Federated Security Approaches for IT and OT

GT SSLR 2021

Léo LAVAUR, IMT Atlantique, Cyber CNI, Rennes

2021-05-11

Advisors:

- Marc-Oliver Pahl, IMT Atlantique, Cyber CNI
- Yann Busnel, IMT Atlantique, IRISA
- Fabien Autrel, IMT Atlantique, Cyber CNI

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)

References

[1] J. Kephart and D. Chess, “The vision of autonomic computing”, Computer, 2003.

[2] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions”, Computers & Security, 2019.

[3] S. Rathore, B. Wook Kwon, and J. H. Park, “BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network”, Journal of Network and Computer Applications, 2019.

[4] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, “Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications”, IEEE Access, 2020.

[5] M.-O. Pahl, A. Kabil, E. Bourget, M. Gay, and P.-E. Brun, “A Mixed-Interaction Critical Infrastructure Honeypot,” 2020.

Contents

1. Context

Collaboration to cope with large-scale attacks

Background

- Benefit from real-world use cases
- Exchange with partners* for insights
- Existing works and infrastructures in the chair (CNI testbed, datasets...)

Distributed attacks are more frequent, and also target industrial systems...

- **Mirai (2016)** ⇒ Uses TCP probing, and bruteforces logins
- **WannaCry & NotPetya (2017)** ⇒ Exploit MS17-010
- **AZORult (2018)** ⇒ Uses known C2s
- **Ryuk (2018)** ⇒ Uses Emotet / Trickbot

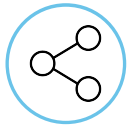
* Airbus Cyber, Amossy, BNP Paribas, EDF, Nokia Labs, SNCF

Background

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

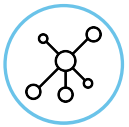
- Benefit from real-world use cases
- Exchange with partners* for insights
- Existing works and infrastructures in the chair (CNI testbed, datasets...)

Large-scale attacks are more frequent, and also target industrial systems...



CTI sharing

Collective situation awareness using threat intelligence



Model sharing

Machine learning from distributed sources

* Airbus Cyber, Amossy, BNP Paribas, EDF, Nokia Labs, SNCF

Thesis objective

Four observations*:

*From 71 reviewed papers, including 15 surveys

(a) Lack of collective knowledge
There is a lack of collective knowledge in cybersecurity, and more particularly in the OT. [2]

(b) Lack of incentives
Trust and privacy are major hurdle for stakeholders to share data. [2]

(c) Insuffisant resiliency
Centralized systems represent a Single Point of Failure and can induce a communication overhead. [3]

(d) Architectural isolation
The siloed architecture of detection systems is an obstacle to their effectiveness. [4]

R.Q: *How to federate knowledge and defense between non-trusting parties?*

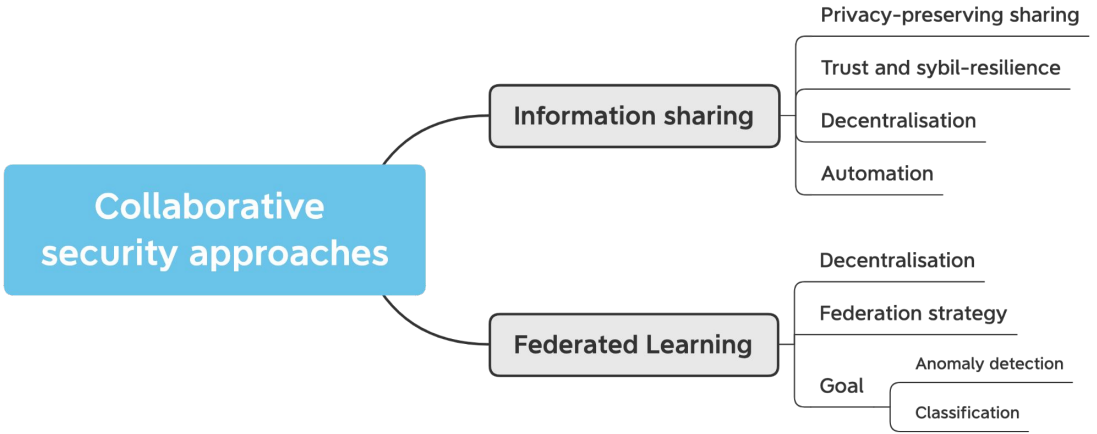
- What to collect?
- What to share?
- How to share it?

2. Current state

Writing a survey on automated collaborative security

Survey* on collaborative security for the IIoT

*From 71 reviewed papers, including 15 surveys



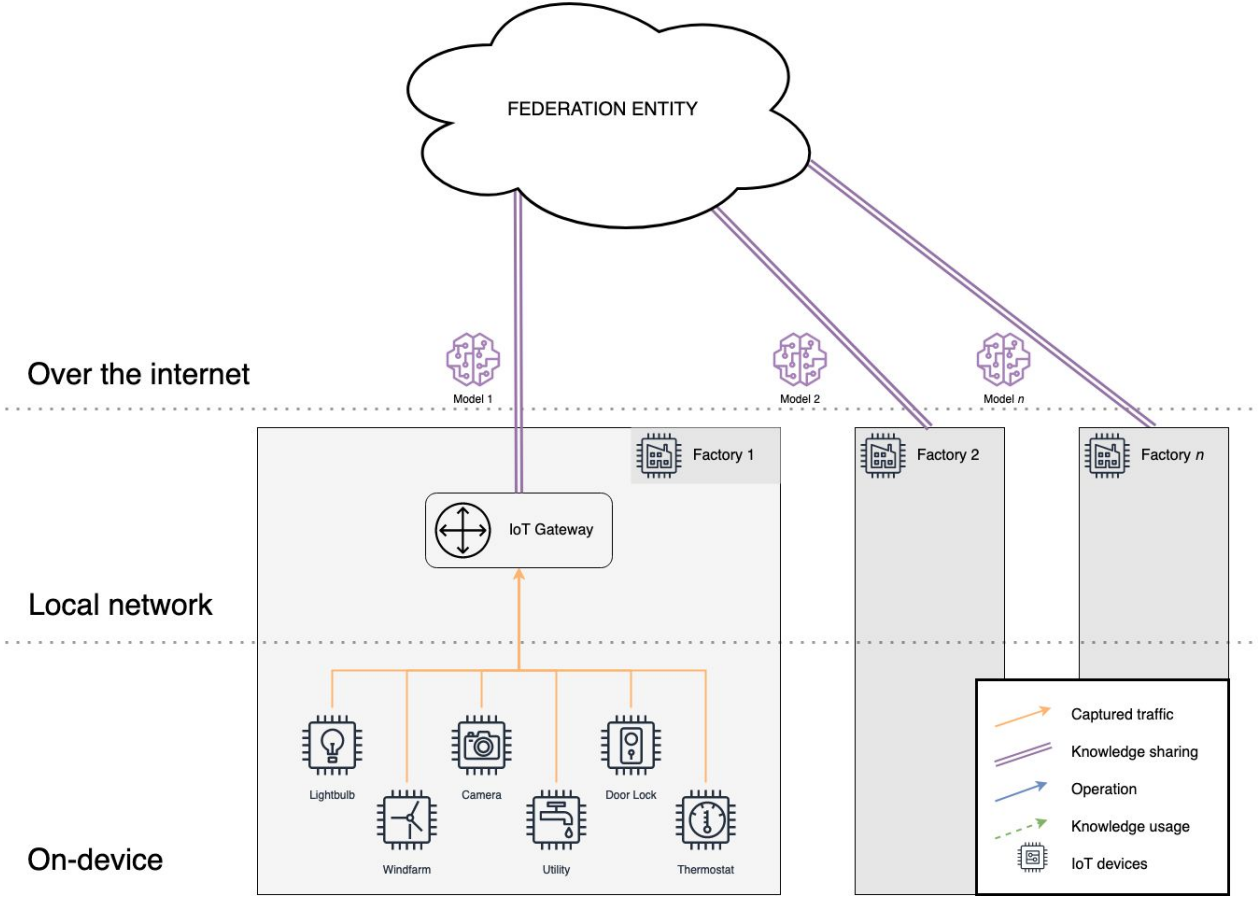


Fig. 1. Reference architecture

- Note: collection of additional data could be performed using a *Honeypot Factory*

3. Next steps

Building experiments on the best use-cases

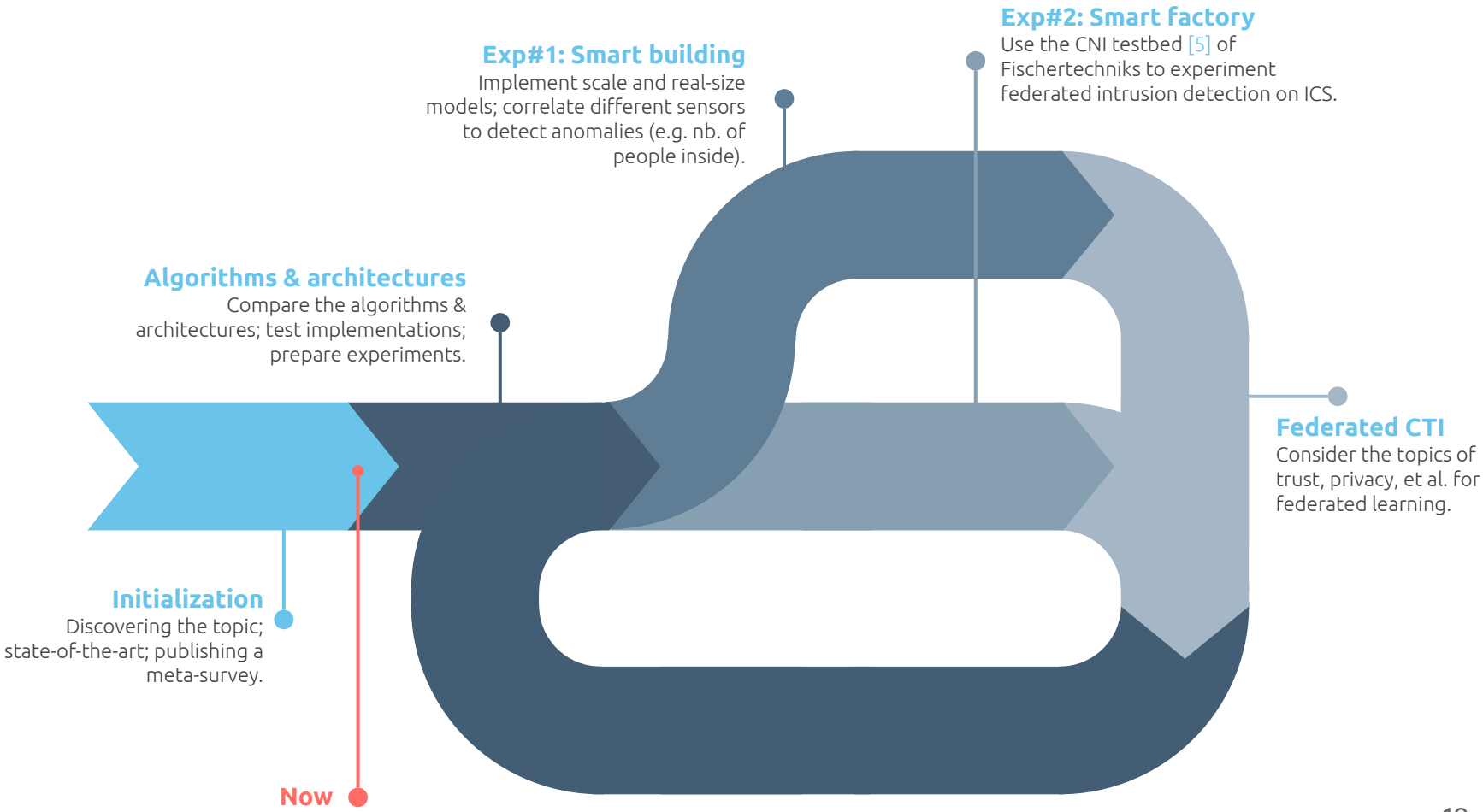
Experiment-driven research

Smart building

How to aggregate and correlate differents types of sensors to detect anomalies in smart buildings?

Smart factory

How to prevent large-scale attacks (botnets, ransomwares) from hurting local infrastructures?


Exp#2: Smart factory
Use the CNI testbed [5] of Fischertechniks to experiment federated intrusion detection on ICS.
Exp#1: Smart building
Implement scale and real-size models; correlate different sensors to detect anomalies (e.g. nb. of people inside).
Algorithms & architectures
Compare the algorithms & architectures; test implementations; prepare experiments.
Federated CTI
Consider the topics of trust, privacy, et al. for federated learning.
Initialization
Discovering the topic; state-of-the-art; publishing a meta-survey.
Now

Conclusion

- Federated architectures for knowledge & defense
- Ongoing survey: identify the possibilities from the literature
- 2 use cases & 2 experiments
    a. Smart Buildings using scale- and real-size models
    b. Smart Factories using CNI testbed