APSYS .Lab

Spark the future. Craft tomorrow.

LAAS CNRS

MIRAGE : UN FRAMEWORK OFFENSIF POUR L'AUDIT DU BLUETOOTH LOW ENERGY

SSTIC 2019 - Rennes

Romain CAYRE - Jonathan ROUX - Eric ALATA - Vincent NICOMETTE - Guillaume AURIOL

AN **AIRBUS** COMPANY

PLAN DE LA PRÉSENTATION

- **Contexte** et **problématique**
- **Architecture** de Mirage
- Présentation du **Bluetooth Low Energy**
- Présentation des **modules offensifs**
- **Conclusion** et **perspectives**

CONTEXTE ET PROBLÉMATIQUE

SÉCURITÉ DES OBJETS CONNECTÉS

Problématiques et enjeux

CONTEXTE : CONCEPTION D'UN IDS

Collecte des données

Observation d'une utilisation légitime

Apprentissage

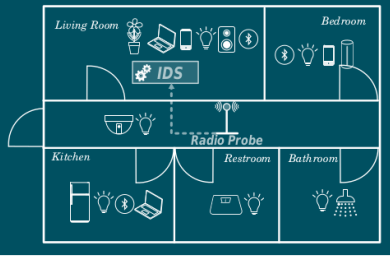
Génération d'un modèle

Détection

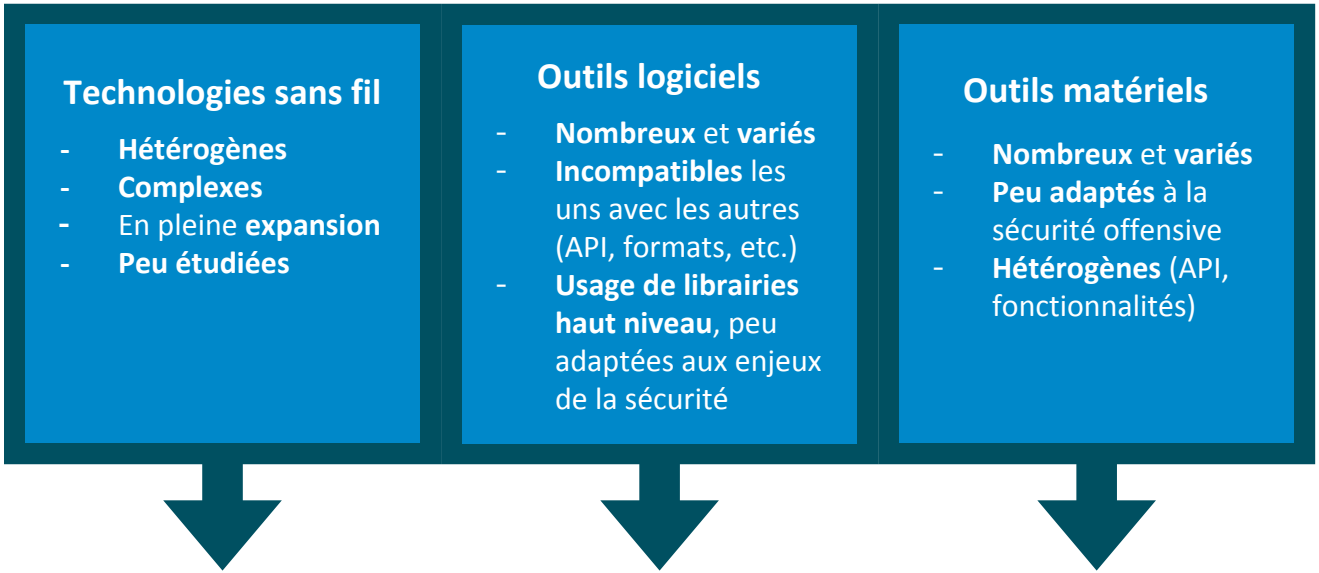
Mise à l'épreuve du modèle

Génération de campagnes d'attaques

Stage de fin d'études au LAAS-CNRS



SÉCURITÉ OFFENSIVE - PANORAMA



CONSÉQUENCES

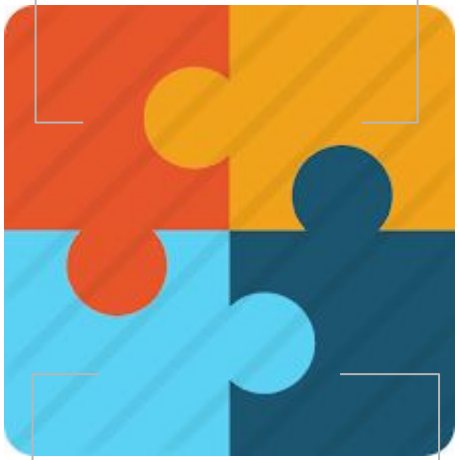
- **Frein au développement** des outils offensifs
- **Limitations** importantes pour **l'automatisation**
- Beaucoup de **développements inutiles** ou **redondants**
- L'analyste doit assimiler de **nombreuses informations techniques** peu pertinentes

ARCHITECTURE DE MIRAGE

PHILOSOPHIE DU FRAMEWORK

Approche unifiée

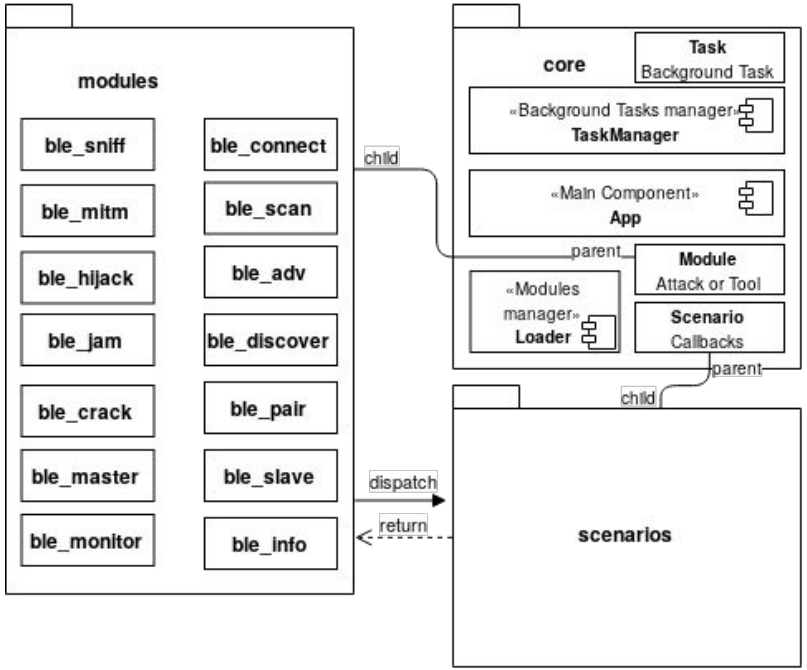
Approche modulaire

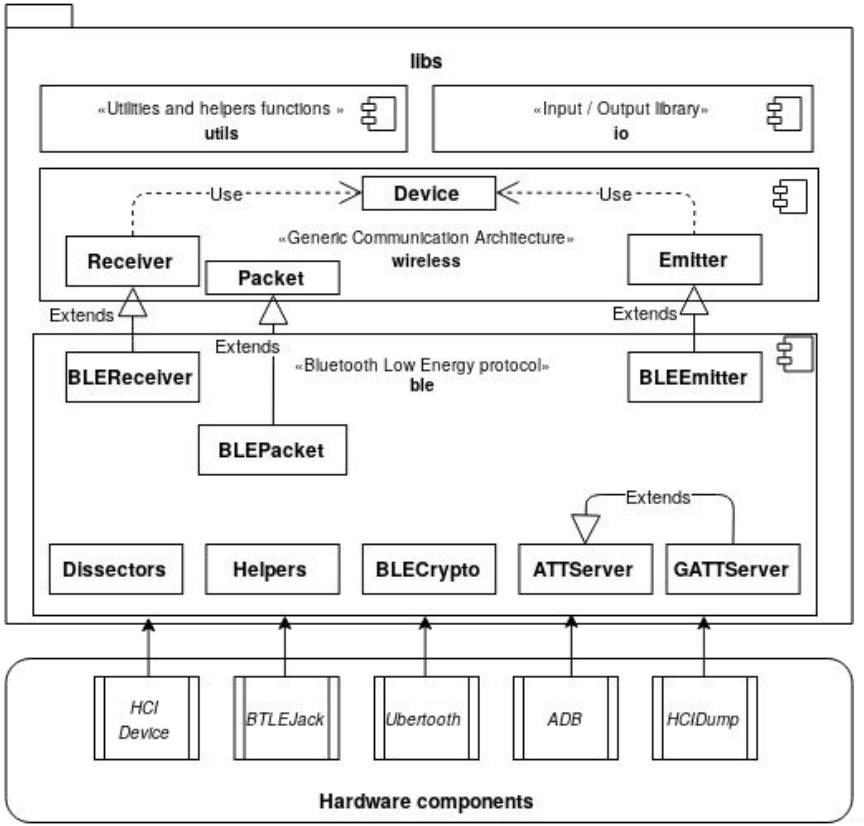


Approche générique

Approche bas niveau

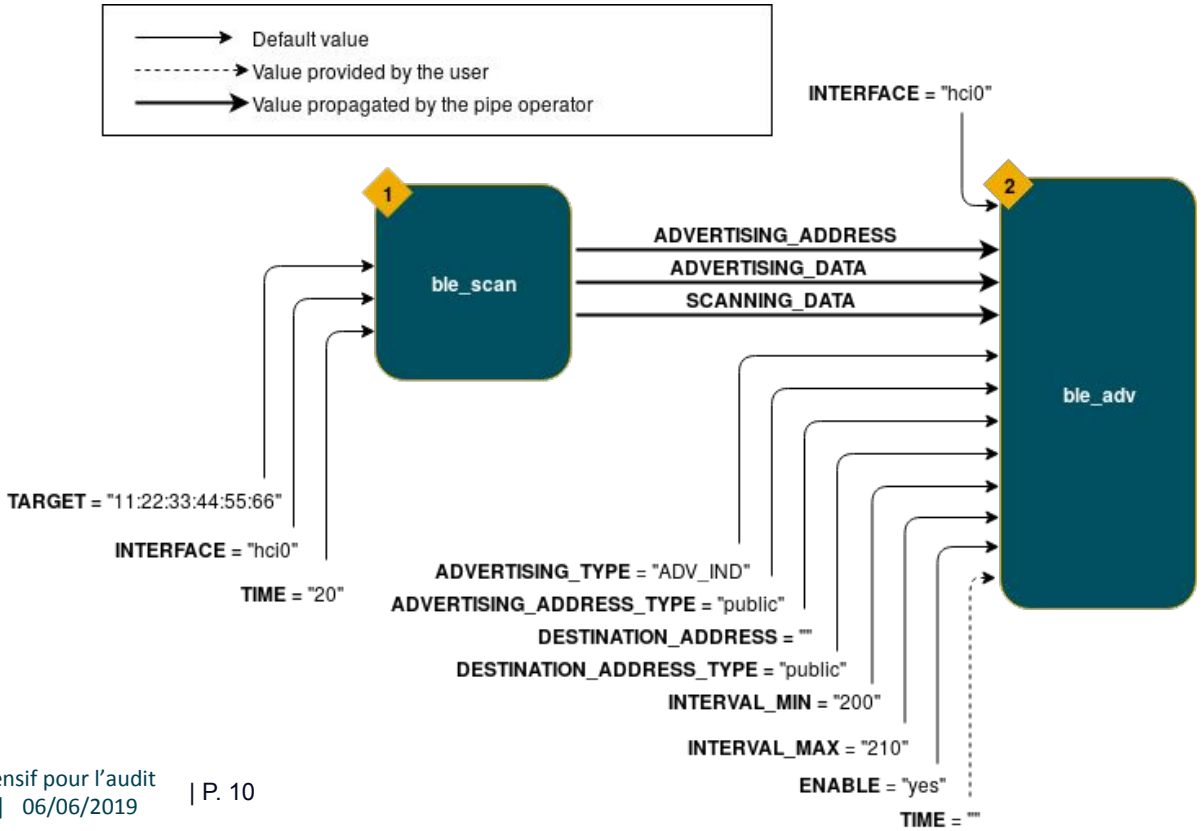
MIRAGE : ARCHITECTURE GLOBALE





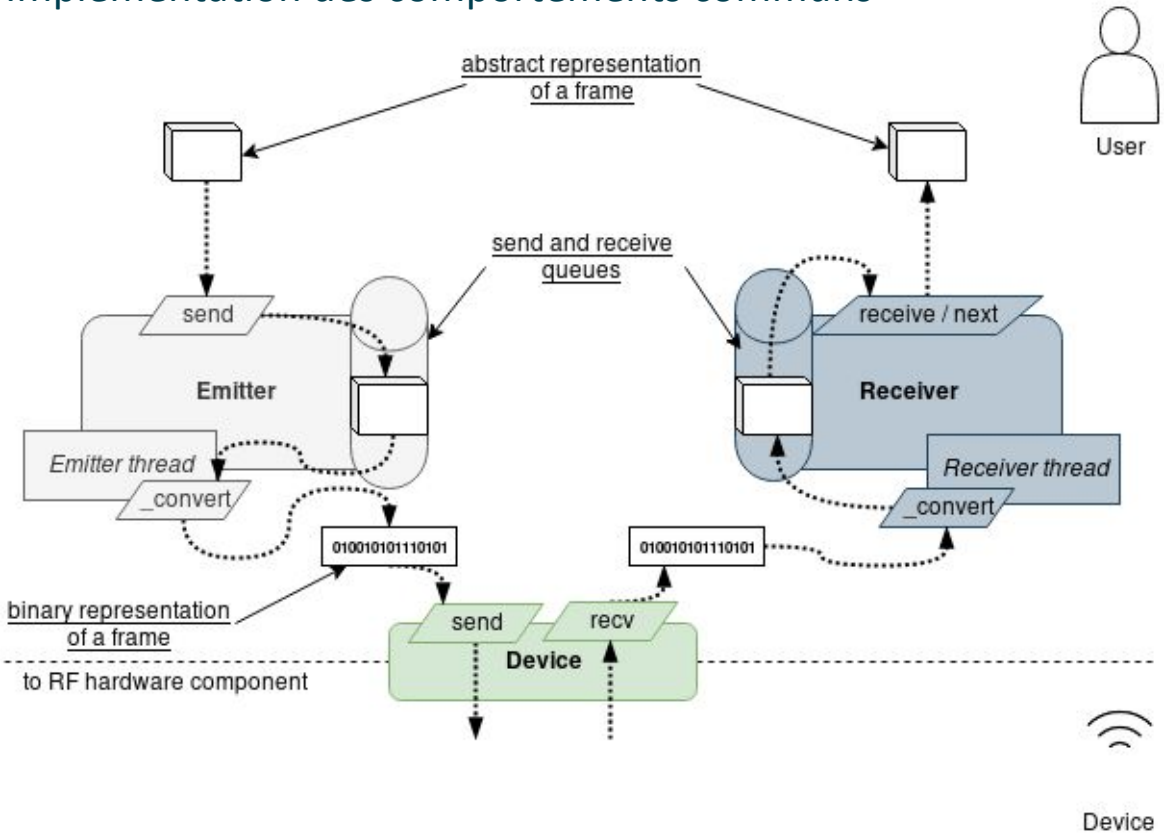
MIRAGE : CHAÎNAGE DE MODULES

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



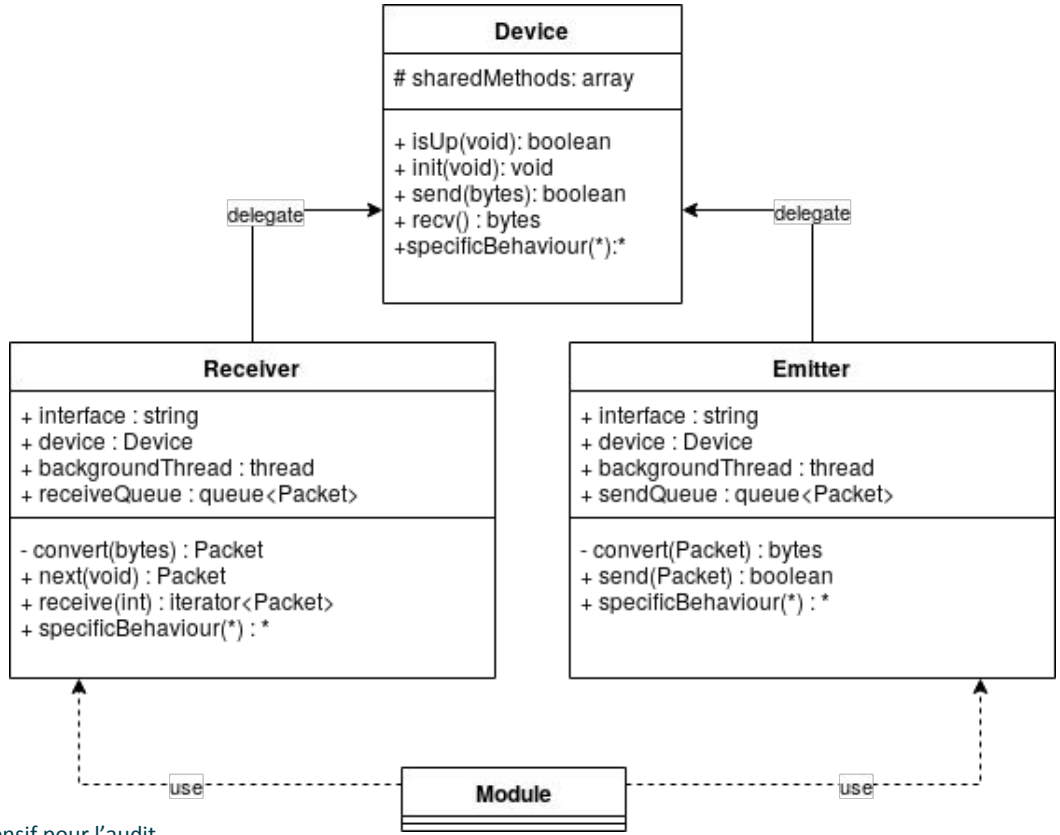
MIRAGE : ARCHITECTURE DE COMMUNICATION GÉNÉRIQUE

Implémentation des comportements communs

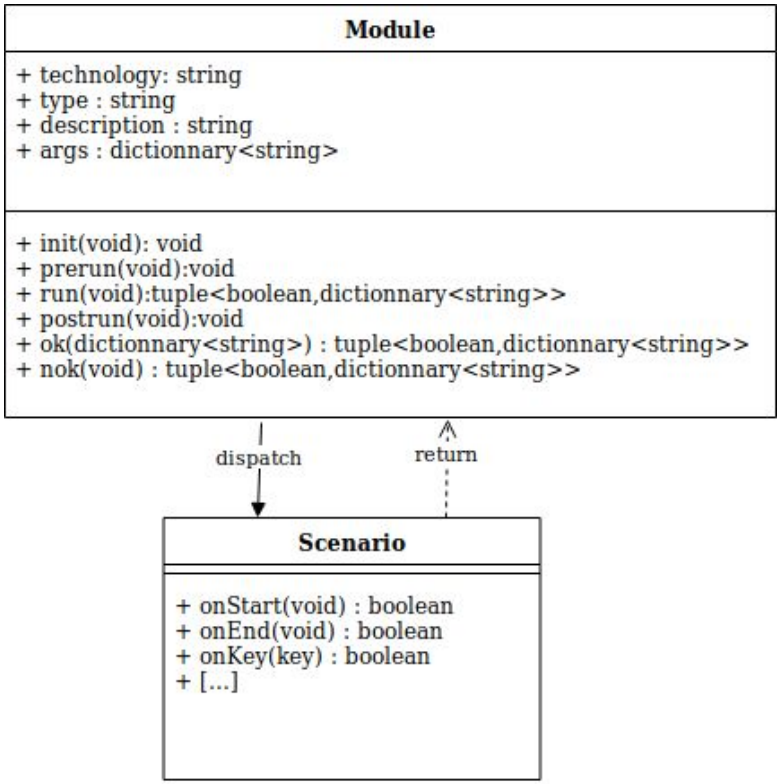


MIRAGE : ARCHITECTURE DE COMMUNICATION GÉNÉRIQUE

Implémentation des comportements spécifiques

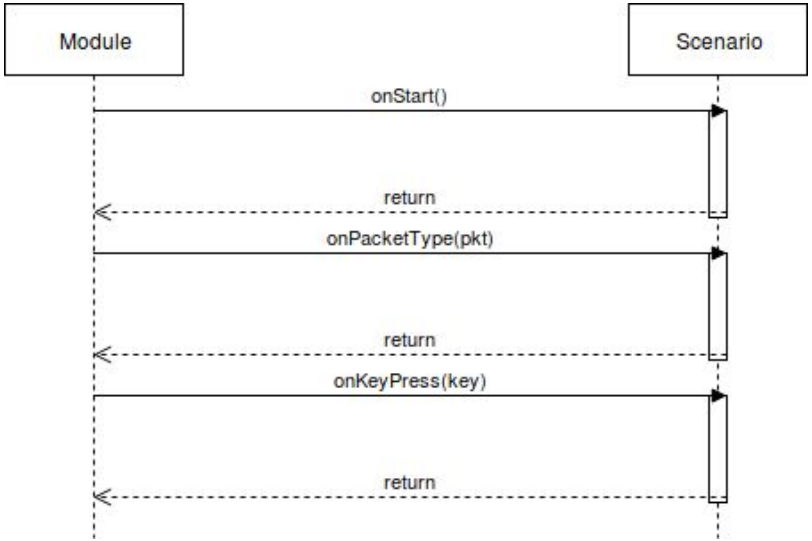


MIRAGE : MODULES ET SCÉNARIOS



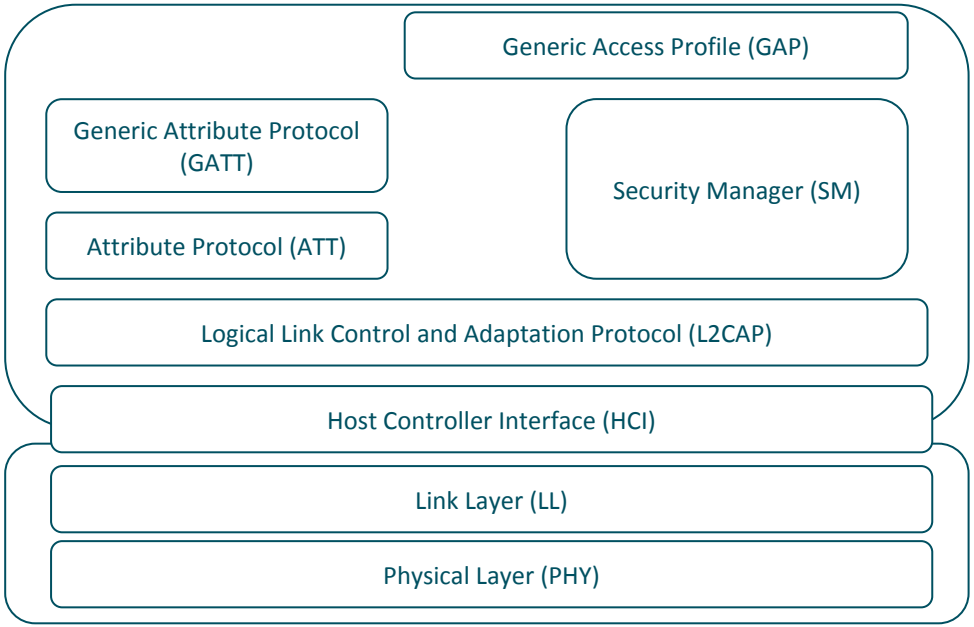
Présentation des modules et scénarios ↑

Mécanismes d'exécution d'un scénario ↓



PRÉSENTATION DU BLUETOOTH LOW ENERGY

BLUETOOTH LOW ENERGY - PILE PROTOCOLAIRE



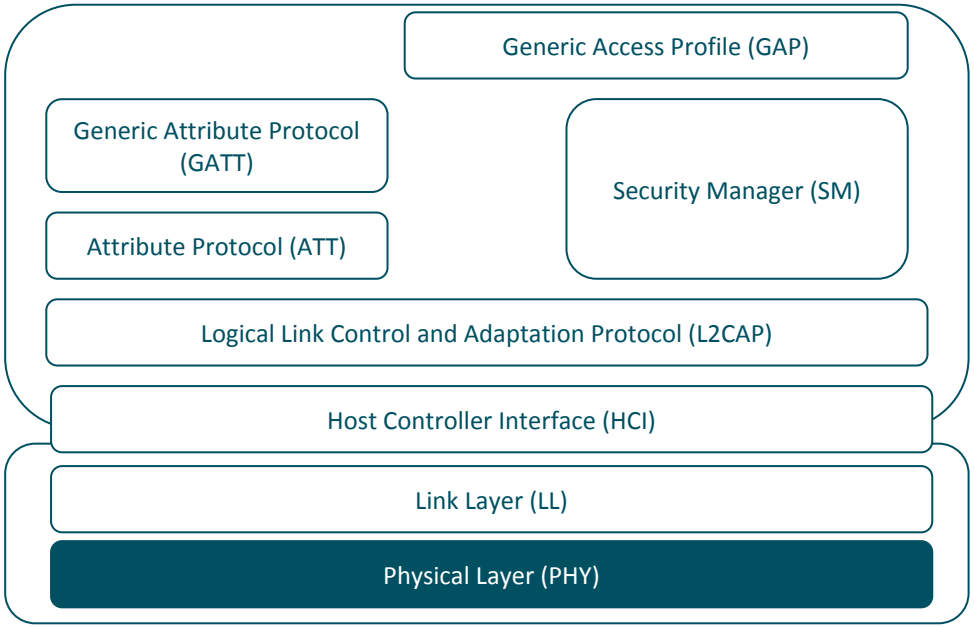
BLE utilise une pile protocolaire composée de deux composants :

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

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

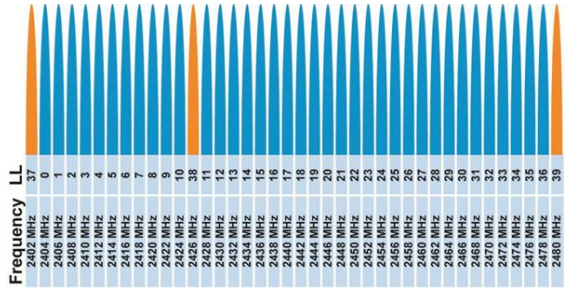
Bluetooth SMART

BLUETOOTH LOW ENERGY - COUCHE PHYSIQUE

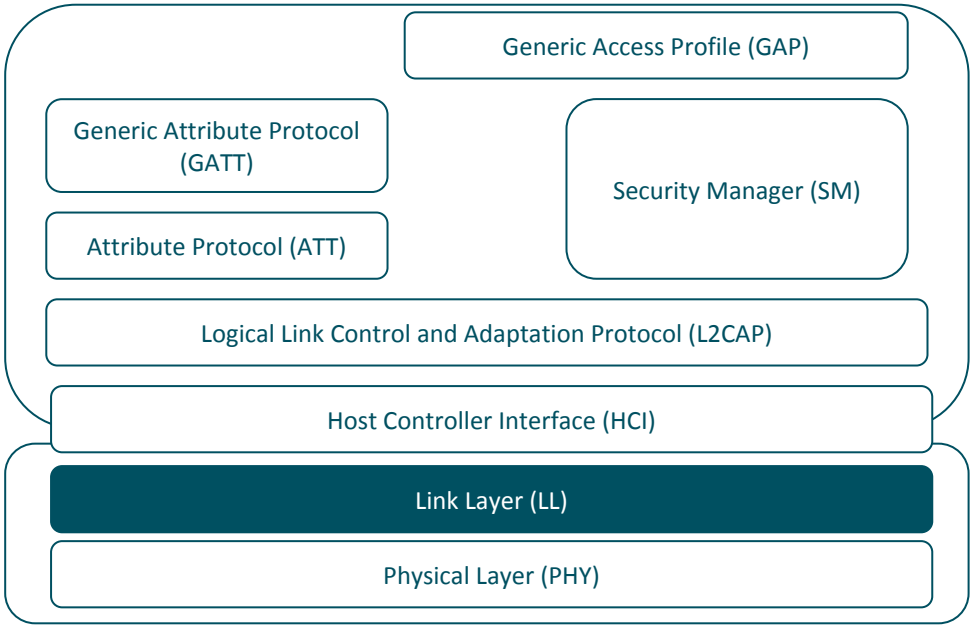


La couche physique repose sur un algorithme **de saut de fréquence linéaire,** rendant les **approches passives complexes.** Deux solutions existent :

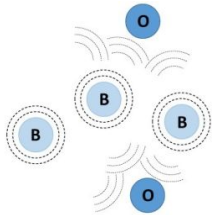
- Observer **le message d'initiation de connexion,** contenant les **paramètres de l'algorithme**
- Récupérer **les paramètres** par l'intermédiaire **d'heuristiques**



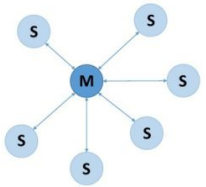
BLUETOOTH LOW ENERGY - COUCHE LIAISON



La couche liaison définit **deux modes** :

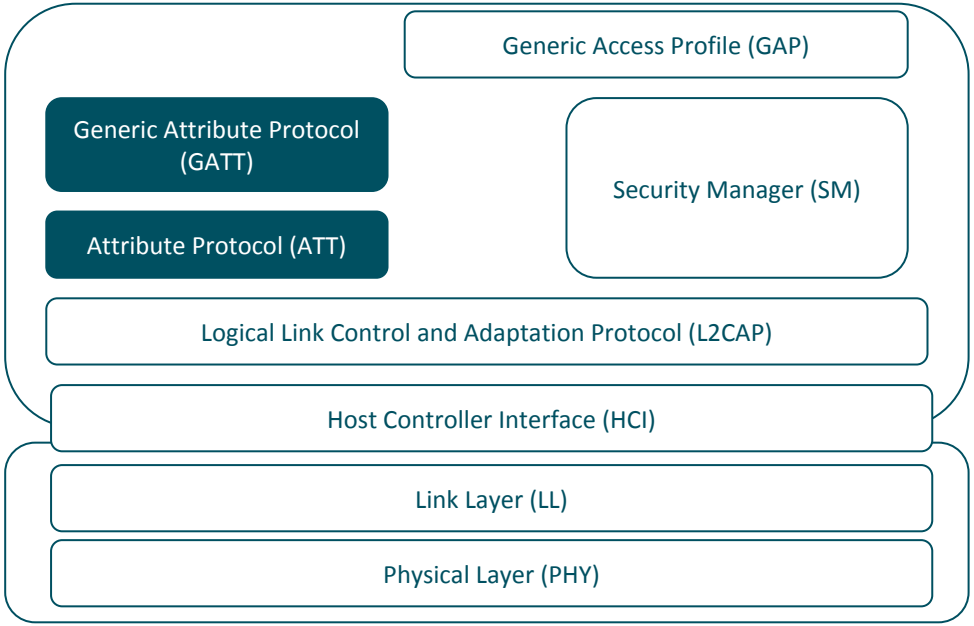


- **Un mode d'*advertising***, comparable à un mécanisme de diffusion de messages en *broadcast*



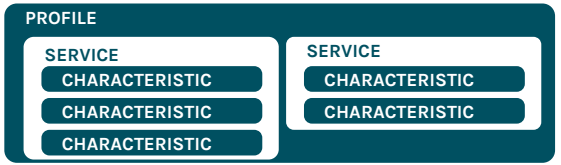
- **Un mode *connecté***, correspondant à une topologie Maître / Esclave (*Master / Slave*)

BLUETOOTH LOW ENERGY - COUCHES APPLICATIVES



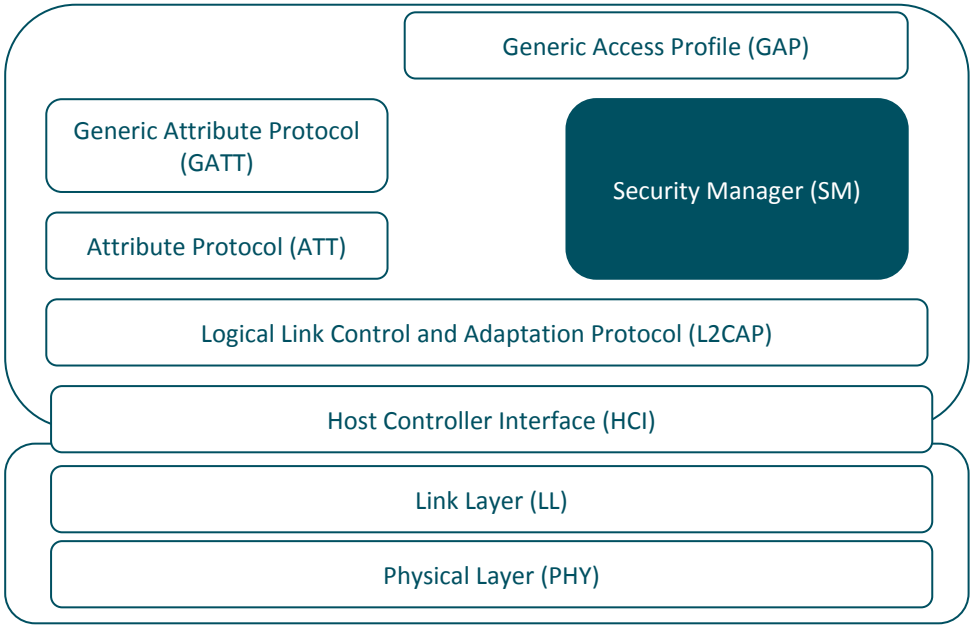
Les couches ATT et GATT sont les couches applicatives principales.

- 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.

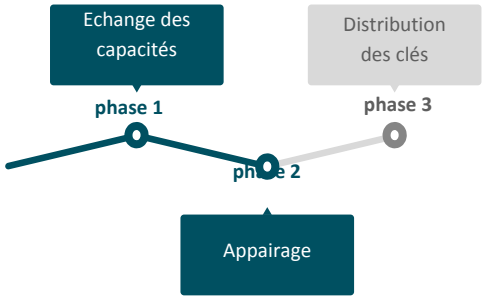


- La **couche GATT** spécialise la couche ATT en distinguant des services primaires et secondaires, contenant des caractéristiques.

BLUETOOTH LOW ENERGY - SÉCURITÉ



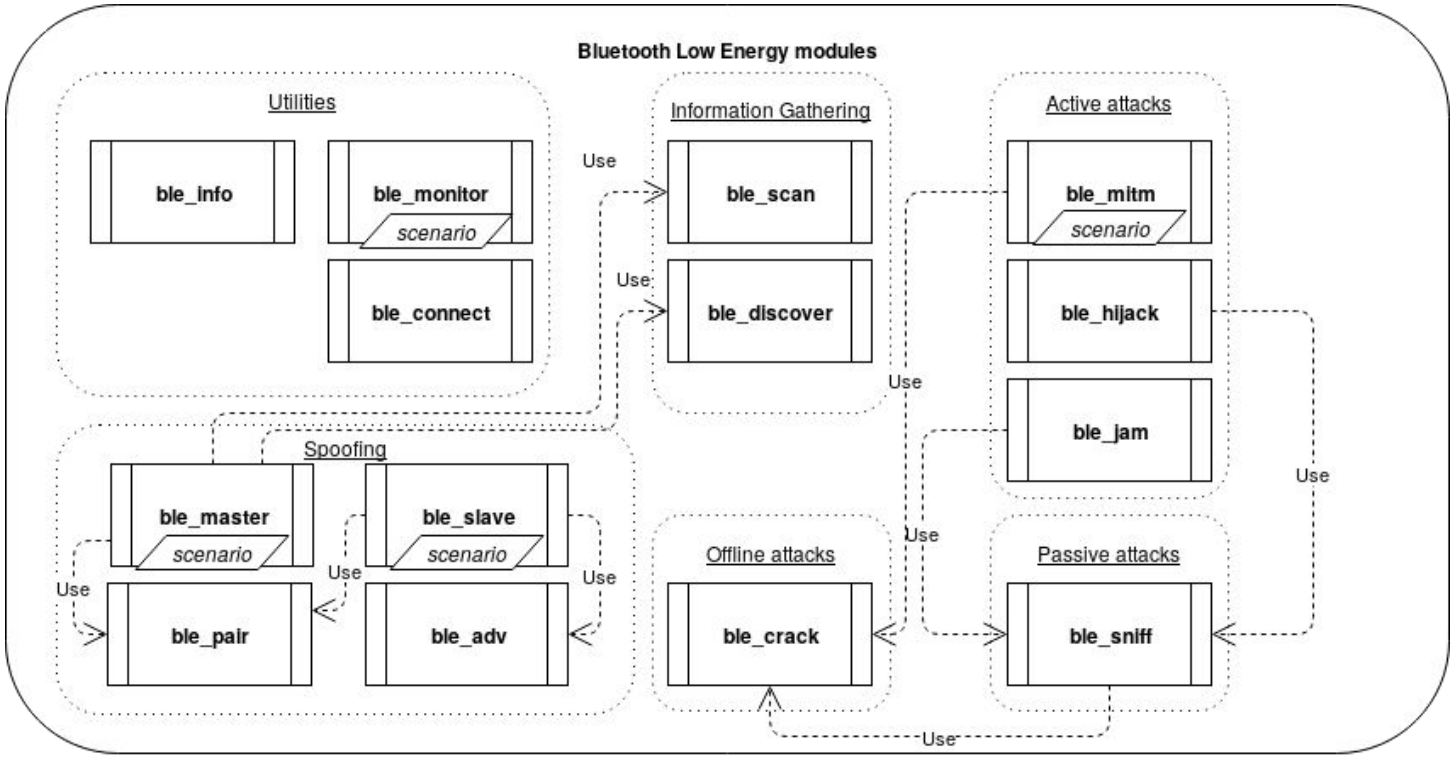
La couche Security Manager gère la sécurité du protocole.



- 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…

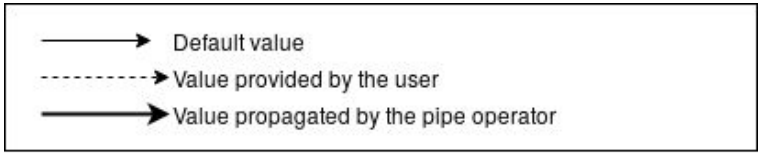
PRÉSENTATION DES MODULES OFFENSIFS

MODULES - VUE D'ENSEMBLE



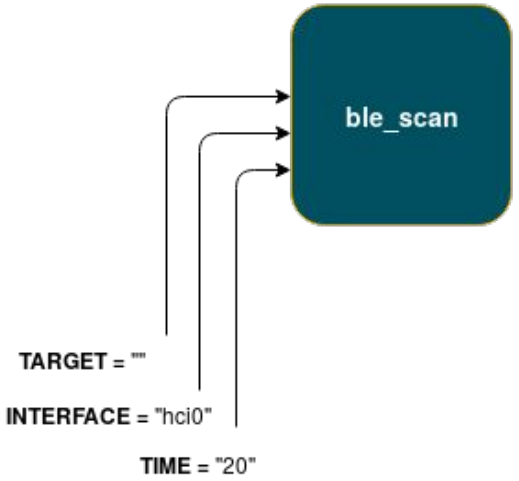
MODULES - COLLECTE D'INFORMATIONS / BLE_SCAN

- 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

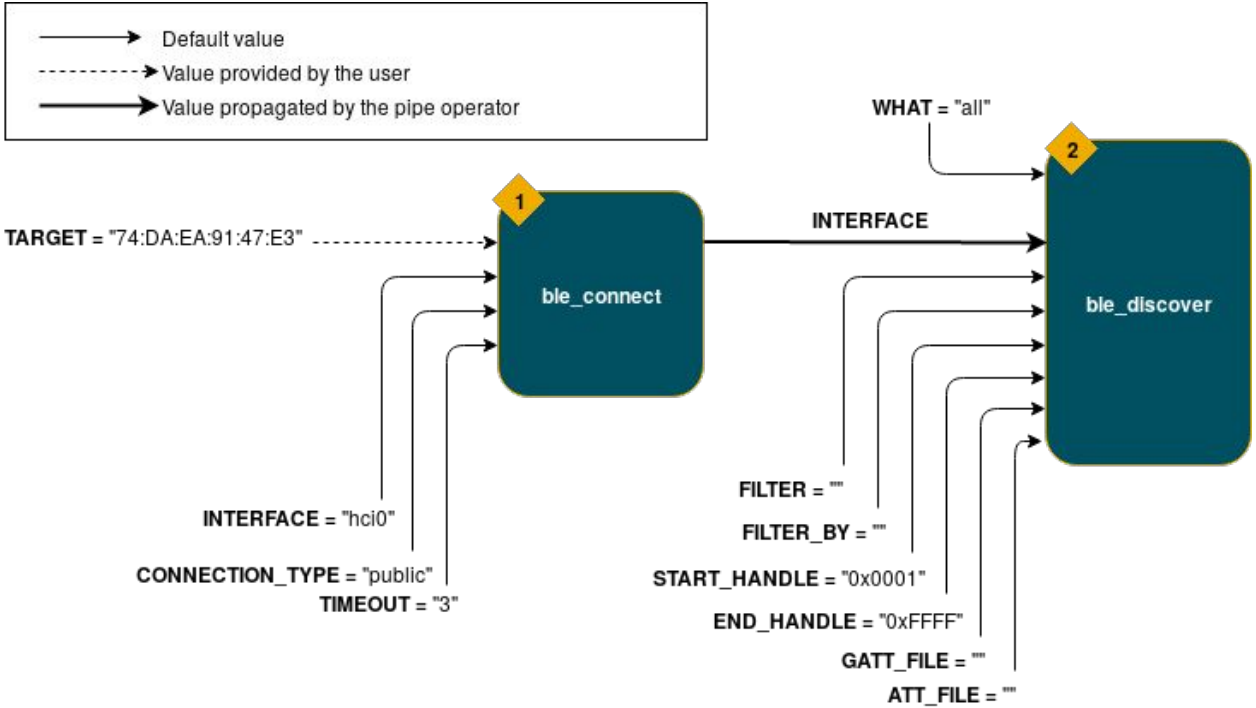



```
$ sudo ./mirage.py ble_scan
[INFO] Module ble_scan loaded !
[SUCCESS] HCI Device (hci0) successfully instanciated !

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

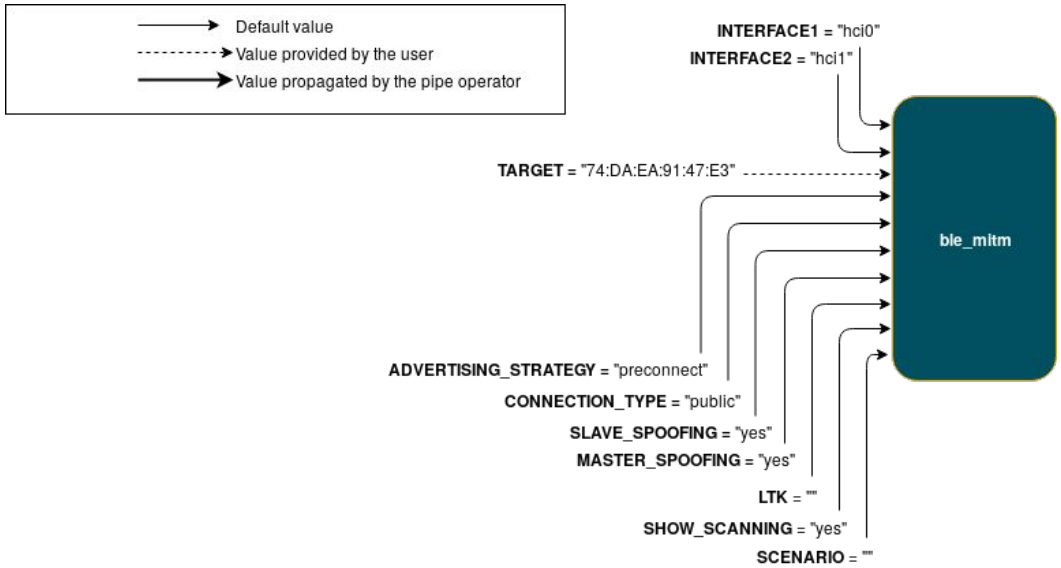


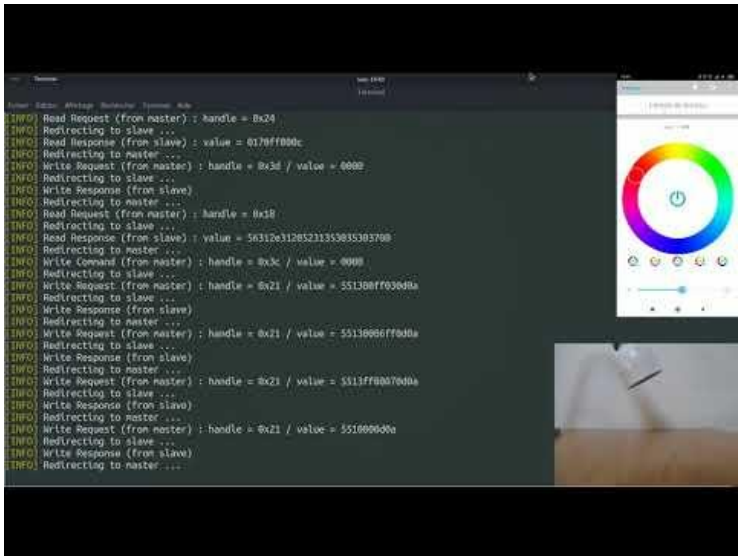
MODULES - COLLECTE D'INFORMATIONS / BLE_DISCOVER



- 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

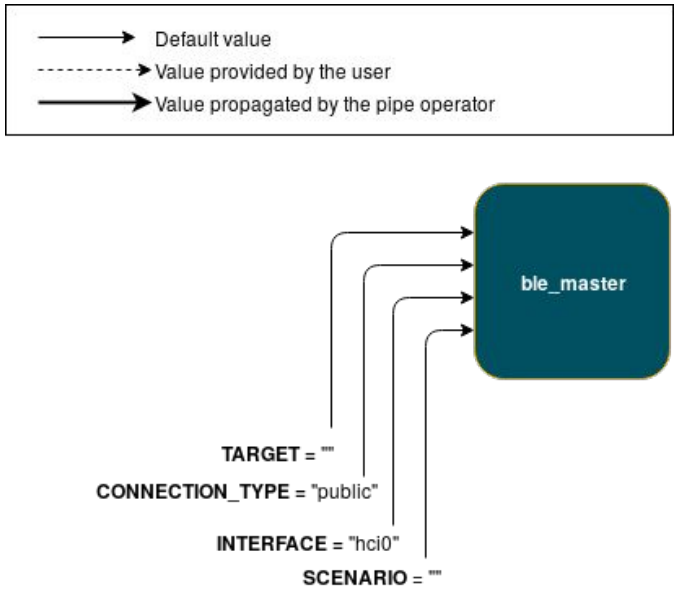
MODULES - ATTAQUE ACTIVE / BLE_MITM

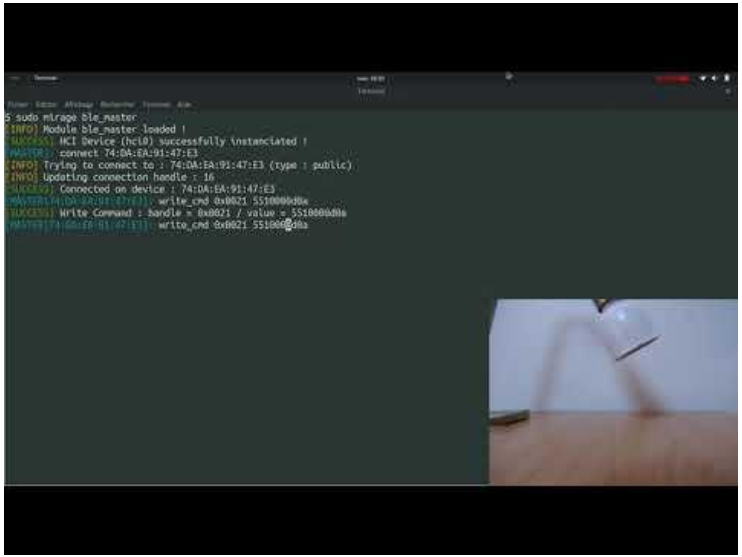




- Module d'**attaque active,** personnalisable via les **scénarios**
- implémente les **stratégies d'attaque** de *BTLEJuice* et *GATTacker*
- **Résout les problématiques** liées à l'usage de bibliothèques haut niveau
- **Gestion des mécanismes d'appairage :** crack de la *Temporary Key*
- **Gestion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

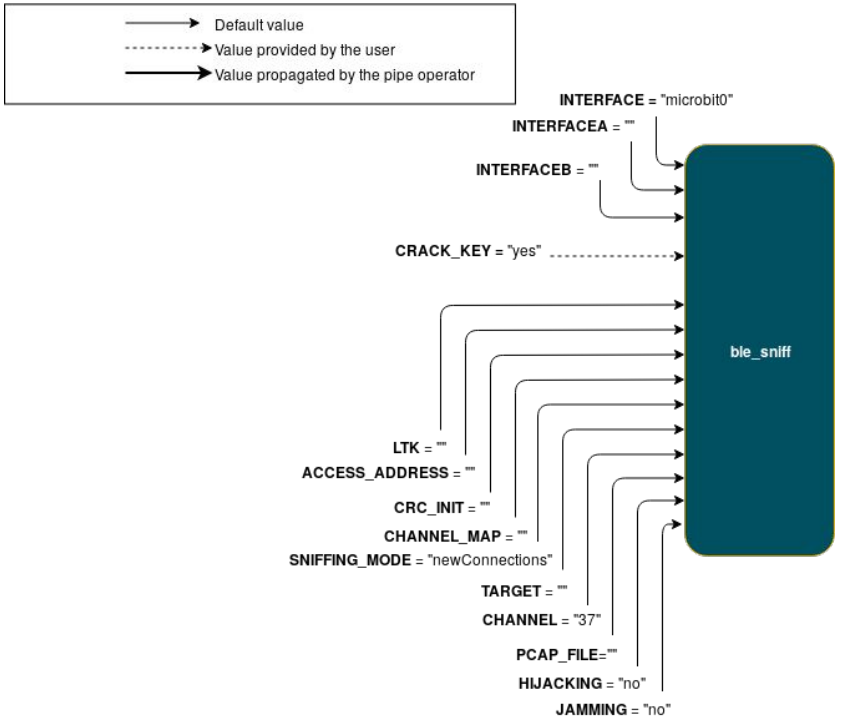
MODULES - ATTAQUE ACTIVE / BLE_MASTER

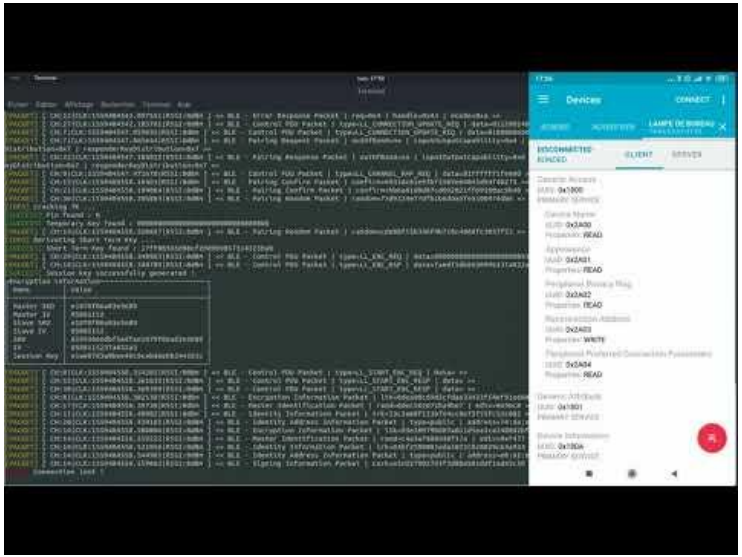




- Module d'**attaque active / simulation d'équipement**
- implémente le comportement d'un équipement **master**
- **Utilisable en mode CLI** et **personnalisable** via les scénarios
- Peut être utilisé **seul** ou **dans une exécution chaînée**

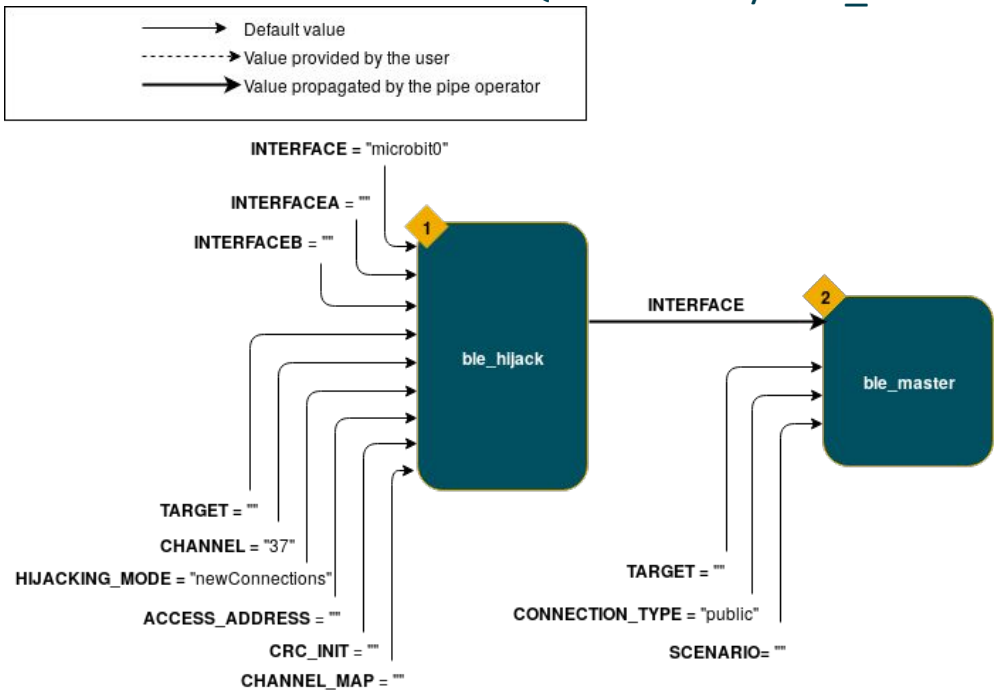
MODULES - ATTAQUE PASSIVE / BLE_SNIFF

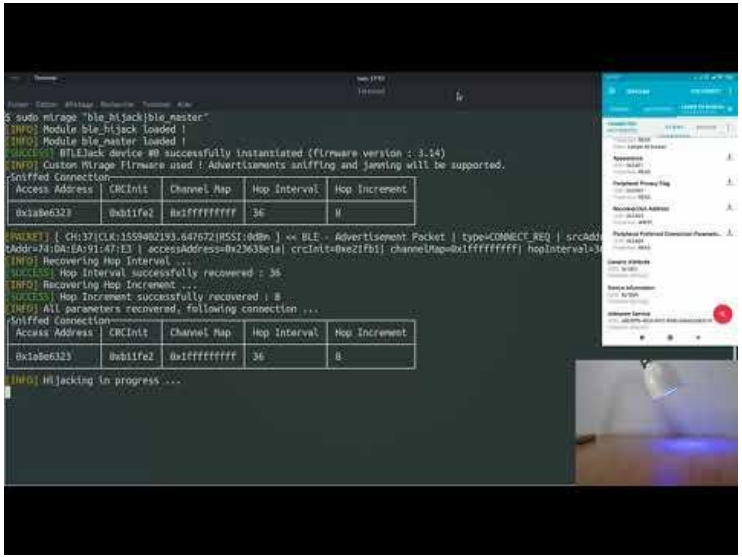




- Module d'**attaque passive**
- **Compatible avec BTLEJack et Ubertooth**
- **Gestion des mécanismes d'appairage :** crack de la *Temporary Key*
- **Gestion du chiffrement :** déchiffrement du trafic en "temps réel"

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**)

CONCLUSION ET PERSPECTIVES

CONCLUSION ET PERSPECTIVES

Mirage a permis de répondre aux problématiques **d'évaluation de l'IDS**:

- **Automatisation** de comportements offensifs
- **Simulation d'attaques réalistes** et **complexes**

Il nous a également permis d'auditer plusieurs objets connectés disponibles dans le commerce, **20 vulnérabilités** concernant **5 objets** sont actuellement en cours de *disclosure*.

Plusieurs pistes nous semblent intéressantes à explorer :

- Ajout de nouveaux protocoles, implémentation de nouvelles attaques : **vers l'audit d'environnements complets**
- Utilisation des modules existants **côté défensif** : **stratégies de détection / prévention d'intrusion** (utilisation des modules offensifs en réaction à une tentative d'intrusion)

L'outil 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/

REMERCIEMENTS

Damien Cauquil

Pour sa gentillesse, sa patience et sa pédagogie lors de nos échanges de mails.

Sa connaissance du Bluetooth Low Energy et son expérience m'ont beaucoup aidé lors du développement de Mirage.

Mike Ryan

Pour sa disponibilité sur IRC, ses conférences et les nombreux travaux et outils qu'il a publié librement.

Ses travaux sur la sécurité du Bluetooth Low Energy ont été des ressources indispensables.

Les reviewers de SSTIC

Pour leurs relectures avisées et la pertinence de leurs conseils.

Toutes les fonctionnalités de Mirage liées à l'appairage, au chiffrement ou au monitoring HCI leur sont dû.

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

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

APSYS .Lab

Spark the future. Craft tomorrow.

LAAS CNRS

MIRAGE : UN FRAMEWORK OFFENSIF POUR L'AUDIT DU BLUETOOTH LOW ENERGY

SSTIC 2019 - Rennes

Romain CAYRE - Jonathan ROUX - Eric ALATA - Vincent NICOMETTE - Guillaume AURIOL

AN **AIRBUS** COMPANY