IoTMap: a modelling system for heterogeneous IoT networks

Jonathan Tournier
François Lesueur, Frédéric Le-Mouël (CITI-INSA Lyon)
Laurent Guyon, Hicham Ben-Hassine (Algosecure)
first.last@insa-lyon.fr
first.last@algosecure.fr

30 june 2020

: @AlgoSecure

: `https://github.com/AlgoSecure/iotmap`

Whoami

- PhD student
- Thesis subject: IoT security
- RedTeamer/security consultant at AlgoSecure
- CTF and appsec tools enthusiast

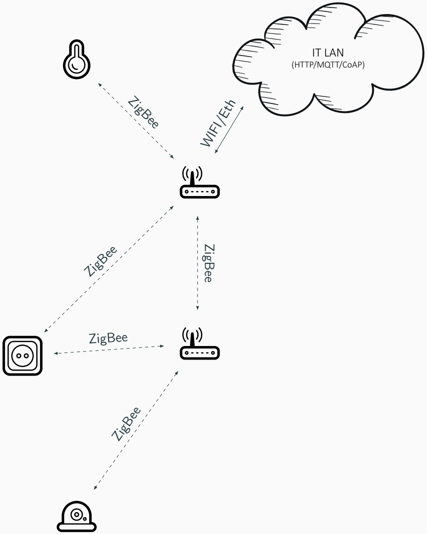
CITI-INSA Lyon

- Hosted at INSA Lyon
- Academic lab
- Focus on connected objects

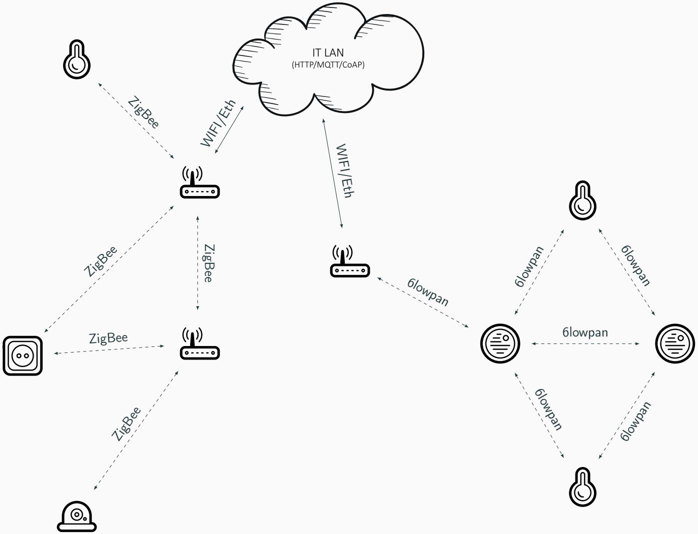
AlgoSecure

- Based in Lyon
- Human-size structure
- Involved in innovation and research

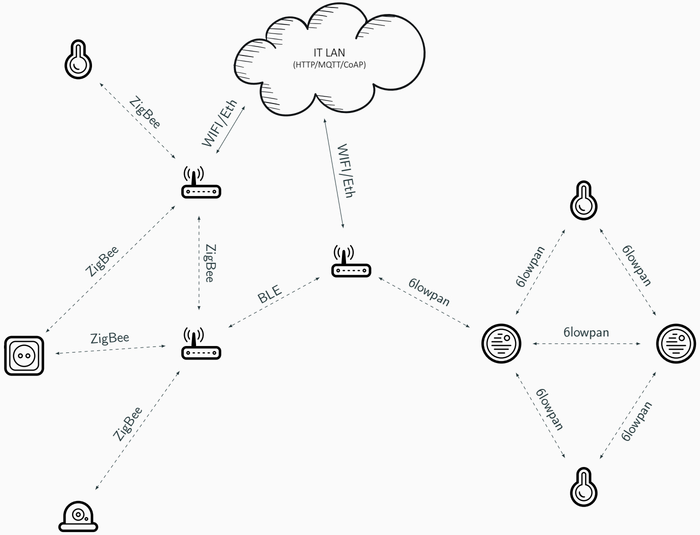
What are heterogeneous IoT networks?



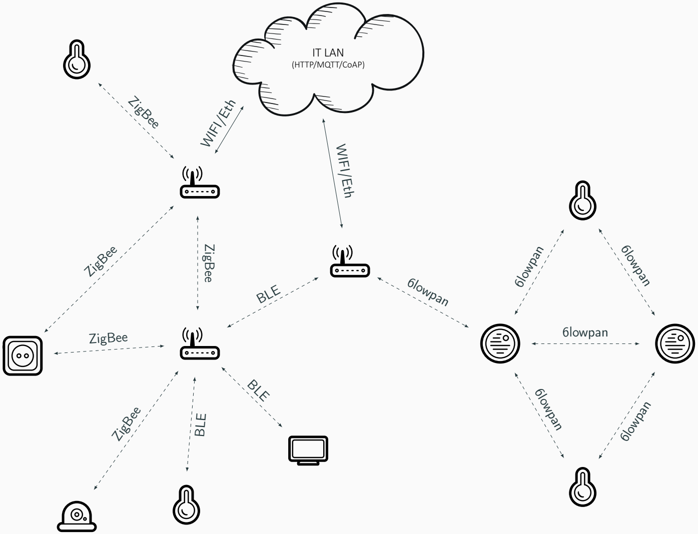
What are heterogeneous IoT networks?



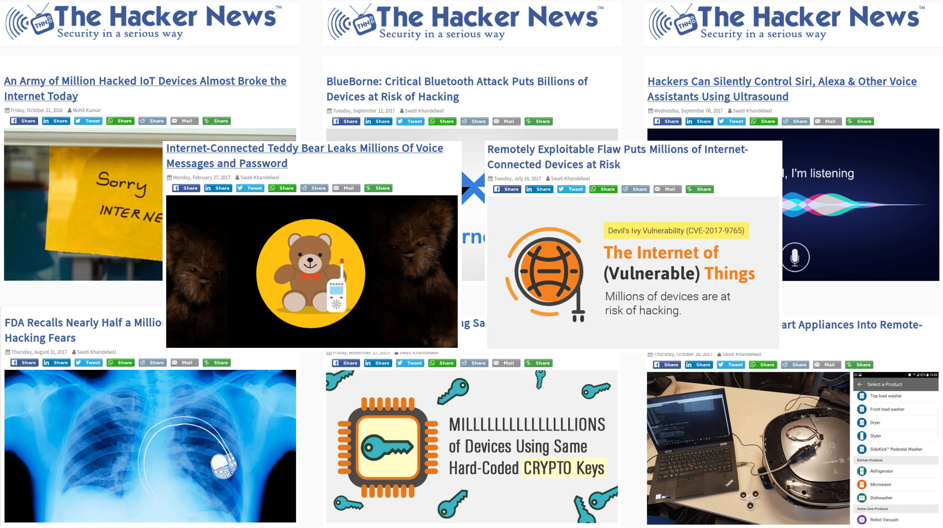
What are heterogeneous IoT networks?



What are heterogeneous IoT networks?



What about IoT security ?



The Hacker News™ Security in a serious way

An Army of Million Hacked IoT Devices Almost Broke the Internet Today

Friday, October 21, 2016 Mohit Kumar

Share Share Tweet Share Share Mail Share
Sorry
INTERNE

The Hacker News™ Security in a serious way

BlueBorne: Critical Bluetooth Attack Puts Billions of Devices at Risk of Hacking

Tuesday, September 12, 2017 Swati Khandelwal

Share Share Tweet Share Share Mail Share
rn

The Hacker News™ Security in a serious way

Hackers Can Silently Control Siri, Alexa & Other Voice Assistants Using Ultrasound

Wednesday, September 06, 2017 Swati Khandelwal

Internet-Connected Teddy Bear Leaks Millions Of Voice Messages and Password

Monday, February 27, 2017 Swati Khandelwal

Remotely Exploitable Flaw Puts Millions of Internet-Connected Devices at Risk

Tuesday, July 18, 2017 Swati Khandelwal

Share Share Tweet Share Share Mail Share
Devil's Ivy Vulnerability (CVE-2017-9765)
The Internet of (Vulnerable) Things
Millions of devices are at risk of hacking.

FDA Recalls Nearly Half a Millio Hacking Fears

Thursday, August 31, 2017 Swati Khandelwal

g Sa

Friday, November 27, 2015 Swati Khandelwal

art Appliances Into Remote-

Thursday, October 26, 2017 Swati Khandelwal

How to improve IoT security

Using penetration testing as a solution to evaluate and improve the security

Penetration testing steps

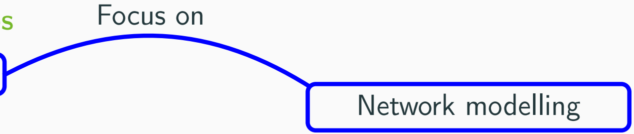
- Information gathering
- Threat modelling
- Vulnerabilities analysis
- Exploitation
- Post exploitation
- Reporting

How to improve IoT security

Using penetration testing as a solution to evaluate and improve the security

Penetration testing steps

- Information gathering
- Threat modelling
- Vulnerabilities analysis
- Exploitation
- Post exploitation
- Reporting



Focus on

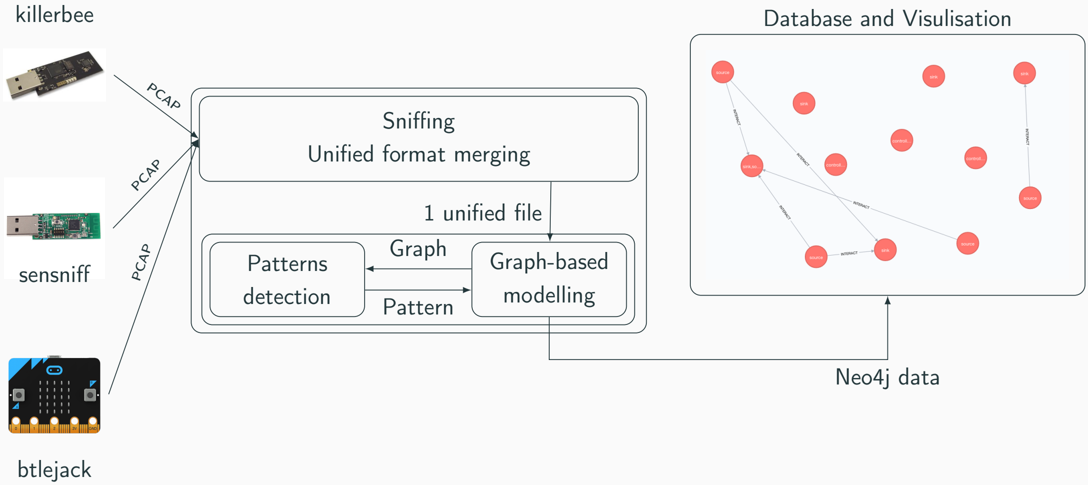
Network modelling

IoT network modelling | Existing tools

- KillerBee, SecBee, Zmonitor for ZigBee
- LiveNet for 802.15.4, WiFi
- Gattacker, btlejuice, btlejack for BLE
- EZ-force for ZWave
- foren6 for 6lowpan

⟶ What about heterogeneous IoT networks ?

IoTMap



killerbee

sensniff

btlejack

PCAP

PCAP

PCAP

Sniffing
Unified format merging

1 unified file

Patterns detection

Graph

Pattern

Graph-based modelling

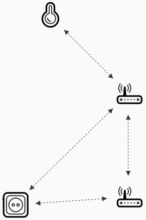
Neo4j data

Database and Visulisation

IoTMap | Modelling module

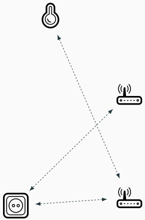
1 - Data link graph

- Point to point communications
- Unified format file as input



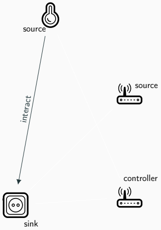
2 - Network graph

- End to end communications
- Use nwk-relative information



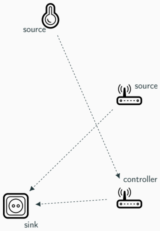
4 - Application graph

- Detected applications
- Defined patterns



3 - Transport graph

- Role of devices and data flow
- Defined patterns

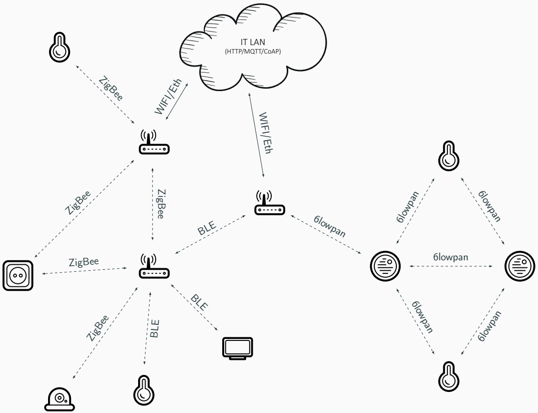


Demonstration | Setup

- 3 protocols: ZigBee, Ble, 6lowpan
- 12 devices:

BLE:	2x Micro:Bit
ZB:	Hub, outlet, 2x sensors (temp and motion)
6PAN:	4x TI sensortags cc2550
Multi:	2x RPi

- Several applications
  - Monitoring
  - Actuator-Sensor
- 1 hour of traffic interception



Demonstration

Conclusion

Statement

- IoT Security is mostly focused on monoprotocol
- Heterogeneous networks will be more and more present
- Legacy networks still remain the weak piece
- Study the IoT security from a global vision

Future works

- Improve automatic tasks for information gathering
  - Encrypted traffic analysis
  - Add more patterns
  - Add more protocols
- (a lot of bugfixes)

IoTMap: a modelling system for heterogeneous IoT networks

Jonathan Tournier
François Lesueur, Frédéric Le-Mouël (CITI-INSA Lyon)
Laurent Guyon, Hicham Ben-Hassine (Algosecure)
first.last@insa-lyon.fr
first.last@algosecure.fr

30 june 2020

: @AlgoSecure

: `https://github.com/AlgoSecure/iotmap`