Smart Behavioural Filter for SCADA Network

Giovanni Corbò, Chiara Foglietta(✉), Cosimo Palazzo, and Stefano Panzieri

University "Roma TRE", Via della Vasca Navale 79, 00146 Rome, Italy
corbo.giovanni@gmail.com,
{chiara.foglietta,cosimo.palazzo,stefano.panzieri}@uniroma3.it

Abstract. Industrial Control Systems (ICS) are jeopardized from a large set of threat vectors, which exploit their vulnerabilities in order to impact the physical Critical Infrastructures they control. The Information Technology (IT) classical approach to cyber attacks can not be applied to ICS due to their extreme differences from main priorities to resource constrains. Therefore, innovative approaches and equipment must be developed in order to suit with ICS world.

In this paper, a Smart Behavioural Filter (SBF) for the PLCs/RTUs is proposed aiming to secure the PLC/RTU itself against logic attacks, that are stealth for other more classical security approaches. Those logic attacks are usually anomaly behaviours, for instance a large number of open/close commands towards a valve. This smart field equipment can communicate with other equipment like itself in order to react in short time to cyber attacks and increase the resilience of the physical system. It can also generate alarms for the local Intrusion Detection System (IDS) The proposed equipment has been developed and validated in a real test-bed within the FP7 CockpitCI project. The results are promising.

Keywords: Industrial control systems · Security · Logic filtering · Redundancy

1 Introduction

Geographically distributed physical processes are continuously monitored and controlled by means of a SCADA system. An important set of those physical systems is usually defined as critical infrastructures, e.g., power grids, water pipelines and transport networks. Nowadays, the SCADA systems faced new challenges due to the increase of interconnected devices and due to the use of standard hardware, software and network.

SCADA systems are usually composed of a set of networked devices, such as sensors, actuators, controllers and communication equipment. The SCADA server (also called Master Terminal Unit - MTU) gathers real-time data from Remote Terminal Units (RTUs) and issues control commands (i.e., open or close electrical switches) towards field devices to control the physical process. Due to the cyber-physical interaction, a cyber incidence can have a direct effect on the physical world, as demonstrated by the Stuxnet worm attack that turned

L.A. Maglaras et al. (Eds.): INISCOM 2016, LNICST 188, pp. 101–110, 2017.
DOI: 10.1007/978-3-319-52569-3_9

off a centrifuges' control system in a nuclear plant [1]. Stuxnet provided proof-of-concept and demonstrated the feasibility of a cyber attack to change the physical processes. Highly-skilled attackers have the potential to be the most harmful, causing a loss of observability, controllability or eventually the loss of power in the physical system. In this paper, a highly-skilled attacker is a person with multiple capabilities: the ability to stealthy penetrate within a telecommunication network and the ability to discover the physical process controlled by the network.

In [2], the various type of attacks on SCADA systems have been grouped into network protocol and application protocol attacks. In the network protocol attacks, the hacker exploits weak points of network protocols, such as Modbus TCP/IP, that have a number of serious vulnerabilities [3]. The common types of those attacks are Denial of Service (DoS), scan and host discovery. Application protocol attacks can cause damage to field devices by sending out improper commands, because authentication or cryptographic mechanisms are not supported. In general, application protocol attacks use unconventional commands at irregular interval, substituting the regular and predictable sets of commands used for communication between SCADA servers and field devices. In both cases, these attacks are preceded by some steps of information gathering devoted to finding vulnerability security flaws in the network.

In this paper, we consider a highly-skilled attacker able to gain the access of a SCADA network and to disrupt the physical process before the intrusion is detected. A false logic attack, as in [4,5], is invisible to Intrusion Detection System (IDS) for SCADA networks, because it uses well-formed packets with a content that is allowed even if a logic constraint is violated.

1.1 Contributions

The contribution of this paper is twofold. Although an host-based intrusion detection system for anomaly behaviour is not new, its use within a SCADA network is still a research area that is far from being completely explored. The appliance presented in this paper is a behavioural filter that has to be inserted between each Remote Terminal Unit (RTU) or Programmable Logic Controller (PLC) and the field network in order to intercept packets carrying incorrect or dangerous commands.

Second, the appliance (Smart Behavioural Filter - SBF) communicates with other similar appliances and with a possible local Intrusion Detection System (IDS) through an additional secure channel in order to generate another invisible network for transmitting/receiving alert messages.

1.2 Paper Organization

The paper is organized as follows: Sect. 2 surveys the literature of the appliances for anomaly behaviour; in Sect. 3 the ecosystem made of several smart appliances in a SCADA network is described in order to provide an overall picture of the main functionalities; in Sect. 4 the Smart Behavioural Filter (SBF) is detailed

in terms of functionalities and design; the implementation and the first results are presented in Sect. 5; finally, conclusions and future works are in Sect. 6.

2 Related Works

A SCADA system is considered a critical control system since it monitors and controls the performance and availability of other critical infrastructures, such as transport systems, energy suppliers, water treatment systems or communication systems.

SCADA networks are vulnerable to threats as the traditional IT networks. Moreover, SCADA networks have different risk management priorities: in SCADA network, availability is preferred to confidentiality, while in IT systems the priorities are turned around. This makes difficult implement traditional IT solutions for security within SCADA networks [6].

During the last years, several defence approaches have been studied. One of the first recommendation is to segment the SCADA network from the enterprise one using suitable firewalls in order to protect PLCs/RTUs from unauthorized requests that originate from outside the field. [7] In time-critical systems, firewalls must be carefully introduced for reducing additional packet latency. Filtering unwanted traffic by means of a firewall can increase the network performances [8].

Firewall are classified into two categories: Packet filtering and application firewall. Packet filtering has been recommended as an effective way to protect field devices from network protocol attacks. This appliance monitors incoming and outgoing packets and allows them to route or drop based on filtering rules using layer three and four on OSI model [2].

An application firewall (or proxy server) is placed between a client application and a server, acting as an intermediary never allowing a direct connection between them. [9] The application firewall adds the capability of examining specific application traffic, such as FTP services, OPC servers or others. Coverage for SCADA applications is limited and performance impact is typically greater than other firewall types. The benefits of using this method are important because the application firewall is the only thing exposed to untrusted traffic. The disadvantage of the approach is that it must be tuned to each application allowed [10].

In this paper, we present an advanced filter for detecting false logic attacks. A false attack [4] takes into account two different approaches:

- False data values, where the attacker changes the data coming from sensors, see the literature related to false data injection [11];
- False logic commands, where the attacker changes the logic of the control commands. This type of attack is the main focus of this paper.

In [4,5], the feasibility of a false logic attack is modelled considering the case of two valves that can be opened or closed. Two logic constrains are considered: (1) they cannot be both in open state, and (2) valve 1 should be opened before valve 2. The results of this paper demonstrates how a traditional Intrusion

Detection System (IDS) is not able to effectively protect the physical process. The Smart Behavioural Filter (SBF) is able to detect the violation of a logic constraint that can been implemented as a rule.

In the following Section, the ecosystem is detailed. The smart ecosystem is realized using a set of Smart Behavioural Filters (SBFs) placed just in front of the PLCs that can interact between them and with a local IDS using an additional radio-frequency channel.

3 Smart Ecosystem

In Fig. 1, the architecture of the smart ecosystem is depicted. The Smart Behavioural Filter filters the commands coming from the SCADA system through a set of rules and also the information coming from the other elements of the smart ecosystems. The SBF has three channel:

1. A legacy channel for receiving/sending command packets from and to the SCADA system;
2. An additional channel for communicating with the PLC/RTU in order to send authorized commands;
3. An additional channel for exchanging messages with the other SBFs or with an IDS. This channel has been realised using radio-frequency module.

The aim of this ecosystem is a local and fast reaction to advanced cyber attacks. The SBF that intercepts a false logic attack can block the commands and then is able to send an alarm to the IDS and to other near SBFs using the radio frequency. In this way, the SBF can increase the alert level and therefore augment the security controls in event of cyber attacks to other near facilities.

4 Smart Behavioural Filter (SBF)

Traditional RTUs/PLCs send to the SCADA server the actual data coming from sensors, receive commands to be translated for the actuators and execute fast and real time control strategies related to the physical process. The difference between a PLC and an RTU is usually hard to find especially because their functionalities overlap with each other. In this paper we use both the terms RTU and PLC for identifying a remote controller which communicate with the SCADA server. The PLC is able to detect the disconnection of a sensor or an actuators.

The Smart Behavioural Filter (SBF) wants to add a new class of logical errors, detected directly by the PLC. Those errors are usually malicious cyber attacks but can also be generated from unintentional commands coming from an operator. These false logic errors are, among the others: contradictory instructions, dangerous or out of the normal operating cycle, or abnormal sequence of operations.

The Smart Behavioural Filter (SBF) intends to create a further security element for industrial control systems. This new appliance element was created

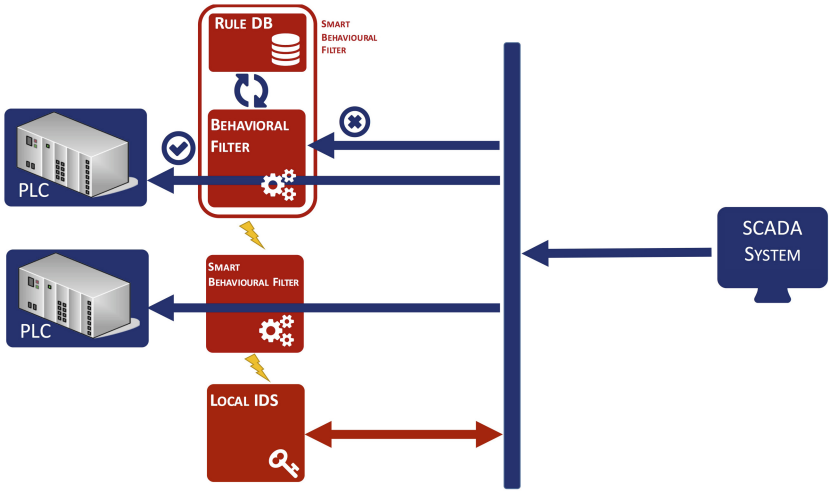

Fig. 1. System diagram of the smart ecosystem, where blue icons represent the legacy SCADA system and the red ones represent the elements of the smart ecosystem.Color figure online

as a security system at application level which is able to work on industrial communication protocols. The technological solutions implemented in the SBF are mostly known and simple to apply but the smart combination allows us to get a very interesting and innovative element in the context of industrial security.

The SBF, in Fig. 2, is made of two main modes: the passive and the reactive one. The first concept is related to the filtering action, mainly related to logical constraints. The second one is related to the response and mitigation action: an SBF can cooperate with other SBFs in event of an external attacks, and can eventually change its operating mode until the complete isolation from the external world.

In order to filter packets, PLC registers and coils have been mirrored within the SBF in order to understand the impact of the received commands. The first important cyber security feature of SBF concerns the capability to create a kind of SandBox (a virtual controlled environment) that replicates the information system of a PLC. In those circumstances, an hypothetical intruder, which enters into the SCADA network, believes he is changing the registers/coils value into the PLC performing successfully the cyber attack but without have any effect on system thanks to the SBF. The Ethernet module of the PLC is securely connected to the Ethernet module of the SBF, that substitute the PLC port. In this way, the SBF can guarantee to be undetectable to an intruder, who beliefs to communicate with the original PLC.

SBF implements a rule-based filtering, able to understand the effects of specific commands thanks to a set of rules. Those rules have been hard-wired into the SBF starting from the knowledge of the physical processes. For a Medium

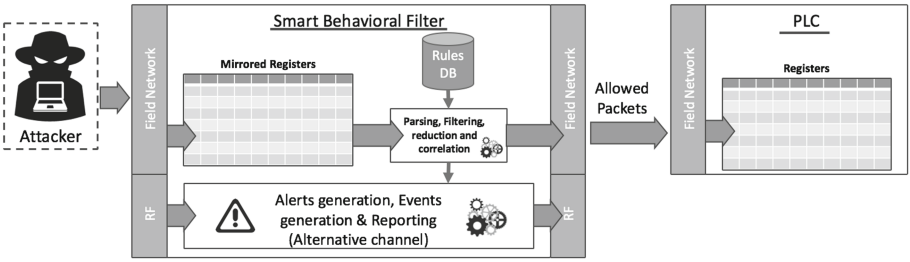

Fig. 2. Diagram of the Smart Behavioural Filter

Voltage power grid, the SCADA system reconfigures the physical network after a permanent failure, in well-define scheme. Therefore, the reconfiguration is a sequence of commands sent from the SCADA control system to the PLCs connecting the electrical switches. The possible reconfiguration procedures are modelled within the set of possible rules inside the SBF. The SBF is an application-level behavioural filtering performing an anomaly detection highly specialized in its own operative context.

In order to be an active appliance, each SBF is equipped with its own Radio Frequency (RF) Module able to create a mesh-network between all the PLCs/RTUs with SBFs and with a possible local IDS. The radio frequency module has a limit due to the distance of the transmission channel. This RF element, in combination with the SBF, establishes a redundant wireless network between PLCs/RTUs of the same system and then a further preferential (or alternative) communication channel where transmits system alerts.

The system alerts can eventually activate specific rules that increase the security status of the PLC. The security status can require an higher level of authentication in performing specific commands. In the worst case, the PLC can be isolated from outside world for a limited amount of time in order to avoid a more dangerous situation and preserve the physical process actuators.

The additional radio frequency channel creates a new security issue, but it is invisible to a hacker which penetrates in the classical telecommunication network. The additional channel can exploit secure communications, such as encryption, due to the small dimension of the exchanged messages.

Briefly summarizing, an SBF is able to:

1. Mirror the PLC registers to deceive the intruder;
2. Recognize false logic events or sequence of events;
3. Alert the other closest SBFs and the eventual local IDS;
4. Change its security status in accordance with a pre-set strategy.

Another feature of the SBF is the undetectability and the transparency at the communication level and for a malicious attacker. In the following section the implementation and some results are explained.

5 Implementation and First Results

In order to implement the features described in the previous section, we need a platform that could:

- Receive commands from the field network
- Reconstruct the instructions received
- Filter through the rules' instructions
- Send the filtered commands to the connected PLC
- Send and receive alarm messages to/from the other SBFs
- React to cyber attacks through a set of fixed rules

A standard RTU/PLC has a modular design, and usually consists of a Power Supply, a CPU, and an Input/output card. The actual and initial implementation of the SBF is realized on hardware using a microcomputer such as Raspberry PI, as in Fig. 3.

In order to test the SBF, we consider as PLC a Schneider Electric Modicon M340 [12] with Modbus TCP/IP interface. The SBF receives packets and it is invisible to the downstream PLC and also to the rest of the control network. The SBF is advanced network card with additional processing capabilities.

Fig. 3. Implementation of the SBF using a Raspberry Pi microcomputer. Two USB ports are used for exchanging commands with the PLC (with a network adapter) and the other SBF, using an USB radio frequency module.

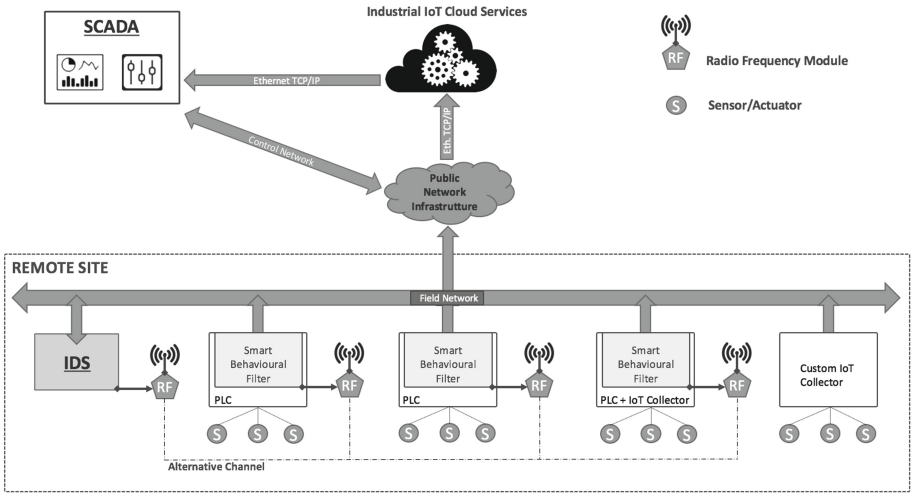

Fig. 4. Future development and possible integration with Internet of Things (IoTs)

The SBF has been integrated within the existing Roma TRE testbed [13]. The testbed is made of a SCADA server, a PLC and an IDS. Specifically, the IDS has been given the ability to communicate through the radio frequency (RF) protocol with the mesh network created by SBFs. This feature improves globally and locally the situational awareness. A soon as the IDS recognizes a potential threat it warns the control room and sends a broadcast alert message to the radio frequency network. Depending on the danger degree, the SBF can automatically reconfigure themselves in an attempt to mitigate the threat.

The results are promising: the Smart PLC (PLC and SBF, together) succeeds to recognize the dangerous instructions and sends an alert message to the control room. At the same time provides information on the incident to the other reachable Smart PLC that are reconfigured in an appropriate way and, in case it is required, turn over the alert message to the control room. The IDS is able to communicate the details of an attack to the network of Smart PLC which reconfigures itself, thus obtaining an automatic response to the ongoing threat.

Depending on the type of attack will also change response policies. Smart PLCs will then be able to decide and implement the best strategy in each case.

The SBF has been implemented and validated within the FP7 European CockpitCI project (www.cockpitci.eu).

6 Conclusions and Ongoing Works

In this paper, we present a Smart Behavioural Filter (SBF) able to detect and block commands that are anomalous from a logic point of view. This anomalous behaviour can be interpreted as a very specific cyber attack performed by a high-skilled attacker.

The SBF is a passive firewall and is also a local reaction module for mitigating risk of cyber attacks. In order to exchange securely information, the SBF has an additional and invisible radio frequency channel among SBFs and the IDS.

The SBF can be improved considering rules that can be modified or generated through an on-line training of the physical system.

Actual works are more related to the industrial Internet of Things (IoTs), see Fig. 4. The SBF can also be applied in the modern industrial system. This is possible integrating a further module which is entrusted with the task of IoT Connector. This connector enables the outsourcing of the data coming from industrial sensors to collect and analyse them thanks to Industrial Cloud IoT. Therefore, the SCADA system transfers some functionalities to the Industrial Cloud IoT to improve performances, decrease start-up plant costs and enhance data mining.

Acknowledgement. The research paper is partially supported by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 700581 (ATENA - Advanced Tools to Assess and Mitigate the Criticality of ICT Components and Their Dependencies over Critical Infrastructures)

References

1. Kushner, D.: The real story of stuxnet. IEEE Spectr. **50**, 48–53 (2013)
2. Kang, D.H., Kim, B.K., Na, J.C.: Cyber threats and defence approaches in SCADA systems. In: 16th International Conference on Advanced Communication Technology, pp. 324–327, February 2014
3. Huitsing, P., Chandia, R., Papa, M., Shenoi, S.: Attack taxonomies for the modbus protocols. Int. J. Crit. Infrastruct. Prot. **1**, 37–44 (2008)
4. Li, W., Xie, L., Liu, D., Wang, Z.: False logic attacks on SCADA control system. In: Services Computing Conference (APSCC), 2014 Asia-Pacific, pp. 136–140, December 2014
5. Li, W., Xie, L., Deng, Z., Wang, Z.: False sequential logic attack on SCADA system and its physical impact analysis. Comput. Secur. **58**, 149–159 (2016)
6. Alcaraz, C., Fernandez, G., Roman, R., Balastegui, A., Lopez, J.: Secure management of SCADA networks. Novatica, New Trends Netw. Manage. **9**, 22–28 (2008)
7. Nivethan, J., Papa, M.: On the use of open-source firewalls in ICS/SCADA systems. Inf. Secur. J. A Global Perspect. **25**, 1–11 (2016)
8. Sheth, C., Thakker, R.: Performance evaluation and comparative analysis of network firewalls. In: 2011 International Conference on Devices and Communications (ICDeCom), pp. 1–5, February 2011
9. Aziz, M.Z.A., Ibrahim, M.Y., Omar, A.M., Rahman, R.A., Zan, M.M.M., Yusof, M.I.: Performance analysis of application layer firewall. In: 2012 IEEE Symposium on Wireless Technology and Applications (ISWTA), pp. 182–186, September 2012
10. Mahan, R.E., Fluckiger, J.D., Clements, S.L., Tews, C.W., Burnette, J.R., Goranson, C.A., Kirkham, H.: Secure data transfer guidance for industrial control and SCADA systems. Pacific Northwest National Laboratory (2011)
11. Hug, G., Giampapa, J.A.: Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans. Smart Grid **3**, 1362–1370 (2012)

12. Modicon M340 - Schneider Electric
13. Di Pietro, A., Foglietta, C., Palmieri, S., Panzieri, S.: Assessing the impact of cyber attacks on interdependent physical systems. In: Butts, J., Shenoi, S. (eds.) ICCIP 2013. IAICT, vol. 417, pp. 215–227. Springer, Heidelberg (2013). doi:10.1007/978-3-642-45330-4_15