IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Federated Security Approaches for IT and OT

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]

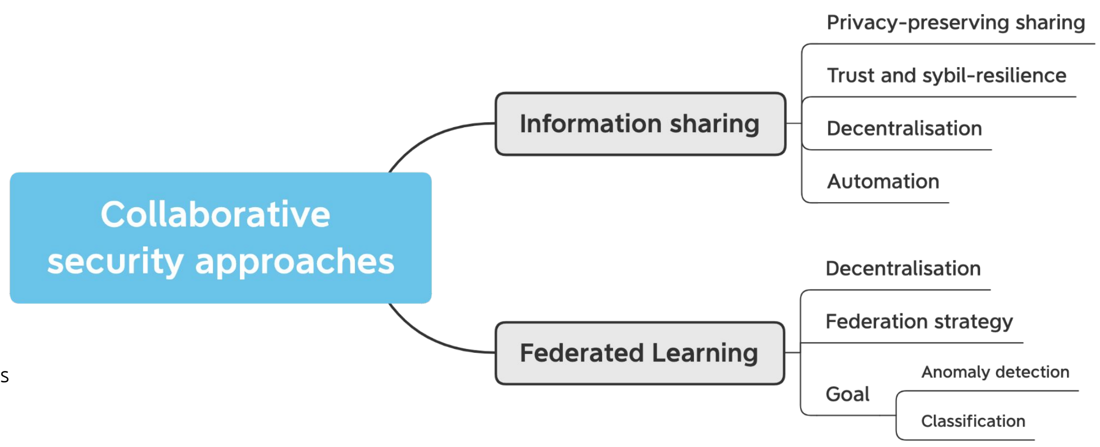
Research Question:

How to federate knowledge and defense between non-trusting parties?

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

Survey* on collaborative security for the IIoT

*From 71 reviewed papers, including 15 surveys


Collaborative security approaches

Information sharing
- Privacy-preserving sharing
- Trust and sybil-resilience
- Decentralisation
- Automation

Federated Learning
- Decentralisation
- Federation strategy
- Goal
  - Anomaly detection
  - Classification

Authors

Léo LAVAUR

Marc-Oliver PAHL
Yann BUSNEL
Fabien AUTREL

Partners

Overview

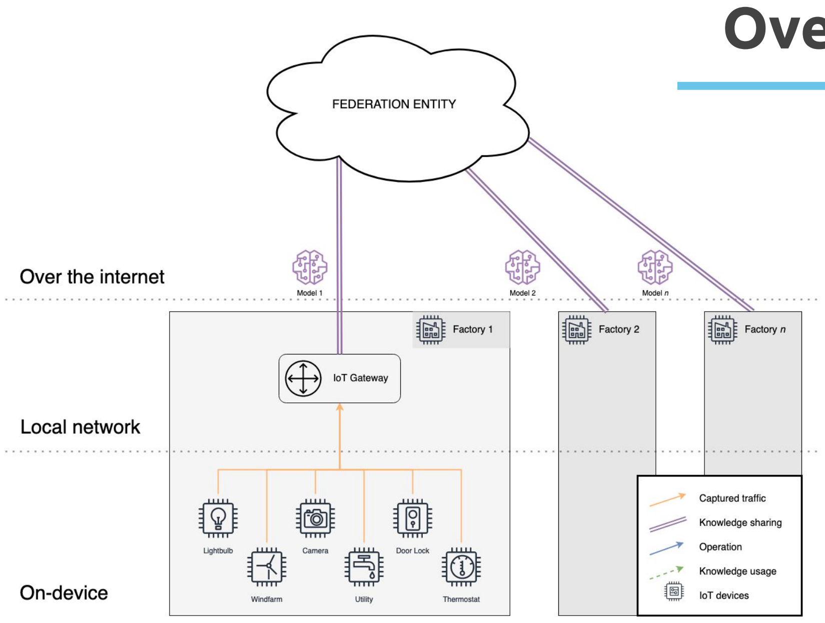
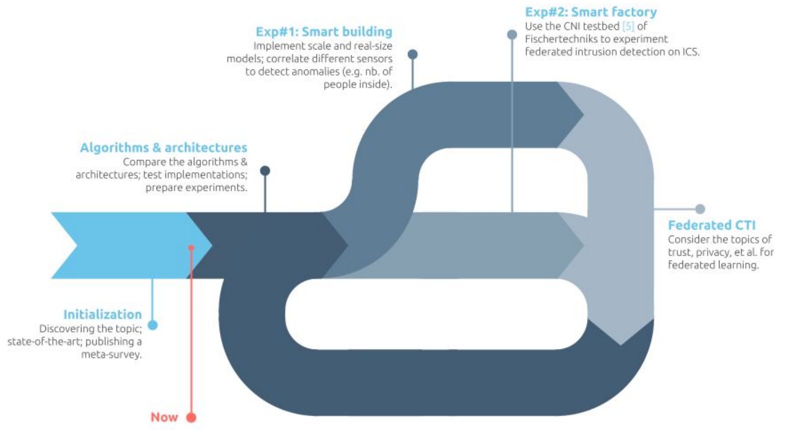


Fig. 1. Reference architecture


Initialization
Discovering the topic; state-of-the-art; publishing a meta-survey.

Algorithms & architectures
Compare the algorithms & architectures; test implementations; prepare experiments.

Exp#1: Smart building
Implement scale and real-size models; correlate different sensors to detect anomalies (e.g. nb. of people inside).

Exp#2: Smart factory
Use the CNI testbed [5] of Fischertechniks to experiment federated intrusion detection on ICS.

Federated CTI
Consider the topics of trust, privacy, et al. for federated learning.

Now

Fig. 2. Course of action

Experiments

Fig. 3. *Cencyble* (IMT Atlantique) -- office used as a real-size model

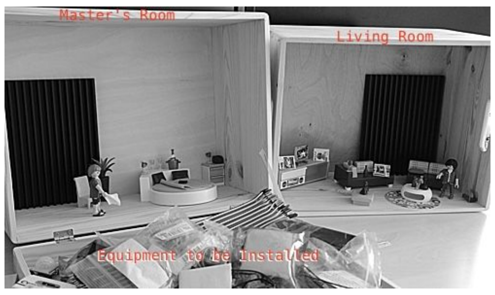


Fig. 4. S2O spaces (TUM) -- scale models for smart building experimentations

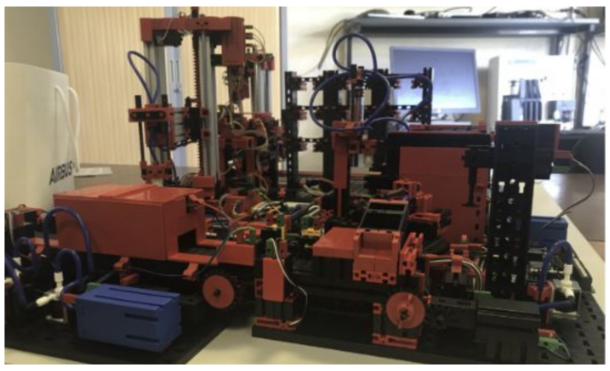


Fig. 6. Industrial testbed (Chaire CyberCNI) -- attack scenarios on real production lines

Contact: leo.lavaur@imt-atlantique.fr

11 Mai 2021 - GT SSLR 2021