Exploiting system model for securing CPS: the anomaly based IDS perspective

Riccardo Colelli
Department of Engineering
University of Roma Tre
Rome, Italy
colelli.riccardo@gmail.com

Stefano Panzieri
Department of Engineering
University of Roma Tre
Rome, Italy
stefano.panzieri@uniroma3.it

Federica Pascucci
Department of Engineering
University of Roma Tre
Rome, Italy
federica.pascucci@uniroma3.it

***Abstract*—Industrial Control systems traditionally achieved security by using isolation from the outside and proprietary protocols to communicate inside. This paradigm is changed with the advent of the Industrial Internet of Things that foresees flexible and interconnected systems. In this contribution, the threats coming from this new approach are analyzed and a framework for identify them is proposed. It is based on the common signature based intrusion detection system developed in the information technology domain, however, to cope with the constraints of the operation technology domain, it exploits anomaly based features. Specifically, it is able to analyze the traffic on the network at application layer by mean of deep packet inspection, parsing the information carried by the proprietary protocols. Two different topologies are adopted to cope also with legacy systems. A simple set up is considered to prove the effectiveness of the approach.**

***Index Terms*—Automation Systems, New Implementation Approaches, Industrial Informatics**

I. Introduction

Supervisory Control And Data Acquisition (SCADA) systems are used to monitor and control remotely industrial processes and critical infrastructures. The proper operating of these systems is essential for the economy of a Country and the stability of modern societies. Thus, there is the need to protect this critical infrastructures from threats.

In the last few years the convergence of Information Technology (IT) and Operation Technology (OT) exposes those systems to cyber threats: Stuxnet virus [1] represents the first attempt to stealthily disrupt an industrial control system, as well as the recent Ukraine power grid cyber attack [2].

Nowadays, the IT and the OT domains are becoming even more linked due to Industrial Internet of Things (IIoT) revolution. According to the IIoT paradigm, indeed, most of the devices in the factory (i.e., robots, sensors, actuators, Human Machine Interface - HMI) are connected and exploit new technologies, such as cloud and big data analytics. The large number of the device connected to flexible and smart network introduces new surfaces for attacks.

Several tools have been introduced in the IT domain to protect systems and to implement the most effective countermeasure reducing malicious attacks. They rely on the well-know paradigm of securing data by means of protecting Confidentiality, Integrity, and Availability (CIA). In the OT similar tools can be also applied, however, the main goal is to protect plants and critical infrastructures, so the priorities are reversed (i.e., AIC).

A common approach to identify malicious events in IT domain is represented by the Intrusion Detection System (IDS). This tool plays a key role also in the new paradigm of industry; therefore, IDS for SCADA systems gained importance [3] [4]. Most of the IDS developed for IT can be applied also in the OT domain. Snort [5] is most popular open-source packet sniffer and logger. The basic feature of Snort is to define rules (signatures) which can be used to detect a large set of attacks. Another open source tool is Suricata [6]: it shares with Snort the signature syntax. The Bro network security monitor [7] is an open-source security platform. It converts network traffic into series of events that can be analyzed using Bro scripting.

In this paper an IDS for OT domain is presented: the main contribution is related with the features analyzed to identify threats. Specifically, the proposed IDS is able to identify anomalies in the monitored process. The developed IDS protects both the transportation layer and the application level, since deep packet inspection is adopted. Two different topologies have been considered, to allow compliance with legacy system.

The proposed IDS has been developed using Scapy [8] to analyze traffic in the network. This tool allows the device to have all the features of IDS, in particular four components: event generators, event analyzers, response units and event databases [9]. The industrial protocol considered in this work is a device-independent and fieldbus-independent interface the Automation Device Specification (ADS), used in TwinCAT Beckhoff Systems [10]. It offers more flexibility and interoperability than protocol like Modbus, and matches the needs coming from industrial Internet of Things (IoT) [11]. Although Scapy is able to decode packets of many protocols, however, it does not provide support for ADS, to this end a specific parser has been also developed.

This paper presents some preliminary results obtained applying the proposed IDS-anomaly based approach: thus, the effort is mainly on the implementation of this IDS using a specific industrial protocol, rather than on the evaluation of the robustness of the methodology. The paper is organized as follows. The proposed method is depicted in section II, the implementation and the validation is described in section III,

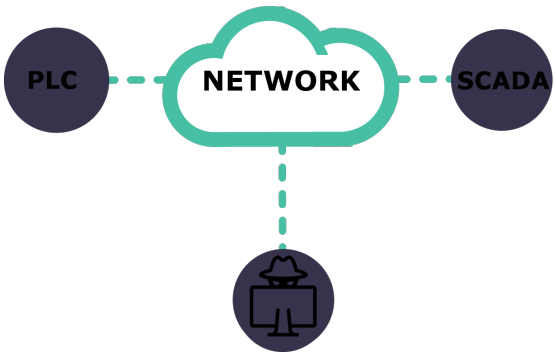


Figure 1. Network.

some conclusive remarks are proposed in section IV.

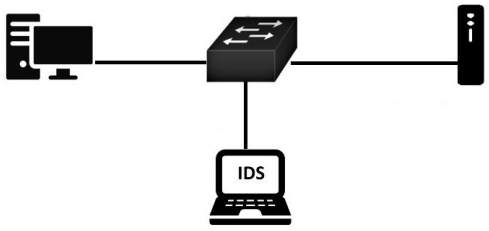
II. Proposed Method

The securing strategy proposed in this contribution addresses the protection of data exchanged between devices devoted to real-time control (e.g., Programmable Logic Controller - PLC) and SCADA system in an industrial set up. Specifically, the scenario foresees by the IIoT paradigm is investigated.

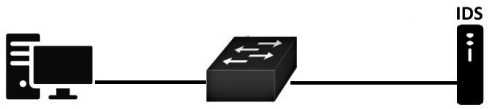
As shown in Fig. 1, two main actors have been considered: a real-time device (a PLC) and a SCADA system. The registers in the PLC are directly connected to actuators and sensors on the field-bus. The PLC forwards the information to the SCADA system, which monitors the process and provides the operator with a graphical interface. The PLC and the SCADA system are connected by network services, that bring vulnerabilities and weaknesses. Cyber-attacks on the communication channel are investigated: to this end, an attacker is supposed able to gain access to the network so to discover the weaknesses of the controlled process.

To protect the communication channel, an IDS both signature and anomaly based is developed. The first one behaves like an anti-virus software: some rules are established and a violation of them produces an alert. The IDS is able to analyze the packets in the network: using the signatures, the IDS detects the threats commonly revealed in the IT domain.

If an attack does not violate any rules, this kind of IDS cannot detect the intrusion, since rules are established according to known attacks. To overcome these limits, the proposed IDS is able to parser the industrial protocol using deep packet inspection approach. Thus, the payload of network packet is analyzed at application level to discover anomalies in the sequence of commands provided by the SCADA system to the PLC. To this end, the IDS knows the nominal behavior of the system and is able to detect deviations: therefore, it can detect new threats. Furthermore, it exploits a database to collect alerts. Specifically, the IDS feeds three different tables. The first one stores attacks on network protocol TCP/IP, e.g. port scan, man-in-the-middle, denial of service identified using the signature approach. The second one collects commands



(a) IDS network based.



(b) IDS host based.

Figure 2. Topologies of the IDS.

that are exchanged between the devices. Finally, third table gathers anomalies obtained from analysis on the behavior of the system according to the data in the second table.

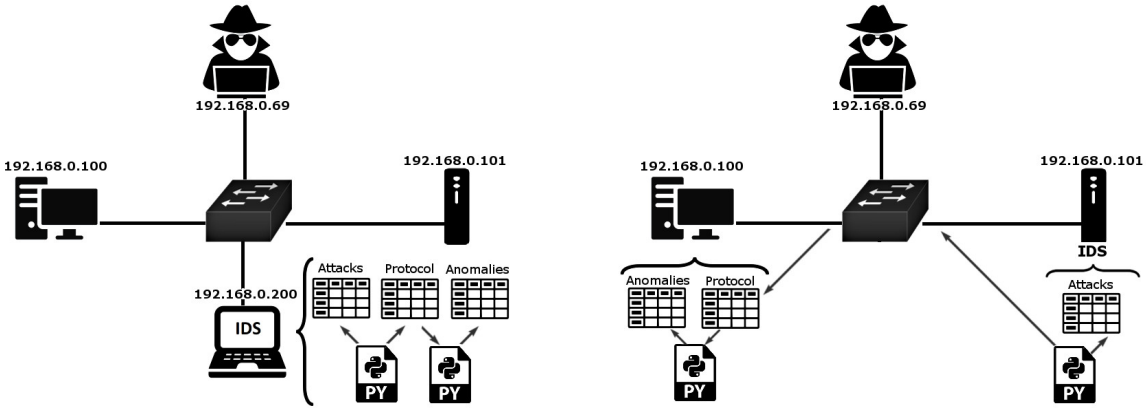
Two different topologies have been used to implement the proposed approach: the *network-based* and the *host-based*, as shown in Fig. 2. The first one is able to cope with legacy system, while the second one handles the new IIoT devices.

A. IDS network based

The first implementation of the proposed IDS relies on mirroring techniques implemented on most of the commercial switches and routers. Thus, the IDS is connected to the monitoring port and all the traffic of the network is analyzed.

The IDS is implemented exploiting the packet manipulation tool Scapy. Based on Nmap and written in Python, Scapy is able to analyze traffic on the network and send packets to the other devices. It analyzes all the traffic between the SCADA system and the PLC. The IDS is placed on the network in order to identify possible malicious attack and it contains inside all the tables previously described. In this approach, the Maria DB is used to implement the IDS database.

When IDS identifies an intrusion, it communicates promptly to the monitoring network operator in the control room. IDS network-based has a HMI to communicate network status to the operator. The interface reads the information stored in the database by the IDS network analyzer according to the different tables. Network HMI allows to view attacks from the network level that are reported in the first table (e.g., Port Scan and ARP poisoning aimed to eavesdropping). Furthermore,



(a) Database in the IDS network based.

(b) Database in the IDS host based.

Figure 3. Database configurations.

interface has a field for viewing the variables monitored, in this way there is a redundancy with the main HMI in the SCADA in order to guarantee the robustness of the system under attack. Concerning the third table, as mentioned above, it contains notification of a variable with an anomalous value. To build this table, a Python script able to parser the ADS protocol by Beckhoff TwinCAT has been developed. Finally, the anomaly based IDS runs together with the IDS analyzer and compares values from the second tables with the model of the process in order to notify that intrusion has occurred.

B. IDS host based

The second topology, namely IDS host-based, exploits the features of the IIoT provided by the embedded PC. These devices, which are also able to perform real-time tasks, are equipped with a full operating system (e.g., Windows OS).

According to the host based approach, the IDS is implemented on the embedded PC. In this way, the IDS monitors only the flows of data between the SCADA system and the embedded PC. All the strategies for identifying an intrusion are moved into the device to be monitored, i.e., the real-time device. This set-up foresees the physical separation between signature based IDS and anomaly based IDS. Specifically, the signature based IDS is implemented on the real-time device, while the behavior analyzer is moved to the main SCADA. This design provides two major advantages. The first one is related to the computational load: the IDS, indeed, is implemented on real-time devices devoted to process control, that cannot be overloaded. The second one is related to flexibility of the database, that can be implemented as a remote database in the industrial cloud.

III. VALIDATION

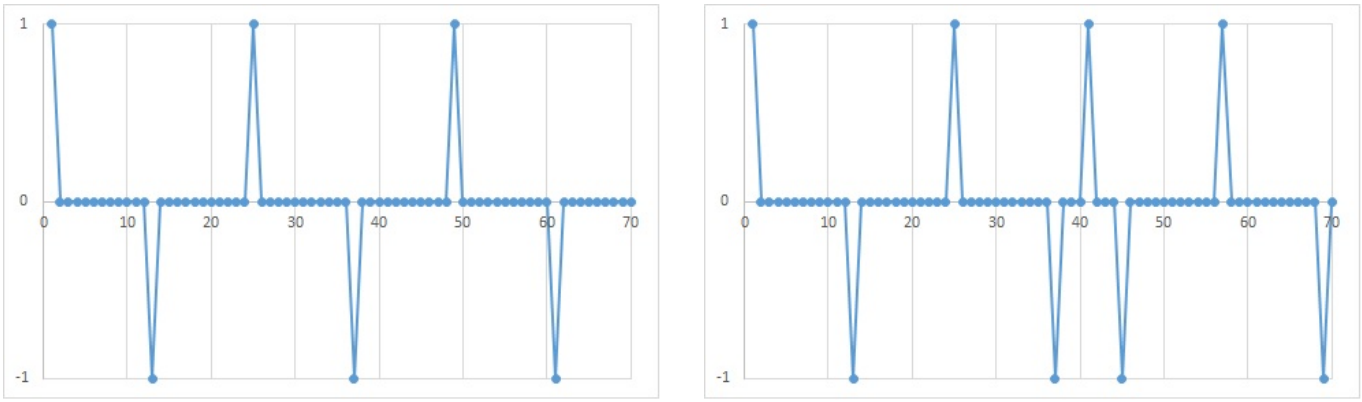
To prove the effectiveness of the approach, both the proposed anomaly based IDSs has been tested. Here, only the results obtained using the host based approach has been reported.

In this framework, the real-time device is represented by CX2030 and communicate with the SCADA system according to the Automation Device Specification (ADS). The protocol developed within the TwinCAT architecture communicate exploiting UDP/IP or TCP/IP stacks as transport layer. SCADA and real-time device are connected by means of a switch to the network.

The embedded PC is connected to a virtual system, that emulates a simple Automated Guided Vehicle (AGV). The AGV navigates between two target points on a straight path. When the AGV reaches a target point, it stops and go back to the other one.

An attacker is connected to the switch, as shown in Fig. 3. To test the proposed system, the malicious agent proposes two different attacks. During the first one, the transportation layer is targeted: an ARP poisoning is performed using the Kali Linux tool named Ettercap. The attacker captures data on the network by associating his MAC address with the IP address of the target. The signature based IDS analyzer is able to detect the ARP poisoning by comparing the MAC address with the corresponding IP address. This solution, that can be not effective in the IT domain, is successful on the industrial network, since the topology is static. The second attack targets the application layer. The attacker performs a two stages attack. At the beginning, he/she only knows the machines to be targeted and eavesdrops the data exchanged. By parsing the protocol, the attacker is able to form a rough idea on the system attacked (i.e., the nominal behavior, the expected values, etc) and tries to perform a more complex attack by modifying the data in the packet and by disrupting the process.

In the IDS, a parser for ADS has been implemented to deeply inspect the packets and analyze them at application layer. Since Scapy does not support for ADS, a proper parser has been also implemented. The anomaly based IDS grabs the control variables and store them in the protocol table (i.e., the sensor output that detect the AGV on the target points). By comparing the nominal operating mode with respect to the actual one, it is possible to detect anomalies. In Fig. 4 the nominal behavior and the disrupted one are presented.



(a) Nominal behavior.

(b) Disrupted behavior.

Figure 4. AGV behavior.

Under normal operating conditions, the AGV reaches the targets point regularly. When the system is attacked, the signals are faked: specifically the AGV seems to reach a target point, so the control algorithm send it back to the other one. The IDS identify the behavior mismatch and set an alarm in the alert table.

IV. Conclusion

In this contribution, an IDS for industrial control system is presented: the objective of the IDS is to exploit IDS signature based to cope with the threats in IT domain and develops specific anomaly based IDS in the OT domain by deeply inspecting the protocol used to exchange data in the industrial control system. To this aim, a specific parser for industrial protocols is developed and a baseline for the nominal behavior of the plant is formed. A database is continuously update to collect data about the process, information on the attacks and alerts on faulty behavior. The proposed approach copes with the requirements of legacy system and the IIoT paradigm, since two different topologies can be adopted to implement it.

The proposed approach has been implemented over Beckhoff CX2030 and a SCADA system, controlling the motion of a virtual AGV. The obtained results are encouraged, since the IDS does not introduce significant delay in the system and it is able to improve the awareness of the system.

Although the results are promising, there is still room for improvements. The IDS is supposed inside the operating domain: in an industrial set up, indeed, the a firewall protect the perimeter, so the IDS analyzes all the packets that have passed the firewall. A more efficient approach would be obtained by inserting in the network two IDSs, one before and the other one after the firewall, to get insights on how an attack starts and where a threat comes from.

The Database is designed to be flexible: the tables that are filled by the IDS can be local or remote. This allows to implement the Database either in a local machine or directly in the cloud. In future development the proposed solution can be tested using some public database.

The anomalies considered in this work are simple, however, more complex approach can be adopted by exploiting the model of the plant. In this way, the IDS would be able to detect faults and attacks, improving the maintenance schedule of the system.

References

[1] Antiy Labs, “Report on the Worm Stuxnet’s Attack”, Anity CERT, October 2010

[2] “Analysis of the Cyber Attack on the Ukrainian Power Grid”, Defense Use Case, March 2016

[3] J. Verba and M. Milvich, “Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS),” 2008 IEEE Conference on Technologies for Homeland Security, 2008, Pages 469 - 473

[4] K. Wong, C. Dillabaugh, N. Seddigh and B. Nandy, “Enhancing Suricata intrusion detection system for cyber security in SCADA networks” 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), 2017

[5] M. Roesch, “SNORT - Lightweight Intrusion Detection for Networks,” in Proceedings of LISA’99: 13th System Administration Conference, Seattle, Washington, USA, 1999.

[6] “Suricata Intrustion Detection System,” [Online]. Available: https://suricata-ids.org/. (Accessed 11/06/2018).

[7] “The Bro Network Security Monitor,” [Online]. Available: https://www.bro.org/. (Accessed 11/06/2018).

[8] “Scapy,” [Online]. https://scapy.readthedocs.io/en/latest/ (Accessed 11/06/2018)

[9] I. Corona, G. Giacinto and F. Roli, “Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues” Information Sciences 239, 201-225, 2013

[10] https://infosys.beckhoff.com Accessed 07/06/2018

[11] G. Falco, C. Caldera and H. Shrobe, “IoT Cybersecurity Risk Modeling for SCADA Systems,” IEEE Internet of Things Journal 2018