



Institut Cybersécurité Occitanie



Analyse des menaces émergentes de l'IoT

À l'interface logiciel/matériel pour les technologies sans fil de l'Internet des Objets

Pierre Ayoub

Friday 05, 2025

LAAS-CNRS / TRUST

**Défis
Clés
OCCITANIE**



- *Vincent Nicomette*
LAAS-CNRS / INSA Toulouse
- *Guillaume Auriol*
LAAS-CNRS / INSA Toulouse
- *Romain Cayre*
LAAS-CNRS / INSA Toulouse

Introduction

INTRODUCTION OF IOT PROTOCOLS – A FEW EXAMPLES

Low-Power



Let's add complexity...

Mesh



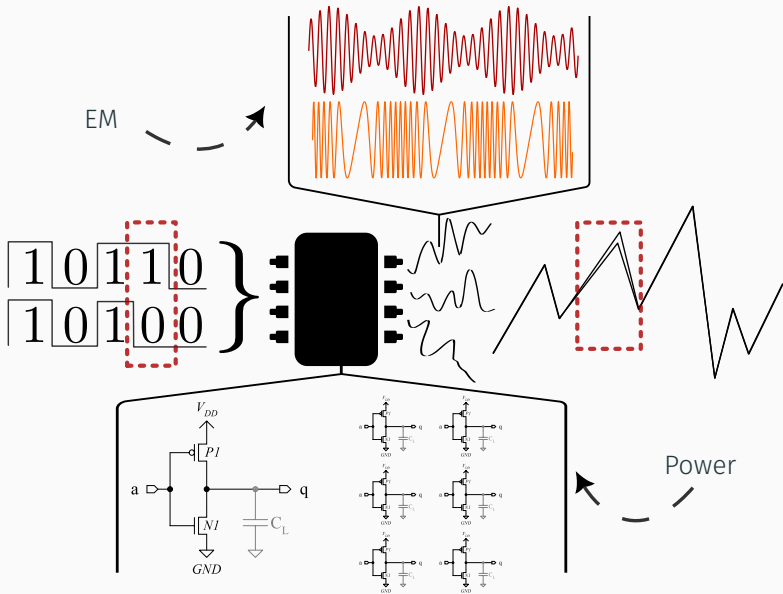
Let's add more complexity...

IP-addressable



Threats from EM Side Channels

ELECTROMAGNETIC SIDE CHANNELS

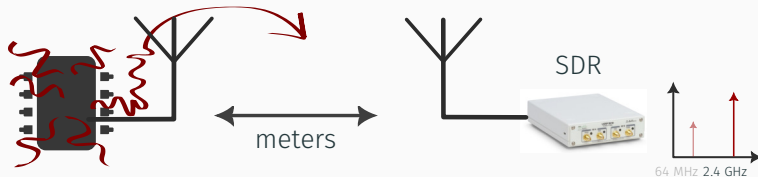


SCREAMING CHANNELS



Conventional side-channel: Near-field (NF)

Screaming Channels: Far-field (FF)



SCREAMING CHANNELS – FROM LABORATORY TO REAL WORLD

Screaming Channels is an **electromagnetic side-channel** attack...

- that can impact **system-on-chip (SoC)** with **radio transceivers**
- **enabling** long-distance attacks



Experimental
Firmware
Camurati et al., 2018



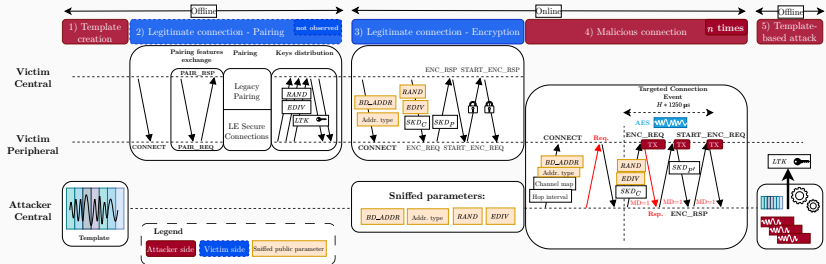
Google Eddystone
Camurati et al., 2020



Bluetooth Low Energy
Ayoub et al., 2024

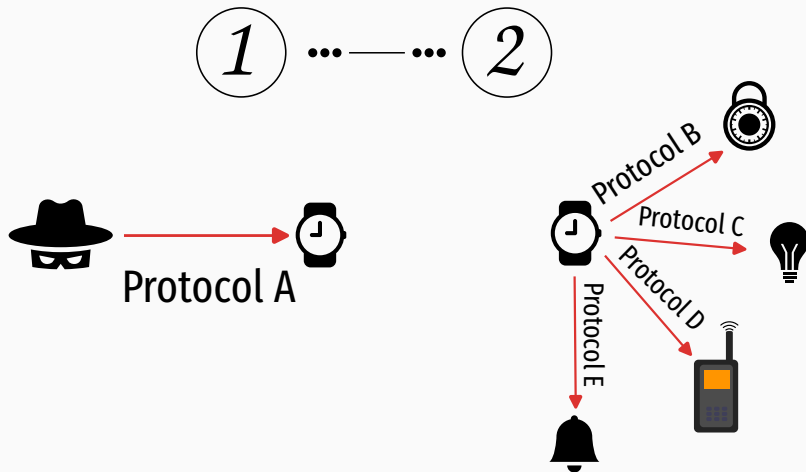
BLUESCREAM: SCREAMING CHANNELS ON BLE

Manipulating a full protocol add a **layer of complexity**...



Threats from Cross-Protocol Physical Layer Pivoting Attack

CROSS-PROTOCOL PHYSICAL LAYER PIVOTING ATTACK



CROSS-TECHNOLOGY COMMUNICATION (CTC)

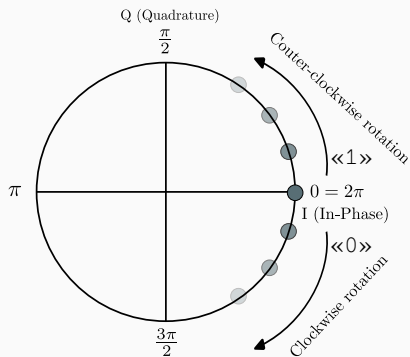
Definition

Allows **heterogeneous** protocol to **communicate**

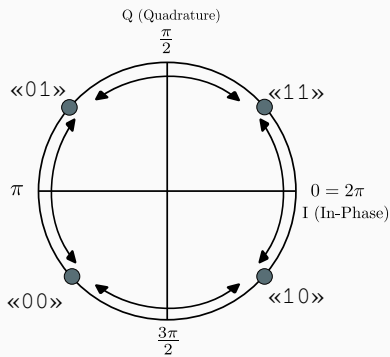
Root causes

- **Similarities** on how physical layer is used to transmit information
 - → **Modulation**
- **Shared** physical layer resources
 - → **Frequency band, Harmonics**

WAZABEE: FROM BLUETOOTH LOW ENERGY TO ZIGBEE



GFSK (BLE)



O-QPSK (Zigbee)

Perspectives

NEW ATTACK PARADIGMS

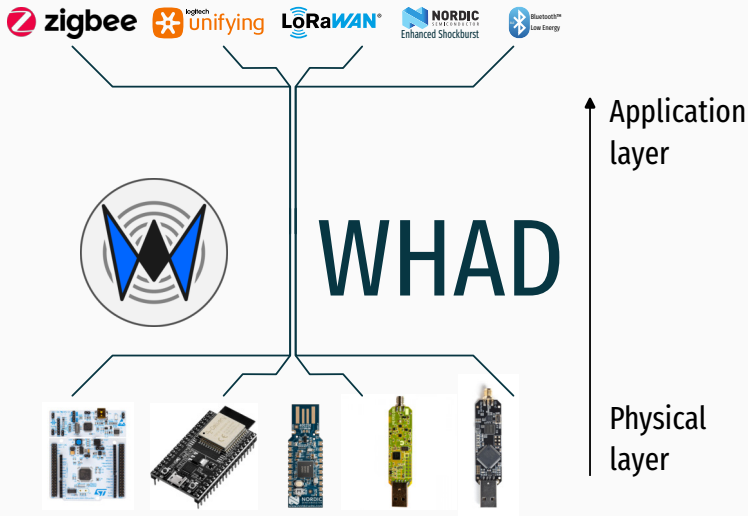
The attack surface is increasing...

- Screaming Channels
 - Lot of system on chips have not been assessed
 - Lot of protocols have not been assessed
- Cross-Protocol Pivoting Attacks
 - Could propagate very far in Mesh networks
 - IP addressable networks could lead to unexpected vulnerabilities

Problems

- Physical layer heterogeneity
- Hardware incompatibility

WHAD – WIRELESS HACKING DEVICES



WHAD – WIRELESS HACKING DEVICES



Research directions

- **Generalizing Screaming Channels** on more IoT protocols
- **Systematizing Cross-Communication Technology (CTC)** impact on IoT security

Thank you for your attention!

Questions?

Backup Slides

TALKS DURING THE YEAR

