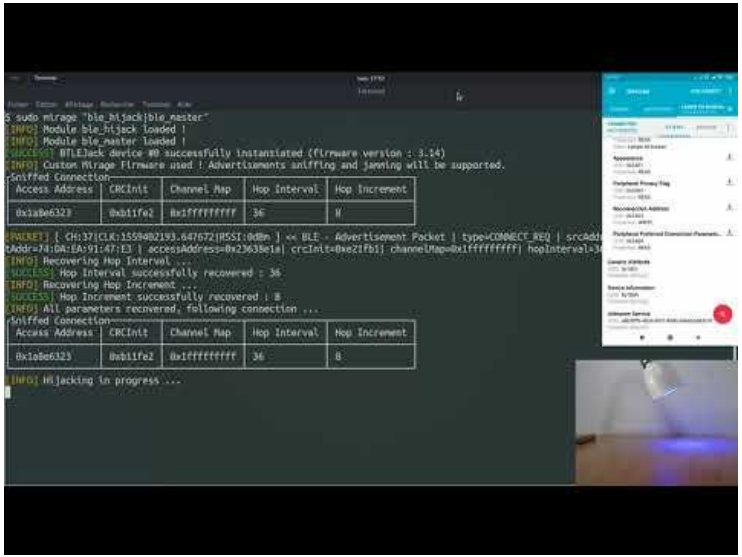




- Module d'**attaque passive**
- **Compatible avec BTLEJack et Ubertooth**
- **Gestion des mécanismes d'appairage :** crack de la *Temporary Key*
- **Gestion du chiffrement :** déchiffrement du trafic en "temps réel"

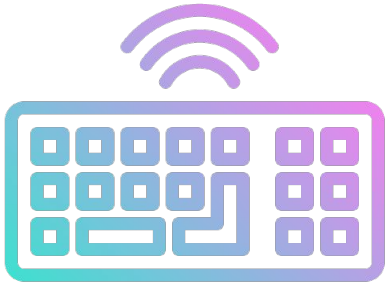
MODULES - ATTAQUE ACTIVE / BLE_HIJACK





- Module d'**attaque active**
- **Implémente l'attaque de BTLEJack : hijacking** de connection
- Peut être utilisé **dans une exécution chaînée** (remplace **ble_connect**)

MODULES - ATTAQUES D'INJECTION HID



Simulation de clavier HID BLE

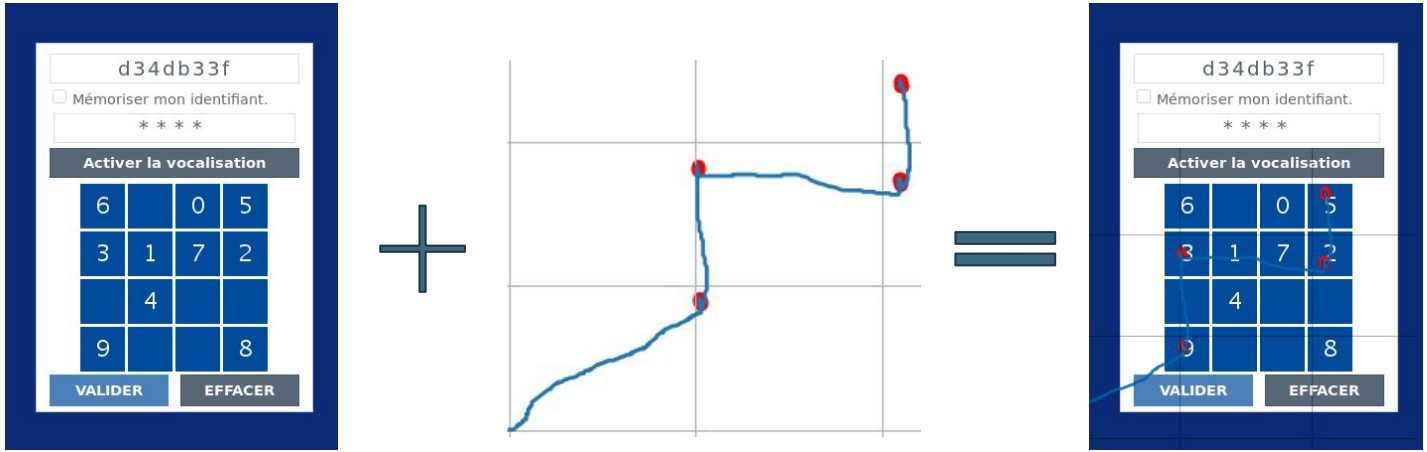
- implémentation du protocole HID over GATT
- attaque implémentée comme scénario de *ble_slave*

Injection de frappes non chiffrées ESB

- implémentation d'une des vulnérabilité de mousejack (Cert VU#981271)
- attaque implémentée comme scénario de *esb_ptx*

- **Réutilisation de composants logiciels:** réutilisation des dissecteurs/constructeurs HID et du parser Duckyscript
- **API similaire:** les scénarios proposent des API manipulables de la même façon (INTERACTIVE, DUCKYSCRIPT, TEXT)

MODULES - ENCHAÎNEMENT D'ATTAQUES COMPLEXES



- **Stratégie d'attaque complexe :** plusieurs modules d'exploitation enchaîné consécutivement dans l'optique d'atteindre un objectif précis
- **Compromission d'un clavier virtuel de banque** par l'intermédiaire d'une souris sans fil Logitech.

SÉCURITÉ DÉFENSIVE: ENJEUX ET PERSPECTIVES

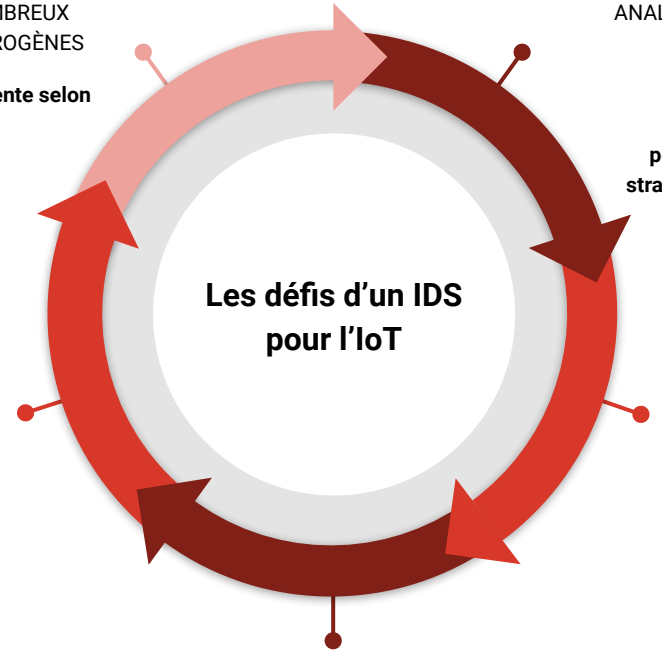
SÉCURITÉ DÉFENSIVE - ENJEUX

- **A l'heure actuelle,** il est difficile d'assurer la sécurité des objets connectés dès leur conception:

  - **Manque de compétence** des fabricants
  - **Limitations d'ordre matérielles** (cryptographie)
  - **Contraintes économiques** ("Time to market")

=> **Approches "en aval":** détection / prévention d'intrusion

SÉCURITÉ DÉFENSIVE - ENJEUX



MONITORER DE NOMBREUX PROTOCOLES HÉTÉROGÈNES

Connaissance différente selon les protocoles

ANALYSER LES INTERACTIONS ENTRE LES PROTOCOLES

Certains caractéristiques physiques des protocoles permettent d'envisager des stratégies "pivot" sur d'autres technologies.

DOMAINE EN EXPANSION

De nouvelles attaques de plus en plus inventives apparaissent chaque jour

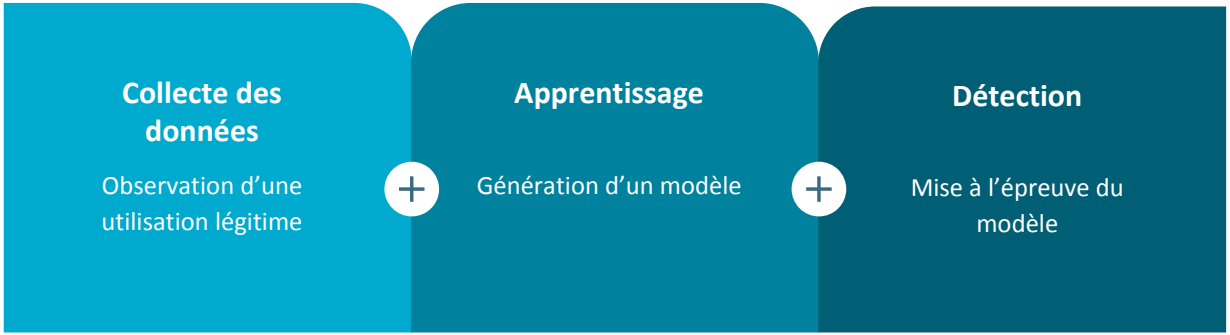
ENVIRONNEMENT DYNAMIQUE

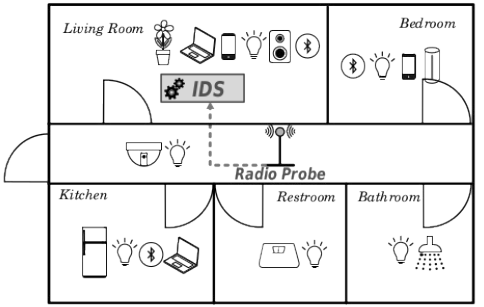
Environnement composé de nombreux noeuds mobiles, plus ou moins légitimes (smartphone, montres connectées, etc.)

PAS DE CENTRALISATION DU TRAFIC

Déploiement progressifs de topologies "pair à pair" ou "Mesh"

SÉCURITÉ DÉFENSIVE : TRAVAUX MENÉS AU LAAS-CNRS

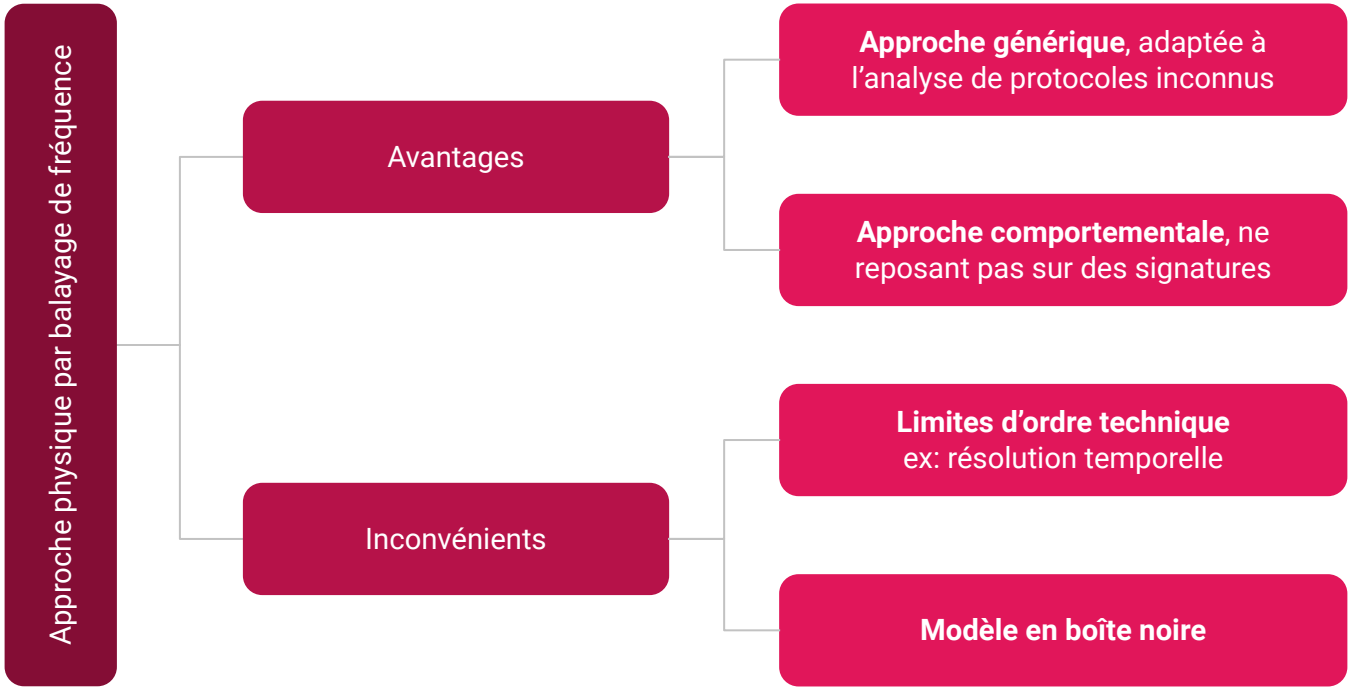




L'approche de la thèse de Jonathan Roux a permis d'explorer les points suivants:

- **Monitoring physique de larges bandes de fréquences (SDR en mode "Sweep")**
- **Génération d'un modèle des communications légitimes (Machine Learning)**
- **Localisation spatiale, fréquentielle et temporelle des intrusions**

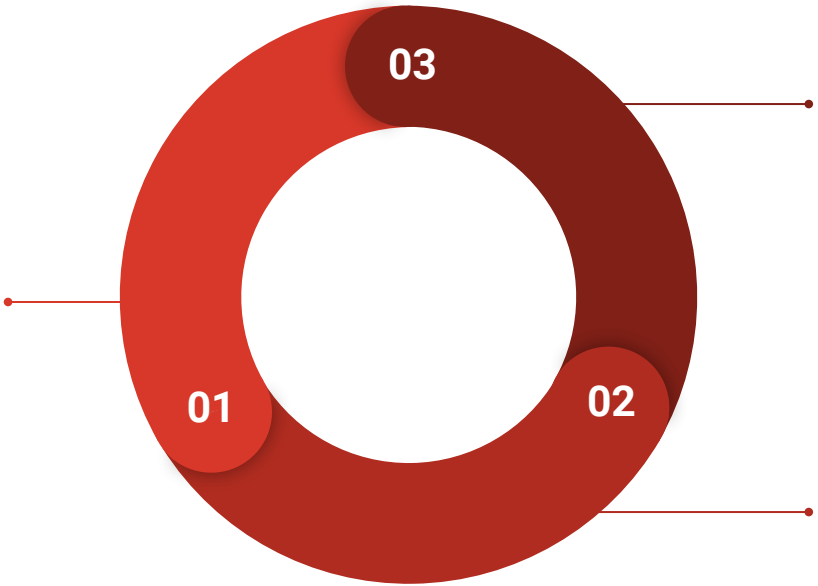
SÉCURITÉ DÉFENSIVE : TRAVAUX MENÉS AU LAAS-CNRS



SÉCURITÉ DÉFENSIVE : APPROCHE MULTI-COUCHE

Identification et caractérisation des attaques

Une approche multi-couche permettrait d'identifier les tentatives d'intrusions, mais également de caractériser la séquence d'attaques correspondante.



Corrélation des métriques de différentes couches

L'approche multi-couche permettrait de détecter des incohérences entre une modélisation de l'environnement radio niveau physique et niveau liaison, par exemple.

Exploitation de la connaissance acquise sur certains protocoles

L'analyse multi-couche permet d'intégrer et d'analyser de façon différente les protocoles selon le degré de connaissance qu'on a sur eux.

SÉCURITÉ DÉFENSIVE : APPROCHE MULTI-COUCHE

Collecte passive de métriques physiques

Collecte passive de métriques liaison

Inférence de la topologie des réseaux identifiés

Métriques couche physique

Métriques couche liaison

Métriques couche réseau

Caractéristiques basée sur une taxonomie des attaques

Corrélation et analyse des métriques

Détection / identification des attaques

Réaction / Prévention d'intrusion

SÉCURITÉ DÉFENSIVE : PISTES DE RECHERCHE

- **Fingerprinting physique d'émetteurs**: identifier les émetteurs par l'analyse physique de signaux radios

- **Analyse automatisée de protocoles:** inférer automatiquement un certain nombre de caractéristiques du protocole (modulation, datarate, codage…)

- **Inférence de topologies:** inférer de l'observation de la couche liaison les différentes topologies présentes dans l'environnement radio

- **Utilisation de Mirage à des fins défensives:** exploiter les piles protocolaires et les modules de collecte d'information passive implémentés dans Mirage à des fins défensives

Merci pour votre attention !

L'outil Mirage est open-source (licence MIT) et disponible à l'adresse suivante :

Dépôt principal : https://redmine.laas.fr/projects/mirage

Documentation : http://homepages.laas.fr/rcayre/mirage-documentation/

Dépôt principal : https://redmine.laas.fr/projects/mirage

Documentation : http://homepages.laas.fr/rcayre/mirage-documentation/

SÉCURITÉ IOT: DE L'OFFENSIF AU DÉFENSIF

RéSIST, 8 octobre 2019 - TOULOUSE

Romain CAYRE - rcayre@laas.fr

AN **AIRBUS** COMPANY