http://dx.doi.org/10.14236/ewic/ICS2018.6

Identifying S7comm Protocol Data Injection Attacks in Cyber-Physical Systems

Oliver Eigner
University of Applied Sciences
St. Pölten
Institute of IT Security Research
St. Pölten, Austria
www.fhstp.ac.at
oliver.eigner@fhstp.ac.at

Philipp Kreimel
University of Applied Sciences
St. Pölten
Institute of IT Security Research
St. Pölten, Austria
www.fhstp.ac.at
philipp.kreimel@fhstp.ac.at

Paul Tavolato
University of Applied Sciences
St. Pölten
Institute of IT Security Research
St. Pölten, Austria
www.fhstp.ac.at
paul.tavolato@fhstp.ac.at

Cyber-physical systems are found in production and industrial systems, as well as critical infrastructures which play a crucial role in our society. The integration of standard computing devices and IP-based technology in cyber-physical systems increases the threat of cyber-attacks. Furthermore, traditional intrusion defense strategies are often not applicable in industrial environments. This paper focuses on the widely used Siemens S7 communication protocol and presents an approach to detect anomalies in network packets by training a model with neural networks and applying the model on current network traffic. In order to stay close to practice we built an experimental setup with industry controllers, sensors and actuators. To check the applicability of the model we launched supervised S7 protocol attacks against the setup. The results show that this approach can detect anomalous network packets with satisfactory accuracy.

Cyber-Physical System, Anomaly Detection, S7 Communication Protocol

1. INTRODUCTION

Entering the era of Internet of things (IoT) and Industry 4.0, most industrial devices and systems communicate over Internet. Such cyber-physical systems (CPS) were designed to meet availability and reliability requirements. Therefore cyber security measures were often deemed nonessential and not implemented. CPSs are found in various services such as electricity, water purification and transportation, to function properly (1). Dependencies on cyber infrastructure in industrial facilities and open communication result in more opportunities for cyber-attacks and raise security risks of the industrial plant. CPSs are usually controlled and monitored by an industrial control system (ICS). ICSs often control and monitor critical infrastructures, which are essential for the functioning of a society and economy. If these systems were compromised, it would cause serious consequences.

In order to succeed in protecting these environments and identifying any attacks on cyber-physical systems, the communication within the control systems must be secured and monitored. Although there are a few solutions available that monitor network activity of control systems, the ongoing operations of an industrial CPS, which is prone to modification by an adversary, are usually not supervised. However, the interconnectivity as well as the trend of integration of standard computing devices into industrial environments vastly increase risks and threats. This is reflected by the growing concern and the growing priority given to the security of industrial systems in recent years. Incidents like the Stuxnet worm, which led to physical damage of centrifuges at an Iranian uranium enrichment plant in 2009 (2), or the BlackEnergy-borne power outage in 2015 (3), as well as researchers from Georgia which demonstrated ransomware attacks targeting supervisory control and data acquisition (SCADA) devices (4) have captured media attention and increased the awareness on security.

In order to secure such systems and industrial devices, certain security controls monitoring the communication and operational processes, must be implemented to detect any anomaly and to take appropriate countermeasures. Besides, conventional intrusion defense strategies for common IT systems are often not applicable and portable in industrial environments.

© *Eigner et al. Published by*
BCS Learning and Development Ltd.

The Siemens[1] S7 communication protocol is one of the leading protocols used in industrial networks. Siemens S7 Programmable Logic Controllers (PLCs) are estimated to constitute over 30% of the world-wide PLC market. The platform is so popular that attackers focus on gaining access to industrial networks via S7 communication protocol vulnerabilities. (5)

In this paper we present an approach to detect anomalies in industrial systems by training a model with neural networks and applying the model current network traffic. The model which is based on supervised cyber-attacks on CPSs is trained, in order to detect anomalous S7 protocol packets. All sensor and system data was obtained from a custom-built industrial experimental setup, a conveyor belt system, which uses industrial devices in order to provide real-time data and ensures applicability of the approach.

The rest of the paper is structured as follows. Section 2 gives a short overview of related work. In Section 3 we describe our experimental setup and used industrial devices. Section 4 presents the modeling procedure approach. In section 5 we perform S7 communication protocol attacks against our test environment. It also describes experimental classification results and shows the statistical performance of the model. Section 6 concludes the paper with some ideas for future work.

2. RELATED WORK

Since the S7 communication protocol is proprietary, only few information about attacks against it is published. One exception is described in the work of Beresford (6). The author explained that the standard S7 communication protocol is not encrypted, or authenticated, it is susceptible to session hijacking, Denial of Service (DoS) attacks, spoofing, and other attacks. Once an attacker gains access to the control network, they can fully access the industrial devices including the PLC and launch attacks against the engineering workstations as well.

Kleinmann and Wool (7) present a model-based intrusion detection system which is designed for S7 communication protocol networks. Their approach is based on the key observation that the communication traffic of the S7 protocol to and from a PLC is highly periodic. The authors studied the traffic and as a result, each HMI-PLC communication can be modeled by using its own unique deterministic finite automaton.

[1] https://www.siemens.com/global/en/home.html

In (8) the authors studied the periodicity characteristics of the industrial communication. Their results show that CPS traffic is similar to SNMP traffic, because both represent regular time series, due to the fact that the data is logged in a periodical fashion. The area of CPS-specific intrusion detection and anomaly detection systems is quite active. Media attention to cyber-attacks on cyber-physical systems such as Stuxnet (e.g. Chen (9)) has highlighted the need for reliable early-detection systems. Various approaches can be found in the field of attacks on industrial control systems or anomaly detection, as well.

An intrusion detection system based on telemetry and periodicity patterns of network traffic in cyber-physical systems is proposed by Zhang et al. (10). The system analyzes periodicity characteristics in industrial networks and tries to classify them by using their intrusion detection algorithm. They are able to detect communication attacks such as response injection attacks with their proposed system by combining periodic and telemetric system data.

The lack of intrusion detection systems for cyber-physical systems is one of the challenges addressed in the work of (11) and (12). In (11), an IDS is proposed that is mainly based on the Modbus protocol specification, but also assumes regularity and stability with regard to topology, communication and configuration. They generated industrial traffic and derive characteristics from Snort network intrusion detection system Modbus/TCP rules. A different approach is used in (12), where a framework is implemented as an add-on component for any unsupervised approach in order to improve its performance. The authors tested their framework by using three different unsupervised intrusion detection algorithms.

In (13), examples of anomaly detection systems in SCADA environments are listed. The authors present current work and further outline the possibilities and constraints of the approaches. They evaluate various anomaly detection algorithms and found out that most systems are based on the analysis of network protocol communications and do not factor in the system behavior.

In (14), the authors use data from a live industrial process control network and subsequently present a machine learning based approach to anomaly detection.

Peng et al. (15) give an overview of anomaly detection approaches for identifying fingerprinting attacks on industrial control systems. Further, they

demonstrated how to increase security for these systems and also listed various attacks for CPSs.

A model-based intrusion detection approach is described by Cheung et al. (16). They detect attacks that cause the system to behave outside of the models. They constructed with the goal of specifying the predicted behavior of the system. Further the authors developed a prototype for monitoring Modbus/TCP network traffic that evaluate three model-based techniques. They define protocol-level models based on the Modbus/TCP application protocol and apply custom IDS rules to detect violations in the Modbus/TCP specification in an early stage.

In (17), a novel method involving passive finger-printing for industrial networks without deep packet inspection and experience on real environments is proposed. Their goal is to provide information as to which devices belong to the CPS part like industrial devices or systems, by analyzing industrial traffic. Further, the authors are able to identify devices in critical infrastructures and are able import an initial rule to define the normal behavior by using an anomaly-based industrial detection system.

3. EXPERIMENTAL SETUP

Our CPS testbed provides a broad range of Siemens industrial devices, physically applied, with no simulation and processes data in real-time. A graphical interface for operators is used in order to allow control of the system and logging across our industrial environment. Nevertheless, the routing and packet delay of these systems remain under lab environments and physical network device responsibility. The network architecture of the testbed was built very similar to real industrial systems and is representative of real-world large scale distributed systems.

In our experimental setup, as shown in Figure 1, we created a simple industrial system, a conveyor belt, using hardware components such as a Siemens PLC, HMI and infrared light barrier sensors. The work flow of the system is controlled by the programmed logic on the PLC and input sensors, by providing process information which is sent to the PLC. The operation of the system resembles a real conveyor belt and therefore allows us to gather realistic data in real-time that could represent a cyber-physical system. In order to acquire and analyze data from the system, we developed a prototype implementation of an anomaly detection system, running on a Raspberry Pi 3, which was integrated into our experimental setup. The main parts of the system are acquisition of data, the extraction of features and the training of a model using neural networks. In our tests the acquisition process and the machine learning process could run in real-time on the Raspberry, as the network traffic was manageable.

The whole work flow and all occurring events are controlled and triggered by the PLC. In our previous papers (18) (19), a detailed description of the software and hardware implementation of the experimental setup can be found.

4. MODELING PROCEDURE

In order to detect any discrepancies in the control network, a formal model representing behavior of the cyber-physical system is needed. For our setup, the input domain of the model includes the connected network, the physical components of the system (sensors and actuators) as well as the control components. The traffic on this network, specifically the S7 protocol, represents the main domain for the modeling process. The S7 protocol, which is Siemens proprietary, defines the syntax and semantics of the traffic. In our approach we use the protocol data on the network to model the systems behavior. We assume that the data flow can be acquired and analyzed in real-time.

4.1. Data Acquisition

The first step in the data acquisition process was the definition of an adequate time acquisition interval Δt. Thus, we analyzed the activities of the system during normal operation, i.e. the processing of *k* elements. We identified that network traffic is essentially periodic, as the same sequence of protocol data is sent over the network.

With the definition of Δt we analyze the network packets transmitted to and from the PLC. They mainly contain measurements from the sensors and commands sent to the actuators. As all packets run through the PLC, it holds all process-specific data which can be retrieved. Thus, the training data for

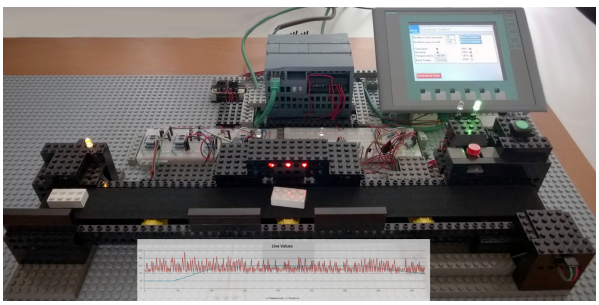

Figure 1: *Lab environment for our testbed*

modeling is acquired directly from the PLC. The S7 protocol contains function calls to read out the values of specific variables of the PLC as well as the inputs and outputs. To achieve a real-time monitoring of our control system, the data acquisition process polls data from the PLC every 50 ms. The following variables are acquired:

- Inputs and outputs of the PLC, e.g. buttons, infrared sensors, conveyor motor control.
- Internal PLC variables, e.g. parts on conveyor, process start and end times.
- Sensor data, e.g. temperature.

These variables are acquired in each polling request and represent the behavior of the system within an interval Δt.

4.2. Feature Extraction

Each recorded time interval is represented by a time series of process data of the PLC. For the modeling procedure the dimensionality of the acquired data needs to be reduced, as time series data with varying lengths are difficult to train with a classification algorithm. We used feature extraction to calculate values representing the behavior within an interval. A broad range of features was tested and selected based on their information gain. The following features were extracted:

- the minimum and maximum value of a variable
- the standard deviation of a variable
- the arithmetic mean of a variable
- the round-trip time of protocol packets
- the amount of S7 protocol packets per second

The features are extracted for each defined time interval, thus representing the state of the system within the time frame of one interval.

4.3. Training the Neural Network

In order to automatically detect deviations in the acquired data we created a feed-forward neural network which is trained by a back propagation algorithm (multi-layer perceptron). In a feed-forward neural network the connections between the units do not form a directed cycle. The information moves in only one direction, forward, from the input nodes, through the hidden nodes to the output nodes. The training data includes anomalous data of supervised attacks, which will be discussed in the next Section.

5. EVALUATION

To evaluate the performance of the model we executed several supervised cyber-attacks against the experimental setup. The attacks exploit various security flaws of the S7 protocol and the PLC to read out information and inject data.

5.1. Attacks against the Setup

We developed a S7 communication protocol client which provides functions to read and write specific data over the S7 protocol. By default no authentication is required to setup the communication and request data from the PLC. This shows one of the inherent security flaws of the protocol.

5.1.1. Information Gathering Attack

Using the S7 *ReadArea* function we gather information about all data blocks of the PLC. This includes the inputs, outputs and the internal PLC variables. This attack also allows to accurately map variables on the PLC, as function calls for non-existent memory addresses return an out-of-bounds error message.

5.1.2. Modification of Internal PLC Variable

This attack targets certain set points of PLC variables. In PLC logic set points are used as thresholds which often trigger some action (e.g. specific action when maximum temperature is reached). These set points are stored in memory addresses which can be overwritten by the S7 *WriteArea* function, provided the address is known.

5.1.3. Continuous Modification of Variables

This attack continuously modifies variables which are used and modified by the PLC logic during operation. By setting the request time for the modification fairly low, $<$10 ms, this allows an attacker to continuously overwrite specific values, which may cause unexpected behavior on the PLC.

5.1.4. Man-in-the-Middle (MitM) Attacks

MitM attacks were executed to intercept the entire traffic of the control network. This allows an attacker to gather information about data flows from the system.

As this is a supervised classification, only the aforementioned attacks can be classified with significant confidence. However, unknown attacks, which often deviate from normal behavior, could also be detected by looking at varying confidence levels for various classes.

5.2. Results

For each of the attacks mentioned beforehand the system behavior is acquired. The instances are

assigned a label in order to allow training by an algorithm. The training set contains 110 instances, 50 valid and 20 for each attack, respectively. This data is used as input for the neural network. To estimate the statistical performance of the neural network we performed a 10-fold cross-validation. The result of the cross-validation is shown in Table 1. The process achieved an overall accuracy of approximately 97%, with three misclassifications. It should be noted that the model could identify passive attacks, such as MitM, with high precision. This can be attributed to the fact that MitM attacks alter the round-trip time of S7 packets, thereby become classifiable.

With the resulting model we present a basis for identifying potential anomalies in the control network traffic from our experimental setup. The results are overall promising, as anomalous S7 packets could be detected with high accuracy.

Table 1: *Confusion Matrix of Cross-Validation Statistics*

a	b	c	d	e	<– classified as
49	0	1	0	0	a = valid
0	19	0	0	1	b = S7 info gath
0	0	20	0	0	c = S7 continuous
0	0	0	20	0	d = S7 set point
1	0	0	0	19	e = MitM

6. CONCLUSION

Securing of CPSs from cyber-attacks has high priority for many industry facilities. While many intrusion detection systems exist, they focus mainly on network traffic behavior or perimeter security. Our paper proposes an supervised learning approach for anomaly detection in monitoring CPS network traffic.

An experimental setup under lab environments with real industrial devices was set up and data generated during normal system operations was analyzed to train our behavioral model, in order to show the viability of anomaly detection and classification procedure in cyber physical systems. Consequently various S7 communication protocol cyber-attacks were performed against the testbed. Based on these supervised attacks, a model was trained using neural networks. If an anomaly is detected, the classification process is started to classify the anomaly by applying our model and calculating predictions for trained classes. The accuracy of the process achieved 97%, with three misclassifications.

Attacks against the lab environment can be detected using our anomaly detection and classification approach. Especially known cyber-attacks that have already been trained by the classifier, can all be classified with high accuracy in real-time.

Further work will cover the improvement of used algorithms by widening the spectrum of anomaly detection to other types of industrial cyber-attacks. Furthermore, we are also testing our approach on real data from production facilities.

ACKNOWLEDGEMENTS

Our project is funded by the KIRAS program of the Austrian Research Promotion Agency (FFG). KIRAS funds projects in the field of security, with IT security being a subcategory in this context.

REFERENCES

[1] K. D. Bettenhausen and S. Kowalewski, “Cyber-physical systems: Chancen und Nutzen aus Sicht der Automation,” *VDI/VDE-Gesellschaft Mess-und Automatisierungstechnik*, 2013.

[2] N. Falliere, L. O. Murchu, and E. Chien, “W32. stuxnet dossier,” *White paper, Symantec Corp., Security Response*, vol. 5, 2011.

[3] D. U. Case, “Analysis of the cyber attack on the ukrainian power grid,” *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[4] D. Formby, S. Durbha, and R. Beyah, “Out of control: Ransomware for industrial control systems,” 2017.

[5] Electrical Engineering Blog, “The top most used plc systems around the world.” http://engineering.electrical-equipment.org/electrical-distribution/the-top-most-used-plc-systems-around-the-world.html, May 2013.

[6] D. Beresford, “Exploiting siemens simatic s7 plcs,” *Black Hat USA*, vol. 16, no. 2, pp. 723–733, 2011.

[7] A. Kleinmann and A. Wool, “Accurate modeling of the Siemens S7 scada protocol for intrusion detection and digital forensics,” *Journal of Digital Forensics, Security and Law*, vol. 9, no. 2, p. 4, 2014.

[8] R. R. R. Barbosa, R. Sadre, and A. Pras, “A first look into scada network traffic,” in *2012 IEEE Network Operations and Management Symposium*, pp. 518–521, April 2012.

[9] T. M. Chen, “Stuxnet, the real start of cyber warfare? [editor’s note],” *IEEE Network*, vol. 24, pp. 2–3, November 2010.

[10] J. Zhang, S. Gan, X. Liu, and P. Zhu, "Intrusion detection in scada systems by traffic periodicity and telemetry analysis," in *2016 IEEE Symposium on Computers and Communication (ISCC)*, pp. 318–325, IEEE, June 2016.

[11] R. Al-Dalky, O. Abduljaleel, K. Salah, H. Otrok, and M. Al-Qutayri, "A modbus traffic generator for evaluating the security of scada systems," in *2014 9th International Symposium on Communication Systems, Networks Digital Sign (CSNDSP)*, pp. 809–814, July 2014.

[12] A. Almalawi, Z. Tari, A. Fahad, and I. Khalil, "A framework for improving the accuracy of unsupervised intrusion detection for scada systems," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 292–301, July 2013.

[13] I. Garitano, R. Uribeetxeberria, and U. Zurutuza, "A review of scada anomaly detection systems," in *Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011*, pp. 357–366, Springer, 2011.

[14] M. Mantere, M. Sailio, and S. Noponen, "Network traffic features for anomaly detection in specific industrial control system network," *Future Internet*, vol. 5, no. 4, pp. 460–473, 2013.

[15] Y. Peng, C. Xiang, H. Gao, D. Chen, and W. Ren, *Industrial Control System Fingerprinting and Anomaly Detection*, pp. 73–85. Cham: Springer International Publishing, 2015.

[16] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for scada networks," in *Proceedings of the SCADA Security Scientific Symposium*, (Miami Beach, Florida), Jan. 2007.

[17] S. Jeon, J.-H. Yun, S. Choi, and W.-N. Kim, "Passive Fingerprinting of SCADA in Critical Infrastructure Network without Deep Packet Inspection," *ArXiv e-prints*, Aug. 2016.

[18] O. Eigner, P. Kreimel, and P. Tavolato, "Detection of man-in-the-middle attacks on industrial control networks," in *2016 International Conference on Software Security and Assurance (ICSSA)*, pp. 64–69, Aug 2016.

[19] P. Kreimel, O. Eigner, and P. Tavolato, "Anomaly-based detection and classification of attacks in cyber-physical systems," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, (New York, NY, USA), pp. 40:1–40:6, ACM, 2017.