Research Article
Volume 11:9, 2022

Advances in Robotics & Automation

ISSN: 2168-9695 **Open Access**

A Novel Cybersecurity System for the SCADA Protection: ASRO

Andrea Mangiameli[1]*, Lacava G[2] and Martinelli F[2]

[1]*Master of Science Cybersecurity, University of Pisa, Pisa PI, Italy*
[2]*National Research Council, Institute of Informatics and Telematics, Italy*

Abstract

SCADA security is the practice of protecting the supervisory control and data acquisition (SCADA) networks responsible for the increasingly remote management of essential services such as water, natural gas, electricity and transport. In general, these networks connect a very large and heterogeneous number of devices, from simple sensors to complex machines such as 6-axis robots. The cyber-attacks documented in recent years on SCADA infrastructures (e.g. Stuxnet, Shamoon, Havex) have made us realise the importance of protecting these assets.

To date, the defense practices of such systems operate according to standard response protocols such as:

- The passive or active analysis of network traffic;
- The adoption of defence measures via anti-malware;
- Access control and impediment for unaccepted hosts or profiles;
- Partial business continuity in the event of a threat or attack.

What we propose with our work is an intelligent emergency response system (ASRO -Autonomous Smart Response Operator) that allows the same measures to be taken as would be taken by an operator, adapting to the type of threat or attack in progress. This makes it possible to:

- Take the same measures as other devices used in the industry;
- Perform a low-level analysis of the host or host network's internal processes;
- Carry out a remedial action proportionate to the offence, guaranteeing business continuity.

Keywords: SCADA • Cyber-security • System defense countermeasure

Introduction

Threats to utility security have been known for decades. Unsecured computer systems can lead to catastrophic disruptions, disclosure of sensitive information, and fraud.

The use of interconnected microprocessors in industrial systems has grown exponentially over the last decade. In this regard, programmable logic controllers (PLCs) and distributed control systems (DCSs) have been popular for years for industrial process control, the latter now moving towards intelligent electronic devices (IEDs) [1-3]. The problem is that their connection networks have also grown and with them the risk of cyber-attacks has increased. The issue of security has been present for many years, but only recently have organizations been raising the awareness of the engineering community towards these issues.

***Address for Correspondence:** Andrea Mangiameli, Master of Science Cybersecurity, University of Pisa, Pisa PI, Italy, E-mail: andrea.mangiameli@protonmail.com*

Date of Submission: 01 September, 2020, Manuscript No: ara-22-76207; **Editor assigned:** 03 September, 2020, PreQC No: P-76207; **Reviewed:** 18 September, 2022, QC No: Q-76207; **Revised:** 23 September, 2022, Manuscript No: R-76207; **Published:** 30 September, 2022, DOI: 10.37421/2168-9695.2022.11.233

A potential cyber threat to supervisory control and data acquisition (SCADA) systems, ranging from computer system to power system aspects, has been recognized [4,5].

The ever-increasing power of the Internet facilitates even simultaneous attacks on critical infrastructures, from locations that may be different. The maximum impact of an attack is if it gains access to the SCADA system by launching control of the system and with actions that can cause catastrophic damage.

In this work, we aim to present a device to improve the analysis of and response to security threats currently present in SCADA systems used in the management of critical infrastructures. Below we will present the experimental analysis performed for the validation of the ASRO system, presenting the results in terms of performance.

Materials and Methods

The advent of the Internet and the use of Ethernet networks have meant that the traditional connection between devices, which was done in a traditional manner using proprietary technologies, has been superseded.

This has created less isolation and protection from a computer security point of view. To better understand the threats, there must be an awareness of the use and characteristics of the devices that make up such networks in the systems designed to protect them. The connection between corporate networks is realized through the use of hubs, switches and routers from a physical point of view, while from a virtual point of view, the user can access them via intranets created ad hoc or via virtual private networks (VPN), effectively expanding the network of interconnected devices.

For this motive, guidelines and regulations have been developed that describe issues specifically related to SCADA security [6].

In the context of SCADA systems, the importance of the continuity of system operation is always emphasized, e.g. the supply of electricity. Therefore, in addition to guaranteeing CIA properties (Confidentiality, Integrity and Availability) [7], a look is taken at the operational context of such systems [8].

In any case, one could see the importance of the human factor on the success of attacks on critical infrastructures or the leakage of sensitive information from organizations and companies. For instance, an intrusion into the SCADA systems of a global chemical company reportedly occurred where a disgruntled former employee was allegedly trying to disable the plant's conveyor control, material storage, and chemical operating systems but was caught by a programmer happening to notice unusual activity [9]. To counter threats beyond the systems assessment phase, where in Ten C, et al. [4], Cherdantseva Y. et al [6], Sommestad T. et al [10] and Bastow M D [11] an implementation model was proposed to be incisive and not to neglect both the physical part of the systems and their virtual management or Yang Y, et al. [12] and Zhao, Zhiheng and Guo Chen [13] where the authors show some types of cyber-attack patterns related to smart grids and methods to counter them. They rely on systems and devices that operate the passive and active defense phase of the grid and its connected infrastructure.

Lopez C, et al. [2] with regard to the problem of Bad Data Injection, identify in the literature as a countermeasure the strict management of authentication through the use of TLS and SSL protocols with SHA (secure hash algorithm) and HMAC (hash message authentication code).

On the other hand, the monitoring of network traffic, if not adequately protected, can give rise to the theft of real goods, as shown in the work of Mashima D. and Alvaro A. Cardenas [9], where malicious users managing the time series of electricity consumption managed to steal it, forcing the company to lower the prices of the good.

Another example of network traffic analysis was given in the work of Kang D, et al. [14], where a system called IndusCAP-Gate was presented, which analyses traffic by generating whitelists, filtering network traffic on the basis of which it is able to identify and block suspicious traffic.

Yasakethu S. and J. Jiang [15] introduces an IDS (Intrusion Detection System) based on machine learning algorithms and demonstrates how this system can learn information from network traffic in order to recognise threats, but without identifying their type, concentrating on predicting the risk involved.

As analyzed Today's systems operate in the following ways according to standard response protocols such as:

- The passive or active analysis of network traffic [8, 14-17];
- The adoption of defense measures via anti-malware [8];
- Access control and impediment for unaccepted hosts or profiles [2,18];
- Partial business continuity in the event of a threat or attack [5,9].

Discussion

Before moving on to the description of the experimental analysis conducted to validate our system, we provide a description below.

The operating principle of ASRO is based on the fact that it should act like a human operator in response to threats. It consists of the following three modules (Figure 1)

ASRO-Daemon: The software running inside the host, at a low level, which protects and constantly communicates its status with the other two components of the system, namely the ASRO-Box and ASRO-Cloud Service;

ASRO-Box: The physical device which, as a twin of the Daemon, makes a status request to the Daemon which, if altered, uses the Daemon as a backdoor to act as a human operator to intervene on the machine on the basis of a secret configuration file prepared upstream. This can act even if the network is isolated as it has its own independent communication system with the ASRO-RSS.

ASRO-Remote Security Server (ASRO-RSS): Like the ASRO-Box acts in the event that communication with the ASRO- Daemon or the ASRO-Box fails and orders the respondent what action to take to defend the network.

The system is therefore a triad that must always be in communication between its various components, the failure of one defines a state of emergency that instantaneously triggers active defense actions such as:

- **Containment operation:** ASRO-Daemon blocks the further exfiltration of data by creating a confidential communication channel between the ASRO-Box and the contaminated host;
- **Remedy:** ASRO-Box kills related artefacts via a secure socket channel using ASRO-Daemon as a backdoor with root privileges;
- **Detection:** Use the anti-malware countermeasure.

The use of ASRO-Daemon as a temporary backdoor allows ASRO-Box to act at a low level, interposing itself between the uncontaminated network and the contaminated one, isolating all the contaminated hosts and connecting them to it with the operations described above.

It is therefore a network within a network, scalable, which can also be implemented as a backup communication system in the event that the entire network fails and certain essential services need to communicate with each other.

As structured, therefore, the system will have the function of a gateway; the network traffic will therefore be directed to the ASRO-Box, which is connected to the Switch. The structure given to our system allows us to guarantee business continuity by leaving the network traffic unchanged while counteracting the threat.

In our analysis, we performed two types of tests:

a) A comparative test between the ASRO system and some of the best-known anti-malware systems to highlight the differences in terms of detection and response to threats;

b) An efficiency test of the ASRO system to check its response to attacks.

a) To test our system, we relied on a machine on which Windows IoT, which is widely used in industry, is installed. On it, we installed some of the most well-known anti-malware systems such as BitDefender (release August 2022), Windows Denfender (release August 2022), Avast (release August 2022) and ASRO. We subjected these defence systems to the following attack patterns (Figure 2)

- Attack n.1: BushBunny USB attack with payload in action on all the systems listed above;
- Attack n.2: Attack with malicious file downloaded from test e-mail

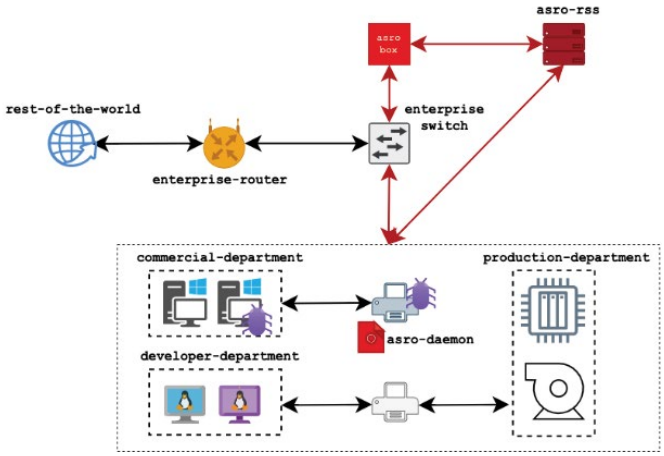

Figure 1. Modules of ASRO system.

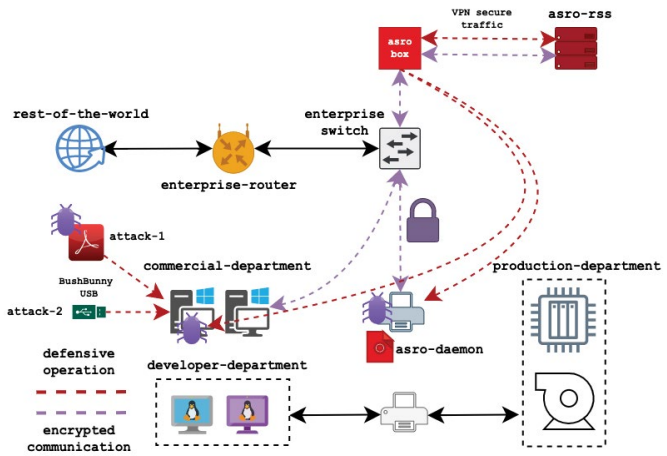

Figure 2. Description of attack models (Attack n.1 and Attack n.2).

accounts.

We have analysed these two cases in detail in order to compare them in an operational test of systems in use today in industrial realities.

b) While to test the performance of our system in terms of effectiveness against real threats, we used the following components:

- VIM 9.0 development environment;
- ARM board of the Arduino Portenta SOM type with Max Carrier;
- C programming language for the code relating to ASRO-Daemon, ASRO-Box;
- Python programming language version 3.8 for the development of the ASRO-RSS part.

To get a more in-depth idea of ASRO's performance, however, we used theZoo repository on GitHub. This repository contains 255 pieces of malware, the most notorious of which will be displayed in the test results section.

Results

a) With respect to the comparative test, we inferred that:

BitDefender, Windows Defender and Avast recognize almost all these types of attacks and malware, but they act directly on the host and their software is internal to the host, so they are susceptible to being isolated as they are within a hostile environment. ASRO, on the other hand, due to its composition, still manages to contain them because the pattern of attacks mentioned above does not affect the functionality and operational capacity of our system. It succeeds in recognizing these threats, unlike the other systems analyzed, because in addition to using the normal software tools provided for recognizing malware (see Virus Total, ClamAV), it uses ASRO-Daemon as a backdoor to allow the ASRO-Box to act at a low level to counter the threats identified. The results of these tests are summarized in the Table 1.

b) For the system efficiency test, the repository used was downloaded locally and, using a Python script, the malware in it was started up one at a time, testing them on three types of machine where the ASRO system was installed, each with a different O.S. In particular, these tests were carried out on: Windows 11, MacOs Monterey and Ubuntu 20.04 LTS (Table 2).

In the table, we have listed the most well-known malware by choosing them from those that have done the most damage in real systems (Wanna Cry was used in 2017 as an encryption system to encrypt user data on PCs and demand a ransom) or known for large-scale malicious events (Figure 3).

On the remaining malware within the repository used, the ASRO system had a 100% detection and response rate to the threat.

Table 1. Results as regard test **(a)** Attack n.1 and **(b)** Attack n.2.

(a) Attack n.1 Bush Bunny

Malware Name	ASRO	Avast	BitDefender	Windows Defender
IoT.Mirai	Found	Not Found	Found	Not Found
AntiExe.A	Found	Not Found	Found	Not Found
Ransomware Thanos	Found	Found	Found	Found

(b) Attack n.2 Malicious PDF file

Malware Name	ASRO	Avast	BitDefender	Windows Defender
IoT.Mirai	Found	Not Found	Found	Not Found
AntiExe.A	Found	Not Found	Found	Not Found
Ransomware Thanos	Found	Found	Found	Not Found

Table 2. Results as regard Test

Malware Name	Victim Host OS	ASRO execution Time	Attack Results
Artemis	Windows 11	Real Time	Failed
AntiExe.A	Windows 11	Real Time	Failed
Ransomware Thanos	Windows IoT su Raspberry PI4	Real Time	Failed
RansomWare Wanna Cry	Windows 11	Real Time	Failed
OSX Hell Riser	macOS Monterey	Real Time	Failed
OSX Mac Security	macOS Monterey	Real Time	Failed
OSX Agent	macOS Monterey	real time	failed
RansomWare Wanna Cry	Ubuntu 20.04 LTS	real time	failed
nJRat	Ubuntu 20.04 LTS	real time	failed

```
ba5de52939cb809eae10fdbb7fac47095a9599a7 is malicious

Elastic v 4.0.44 :  malicious (high confidence)
FireEye v 35.24.1.0 :  Trojan.GenericKD.33916074
Alibaba v 0.3.0.5 :  Trojan:Win32/Vigorf.d125b99c
Arcabit v 1.0.0.889 :  Trojan.Generic.D20584AA
BitDefender v 7.2 :  Trojan.GenericKD.33916074
NANO-Antivirus v 1.0.146.25623 :  Trojan.Win32.Ransom.eoptnj
MicroWorld-eScan v 14.0.409.0 :  Trojan.GenericKD.33916074
Ad-Aware v 3.0.21.193 :  Trojan.GenericKD.33916074
Emsisoft v 2021.5.0.7597 :  Trojan.GenericKD.33916074 (B)
VIPRE v 6.0.0.35 :  Trojan.GenericKD.33916074
McAfee-GW-Edition v v2019.1.2+3728 :  Artemis
GData v A:25.33916B:27.28684 :  Trojan.GenericKD.33916074
Kingsoft v 2017.9.26.565 :  Win32.Troj.WannaCry.cg.(kcloud)
Ikarus v 6.0.26.0 :  Trojan.Win32.Vigorf
Fortinet v 6.4.258.0 :  W32/WannaCryptor.6F87!tr.ransom
```

Figure 3. Detection and active response to wanna cry malware.

Conclusion

In this paper, we presented the ASRO system as a system for countering threats within SCADA systems in an efficient manner. We have compared and validated the effectiveness of such a system by means of experimental tests, reporting excellent results compared to existing systems currently in use in industrial environments. As a future development, we aim to automate the configuration of the network securely using Machine Learning algorithms.

References

1. Creery, A. and E. J. Byres. "Industrial cybersecurity for power system and SCADA networks." *IEEE* (2005): 303-309.
2. Lopez, Carlos, Arman Sargolzaei, Hugo Santana and Carlos Huerta. "Smart Grid Cyber Security: An Overview of Threats and Countermeasures." *J energy power eng* 9 (2015): 632-647.

3. El Mrabet, Zakaria, Naima Kaabouch, Hassan El Ghazi and Hamid El Ghazi. "Cyber-security in smart grid: Survey and challenges." *Comput Electr Eng* 67(2018): 469-482.
4. Ten, Chee-Wooi, Chen-Ching Liu and Govindarasu Manimaran. "Vulnerability Assessment of Cybersecurity for SCADA Systems." *IEEE* 23 (2008): 1836-1846.
5. Davis, C. M., J. E. Tate, H. Okhravi and C. Grier, et al. "SCADA Cyber Security Testbed Development." *IEEE* (2006): 483-488.
6. Cherdantseva, Yulia, Pete Burnap, Andrew Blyth and Peter Eden, et al. "A review of cyber security risk assessment methods for SCADA systems." *Comput Secur J* 56 (2016): 1-27.
7. Zhang, Yichi, Lingfeng Wang, Yingmeng Xiang and Chee-Wooi Ten. "Power System Reliability Evaluation with SCADA Cybersecurity Considerations." *IEEE* 6 (July 2015): 1707-1721.
8. Mitchell, Robert and Ing-Ray Chen. "Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications." *IEEE* 4 (2013): 1254-1263.
9. Mashima, Daisuke and Alvaro A. Cardenas. "Evaluating Electricity Theft Detectors in Smart Grid Networks." In Research in Attacks, Intrusions and Defenses, Berlin: Springer-Verlag Berlin Heidelberg (2012).
10. Sommestad, Teodor, Goran N. Ericsson and Jakob Nordlander. "SCADA system cyber security — A comparison of standards." *IEEE PES General Meeting* (2010): 1-8.
11. Bastow, M. D. "Cyber security of the railway signalling & control system." *IET* (2014): 1-5.
12. Yang, Y., Tim Littler, S. Sezer and K. McLaughlin, et al. "Impact of cyber-security issues on Smart Grid." *IEEE* (2011): 1-7.
13. Zhao, Zhiheng and Guo Chen. "An Overview of Cyber Security for Smart Grid." *IEEE* (2018): 1127-1131.
14. Kang, DongHo, ByoungKoo Kim, JungChan Na and KyoungSon Jhang. "Whitelists Based Multiple Filtering Techniques in SCADA Sensor Networks." *J Appl Math* (2014 June): 1-7.
15. Yasakethu, S. and J. Jiang. "Intrusion Detection via Machine Learning for SCADA System Protection." In Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research (2013): 101-105.
16. Jarmakiewicz, Jacek, Krzysztof Maslanka and Krzysztof Parobczak. "Development of cyber security testbed for critical infrastructure." *IEEE* (2015): 1-10.
17. Pathan, Al-Sakib Khan. "The State of the Art in Intrusion Protection and Detection." Boca Raton, FL: Auerbach Publications (2014).
18. Korman, Matus, Margus Valja, Gunnar Bjorkman and Mathias Ekstedt, et al. "Analyzing the Effectiveness of Attack Countermeasures in a SCADA System." In Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG'17). Association for Computing Machinery, New York, NY, USA (2017): 73–78.

How to cite this article: Mangiameli, Andrea, Lacava G and Martinelli F. "A Novel Cybersecurity System for the SCADA Protection: ASRO." *Adv Robot Autom* 11 (2022): 233.