Comparison of the Intrusion Detection System Rules in Relation with the SCADA Systems

Jan Vávra[1], Martin Hromada[2]

[1] Tomas Bata University in Zlin, Zlin, Czech Republic, e-mail: *jvavra@fai.utb.cz*
[2] Tomas Bata University in Zlin, Zlin, Czech Republic, e-mail: *hromada@fai.utb.cz*

Abstract. Increased interconnectivity, interoperability and complexity of communication in Supervisory Control and Data Acquisition (further only SCADA) systems, resulted in increasing efficiency of industrial processes. However**, t**he recently isolated SCADA systems are considered as the targets of considerable number of cyber-attacks. Because of this, the SCADA cyber-security is under constant pressure. In this article we examine suitability of current state signature based Intrusion Detection System (further only IDS) in SCADA systems. Therefore, we deeply evaluate the Snort and the Quickdraw rules based on signatures in order to specify their relations to SCADA cyber security. We report the results of the study comprising more than two hundred rules.

Keywords: Cyber Security, Intrusion Detection System, Industrial Control System, Signature.

1 Introduction

An increasing number of the cyber-attacks relating to the Supervisory Control and Data Acquisition (further only SCADA) systems have the eminent influence on the SCADA cybersecurity. Accordingly, there is necessity to implement an Intrusion Detection System (further only IDS) in the SCADA systems. Horkan (2015) concluded that the IDS will become an essential part of the SCADA system. Moreover, Pollet (2013) predicted increasing dependency of the SCADA systems on IT; therefore, the percentage of industrial companies utilizing the IDS will rapidly grow. The implementation of the IDS in the SCADA systems has been widely investigated (Cheung et al., 2006; Verba and Milvich, 2008; Valli, 2009; Fovino et al., 2010; Zhu and Sastry, 2013; Yang et al., 2013; Maglaras and Jiang, 2014). Furthermore, Verba and Milvich (2008) suggest that the current state of signature or anomaly based IDS are not suited to be widely deployed in the SCADA systems; accordingly, future research is needed. Moreover, there is a little research dealing with the current state of IDS rules related to the SCADA. The previous research has not fully addressed the type, priorities and number of SCADA rules. This study was designed to investigate the IDS SCADA rules. In this paper, we present the comparison and evaluation between two groups of SCADA-based rules (the Snort and the Quickdraw rules).

adfa, p. 1, 2011.

2 Supervisory Control and Data Acquisition

The SCADA systems are developed for monitoring, management and control of industrial systems. Moreover, the SCADA is an internal part of the Critical Information Infrastructure (further only CII). Nowadays, the CII is an essential part almost every sector of the critical infrastructure (transportation systems, power plants, dams, water treatment, oil production, chemicals, gas distribution, etc.). Therefore, every cyber-attack on the CII systems can be considered as a lethal attack. It can result in fatal damage to the environment, population or a country.

The SCADA have a positive influence on contemporary society; nevertheless, these systems are under increasing pressure to improve efficiency and interoperability. Thus, the recently isolated systems are becoming more dependent on interconnection with external technologies.[1] This trend resulted in the emergence of new vulnerabilities and, accordingly, the protected system becomes more vulnerable to new cyber-attacks.

3 Evaluation of ICT and SCADA Cyber Security

The Evaluation of the main differences between ICT and SCADA cyber security is crucial for this research and especially for the IDS. Accordingly, we used three security criteria (availability, confidentiality and integrity) to describe differences between ICT and SCADA cyber security. Their relationship can be seen in Fig. 1. As a result, confidentiality is the most important security element for ICT. On the other hand, availability is the most important for the SCADA. That is why every threat to the continuity of the SCADA processes is considered as critical.

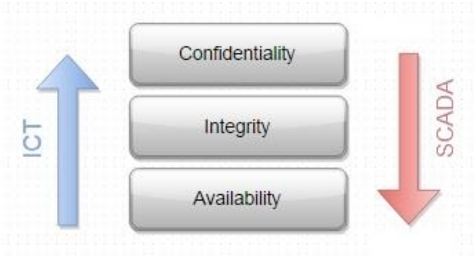


Fig. 1. The **c**omparison of ICT and SCADA cyber security. [2]

4 Intrusion Detection System

An Intrusion Detection System is characterized as a system for detection of an intruder. It is a reactive tool used for monitoring, detecting and recording dangerous behavior in a computer network or a computer system. The IDS inspecting each packet within protected computer network and looking for malicious content.[3] Thus, there are two main detect methodologies (signature and anomaly based). However, we deal only with signature based methodology. Every registered intrusion is reported to the operator who will make appropriate decision to eliminate this threat.

4.1 IDS Architecture

The IDS architecture is composed of four main parts. All parts are interconnected and disruption of one of them has serious consequences to the whole system. The results, given in Fig. 2, show entire common IDS.

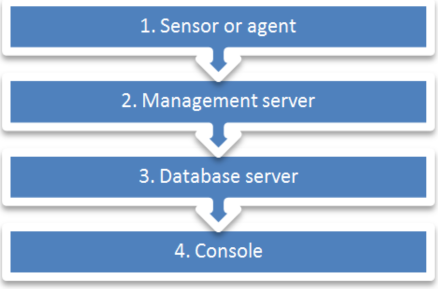


Fig. 2. Common architecture of the IDS.[4]

There is a specification of each IDS component:

- The first and essential element in Fig. 2 is a sensor, which is also known as a agent. It is used for monitoring, recording and evaluating network traffic. The sensor is being used in conjunction with the network intrusion detection system (further only the NIDS) while the agent is used in conjunction with the host intrusion detection system (further only the HIDS).[4]

- The management server is a centralized device that accepts information from the agents or the sensors. These data can be further processed to a qualitatively higher level. The management server can correlate inputs from multiple sensors or agents in order to increase detection capabilities. However, the outputs from the management server can be used in the control and management improvement of particular sensors or agents.

- The database server is designed to store data communication from the sensors or the agents. It can also store knowledge database based on signatures and other detection methodologies for detecting an intrusion.

- The Console is a software interface between the user and the IDS. The console is commonly used for administration or configuration of the sensors or the agents.[4]

4.2 Snort IDS Components

Snort is an open source IDS. This system is divided into five main components which are hierarchically organized. The whole components are shown in Fig. 3.

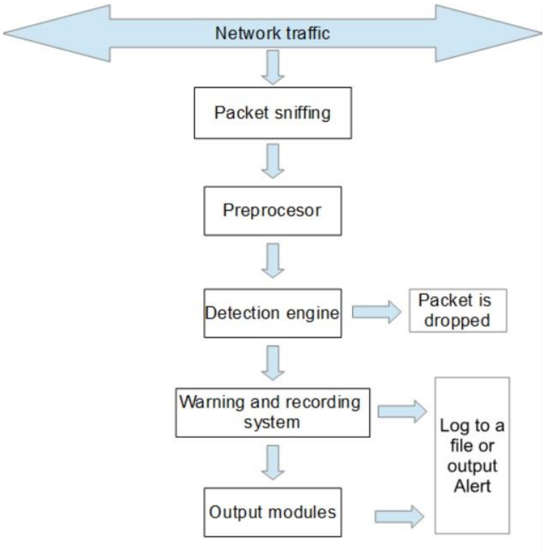


Fig. 3. Snort IDS components.[5]

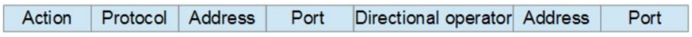
The diagram in Fig. 3 determines the basic architecture of famous Snort IDS. The first fundamental operation of every IDS is to capture particular packets of network traffic. The captured data are modified for the preprocessor. The preprocessor is a component of IDS which is responsible for modifying packets into a standardized form for the detection engine. The detection engine is the most important part of the IDS. Its main purpose is to detect suspicious activity in network traffic. Snort can use more than one detection methodologies. However, if the evaluated packet is harmless, then it is discarded. On the other hand, if the packet is detected as an intrusion attempt, then the record and warning are generated. Output modules finally generate a final message to the user.[5]

5 Signature-Based IDS Detection

The signature-based detection is one of the most basic methods for malware detection. This methodology is based on the comparison. Therefore, the IDS generally use rules to compare real traffic patterns with cyber security signatures. They matches to particular cyber-attacks, moreover each of them is stored in the signature database. This methodology is very effective against known cyber threats and has a low rate of false positive detection. On the other hand, it is often ineffective against unknown threats like zero-day attacks or the modifications of already known cyber-attacks. Furthermore, due to the comparison of every packet in network traffic with all signatures; there is a momentous time-consuming process, which is responsible for slowing down the system operation. This is the serious problem for the SCADA systems.

5.1 Definition of IDS rule based on signature

Each rule-based signature starts with a header. Moreover, within the header are particular criteria, which allow the comparison between the rule and the network traffic. The header also specifies an action for a case when a match is found. The architecture of a Snort header shows Fig. 4.



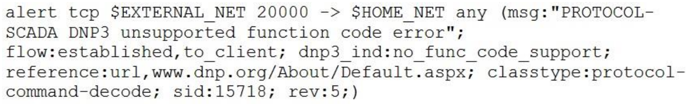
Action	Protocol	Address	Port	Directional operator	Address	Port

Fig. 4. Components of the Snort header.[6]

Each segment in Fig. 4 is subsequently discussed:

- **Action** - this is an action that will take place when the rule exactly matches the packet. This segment is determined by actions such as alerting, logging, ignoring, blocking packet and many others.
- **Protocol** – this segment determines a communication protocol for which the rule is proposed.
- **Address** - the IP address used as source or destination depending on the directional operator.
- **Port** - it can be described as a source or a destination port used in a network communication.
- **Directional operator** – determines, if the address and the port are considered as the source or the destination port.

The remaining part of the rule contains additional criteria for detection of cyber-attacks and the background information. An example of the whole rule can be seen in Fig. 5.



```
alert tcp $EXTERNAL_NET 20000 -> $HOME_NET any (msg:"PROTOCOL-
SCADA DNP3 unsupported function code error";
flow:established,to_client; dnp3_ind:no_func_code_support;
reference:url,www.dnp.org/About/Default.aspx; classtype:protocol-
command-decode; sid:15718; rev:5;)
```

Fig. 5. Architecture of the Snort rule.[7]

Fig. 5 shows the rule for the DNP3 SCADA communication protocol. The IDS is designed to generate the alert message when a rule matches with the data. Moreover, the rule is dedicated for TCP protocol. “$EXTERNAL_NET” and “20000” were set as source IP address and source port. On the contrary, destination IP address and destination port were set as “$HOME_NET” and “any”.

The remaining part of the rule is known as a rule options is responsible for providing additional information. The content of this segment is not static, furthermore, it may change. However, the Fig. 5 shows common rule composition:

- **msg** – it is used for quotations of the rule. In this case, the msg describes communication protocol and background information.

- **flow** – the flow is used for TCP sessions. Moreover, it describes packet direction for which the rule is made. Fig. 5 shows the rule that is applicable only on TCP session.
- **dnp3_ind** – the dnp3_ind is a particular rule option for the DNP3 protocol. It is used to match against flag bits in a DNP3 packet header.
- **reference** – this segment is responsible for accompanying information about the rule. It is not necessary for detection; therefore, it can be ignored.
- **classtype** – the classtype provides a classification of the alert and its priority for the rule. The sample of the classtype is shown in Fig. 5. However, there is a classification of alert without the priority; accordingly, the priority is set on default value in the classification.config file. Furthermore, low priority value represents a high threat.
- **sid** – the sid can be described as a rule ID. Moreover, the sid number up to one million is reserved for Snort rules. The sid number over one million is dedicated for local rules.
- **rev** – the rev determines how many times the rule was modified. It can be also determined as a version of the rule.

6 Methods

The Snort and the Quickdraw SCADA rules were collected due to the evaluation of possibilities of deployment the IDS in the SCADA system. The Snort and the Quickdraw provide databases of SCADA rules used by a considerable number of organizations. This article is dealing with the comparison between the Snort and the Quickdraw SCADA rules. The research is examined according to the following criteria: the number of SCADA rules, the type of cyber-attack alerts and priority of the rule. Thus, the rules were collected from the Snort and the Quickdraw databases. The collected rules are usually used for the Modbus and the DNP3 communication protocols. The Modbus and the DNP3 rules were selected based on their ports; whereas, the Modbus communication protocol uses port 502 and the DNP3 communication protocol uses port 20000. The total sample consist more than 100 rules. In the follow-up phase of the study, we evaluated collected data in order to obtain crucial information for the purpose of the article. In the interest of determining the relationship between rules, a quantitative data analysis was used. Each rule was evaluated and classified.

7 Results

The aim of the article is the evaluation of the cyber threats in relation to the SCADA systems. In order to evaluate the SCADA rules, we determined three objectives. The first objective of the research is to evaluate the data in term of number. The comparison of the SCADA rules is shown in Fig. 6.

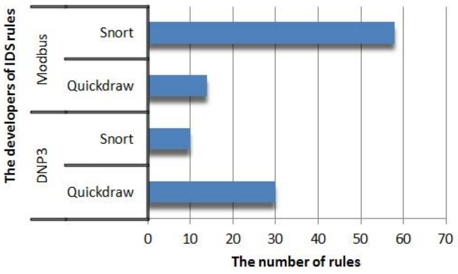


Fig. 6. The comparison of IDS SCADA rules.

Fig. 6 shows the distribution of rules per SCADA communication protocols and provides comparison between the Snort and the Quickdraw rules. As can be seen, Snort provides the highest amount of Modbus rules (58 rules), compared to Quickdraw with 14 rules. On the other hand, Quickdraw has the highest amount of the DNP3 rules (14 rules), compared to Snort with 10 rules.

The second objective of the research is to evaluate cyber-attack alerts. The Fig. 7 shows a representation of the alerts generated by the Snort and the Quickdraw rules in relation with Modbus protocol. Each alert is represented by the percentage of cases. There is an eminent difference between Snort and Quickdraw. The distribution of the rule is divergent. Almost 92% of all Snort rules are focused on protection against Generic Protocol Command Decode. On the other hand, the Quickdraw rules are mainly focused on the defense against Attempted Information Leak with 28% and the Detection of Non-Standard Protocol or Event.

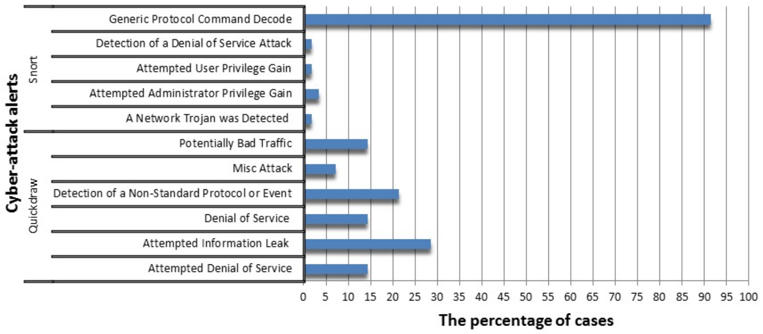


Fig. 7. The comparison of the cyber-attack alerts in relation with Modbus.

In order to meet the second objective, we need to determine the Snort and the Quickdraw cyber-attack alerts in relation with the DNP3 communication protocol. As can be seen in Fig. 8, there is only one alert type of the Snort DNP3 rule. All rules are focused on the cyber-attack based on Generic Protocol Command Decode (100%); whereas, the Quickdraw rules are much more diverse than Snort rules. The Figure shows the distribution of all Quickdraw rules. The rules are mostly responsible for the protection against Attempted Denial of Service (27%) and Potentially Bad Traffic (23%).

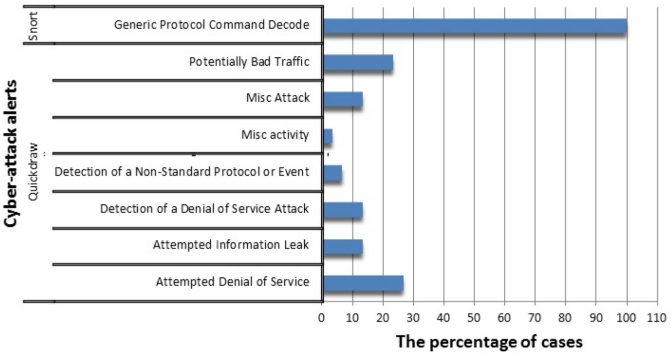


Fig. 8. The comparison of the cyber-attack alerts in relation with DNP3.

The third objective is focused on the specification of the Snort and the Quickdraw rules priorities in relation with the Modbus and the DNP3 communication protocols. The rule with priority 1 is the most crucial for the SCADA system while the rule with priority 3 is the least important for the SCADA system. As can be seen in Fig. 9, the most of the Snort Modbus rules are classified by priority 3 (91%). Moreover, the Quickdraw Modbus rules can be mostly characterized by priority 2 (43%) and priority 1 (36%).

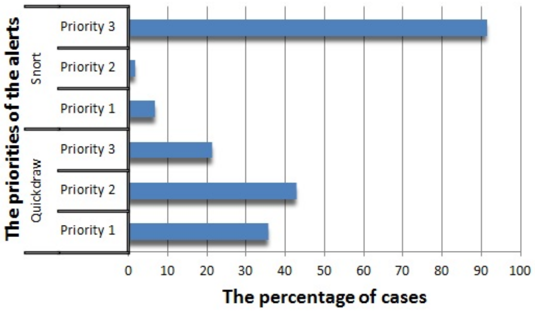


Fig. 9. The distribution of the Modbus priorities.

The second part of the third objective is dealing with the specification of the Snort and the Quickdraw rules priority in relation with the DNP3 communication protocol. The Fig. 10 shows that 100% of the Snort rules are determined by priority 3. In the case of Quickdraw, there is a large group of rules with priority 2 with 73%.

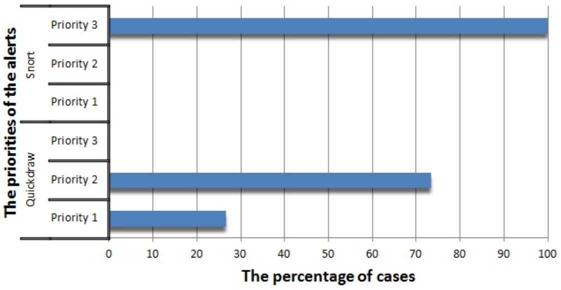


Fig. 10. The distribution of the DNP3 priorities.

8 Discussions

The objective of the article was to evaluate the SCADA cyber security. Therefore, this case study was based on Snort and Quickdraw IDS rules in relation to the SCADA. The results are consistent with earlier studies conducted with IDS rules (Shah and Singh, 2012; Ulltveit-Moe and Oleshchuk, 2010; Khamphakdee et al., 2014).

The assessment of the IDS rules is performed according to different perspectives. In general, the Snort rules are mostly focused on Modbus communication protocol compared to Quickdraw. Moreover, the overall results indicate the dominance of Snort rules in terms of number. However, the diversity of the Snort rules is low; furthermore, the Snort rules are mainly focused on Generic Protocol Command Decode alert. This type of alert has a low priority; accordingly, the Snort rules are not essential for the SCADA cyber security. On the other hand, the Quickdraw rules provide the appropriate diversity. Furthermore, they are mainly aimed at dangerous cyber-attacks. An interesting fact is that Quickdraw rules protecting the SCADA systems against Denial of Service attack. This type of attack represents an eminent danger to the availability of the system; therefore, it is the most critical threat for the SCADA. The overall results indicate that the difference between Snort and Quickdraw rules is noticeable. Every SCADA system relying only on IDS with SNORT rules is vulnerable by a considerable number of cyber-attacks. Nonetheless, it is notable that the Snort provides another layer of cyber security, even though it is not an effective solution.

It should be noted that this study has been primarily concerned with the SCADA-particular rules. However, the considerable number of cyber-attacks is focused on the IT systems interconnected with the SCADA. Marginalization of the IT cyber security can be critical for SCADA. Nonetheless, more research is required in this area in order to determine the reliable cyber defense of the critical information infrastructure.

9 Acknowledgment

This work was founded by the Internal Grant Agency (IGA/FAI/2016/014) and supported by the project ev. no. VI20152019049 "RESILIENCE 2015:RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems" supported by the Ministry of the Interior Security Research Programme of the Czech Republic in the years 2015-2020. Moreover, this work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Programme project No. LO1303 (MSMT-7778/2014) and also by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

10 References

[1] STOUFFER, Keith, Joe FALCO and Karen SCARFONE. *Guide to Industrial Control Systems (ICS) Security* [online]. [cit. 2015-12-01]. Available: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, National Institute of Standards and Technology, 2011.

[2] MACAULAY, Tyson a Bryan SINGER. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton, FL: CRC Press, c2012, x, 193 p. ISBN 14-398-0196-7.

[3] FISK, Mike; VARGHESE, George. *Fast content-based packet handling for intrusion detection*. LOS ALAMOS NATIONAL LAB NM COMPUTING COMMUNICATIONS AND NETWORKING DIV, 2001

[4] SCARFONE, Karen a Peter MELL. *Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology* [online]. 2007 [cit. 2015-12-03].

[5] MEHRA, Pritika. A brief study and comparison of snort and bro open source network intrusion detection systems. *International Journal of Advanced Research in Computer and Communication Engineering*, 2012, 1.6: 383-386.

[6] SHAH, Sagar N.; SINGH, Ms Purnima. *Signature-Based Network Intrusion Detection System Using SNORT And WINPCAP*. In: International Journal of Engineering Research and Technology. ESRSA Publications, 2012.

[7] The Snort Intrusion Detection System. [Online] Avaiable: https://www.snort.org/, 2015.