APSYS .Lab

Spark the future. Craft tomorrow.

LAAS CNRS

OASIS: UN FRAMEWORK POUR LA DÉTECTION D'INTRUSION EMBARQUÉE DANS LES CONTRÔLEURS BLUETOOTH LOW ENERGY

2 juin 2022 - SSTIC 2022

Romain CAYRE - Clément Chaine - Guillaume Auriol - Vincent Nicomette - Géraldine Marconato

rcayre@laas.fr / clement.chaine@insa-toulouse.fr

AN **AIRBUS** COMPANY

CONTEXTE DE CES TRAVAUX

- **Thèse CIFRE** au **LAAS-CNRS** (**équipe TSF**), co-encadrée par **Apsys.Lab, démarrée le 14 janvier 2019**
- **Thématique de recherche:** sécurité des objets connectés et sécurité des protocoles de communication sans fil

- **Stage de M1** de **Clément Chaine**

PLAN DE LA PRÉSENTATION

- **Contexte, problématique** et **pré-requis**
- **Stratégies de détection d'attaques**
- **Conception du framework**
- **Expérimentations**

CONTEXTE, PROBLÉMATIQUE ET PRÉ-REQUIS

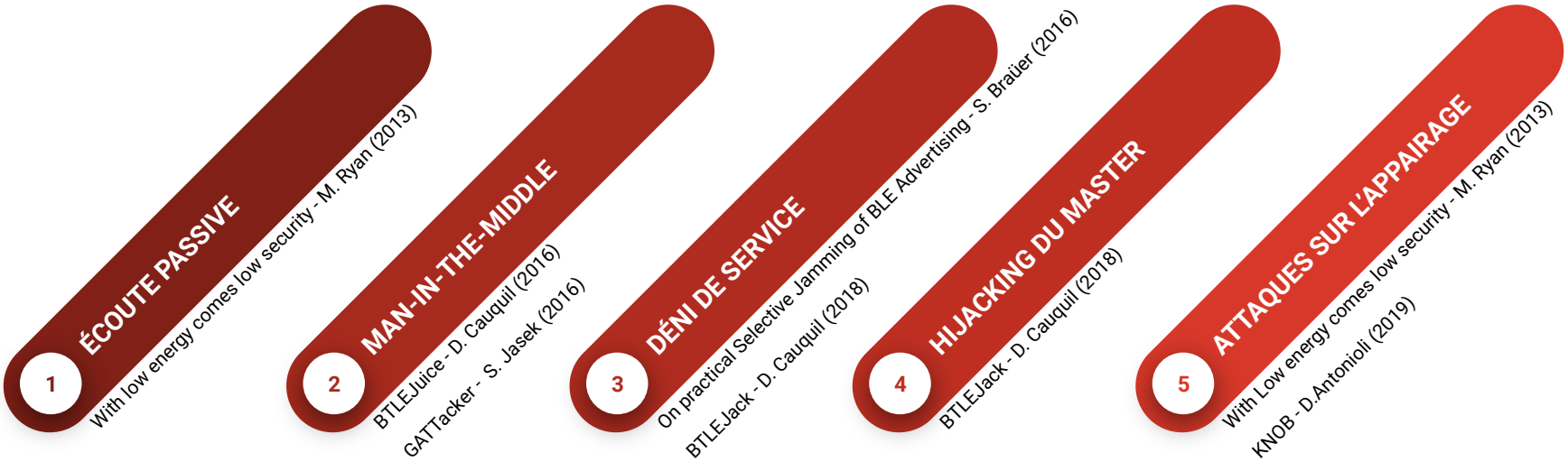
BLUETOOTH LOW ENERGY

Bluetooth SMART

- **Variante légère** du protocole Bluetooth BR/EDR, introduit dans la **version 4.0 de la spécification**
- **Faible consommation d'énergie**
- **Faible complexité** des piles protocolaires
- Massivement déployé (smartphones, ordinateurs, objets connectés, …)

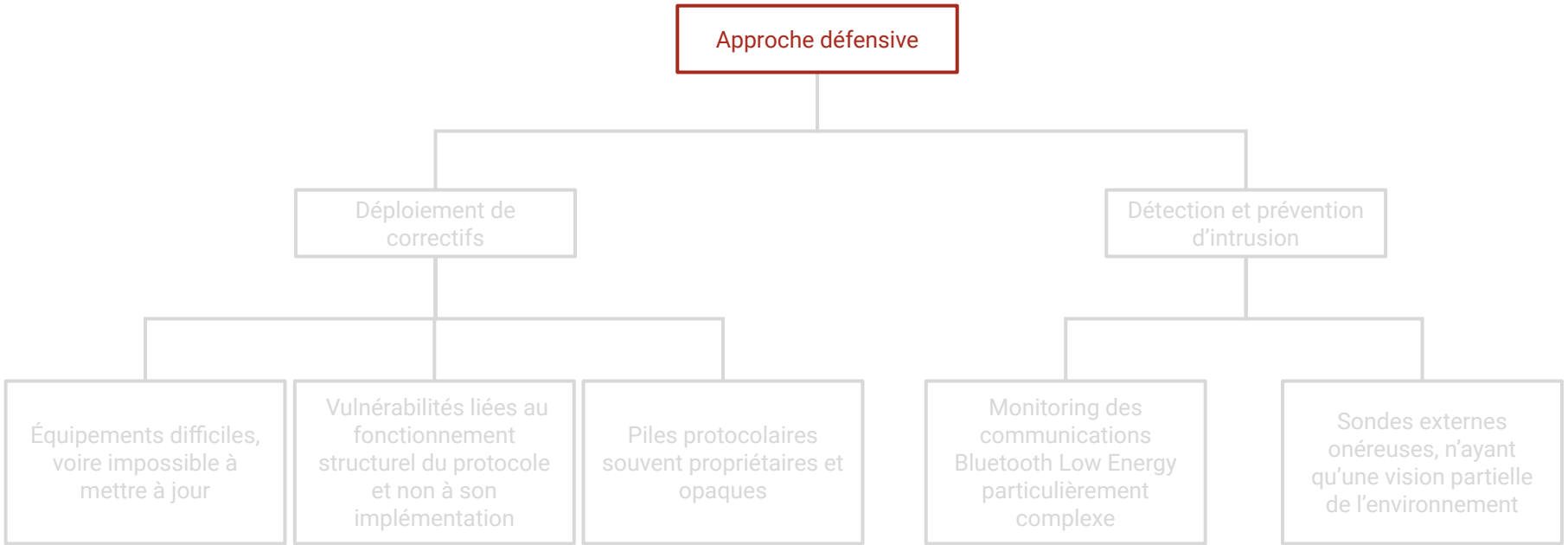
CONTEXTE: RAPIDE ÉTAT DE L'ART OFFENSIF

Avec l'essor des objets connectés, de **très nombreuses vulnérabilités** visant le protocole Bluetooth ont été identifiées et rendues publics ces dernières années (InjectaBLE, Gattacker/BTLEJuice, BTLEJack, etc).



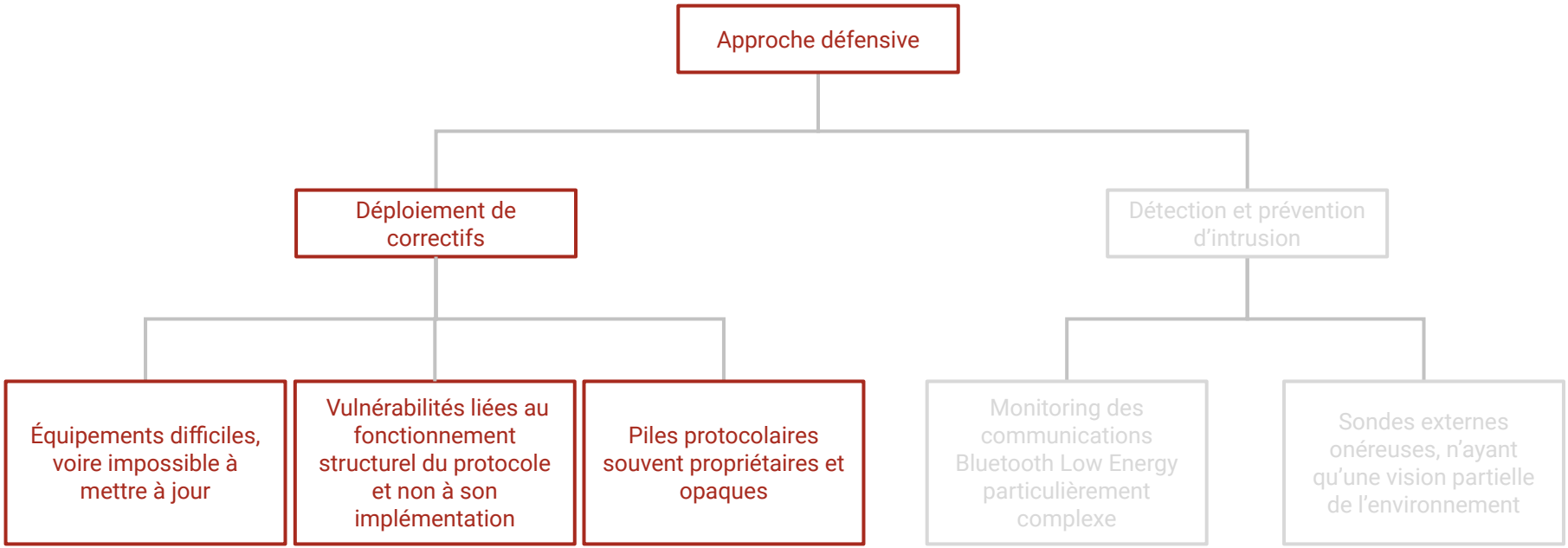
CONTEXTE: MÉCANISMES DÉFENSIFS

Mettre en place une approche défensive adaptée est particulièrement complexe:



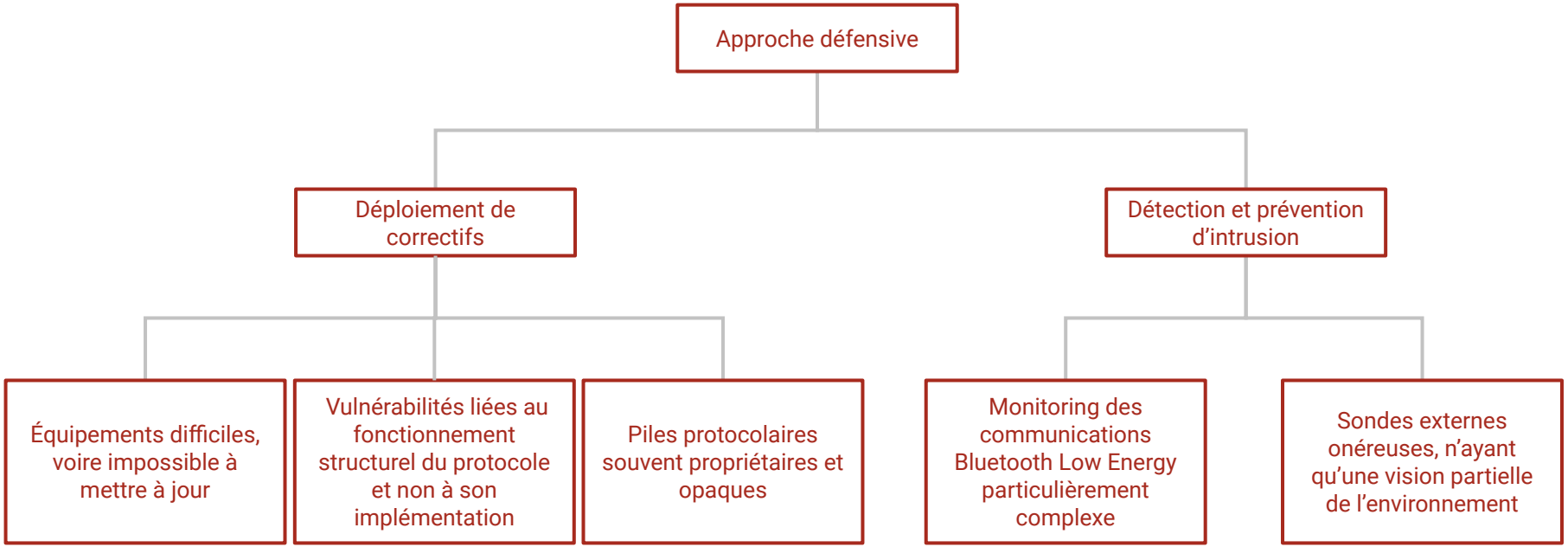
CONTEXTE: MÉCANISMES DÉFENSIFS

Mettre en place une approche défensive adaptée est particulièrement complexe:



CONTEXTE: MÉCANISMES DÉFENSIFS

Mettre en place une approche défensive adaptée est particulièrement complexe:

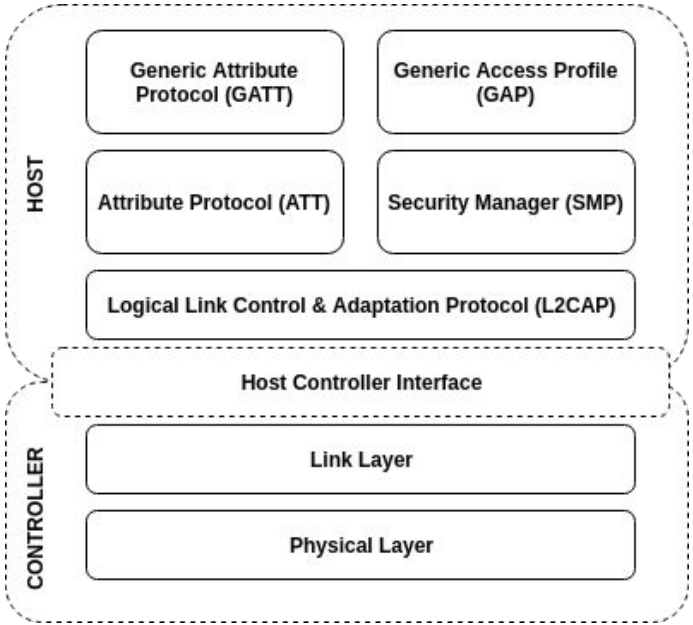


PRÉSENTATION DE L'APPROCHE

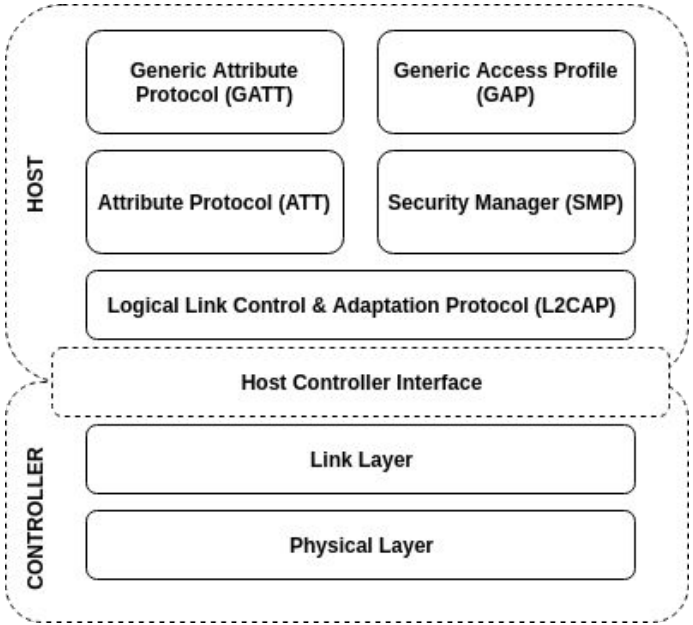
Développement **d'Oasis**, un framework de **détection d'intrusion** embarqué sur les **contrôleurs Bluetooth:**

- permet de **déporter** la détection d'intrusion **sur les noeuds eux mêmes**, résolvant les problématiques liées à la **difficulté de monitoring du protocole** et à la **perception partielle de sondes externes**,
- framework **modulaire**, permettant de développer facilement de **petits modules de détection** en langage C sans nécessiter la rétro-ingénierie des firmwares,
- implémentation sur les contrôleurs de **Broadcom** et **Cypress**, particulièrement répandus, et sur le **nRF51822** de **Nordic Semiconductors**,
- Premier pas vers le développement d'un **système de détection d'intrusion distribué et décentralisé**, particulièrement adapté aux contraintes de l'IoT.

BLUETOOTH LOW ENERGY: PILE PROTOCOLAIRE



BLUETOOTH LOW ENERGY: PILE PROTOCOLAIRE



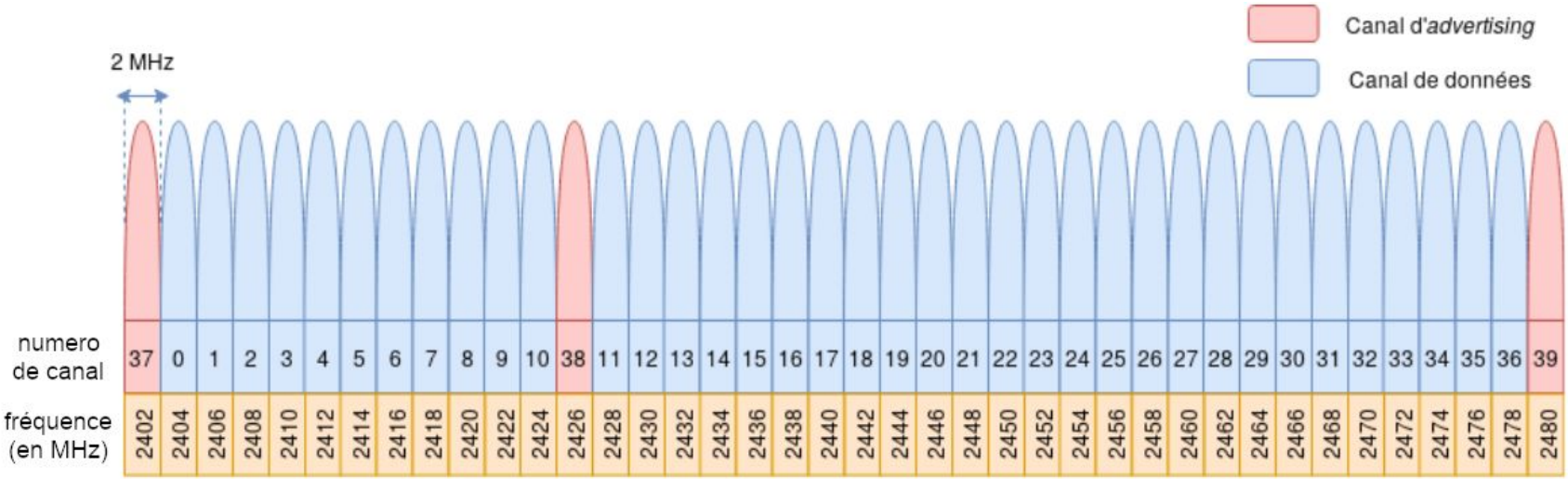
Objectif: Instrumentation du contrôleur

- Accès aux **indicateurs bas niveau** (paquets LL, RSSI, CRC, timestamps…)
- Permet la détection d'attaques visant **n'importe quelle couche**

Challenges:

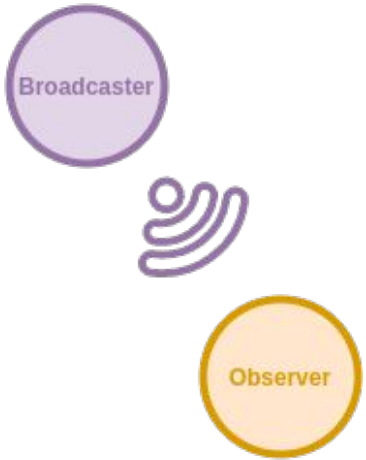
- Implémentation souvent **propriétaire** et **non documentée** (rétro-ingénierie des firmwares)
- Architectures **hétérogènes**
- Pas de mécanismes destiné à **l'ajout de code défensif**
- Fortes **contraintes temporelles**

BLUETOOTH LOW ENERGY: MODE ADVERTISING / MODE CONNECTÉ

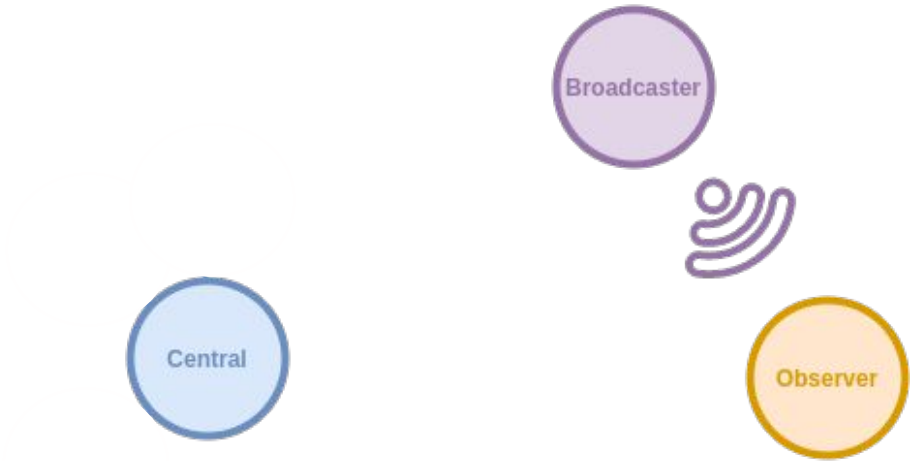


BLUETOOTH LOW ENERGY - ROLES

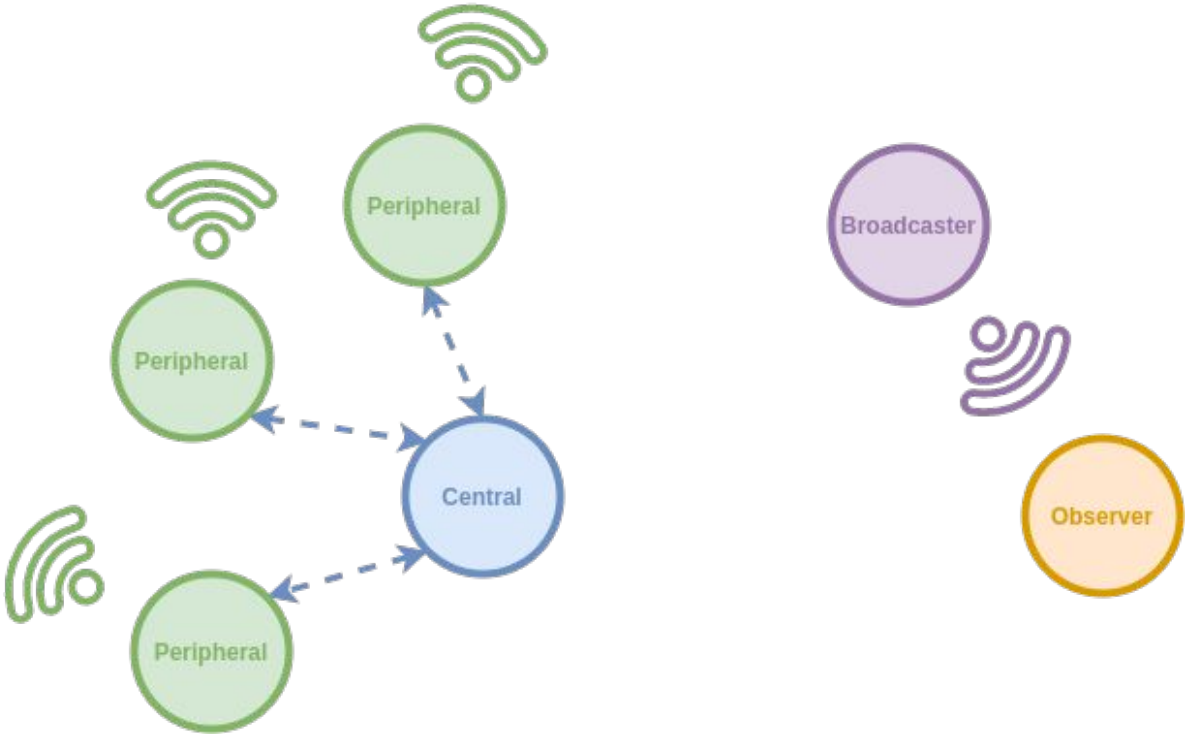
BLUETOOTH LOW ENERGY - ROLES



BLUETOOTH LOW ENERGY - ROLES

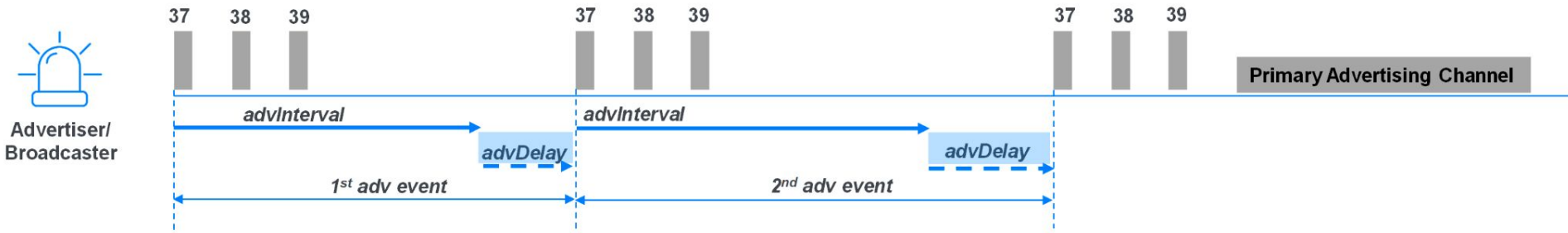


BLUETOOTH LOW ENERGY - ROLES

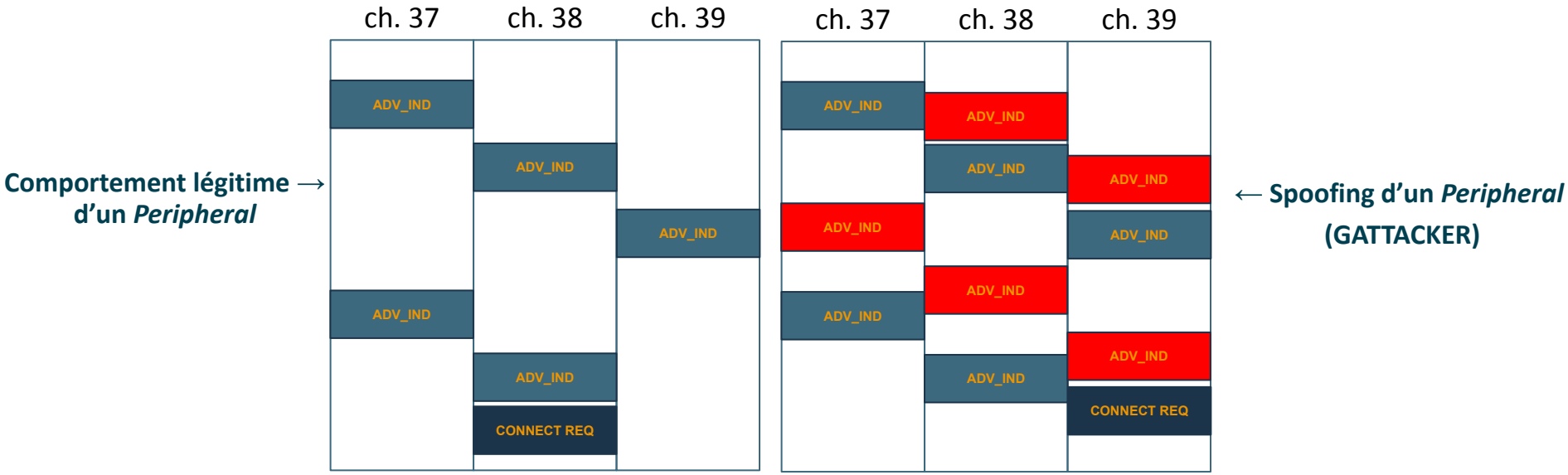


STRATÉGIES DE DÉTECTION D'ATTAQUES

OASIS
MODULE DE DÉTECTION - GATTACKER



OASIS
MODULE DE DÉTECTION - GATTACKER



Comportement légitime → d'un *Peripheral*

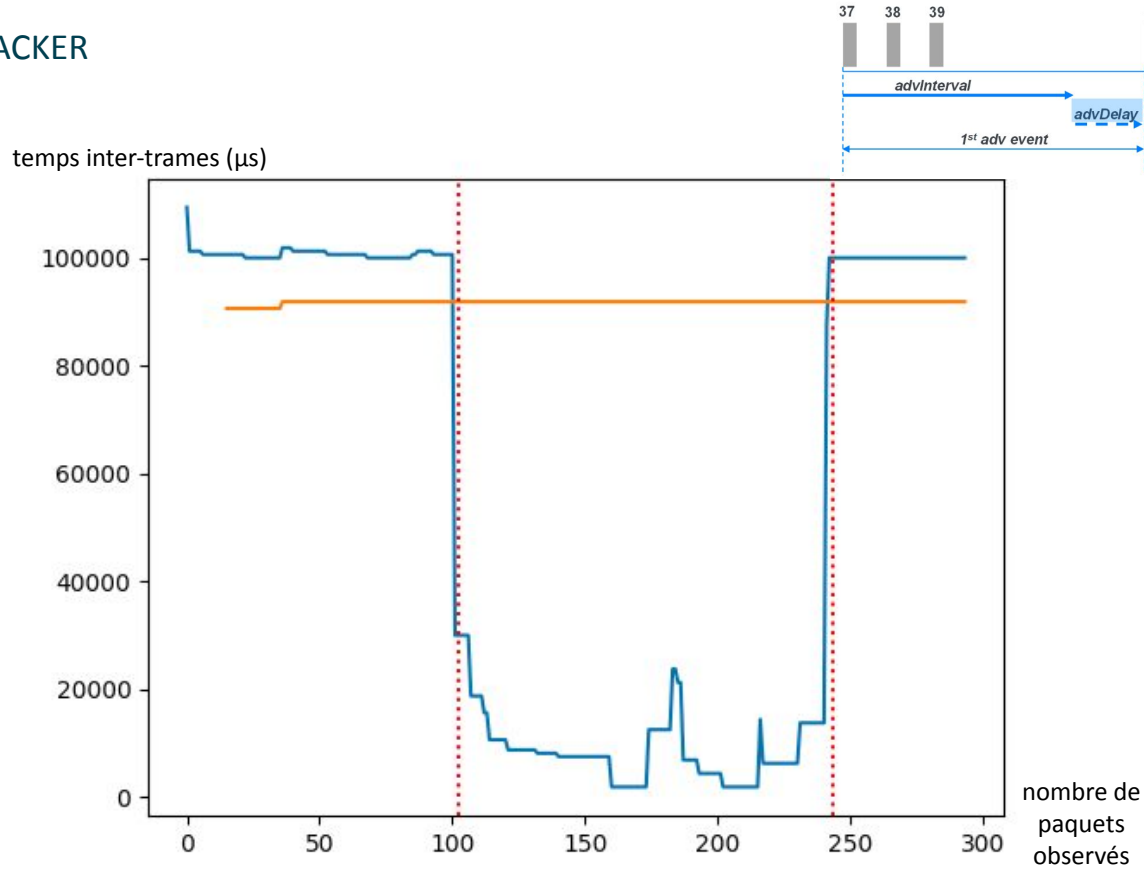
← Spoofing d'un *Peripheral* (GATTACKER)

OASIS

MODULE DE DÉTECTION - GATTACKER

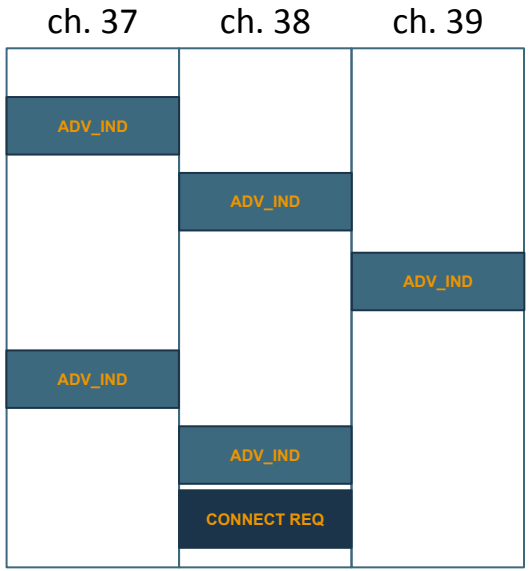
Principe: analyse en temps réel du temps entre deux paquets émis par un même émetteur. En cas d'attaque, on observe une diminution de cette métrique en raison de la superposition des paquets émis par l'émetteur malicieux avec le trafic légitime.

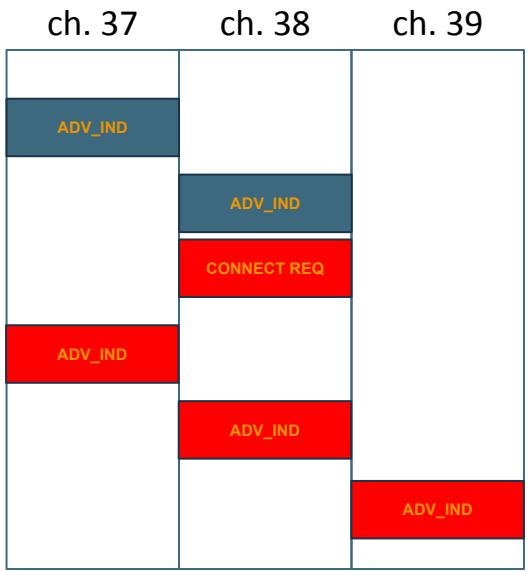
- collecte des timestamps de chaque paquet d'un même émetteur et calcul des temps inter-trames successifs,
- estimation de l'*advInterval* par le calcul du minimum dans une fenêtre glissante (courbe bleue),
- établissement d'un seuil correspondant au pire des cas légitime (courbe orange).



OASIS
MODULE DE DÉTECTION - BTLEJUICE

Comportement légitime → d'un *Peripheral*

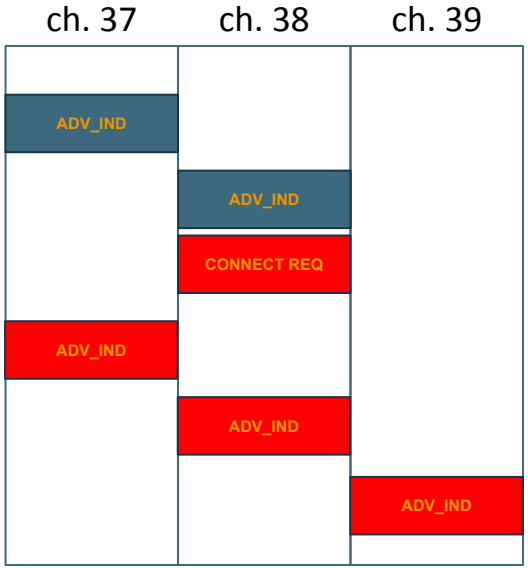




← Spoofing d'un *Peripheral* (BTLEJUICE)

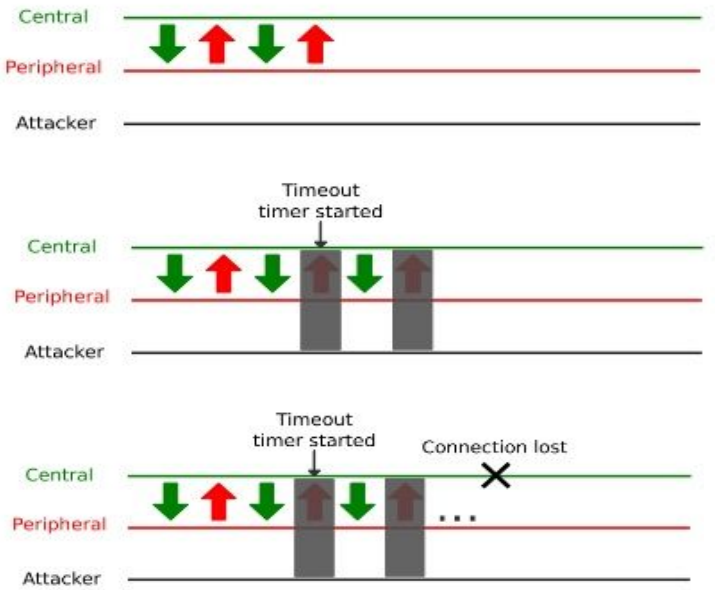
OASIS
MODULE DE DÉTECTION - BTLEJUICE

Principe: lorsque le *Peripheral* reçoit une demande de connexion, il accepte la connexion mais initie également une opération de *scan* en parallèle. L'attaque est détectée si il observe l'émission de paquet d'*advertising* utilisant son adresse BD en parallèle de la connexion.



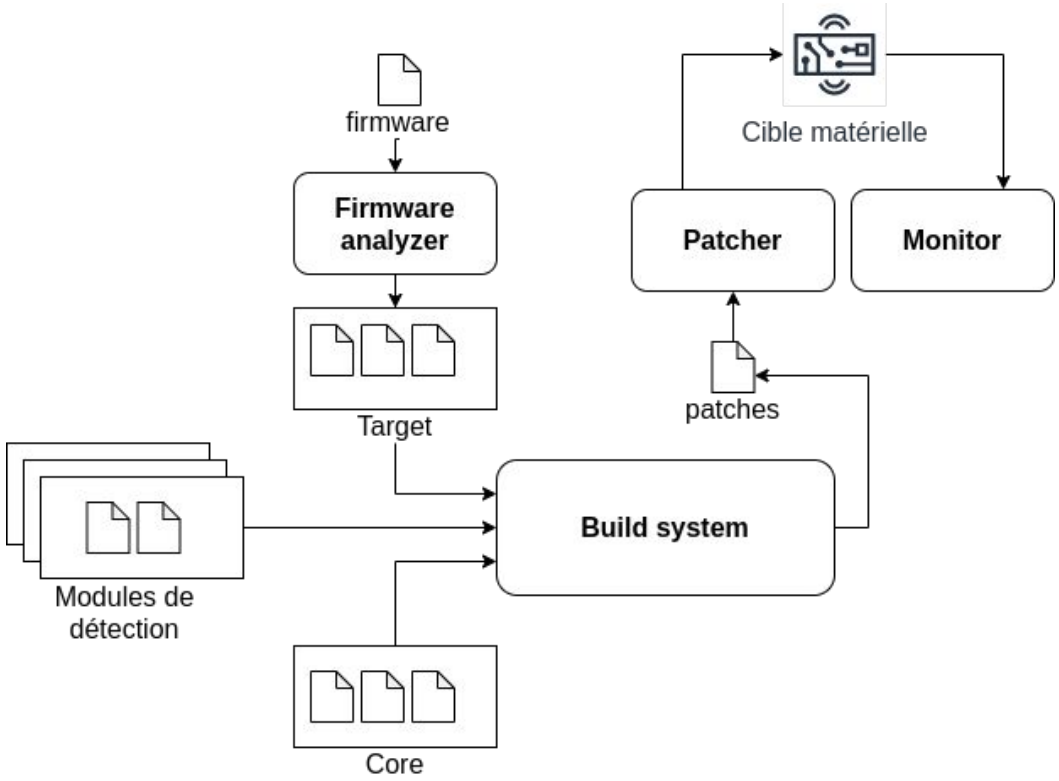
← **Spoofing d'un *Peripheral* (BTLEJUICE)**

Principe: analyse en temps réel du nombre de paquets consécutifs émis par le *Slave* dont le CRC est invalide.



CONCEPTION DU FRAMEWORK

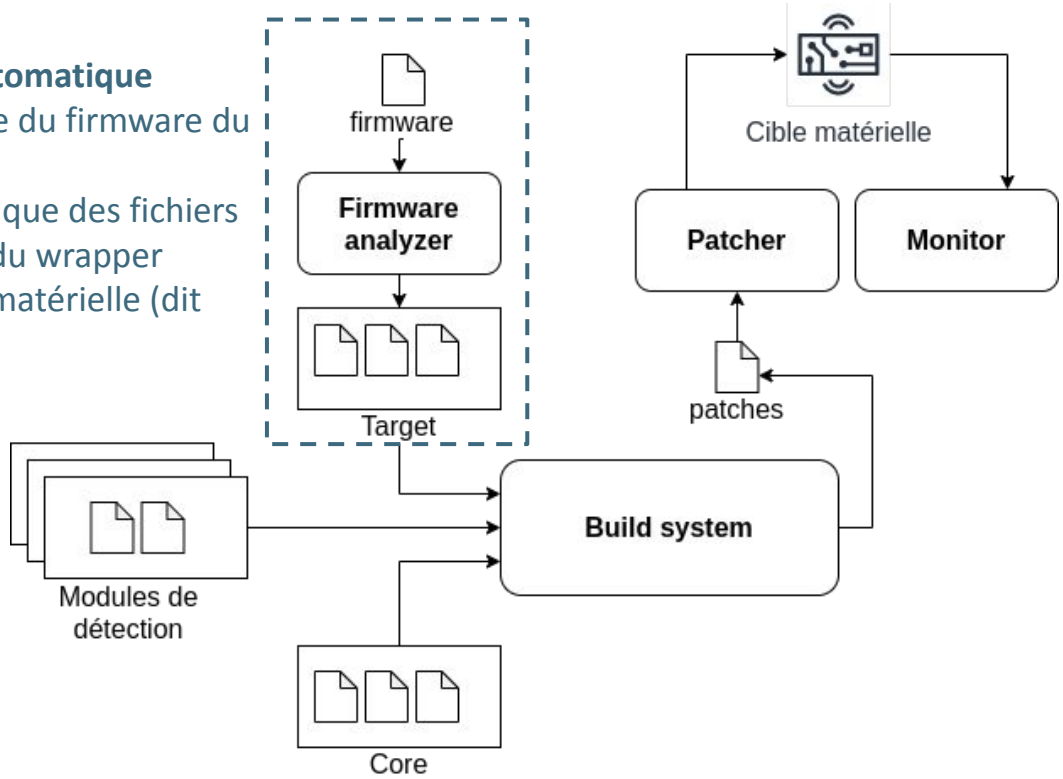
OASIS: ARCHITECTURE



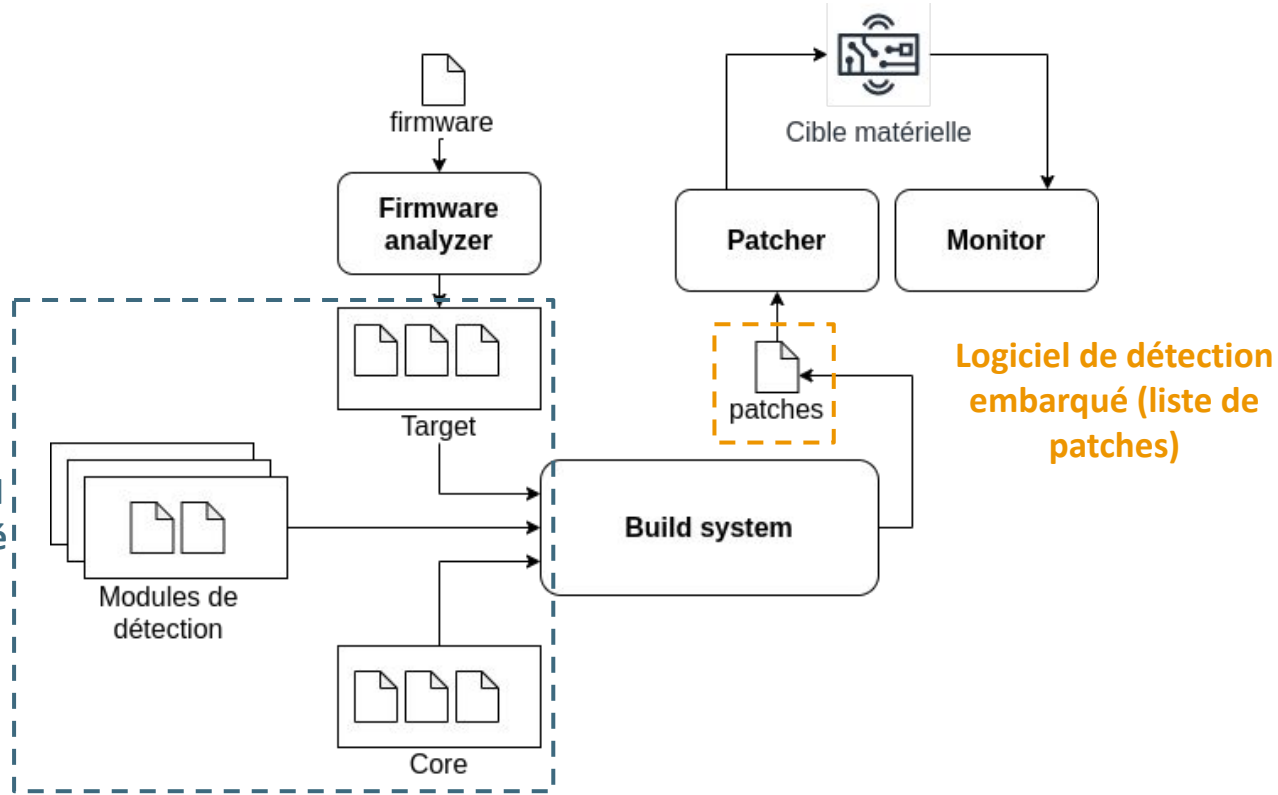
OASIS: ARCHITECTURE

Rétro-ingénierie automatique

- analyse automatique du firmware du contrôleur
- génération automatique des fichiers de configuration et du wrapper décrivant une cible matérielle (dit “target”)



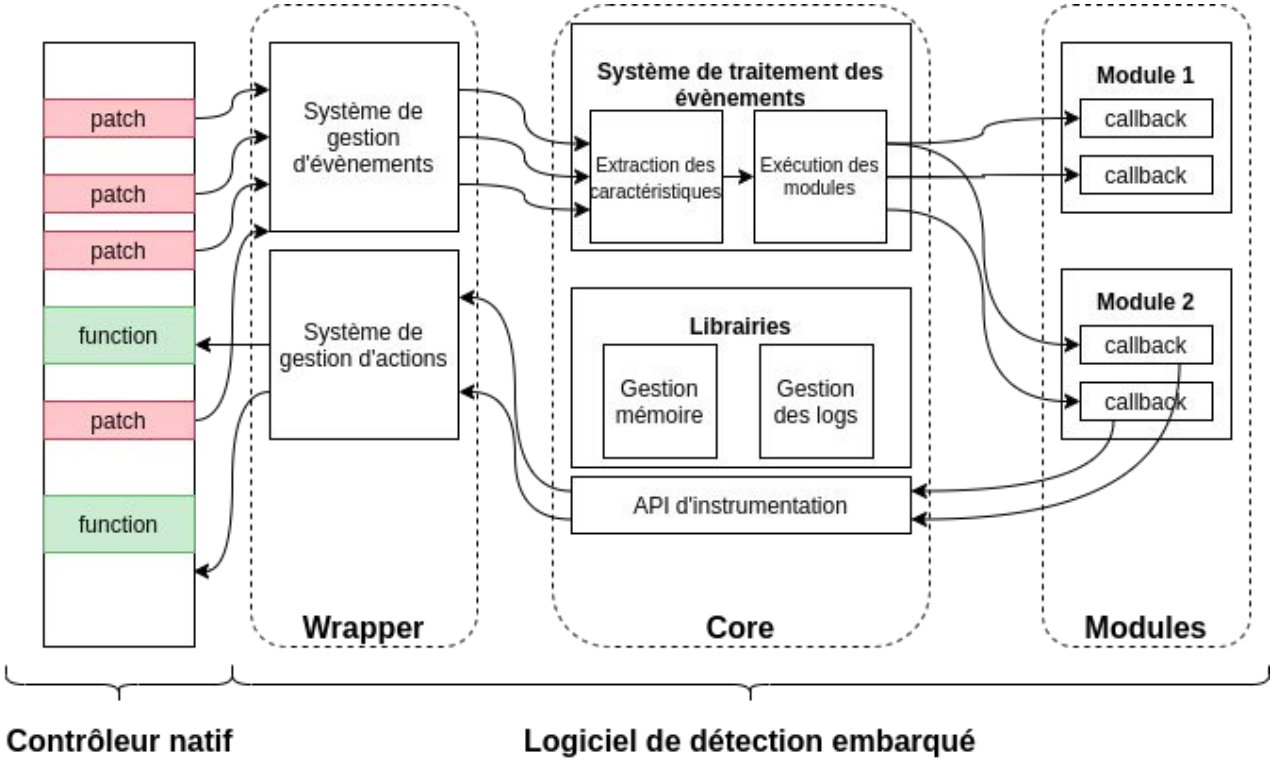
OASIS: ARCHITECTURE



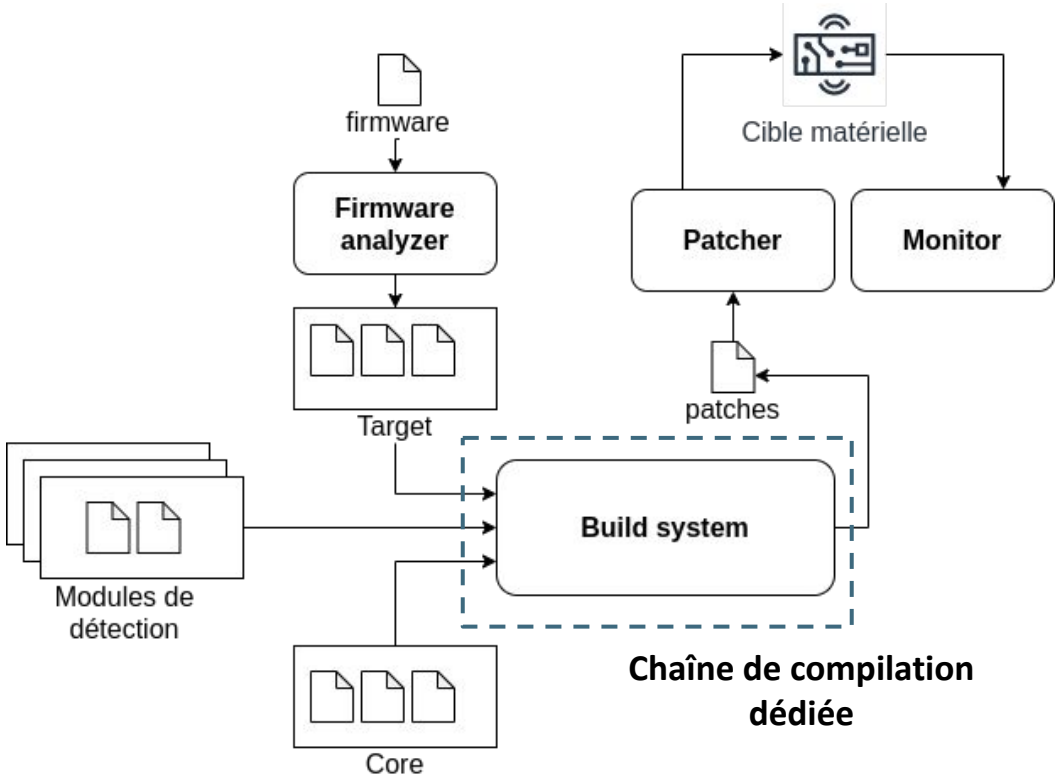
Code source du logiciel de détection embarqué

Logiciel de détection embarqué (liste de patches)

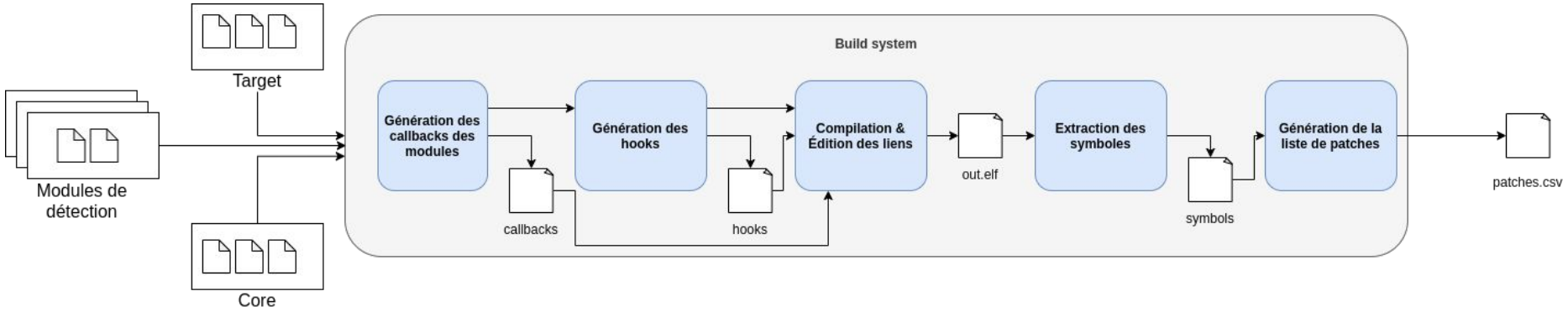
OASIS: LOGICIEL DE DÉTECTION EMBARQUÉ



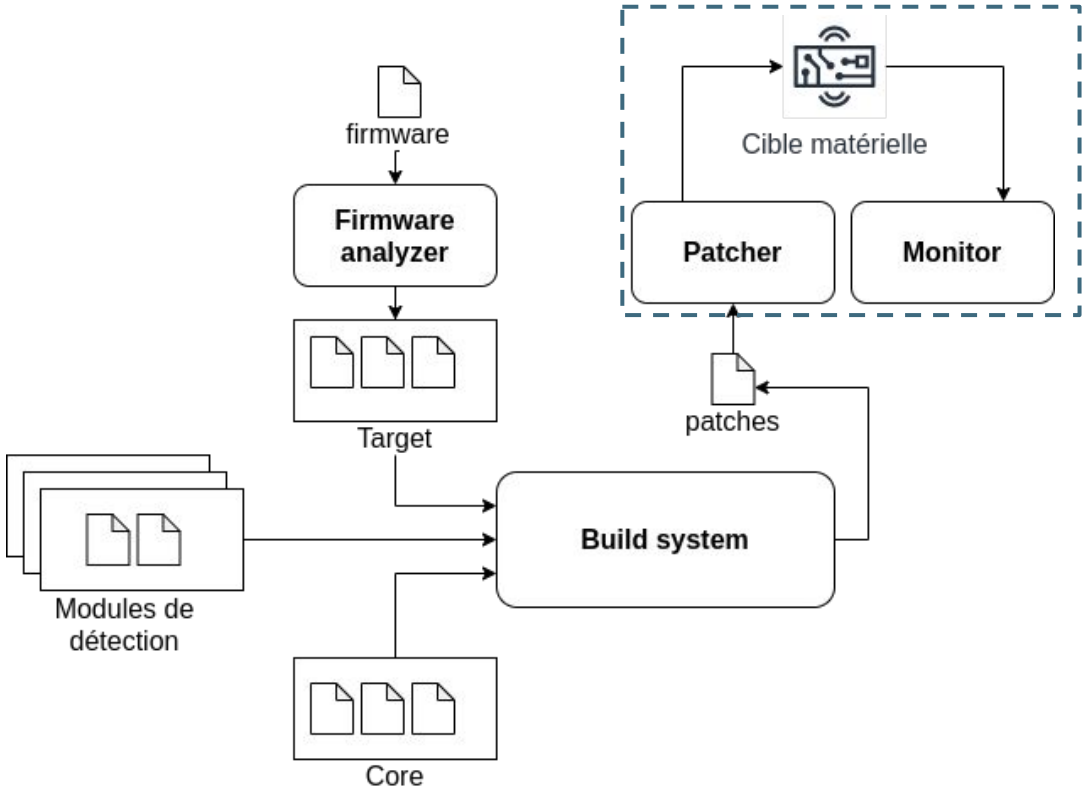
OASIS: ARCHITECTURE



OASIS: BUILD SYSTEM



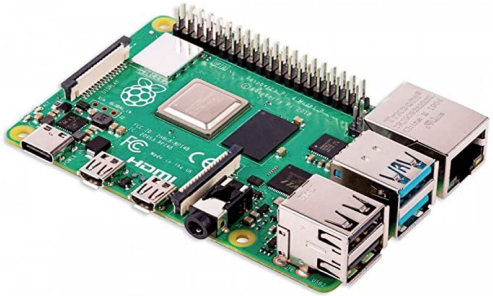
OASIS: ARCHITECTURE



Outils d'interaction avec la cible

EXPÉRIMENTATIONS

OASIS: CIBLES ÉVALUÉES

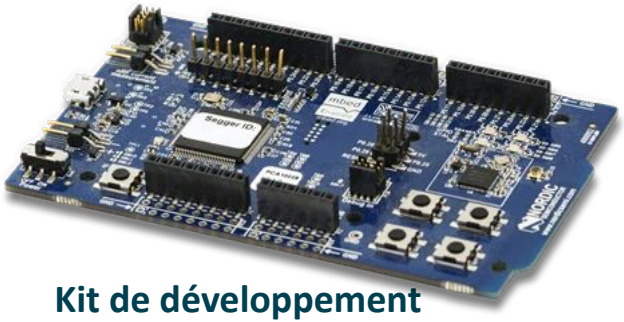


Raspberry Pi 3+/4 (BCM4345C0) [Ra]

Nexus 5 (BCM4335C0) [Ne]

Kit de développement IoT (CYW20735) [D1]

Gablys (nRF51822) [Ga]



Kit de développement (nRF51422) [D2]

OASIS: EXPÉRIMENTATIONS

01	GATTACKER	• 250 attaques, 250 périodes légitimes • Attaques lancées via 2 dongles HCI et Mirage • Équipements de type Scanner: Ra, Ne, D1, D2
02	BTLEJUICE	• 250 attaques, 250 connexions légitimes • Attaques lancées via 2 dongles HCI et Mirage • Équipements de type Peripheral: Ga, D1, D2
03	JAMMING	• 250 attaques, 250 périodes légitimes • Attaques lancées via un HackRF one et hackrf_transfer • Équipements de type Scanner: Ra, Ne, D1, D2
04	KNOB	• 250 attaques, 250 connexions légitimes • Attaques lancées via un dongle HCI et Mirage • Équipements de type Peripheral: Ga, D1, D2
05	INJECTABLE	• 100 injections, 100 paquets légitimes • Attaques lancées via un nRF52 embarquant un firmware malicieux et Mirage • Équipements de type Peripheral: Ra, D1, D2
06	BTLEJACK	• 100 conn. attaquées, 100 conn. sans attaque • Attaques lancées via un nRF51 embarquant un firmware malicieux et Mirage • Équipements de type Central: Ne, D1

OASIS: RÉSULTATS

Experiment	Target	TP	FP	TN	FN	Recall	Precision
GATTacker	*Ra*	250	0	250	0	1.0	1.0
	Ne	250	0	250	0	1.0	1.0
	D_1	250	0	250	0	1.0	1.0
	D_2	250	19	231	0	1.0	0.93
BTLEJuice	*Ga*	245	0	250	5	0.98	1.0
	D_1	239	0	250	11	0.96	1.0
	D_2	250	0	250	0	1.0	1.0
Jamming	*Ra*	238	9	241	12	0.95	0.96
	Ne	250	13	237	0	1.0	0.95
	D_1	247	13	237	3	0.99	0.95
	D_2	250	39	211	0	1.0	0.87
KNOB	*Ga*	247	0	250	3	0.99	1.0
	D_1	250	0	250	0	1.0	1.0
	D_2	249	0	250	1	0.99	1.0
InjectaBLE	*Ra*	99	0	100	1	0.99	1.0
	D_1	100	0	100	0	1.0	1.0
	D_2	94	0	100	6	0.94	1.0
BTLEJack	*Ne*	95	0	100	5	0.95	1.0
	D_1	98	0	100	2	0.98	1.0

- **Très bonnes valeurs de rappel:** stratégies de détection pertinentes pour la détection des attaques
- **Expériences menées en environnement réaliste:** représentatif d'un attaquant réel
- **Très bonnes valeurs de précision:** peu générateur de faux positifs
  - 4 expériences sans aucun faux positif
  - nombre de faux positifs légèrement plus élevé pour les expériences reposant sur le monitoring passif des advertisements (Jamming / GATTacker)
- **Comportement des différentes cibles homogènes:** l'objectif de généricité est atteint avec succès

CONCLUSION ET PERSPECTIVES

- Démontre la faisabilité d'une approche de détection embarqué au sein des contrôleurs BLE
- Développement et validation de stratégies de détection légères pour des attaques protocolaires critiques
- Framework modulaire et léger permettant d'instrumenter les contrôleurs facilement: potentiellement utilisable pour d'autres applications (fuzzing de piles protocolaires, développement embarqué, …)

Perspectives:

- **Extension de l'approche à d'autres protocoles**: Zigbee, Enhanced ShockBurst, ANT+...
- **Établir une communication sécurisée entre les noeuds de détection**: conception d'un système de détection d'intrusion collaboratif, distribué et décentralisé

Dépôt: https://github.com/RCayre/oasis

Documentation: https://homepages.laas.fr/rcayre/oasis-documentation

Merci pour votre attention !