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
References


Contents

1. Context
   Collaboration to cope with large-scale attacks

2. Current state
   Writing a survey on automated collaborative security

3. Next steps
   Building experiments on the best use-cases
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

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

Fig. 1. Reference architecture
3. Next steps

Building experiments on the best use-cases
Experiment-driven research

**Smart building**
How to aggregate and correlate different types of sensors to detect anomalies in smart buildings?

**Smart factory**
How to prevent large-scale attacks (botnets, ransomwares) from hurting local infrastructures?
Initialization
Discovering the topic; state-of-the-art; publishing a meta-survey.

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.

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

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