Federated security approaches for IT and OT

Léo Lavaur
IMT Atlantique, Cyber CNI
leo.lavaur@imt-atlantique.fr

Marc-Oliver Pahl
IMT Atlantique, Cyber CNI
marc-oliver.pahl@imt-atlantique.fr

Yann Busnel
IMT Atlantique, IRISA
yann.busnel@imt-atlantique.fr

Fabien Autrel
IMT Atlantique, Cyber CNI
fabien.autrel@imt-atlantique.fr

***Abstract*—The Internet of Things has begun to spread over a variety of domains, including industry and finance. It represents an increasing threat for both IT and OT. The lack of collaboration results in the same attacks targeting different organizations one after the other. Often employed as an answer to this problem, cyber threat-intelligence sharing induces its own set of challenges: trust, privacy, and traceability.**

This thesis takes advantages of a distributed sharing-oriented architecture and to enhance the security of industrial infrastructures. We study Federated Learning algorithms to build a distributed, autonomic system for detecting and characterizing attacks, as well as providing counter-measures.

Experiments on real-world testbeds at the chair Cyber CNI allow us to validate the theoretical assumptions against realistic infrastructures and scenarios, fitting industrial use-cases.

***Index Terms*—IT, OT, threat intelligence, cooperative sharing, federated learning, distributed ledgers**

I. Motivation

This thesis takes place in IMT's chair Cyber CNI, which focuses its work toward the protection of *Critical Networked Infrastructures*. The chair is supported by industrial partners, allowing to study real-world use-cases and benefit from their inputs — see section IV. The purpose of this thesis is to study the automated sharing of threat intelligence, particularly in critical infrastructures.

Over the years, multiple attacks have been reported to aim the Information Technologies (IT) and Operational Technologies (OT), including the Industrial Control Systems (ICSs) [1]. These threats include information leakage, device takeover, or even physical damages in critical infrastructures. To protect organizations, security systems often rely on network-based attack detection like Intrusion Prevention System (IPS) to identify attacks, and block the traffic. This approach is however inefficient against novel attacks and Advanced Persistent Threat (APT), like Stuxnet in 2016. Behavior-based anomaly detection based on Machine Learning (ML) is often considered the future of attack detection.

More importantly, the same attack can damage different organizations using the same mechanics before its operation is characterized, and actionable threat intelligence can be shared. Botnets are a good example since they infect a considerable amount of devices using the same vulnerabilities. In 2016, the Mirai botnet has been used for multiple world-scale Distributed Denial of Service (DDoS) attacks. One of them targeted the DNS provider Dyn, and is responsible for shutting down parts of the Internet [2]. The malware is still active and new devices get compromised every day, showing the lack of cooperation among the security community. Consequently, detection systems need to move from a siloed architecture to a federated approach; thus unifying the localized ML models.

The discussed situation leads to the following observations: (a) there is a lack of unified knowledge in cybersecurity, and more particularly in the Internet of Things (IoT) [3]; (b) trust and privacy are major hurdle for stakeholders to share data [3]; (c) centralized systems represent a Single Point of Failure (SPoF) and can induce a communication overhead [4]; (d) the siloed architecture of detection systems is an obstacle to their effectiveness [5].

II. Current state

Observations (a) to (c) represent research questions that have been independently addressed by the research community. Our current work is focused on the literature overview of the collaborative aspects of security in the IT and OT. Following some of the precepts of the Systemic Literature Review methodology, we survey the state-of-the-art multiples overlapping domains: Federated Learning (FL) and its limitation, privacy-preserving information sharing, collaborative threat intelligence, distributed ledgers, and attack detection for the IoT and Industrial Internet of Things (IIoT) – see **??**.The questions that our survey tries to answer are as follows:

- What are the most important attacks over the past 10 years, where federated approaches could work?
- What are the topics covered by the academic literature over that rime?
- In which venues or journals was the literatures published?
- Which groups are active in this area?
- What are the still open questions according to existing surveys?

Threat intelligence sharing is often proposed as a solution to observation (a) [6]. Game-theory is studied to provide incentives to stakeholders to make the participants actively involved in sharing communities. Platforms such as MISP [7] have emerged to overcome these issues, and the blockchain is frequently considered in order to provide trust, traceability, and non-repudiation [8].

To solve observations (b) and (d), FL is proposed in association with detection algorithms. FL allows training a global ML for a distributed system containing multiple nodes without sharing the analyzed data itself. Instead, nodes train their models locally, and share their parameters with each other. Architectures based on FL are expected to provide accurate

and faster results in addition to adding privacy and security [9].

To address observation (c), distributed ledgers such as blockchain or Directed Acyclic Graph (DAG) could support decentralized systems while guaranteeing the integrity of the exchanges. Distributed architectures also diminish the communication overhead in federated systems, allowing to reduce both the bandwidth consumption and the latency [4].

The first findings of our research identified the following research question. *What federated strategies could be applied to local ML-based detection systems to improve the security of IT and OT realms?* Several sub-questions arise from the latter, such as:

- What are most appropriate FL approaches? Which strategies for model aggregation?
- What are the security limitations of such approaches?
- What kind of architecture would best support these systems?

III. Related Works

Several surveys have covered parts of the subject, especially the state-of-the-art of FL approaches [5] or the collaborative threat intelligence [10], but none covers both aspects. On the technical side, several security architectures have been introduced to tackle the current issues of the IoT. The authors of [11] propose an AI-enabled architecture to secure the physical layer of the IoT, using modules dedicated to one use-case, while the authors of [4] proposed detection system based on Software-defined networking (SDN) using blockchain-based FL on a three-layer architecture.

FL and blockchain have both been well addressed in the literature, the former for its ability to reduce the communication overhead while improving privacy, the latter to support information-sharing while guaranteeing trust, non-repudiation and tampering resistance. The authors of [9] present DeepFed, a deep FL detection system tailored to deal with Cyber-Phisical Systems (CPSs) while maintaining a centralized architecture. On the other hand, FLchain [12] uses the distributed aspects of the blockchain to remove the single point-of-failure.

The blockchain is also studied to provide incentives to stakeholders and improve participation. Cha *et al.* [6] propose a blockchain-based Cyber Threat Intelligence (CTI) architecture that provides reliability, privacy, scalability, and sustainability. The proposed system reduces network load, and measures organizations' contributions to motivate participation.

IV. Next steps

As mentioned in section II, current work focuses on the literature analysis. Then, we will implement FL algorithms fitting the use-cases of our chair partners. Two use-cases have been currently identified. (I) The first one is the security of the OT, where FL could be implemented to detect attacks targeting CPS at scale. The chair already work on a cyber–physical testbed [13] that will eventually allow us to run attack scenarios on multiple scale-models at once, letting us to use FL to detect the anomalies. (II) The second identified use-case is the smart building that are currently appearing all around the world. FL would be used to detect behavior anomalies, allowing the detection of physical intrusions. A real-world testbed will be made by deploying sensors and devices in our office to emulate smart-building equipments.

Another approach that deserves to be considered is the impact of geographical and geopolitical context on the attacks. In fact, a lot of today's event in the cyberspace are the transposition of real-world conflicts or tensions. This implies a completely different set of challenges due to the linking of abstract concepts taken from social sciences with the technical representation of such event. If addressed, this part of the thesis will probably require collaboration with other teams.

References

[1] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials*, 2019.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, 2017.

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

[4] 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.

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

[6] J. Cha, S. K. Singh, Y. Pan, and J. H. Park, "Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing," *Sustainability*, 2020.

[7] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP - The design and implementation of a collaborative threat intelligence sharing platform," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security - WISCS'16*, New York, New York, USA: ACM Press, 2016.

[8] Y. Wu, Y. Qiao, Y. Ye, and B. Lee, "Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, IEEE, 2019.

[9] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Informatics*, 2020.

[10] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Computers & Security*, 2016.

[11] H. HaddadPajouh, R. Khayami, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things," *Neural Computing and Applications*, 2020.

[12] U. Majeed and C. S. Hong, "FLchain: Federated Learning via MEC-enabled Blockchain Network," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, IEEE, 2019.

[13] M.-O. Pahl, A. Kabil, E. Bourget, M. Gay, and P.-e. Brun, "A Mixed-Interaction Critical Infrastructure Honeypot," 2020.