Distributed Intrusion Detection Methodology of Process Oriented Attacks in Industrial Control Systems

Estelle Hotellier
Naval Group,
Naval Cyber Laboratory,
199 Av. Pierre-Gilles de Gennes,
83190 Ollioules, France

Franck Sicard
Naval Group,
Naval Cyber Laboratory,
199 Av. Pierre-Gilles de Gennes,
83190 Ollioules, France

Julien Francq
Naval Group,
Naval Cyber Laboratory,
199 Av. Pierre-Gilles de Gennes,
83190 Ollioules, France

Stéphane Mocanu
Univ. Grenoble Alpes,
Inria, CNRS,
Grenoble INP, LIG,
38000 Grenoble, France

Abstract—**This paper presents a starting Ph.D topic on intrusion detection in complex industrial control systems. We are interested in network-based, process-oriented attacks, i.e. attacks which do not violate network protocols and target specifically the integrity of the physical process. We consider complex industrial processes with event-driven and time-driven weakly interconnected sub-processes. We consider local security properties of the physical sub-processes but also global properties which cannot be decomposed locally. Therefore we aim to develop an anomaly-based, process-aware, distributed detection methodology for event-driven and continuous dynamical systems.**

I. Introduction

This Ph.D topic concerns the intrusion detection in Industrial Control Systems (ICSs). An ICS comprises a set of networked physical and numerical components interacting together to achieve the control of an industrial process. The devices located closest to the physical process, like sensors, actuators and controllers are designed to guarantee a response time and therefore respect hard real-time constraints [1]. ICSs operation and components are often referred to as Operational Technology (OT) in contrast with usual computer systems Information Technology (IT). OT devices often use specific operating systems and network protocols, they traditionally do not provide security controls. Originally, ICSs were functioning as closed systems and had to deal with internal and accidental risks only. With the deployment of Internet technologies and the interconnection of OT systems with IT technologies, ICSs are no longer isolated systems. As a result, they are now exposed to external and malicious risks and more specifically to network threats inherited from the IT world. ICSs were never designed to face such threats and became vulnerable and prone to network attacks. Statistical studies show that the number of attacks specifically targeting ICSs is constantly rising since 2010 [2].

Intrusion Detection Systems (IDSs) were historically classified into two categories: misuse-based and anomaly-based (also known respectively as ”signature-based” and ”behavior-based”) [3]. Misuse-based IDS rely on specific recognition of malicious actions and are therefore able to detect patterns of previously known attacks. This category stands alone in the IT world with solutions such as Nessus or SNORT. Anomaly-based IDS rely on the definition of a normal behavior of a system. Behavioral methodologies leverage the detection of unknown attacks. Yet, their major disadvantage is the high number of false positives usually generated.

A second IDS classification considers the sources for the data collection which can either be extracted from host components (Host IDS) or from network traffic (Network IDS).

In our research we will study detection of network-based attacks which target the physical process integrity. Moreover, we are interested in attacks which do not violate network protocols and send legitimate controls making them undetectable by signature based IDS. Therefore this work is centered on behavioral detection and concerns NIDS only.

In the next section we present an illustrative use case, followed by an attack typology in Section III. We continue with a short state of the art and we present the challenges of this work and some ideas for the formal modeling.

II. Physical process and system characteristics

In complex ICSs several control objectives coexist in order to enforce a global correct behavior of the process. A full centralized control is ineffective or even impossible for real-life complex ICSs. Therefore a distributed and hierarchical control strategy is currently employed. Lower level control objectives such as motor speed or position control are monitored by means of *local loops*. Then, higher level objectives like trajectory tracking are achieved by the synchronization of local loops via a higher level controller. Consequently, a local loop is the elementary building block of a complex system. It is constituted by a single controller that periodically acquires local sensor data and computes control for the local actuators. To optimize the response time, where possible, local sensors and actuators are directly wired to controller inputs and outputs. That way the only networked component of a local loop remains the controller. In a distributed control system security properties may be local, like insuring the stability of a motor speed, or global, like a maximal trajectory tracking error.

According to what is stated above, two characteristics are important in the framework of distributed control systems for intrusion detection. Firstly, sensors and actuators in local loops cannot be directly network monitored. Secondly, local and global security properties both have to be monitored, with global properties which usually cannot be deduced from local properties.

For our study we consider a classical industrial use-case presenting all the intended features: a soda bottling process flow, Figure 1. In this process several local loops are used to insure the transportation of bottles, caps, and ingredients to their intended work stations. Local loops are synchronized by higher level controllers with the purpose of a timely and regular arrival of components to their production stations. Some of the loops (conveyors and pumps) have continuous time dynamics, others (like capping or packing stations) have discrete event-driven dynamics.

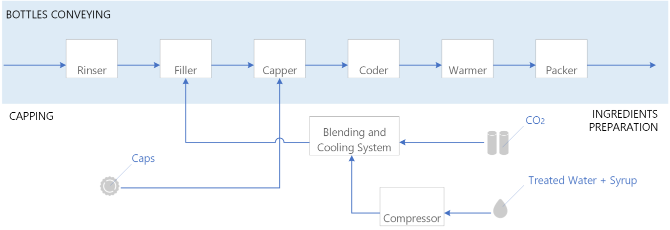

Fig. 1. Bottling process flow

III. Attack typology

We assume that the attacker has a perfect knowledge of the system, network, process and control programs and that he is able to monitor the evolution of devices. He is able to forge frames and packets that not only respect protocol specifications but also show a perfect use of address fields. Our study considers only process-oriented attacks more precisely attacks falling into one of the following two categories:
1. *Attacks on process data*; This category includes attempts to manipulate sensors or actuators values and controller internal variables or parameters. This covers sequence attacks and timing attacks.
2. *Attacks on control logic*; It concerns attempts to force transitions or state changes in controller programs.

Attacks may target local loop security properties such as stability or precision – disruption of the caps arrival rate for example – or global security properties – violation of the maximum waiting time between filling and capping operations.

IV. Related work

A rich literature exists on network-oriented IDS approach. Most of the works exploit flow regularity and communication protocol structure [4, 5]. Among process-oriented IDS, some focus on the payload of communication messages [6, 7], others consider the value and meaning of process variables [8, 9]. All the references studied until now do not consider distributed system and usually do not handle hybrid dynamics (event-driven and continuous time).

V. Detection challenges and approach

With respect to the state of the art, our project will tackle several challenges. Firstly, we will have to deal with distributed detection in a real-time environment and handle the temporal coherence of information from different IDS sensors. Another challenge concerns the IDS sensors data normalization since the considered network is hierarchical and heterogeneous, including both process buses and Ethernet TCP networks. At the monitoring level, via the controller communication interface, we will only be able to handle state variables visible in the network traffic. Furthermore, we will have to develop monitoring formalism for continuous time and hybrid systems. Last but not least we will tackle the verification of higher level controllers behavior with an input/output observation approach. We will capture information from TCP and process bus networks and compare it with reconstructed inputs/outputs according to the controllers charaterization.

As for the modeling formalism, since we aim for a cross-domain multi-objective approach, several formalisms are worth considering. For instance, among the formalisms under study we may consider : discrete continuous and hybrid Automata, Linear Temporal Logic (LTL), Metric Temporal Logic (MTL) and Signal Temporal Logic (STL), but also models derived from system diagnostic such as Bayesian networks.

The approach will be validated using the rich in material G-ICS Industrial Cybersecurity Lab [10], using physical process simulation connected to real control hardware with a hardware-in-the-loop setup.

VI. Conclusion

We present a Ph.D research project aiming for the development of a distributed intrusion detection methodology for complex industrial systems. Our research focuses on the detection of process-oriented attacks for hybrid continuous time and event-driven systems. The research is funded by a CIFRE grant between Naval Group and Inria.

References

[1] K. Stouffer and al., “Guide to Industrial Control Systems (ICS) Security,” *NIST SP 800-82*, 2014.

[2] “Threat landscape for industrial automation systems in 2019,” ICS-CERT, Tech. Rep., 2020.

[3] H. Debar, M. Dacier, and A. Wespi, “Towards a taxonomy of intrusion-detection systems,” *Computer Networks*, vol. 31, no. 8, 1999.

[4] R. R. R. Barbosa, R. Sadre, and A. Pras, “Towards periodicity based anomaly detection in SCADA networks,” in *ETFA 2012*, Krakow, Poland, 2012.

[5] N. Goldenberg and A. Wool, “Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems,” *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, 2013.

[6] M. Caselli, E. Zambon, and F. Kargl, “Sequence-aware Intrusion Detection in Industrial Control Systems,” in *CPSS’ 15*, Republic of Singapore, 2015.

[7] M.-K. Yoon and G. Ciocarlie, “Communication Pattern Monitoring: Improving the Utility of Anomaly Detection for Industrial Control Systems,” in *Proceedings 2014 Workshop on Security of Emerging Networking Technologies*. San Diego, CA: Internet Society, 2014.

[8] A. Carcano and al., “A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems,” *IEEE Trans. Ind. Inf.*, vol. 7, no. 2, 2011.

[9] S. Papa, W. Casper, and S. Nair, “A transfer function based intrusion detection system for SCADA systems,” in *HST 2012*. Waltham, MA, USA: IEEE, 2012.

[10] S. Mocanu and al., “An Open-Source Hardware-In-The-Loop Virtualization System for Cybersecurity Studies of SCADA Systems,” in *C&esar 2019*, Rennes, France, 2019.