PROGRAMME DE RECHERCHE
CYBERSÉCURITÉ

OASIS: An Intrusion Detection System Embedded in Bluetooth Low Energy Controllers

Superviz Workshop - December 16th, 2024

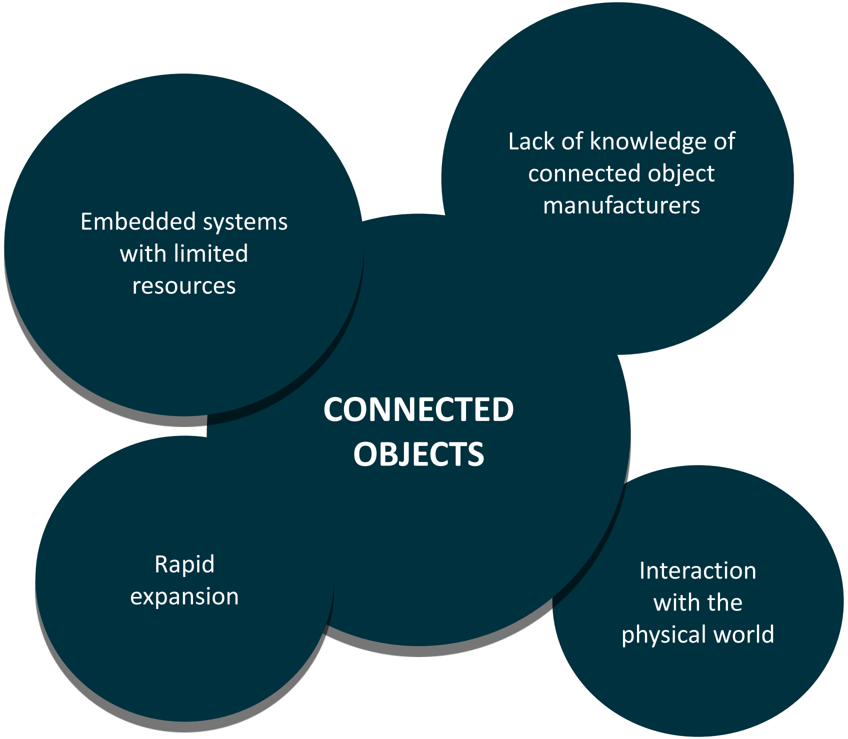
Romain CAYRE - Vincent Nicomette - Guillaume Auriol - Mohamed Kaâniche - Aurélien Francillon

AGENDA

- Introduction (context & prerequisites)
- Embedded software & framework design
- Detection modules
- Experiments: detection & performance
- Conclusion

INTRODUCTION

CONTEXT



Embedded systems with limited resources
Lack of knowledge of connected object manufacturers
CONNECTED OBJECTS
Rapid expansion
Interaction with the physical world

CONTEXT

CONNECTED OBJECTS

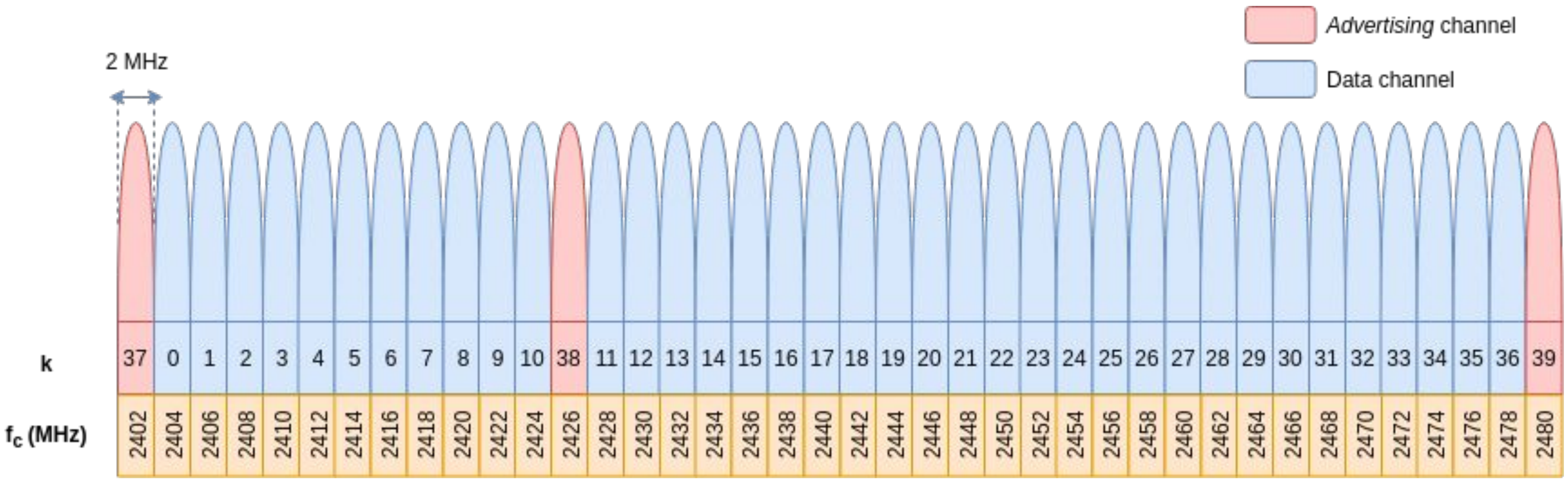
- Embedded systems with limited resources
- Lack of knowledge of connected object manufacturers
- Rapid expansion
- Interaction with the physical world

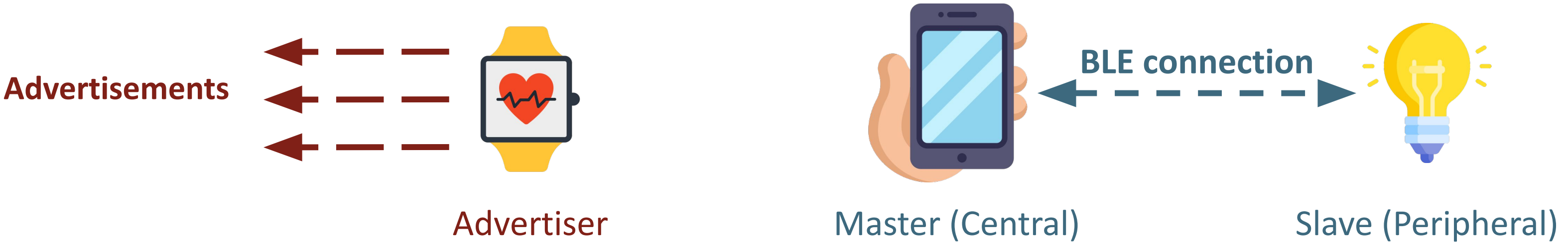
WIRELESS COMMUNICATION PROTOCOLS

- Heterogeneous technologies
- Peer to peer communications
- Mobile equipments
- Co-existence in the same environments

- **Lightweight variant of Bluetooth BR/EDR,** introduced in version 4.0 of the specification,
- Optimized for **low energy consumption,**
- **Low complexity** protocol stacks**,**
- **Deployed in billions of devices** (smartphones, laptops, smart devices, …)

BLUETOOTH LOW ENERGY





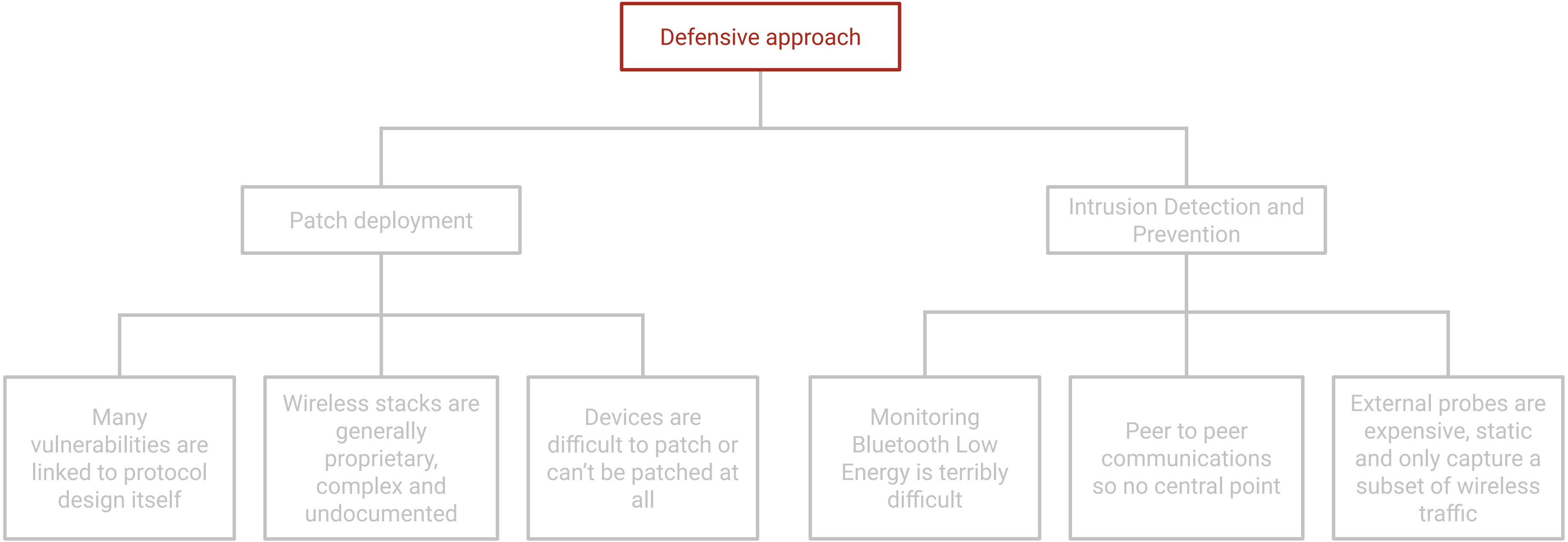
OVERVIEW OF BLUETOOTH LOW ENERGY SECURITY

In the recent years, **many critical vulnerabilities** targeting Bluetooth Low Energy have been found and released publicly (InjectaBLE, Gattacker/BTLEJuice, BTLEJack, etc).

1. **EAVESDROPPING**
   - With low energy comes low security - M. Ryan (2013)
2. **MAN-IN-THE-MIDDLE**
   - BTLEJuice - D. Cauquil (2016)
   - GATTacker - S. Jasek (2016)
3. **DENIAL OF SERVICE**
   - On practical Selective Jamming of BLE Advertising - S. Bräüer (2016)
   - BTLEJack - D. Cauquil (2018)
4. **HIJACKING**
   - BTLEJack - D. Cauquil (2018)
5. **ATTACKS ON PAIRING / CRYPTO**
   - With Low energy comes low security - M. Ryan (2013)
   - KNOB - D.Antonioli (2019)

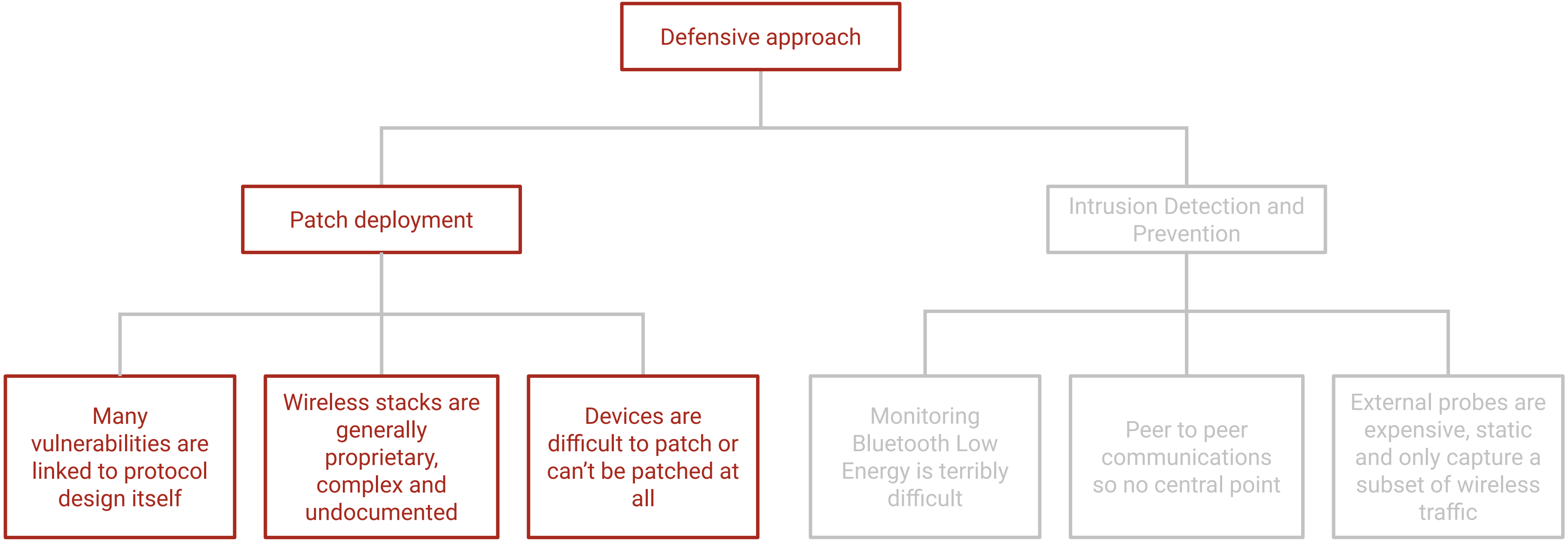
DEFENSIVE MECHANISMS

Building a relevant defensive approach is very complex:



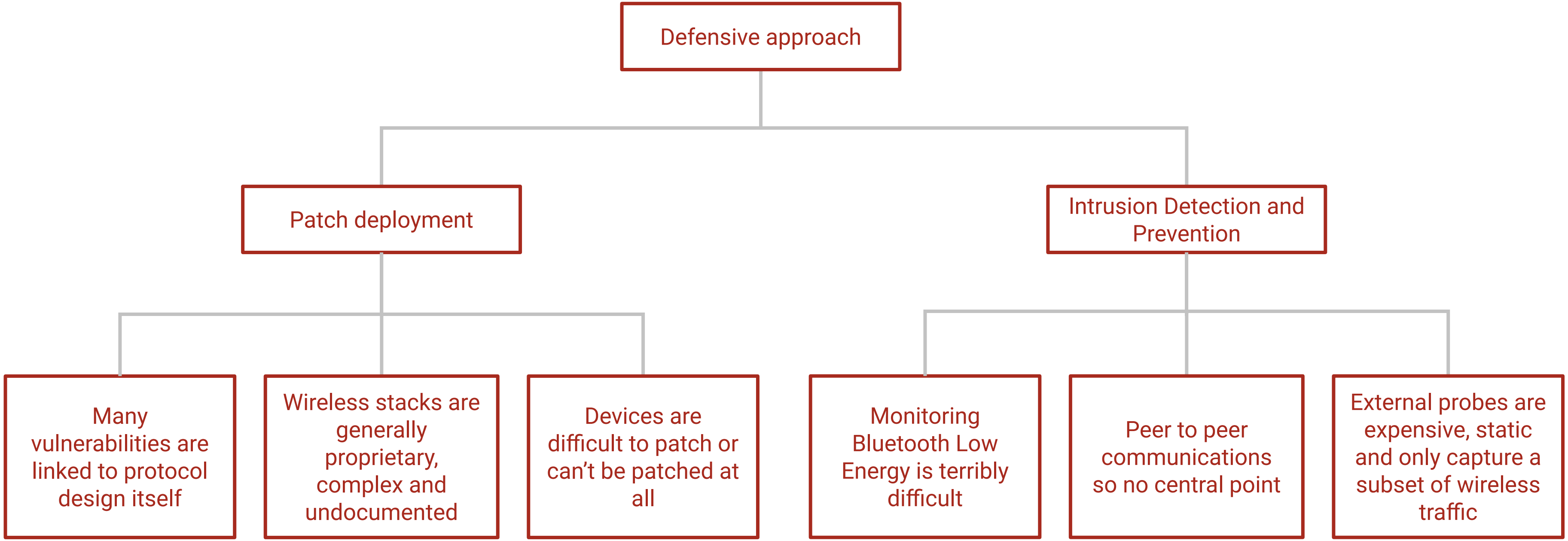
DEFENSIVE MECHANISMS

Building a relevant defensive approach is very complex:



DEFENSIVE MECHANISMS

Building a relevant defensive approach is very complex:



STATE OF THE ART

		BlueShield [36]	MARC [39]	HEKA [23]	I.S. IT [32]	MiTM ML [21]
Online Detection		✔	✔	✘	✔	✘
Extensible		✘	✘	✘	✘	✘
IDS Mobility		✘	✘	✘	✘	✘
Scope		Stationary Networks	Medical	Medical	Beacon Tags	Generic
Detected Attacks	BTLEJuice	✔	✘	✔	✘	✔
	GATTacker	✔	✔	✘	✘	✔
	InjectaBLE	✘	✘	✘	✘	✘
	BTLEJack	✘	✘	✘	✘	✘
	KNOB	✘	✘	✘	✘	✘
	Device DoS	✘	✘	✔	✘	✘
	Replay	✘	✘	✔	✘	✘
	False Data injection	✘	✘	✔	✘	✘
	Physical Intrusion	✘	✘	✘	✔	✘
Modes		Adv.	Adv.	Conn.	Adv.	Adv. / Conn.
Features collection		Static Probe	Static Probe	Manual	Static Probe	Manual
Feat.	**Advertising**	4/4	3/4	0/4	0/4	0/4
	Connection	0/4	0/4	1/4	0/4	0/4
	Metadata	3/7	1/7	0/7	1/7	3/7
Implementation available		✔	✘	✘	✘	✘

- **Few papers** in Intrusion Detection for Bluetooth Low Energy
- Existing approaches are:
  - based on **external probes** and **inherit the limits of BLE sniffers** (or ignore the problem)
  - generally focused on **spoofing attacks** targeting the **advertisement phase**
  - **not reproducible** at all or **based on deprecated tools** and **libraries** (Ubertooth One, python2)

APPROACH OVERVIEW

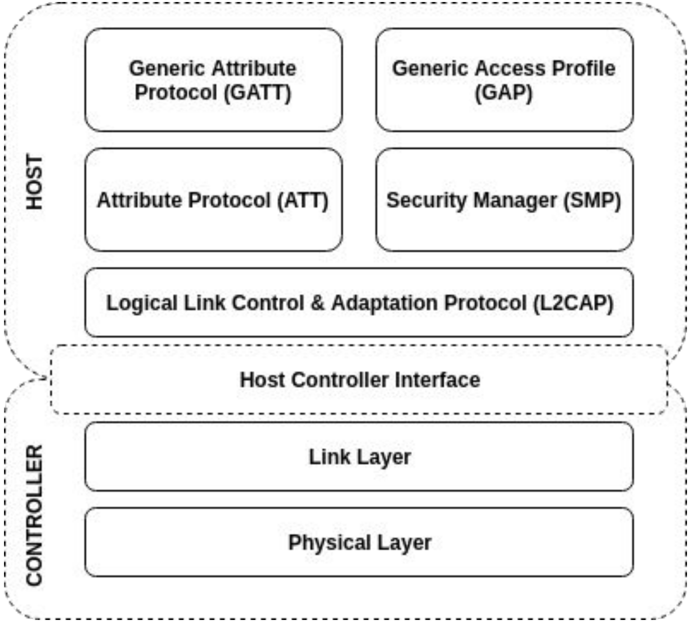
- Deporting intrusion detection **to the nodes themselves**, solving issues linked to the difficulty of **monitoring the protocol** and the **partial perception of external probes.**

- **OASIS**: modular framework, enabling easy development of **small detection modules in C language** without the need to reverse-engineer controller firmwares.

- Implementation on massively deployed controllers from **Broadcom**, **Cypress** and **Nordic SemiConductors**.

- A first step towards the development of a **distributed**, **decentralized intrusion detection system**, particularly suited to IoT constraints.

APPROACH OVERVIEW



Objective: Controller instrumentation

- Access to Link Layer traffic
- Access to low-level indicators (RSSI, CRC, timestamps, ...)
- Allows detection of attacks targeting upper layers
- Strategic position for intrusion prevention

Challenges:

- Proprietary protocol stacks implementations (requires reverse engineering),
- Heterogeneous architectures,
- No mechanism to add defensive code,
- Strong timing constraints.

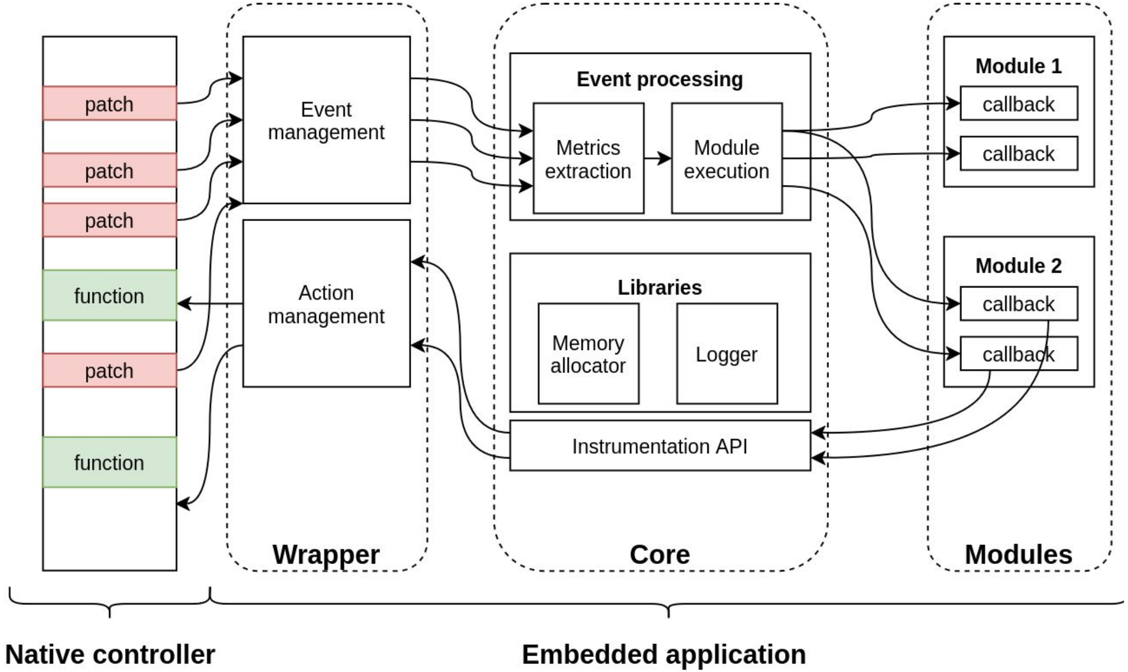
FRAMEWORK & EMBEDDED SOFTWARE

MAIN GUIDELINES

- **Genericity:** the framework allows the development of modules independent of the controllers architectures

- **Modularity:** the IDS is composed of independent modules that can be adapted to various contexts

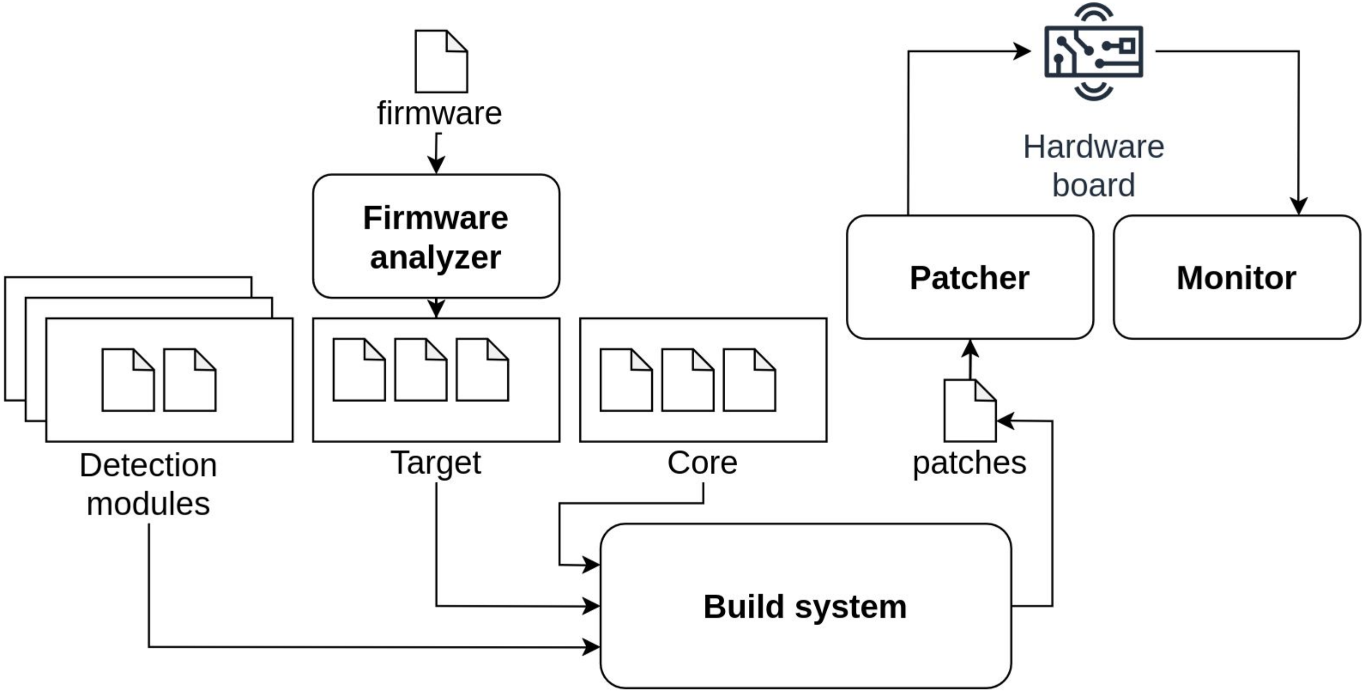
- **User-friendly:** a developer can implement a new modules without deep understanding of the underlying controller architecture



Three main components:

- **A target-specific wrapper,** instrumenting strategic code and structures,
- **A generic core**, extracting various detection features and metrics,
- **A set of defensive modules,** implementing lightweight detection heuristics.

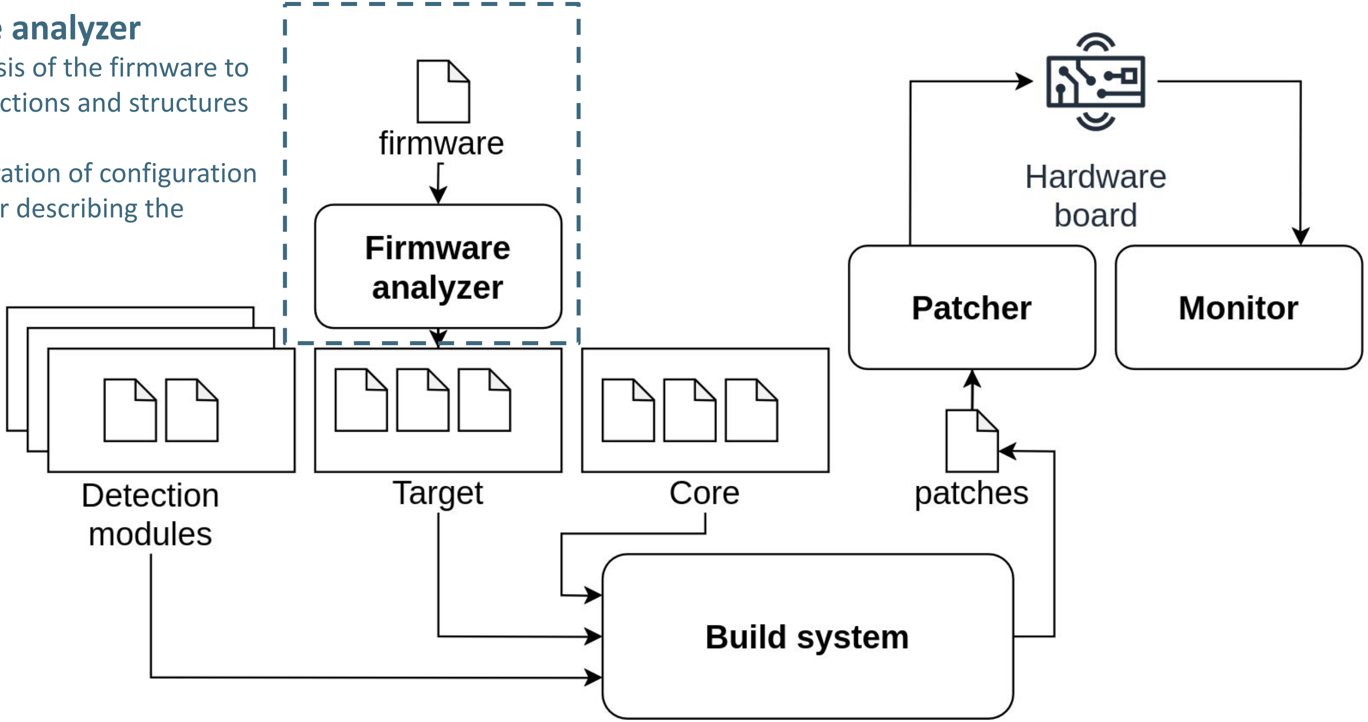
FRAMEWORK ARCHITECTURE



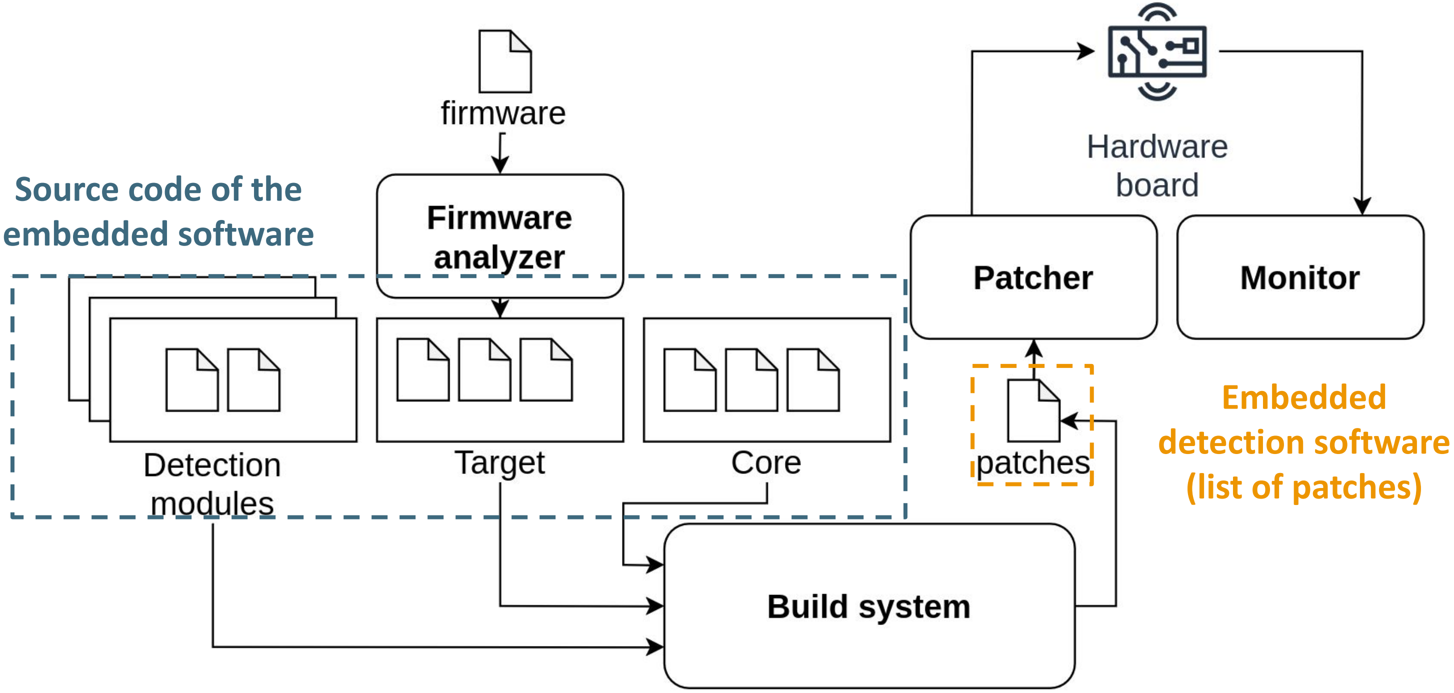
FRAMEWORK ARCHITECTURE

Firmware analyzer

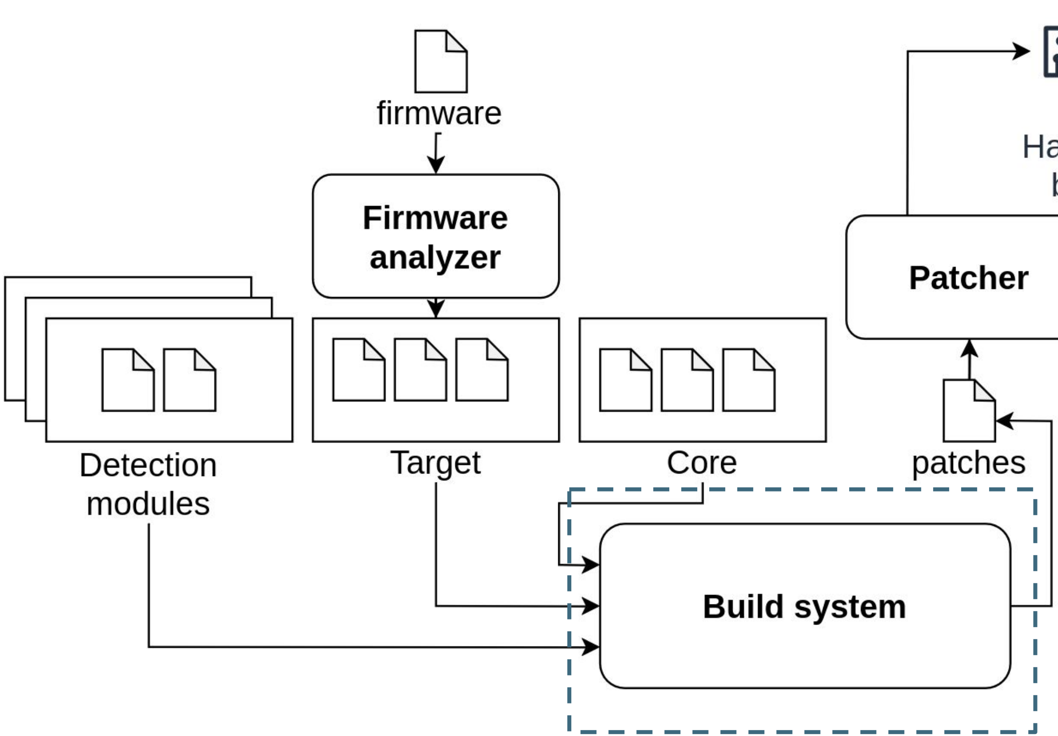
- Automatic analysis of the firmware to find relevant functions and structures
- Automatic generation of configuration files and wrapper describing the « target »



FRAMEWORK ARCHITECTURE

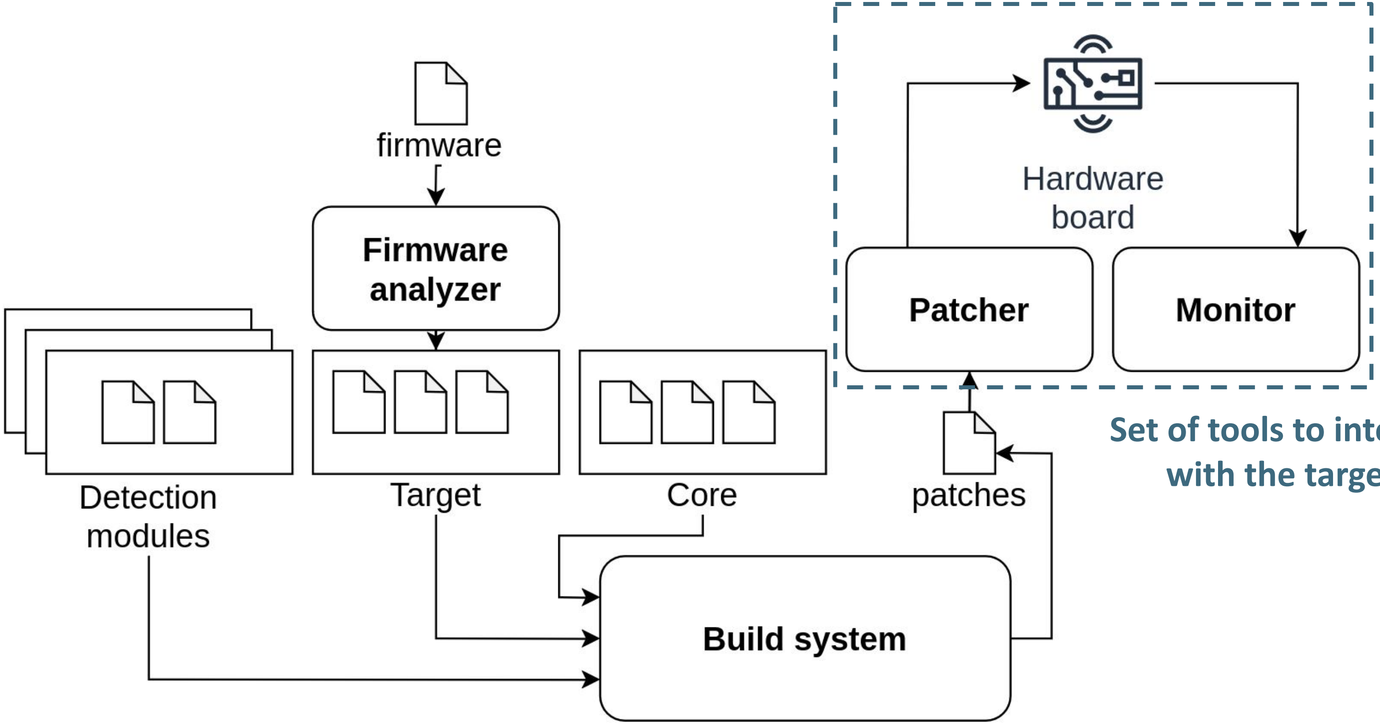


FRAMEWORK ARCHITECTURE



Dedicated build system (hooks generation, compilation, symbols extraction)

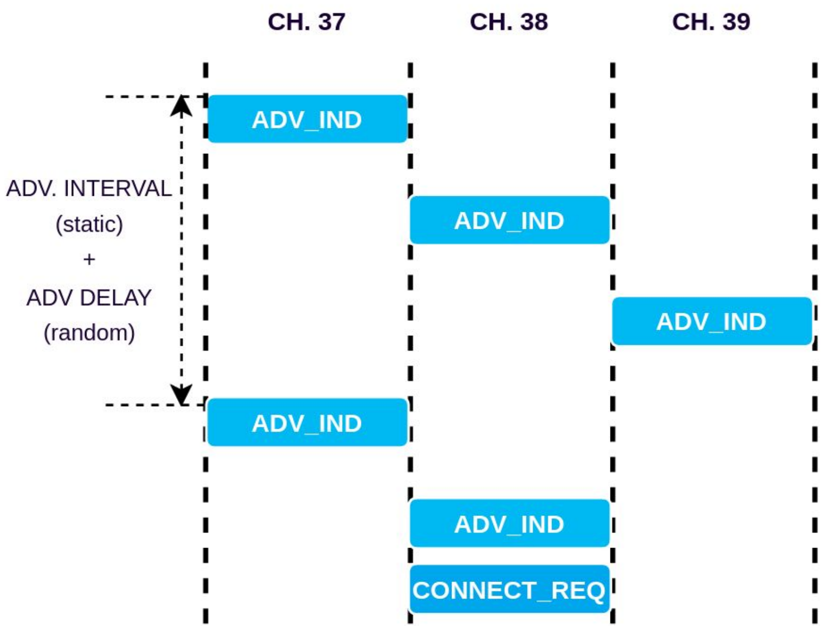
FRAMEWORK ARCHITECTURE



Set of tools to interact with the target

DETECTION MODULES

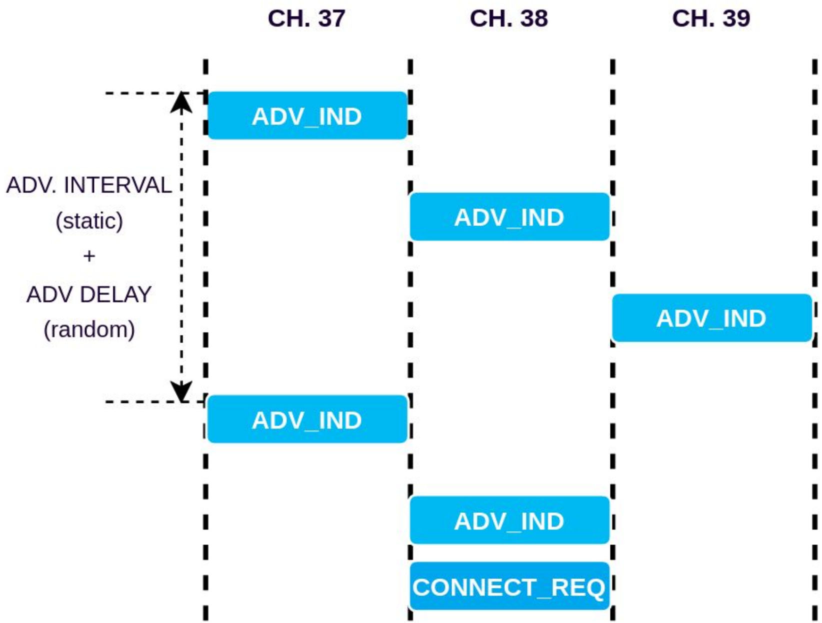
GATTACKER DETECTION



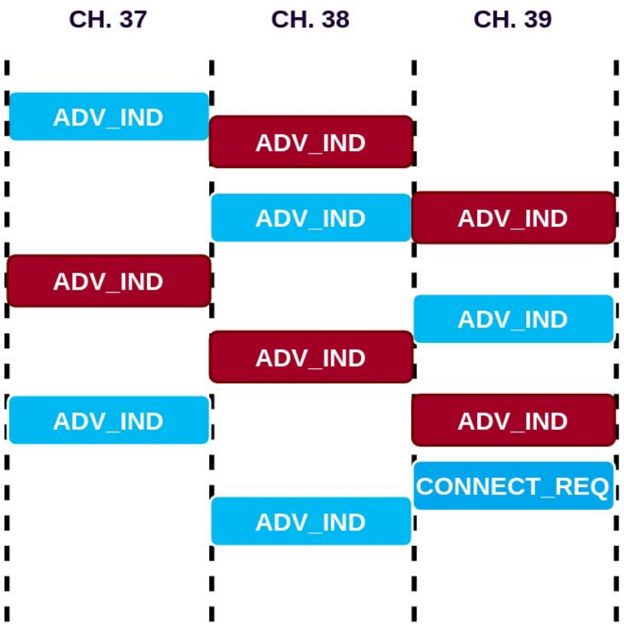
LEGITIMATE PERIPHERAL
ADVERTISING PHASE

PERIPHERAL SPOOFING
GATTACKER ATTACK

GATTACKER DETECTION



LEGITIMATE PERIPHERAL
ADVERTISING PHASE



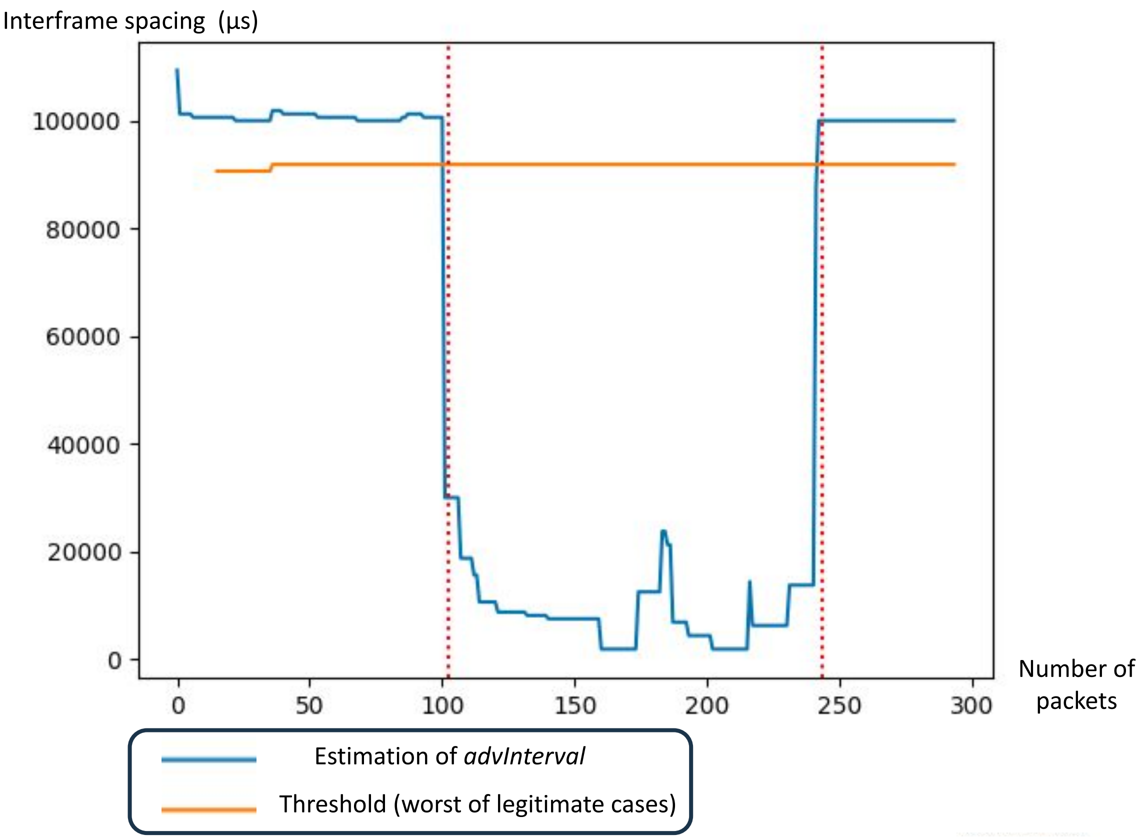
PERIPHERAL SPOOFING
GATTACKER ATTACK

Principle: real-time analysis of the time between two packets sent by the same advertiser

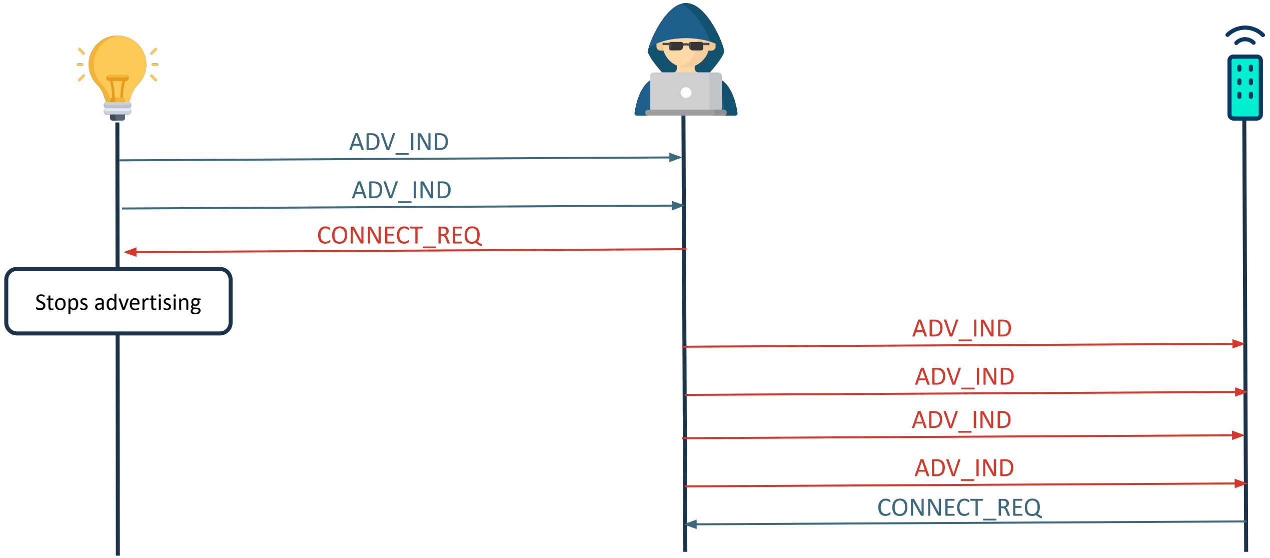
- Computation of the **duration between two consecutive packets** with the same address
- Estimation of the **advertising interval** (minimum in a sliding window)
- Computation of a **threshold** based on the **worst legitimate case**

When an attack occurs:

- **Superposition** of **malicious and legitimate trafic** → the metric significantly **decreases**
- An alert is reported if the **metric is lower** than the threshold



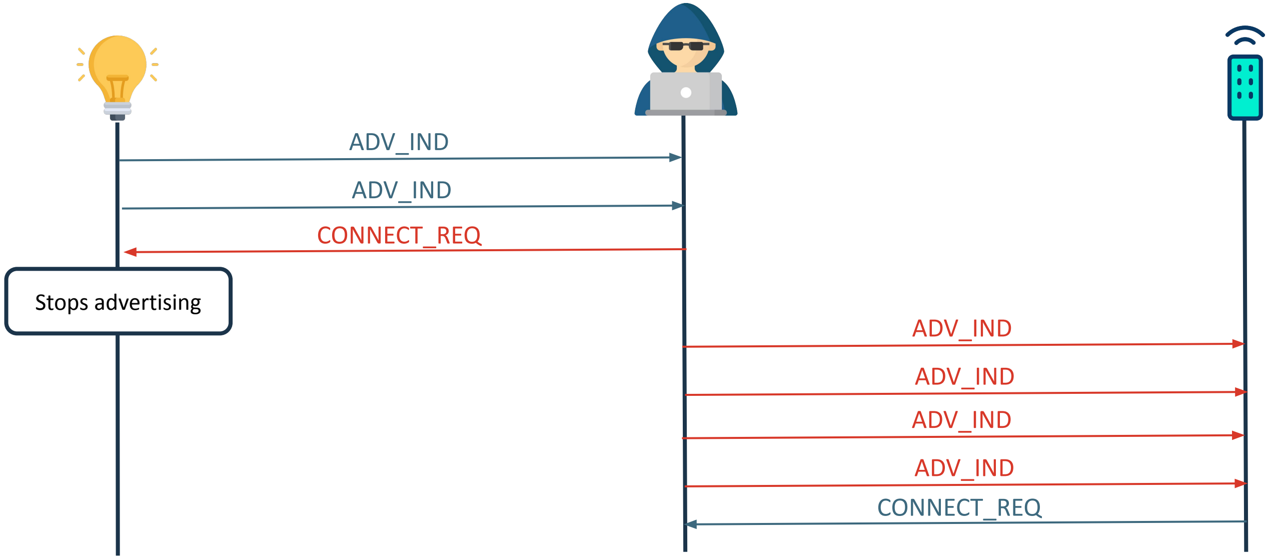
BTLEJUICE DETECTION



LAAS CNRS

BTLEJUICE DETECTION

EURECOM Sophia Antipolis



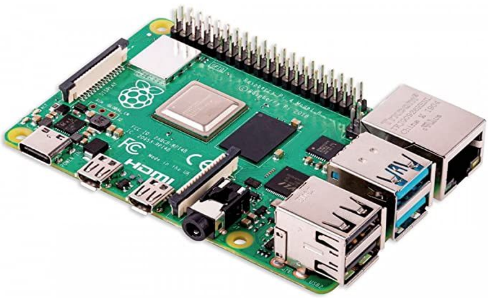
Principle: when a Peripheral accepts a connection, it initiates a scan operation and collects advertising packets.

If an advertisement with the same address is received, a spoofer is detected and an alert is raised.

Concrete example of what instrumenting the controller allow: trigger a scan operation.

EVALUATION

EVALUATED TARGETS



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

Nexus 5 (BCM4335C0) [Ne]

IoT Development Kit (CYW20735) [D1]

Gablys (nRF51822) [Ga]

IoT Development Kit (nRF51422) [D2]

DETECTION EXPERIMENTS

01	GATTACKER	• 250 attacks, 250 periods of legitimate traffic • Attacks performed using Mirage framework (HCI) • Eval. of devices supporting Scan role: Ra, Ne, D1, D2
02	BTLEJUICE	• 250 attacks, 250 periods of legitimate traffic • Attacks performed using Mirage framework (HCI) • Eval. of devices supporting Peripheral role: Ga, D1, D2
03	KNOB	• 250 attacks, 250 periods of legitimate traffic • Attacks performed using Mirage framework (HCI) • Eval. of devices supporting Peripheral role: Ga, D1, D2
04	INJECTABLE	• 100 injections, 100 legitimate packets • Attacks performed using Mirage framework (nRF52) Eval. of devices supporting Peripheral role: Ga, D1, D2
05	BTLEJACK	• 100 attacked connections, 100 legitimate connections • Attacks performed using BTLEJack firmware (nRF51) • Eval. of devices supporting Central role: Ne, D1

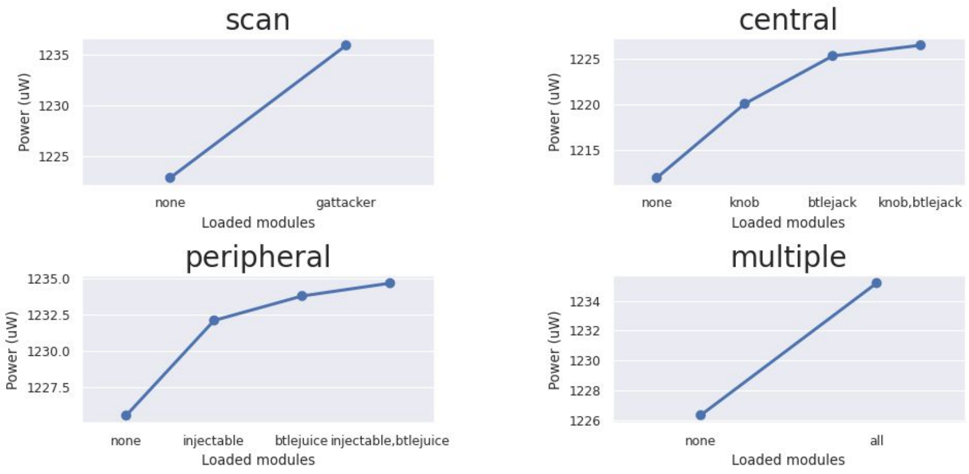
DETECTION EXPERIMENTS

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
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

- **Good recall values:** our detection heuristics successfully detect attacks
- **Experiments performed in realistic conditions:** representative of a real attacker
- **Good precision values:** low number of false positives
  - 4 experiments without any false positive
  - number of false positive slightly higher when the experiment involves advertising packets - more noisy environment (GATTacker)
- **Homogeneous behaviour of targets:** Genericity objective seems to be achieved

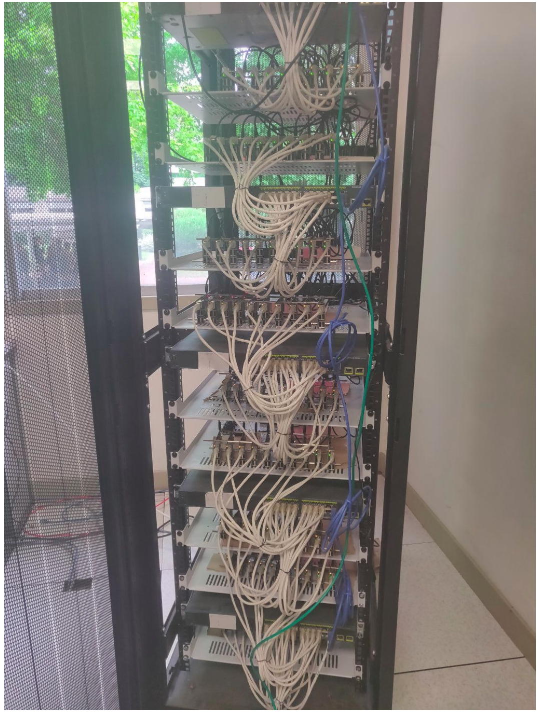
POWER CONSUMPTION EVALUATION - FINE GRAINED ANALYSIS

Profile	Supported modules	Benchmark action
Scanner (P_S)	GATTacker	running a scan
Peripheral (P_P)	InjectaBLE, KNOB, BTLEJuice	accepting connection
Central (P_C)	BTLEJack, KNOB	initiating connection
Multiple (P_M)	all	alternating scan & connections



- **Evaluation of the contribution of each module** (nRF52-DK with Zephyr + Nordic Semiconductor Power Profiler Kit).
- For each profile, we collected **4 minutes long traces** under various configurations (with / without OASIS, running one or a combination of modules).
- Increase between 0.54% (KNOB) and 1.11% (GATTacker):
  - **Low** but **measurable impact,**
  - Results consistent with the **number of modules** and their respective **complexity,**
  - **Marginal cost** of embedding **multiple modules** instead of the **most costly ones.**

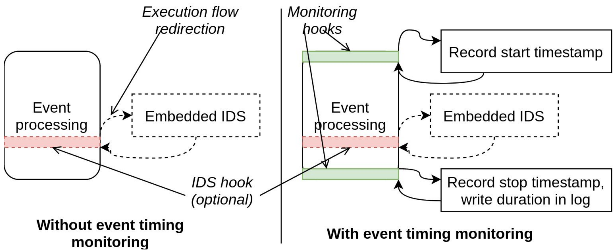
Evaluation of impact in a realistic network of devices (100 Raspberry Pi 3B+)

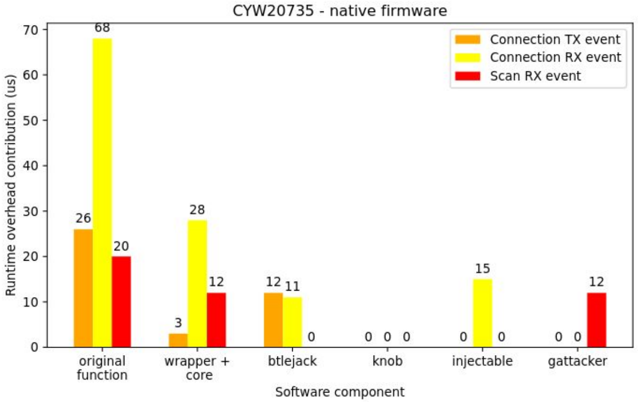


- **144 rounds of experiments of 10 minutes each,** with random connection and communication.
- **For every round, half of the devices** act as **centrals** (initiating scan & connections) and **half** acts as **peripherals** (transmitting advertisements and accepting connections).
- We alternate rounds **with** and **without the embedded IDS and monitored the power consumption of the bay.**
- **Low but measurable effect (0.51% increase):**
  - Mean power consumption **with IDS**: 238.78W (standard deviation of 2.71 %)
  - Mean power consumption **without IDS**: 237.56W (standard deviation of 2.45 %)

EXECUTION TIME EVALUATION

- Analysis on development boards **from two manufacturers (CYW20735 & nRF52-DK),**
- **Lightweight instrumentation to measure execution time with microsecond accuracy,**
- 2 minutes benchmarks on the profiles **under various conditions (without** and **with OASIS and different combinations of modules),**
- In the worst case (CYW20735 with all modules loaded), OASIS introduces an **overhead of 54µs,** leading to 122µs in total for **packet reception processing (< 150µs),**
- **“Naive” implementation:** most processing could be deferred after the packet response.





LAAS CNRS

EURECOM Sophia Antipolis

MEMORY ANALYSIS

- Focus on **static memory** (configurable dynamic memory upper limit)
- **Overall static memory** between **4291 (Nexus 5)** and **6305 bytes (nRF51)**
  - Difference related to wrapper complexity + architecture in use
  - **Static memory consumption between 48 (KNOB) and 500 bytes (InjectaBLE)**
- Could be reduced even more by **fine-grained dependencies management** or **more aggressive compiler optimizations.**

Target \ Component		total (all)	wrapper	core	injectable	btlejack	btlejuice	gattacker	knob
nRF51 SoftDevice (peripheral)	code	5278	1266	2708	496	256	124	380	48
	data	1027	587	427	4	4	1	4	0
Raspberry Pi 3	code	3860	730	1902	432	236	124	384	52
	data	477	41	423	4	4	1	4	0
Nexus 5	code	3798	668	1902	432	236	124	384	52
	data	493	41	439	4	4	1	4	0
CYW20735	code	3904	774	1902	432	236	124	384	52
	data	484	41	430	4	4	1	4	0
nRF52 Zephyr (hci_uart)	code	3886	692	1958	432	236	124	392	52
	data	457	21	423	4	4	1	4	0

CONCLUSION

CONCLUSION

- Show the feasibility of an **intrusion detection approach** embedded in **BLE controllers:**
  - Focus on making an **embedded approach practical for detection low level attacks,**
  - Address the **concrete challenges** related to **current state of BLE deployment: instrumentation of proprietary controllers & performance.**

- **Modular & lightweight framework** enabling **controllers instrumentation**: potentially usable for other applications (protocol stack fuzzing, embedded development, etc.).

- Ongoing work with **Paul Olivier (LAAS-CNRS) to explore an hybrid approach (Host + Controller) based on an open-source stack (Zephyr)** to detect more complex attacks & explore prevention techniques.

- **First step towards a decentralized / distributed IDS approach (secure cooperation between devices).**

Repository (MIT license):

https://github.com/RCayre/oasis

Romain Cayre, Vincent Nicomette, Guillaume Auriol, Mohamed Kaâniche, Aurélien Francillon. OASIS: An Intrusion Detection System Embedded in Bluetooth Low Energy Controllers. *2024 ACM Asia conference on Computer and Communications Security (ASIACCS).*, Jul 2024, Singapore, Singapore.

Thanks for your attention !