BRAIN-IoT

model-Based fRamework for dependable sensing and Actuation in INtelligent decentralized IoT systems

SECURING LOW POWER DEVICE COMMUNICATION IN CRITICAL INFRASTRUCTURE MANAGEMENT

Paul-Emmanuel BRUN, Airbus CyberSecurity SAS

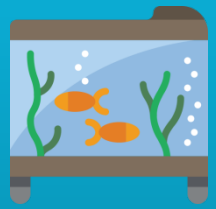
OVERVIEW OF THREATS IN IOT

Target

2017

Dallas Emergency Sirens cyberattack

Vector



2017

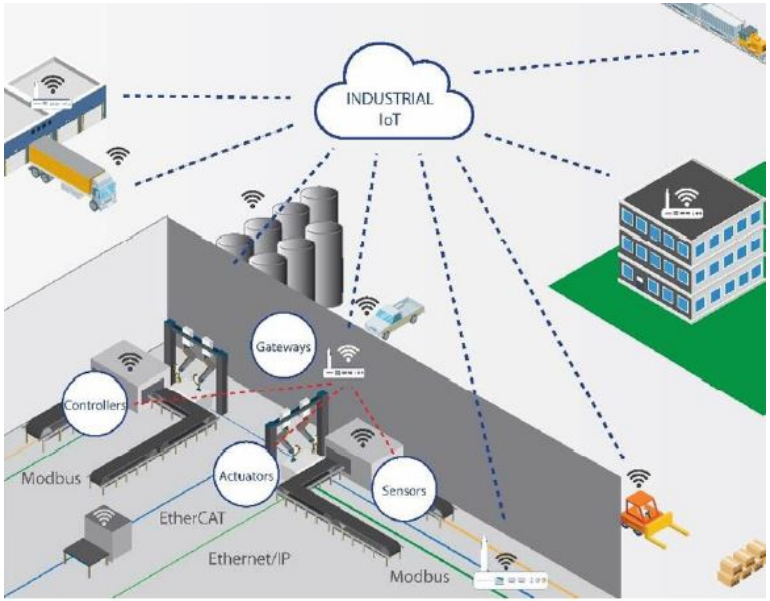
Casino fish tank temperature sensor cyberattack

Weapon

2016 - 2019

Mirai Botnet

INDUSTRIAL IOT CONSIDERATIONS



Potential effects of cyber-incidents involving Industrial IoT:

Business impacts:

- **Production / service downtime**, resulting in overcosts, delays and reputation
- **Quality deficiencies,** resulting financial / reputational damages
- **Reputational damages,** subsequent loss of opportunities

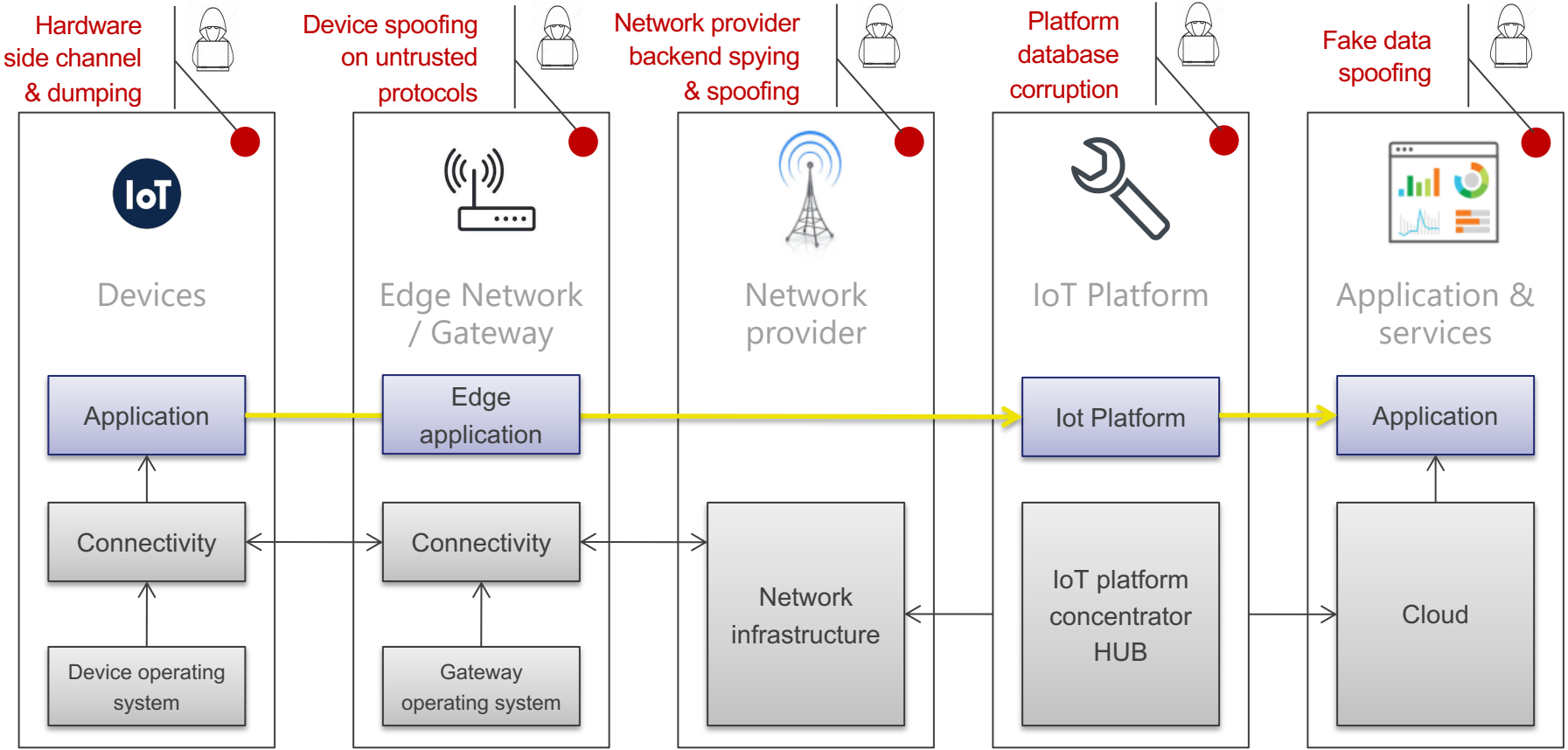
Physical damages:

- **Equipment damages**, recovery costs, impact on production
- **Human safety**, operator / user / society endangered

Damages to intangible assets:

- **Intellectual Property** (IP) **theft** and loss of competitive advantages
- **Private data leakage** resulting in legal and reputational damages

IOT SYSTEM ARCHITECTURE & THREATS

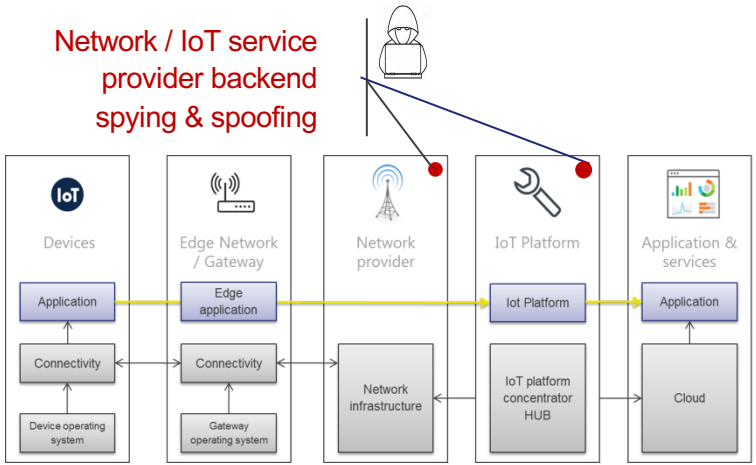


THREATS - EXAMPLE

Example from SHODAN with a widely used IoT protocol, MQTT:

→ **74 000 fully open backend**

Many types of data, such as GPS position, temperatures, actuators, …



MQTT Connection Code: 0

Topics:
$SYS/r1w0595vS/new/subscribes
/device/arduino/key/FUML9QcwADk
/key/FUML9QcwADk/device/arduino
/key/p120mBUEQdE/device/geyser/tag/temperature
abc/123
device/alarm/key/Bj5Xwi1YXEU
device/arduino/key/1qaz2wsx
device/arduino/key/FUML9QcwADk
device/arduino/key/YYuGP7Wi...

MQTT Connection Code: 0

Topics:
$SYS/broker/version
$SYS/broker/timestamp
$SYS/broker/uptime
$SYS/broker/clients/total
$SYS/broker/clients/maximum
$SYS/broker/clients/inactive
$SYS/broker/clients/disconnected
$SYS/broker/clients/active
$SYS/broker/clients/connected
$SYS/broker/clients/expired
$S...

MQTT Connection Code: 0

Topics:
VD089CD901B6E67058B5/TAG/AFFE0002/POS
VD089CD901B6E67058B5/TAG/AFFE0001/POS
si/4443/tagposition/1233
si/4443/tagposition/1238
VD089CD901B6E67058B5/TAG/AFFE0002/POS
VD089CD901B6E67058B5/TAG/AFFE0001/POS
si/4443/tagposition/1238
si/4443/tagposition/1233
TemsPojatno/...

TOTAL RESULTS

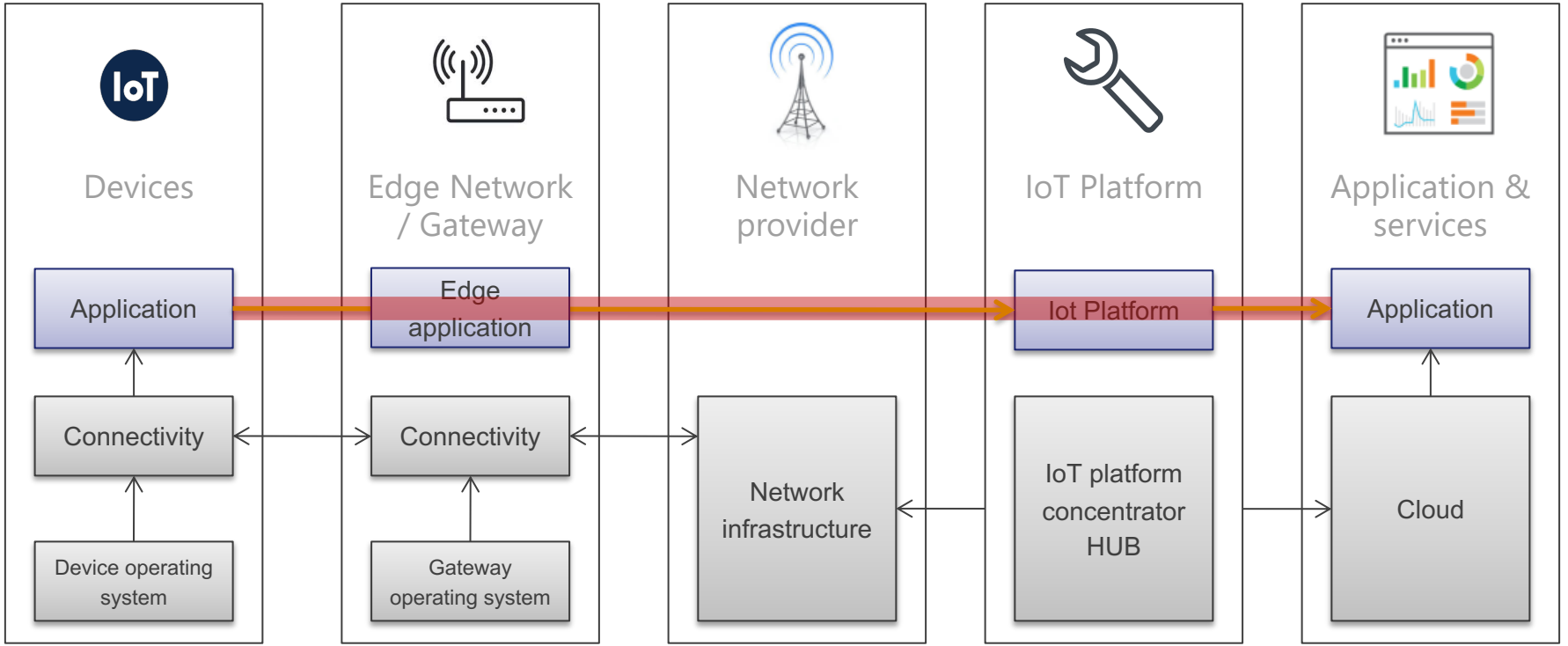
74,507

INDUSTRIAL IOT COMPLEXITY

Heterogeneous protocols	The high level of heterogeneity of protocols (network & applicative), make it difficult to validate the overall system and **ensure end-to-end security**
Protocols and hardware come from mass market	Hardware and protocols are facing **new challenges to reduce costs and increase autonomy**. Those challenges are not compatible with state of the art security mechanisms
Heterogenous constraints and massive deployments	From industry 4.0 to connected transportation and smart city, IoT use cases are broad, and hardware heterogeneity leads to **complex validation processes** for embedded softwares

THE END-TO-END SECURITY PARADIGM

Ensure privacy and security of data through all third parties



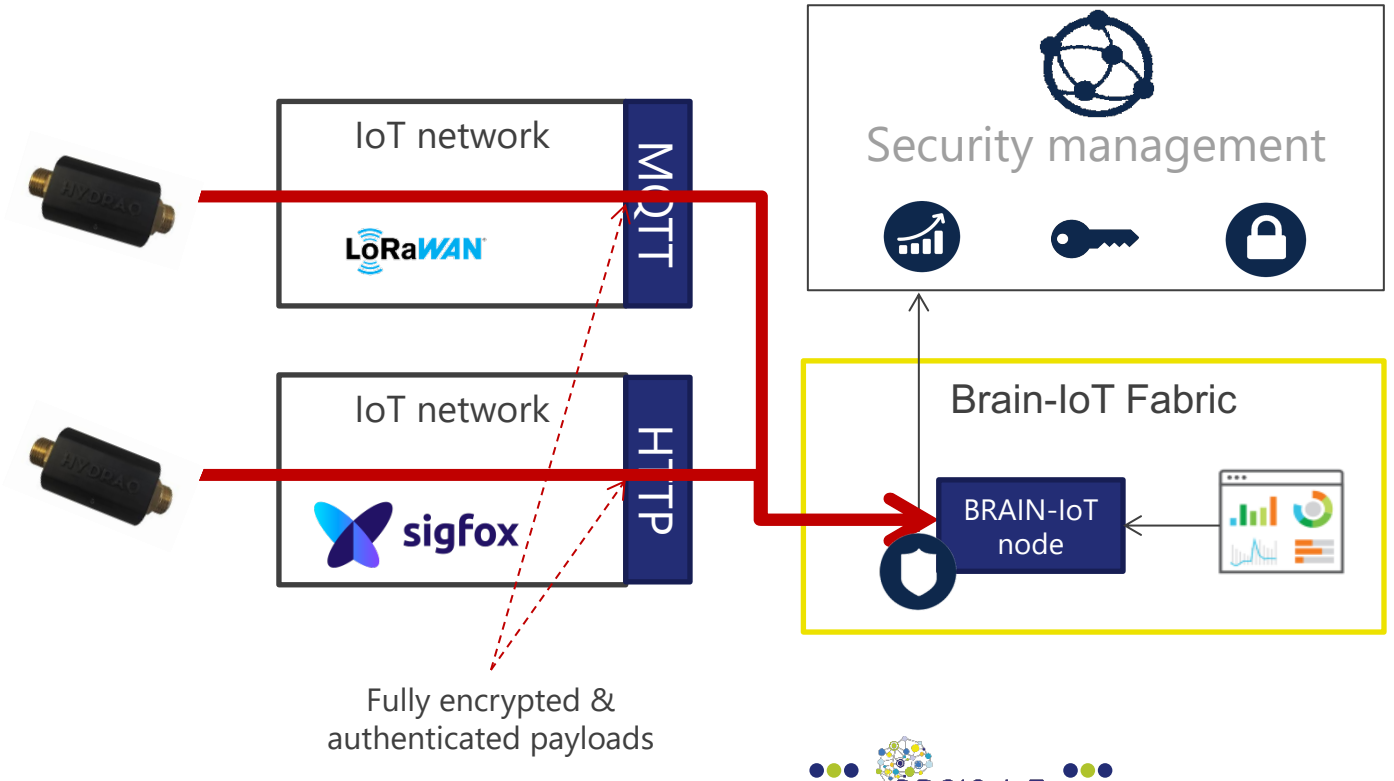
END-TO-END SECURITY – STATE OF THE ART

	Encryption supporting Low Power IoT constraint	Authentication supporting Low Power IoT constraint	End-to-end secure over heterogeneous dataflow
TLS	No	No	No
EDHOC + TLS	Yes	Yes	No
SCHC + TLS	Yes	Yes	Partial (no applicative disruption possible / data overhead)
OSCORE	Yes	Yes	Partial (limited to CoAP - no applicative disruption possible)

As no security layers supports security over multi-applicative protocols (e.g: LoRaWAN -> MQTT -> HTTP), state of the art solution relies on hop-to-hop security, **leading to potential leaks in third party components**

END-TO-END SECURITY – A WATER MANAGEMENT USE CASE
(FROM BRAIN-IOT H2020 PROJECT)

End-to-end authentication over LPWAN networks (Sigfox & LoRaWAN)



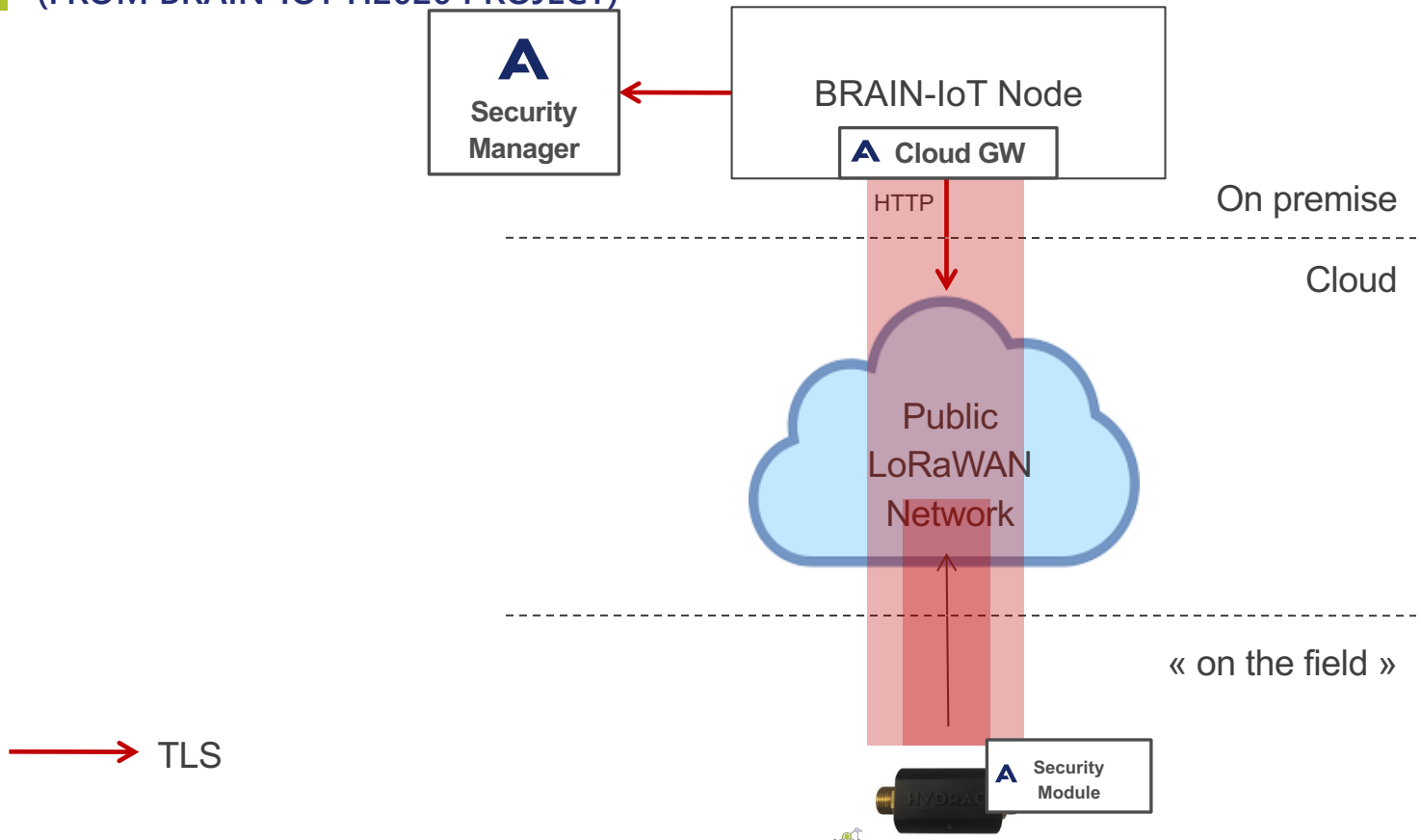
Hardened security:
Protection against attacks on third parties (network provider)

Low impact on energy consumption:
Impact on device lifetime: 0,25%
(30 messages / hour)

Low impact on device bandwidth :
5 bytes for security metadata

BRAIN-IoT

END-TO-END SECURITY – A WATER MANAGEMENT USE CASE
(FROM BRAIN-IOT H2020 PROJECT)



TO CONCLUDE

- 2 pillars of cyber secured systems :
  - Cyber protection
  - Cyber detection

- IoT brings news challenges for cyber monitoring because of :
  - Big amount of data
  - Decentralized architecture

Artificial intelligence is a **key technology** to enable **reliable cyber monitoring** in IoT contexts

CONTACTS

PAUL-EMMANUEL BRUN

IoT System Security Expert

Airbus CyberSecurity SAS

+33 1 61 38 68 02

paul-emmanuel.brun@airbus.com / https://airbus-cyber-security.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780089.

BRAIN-IoT

model-Based fRamework for dependable sensing and Actuation in INtelligent decentralized IoT systems

END-TO-END SECURITY – A WATER MANAGEMENT USE CASE
(FROM BRAIN-IOT H2020 PROJECT)