ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/344543847

Novel Challenges for Anomaly Detection in I&C Networks: Strategic Preparation for the Advent of Information Hiding based Attacks

Article *in* Atw. Atomwirtschaft · October 2020

CITATIONS
0

READS
21

8 authors, including:

Kevin Lamshöft
Otto-von-Guericke-Universität Magdeburg
9 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Tom Neubert
Brandenburg University of Applied Sciences
14 PUBLICATIONS **166** CITATIONS
SEE PROFILE

Mathias Lange
Hochschule Magdeburg
5 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Robert Altschaffel
Otto-von-Guericke-Universität Magdeburg
16 PUBLICATIONS **27** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

SAVELEC View project

Smartest View project

All content following this page was uploaded by Yongjian Ding on 08 October 2020.

The user has requested enhancement of the downloaded file.

nucmag.com

atw

International Journal
for Nuclear Power

2020

10

Electrifying Transport – A Global Perspective

Sustainable Finance Initiative of the EU and Taxonomy – How Green Is Nuclear?

Nuclear Energy – Reliable, Safe, Economical and Always Available to Protect the Environment

ISSN · 1431-5254
24.– €

Issue 10 | 2020

October

Contents

Incorrect text passages were published in the Operating Results in issue 8/9 Vol. 65.

The corrected report can be found online: www.kernd.de/kernd/presse/pressemitteilungen/

Our apologies!

Cover:
View looking down on Vogtle Unit 3 containment vessel. A power reactor of 1,117 MWe net capacity avoids yearly CO_2-emissions amounting to about 10 million (10^6) tonnes, during the lifetime of 60 years 600 million (10^6) tonnes (this corresponds to approx. the yearly total CO_2-emissions of the private transport sector in the EU). ©2020 Georgia Power Company.

G = German
E/G = English/German

Feature

Major Trends in Energy Policy and Nuclear Power

Energy Policy, Economy and Law

Environment and Safety

Report

Novel Challenges for Anomaly Detection in I&C Networks: Strategic Preparation for the Advent of Information Hiding based Attacks

Kevin Lamshöft, Tom Neubert, Mathias Lange, Robert Altschaffel, Mario Hildebrandt, Yongdian Ding, Claus Vielhauer and Jana Dittmann

Planned entry for
KERNTECHNIK 2020

Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag

The work in this paper has been funded by the German Federal Ministry for Economic Affairs and Energy (BMWi, Stealth-Szenarien, Grant No. 1501589A, 1501589B and 1501589C) within the scope of the German Reactor-Safety-Research-Program.

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

1 Introduction

Nowadays, there are a lot of defense mechanisms to secure IT-systems against Cyber attacks. Thus, Cyber attacks have to be more sophisticated than they used to be in order to stay undetected as long as possible and to bypass defense mechanisms. As a result, current threats frequently use steganographic techniques to hide malicious functions in a harmless looking carrier. In *[1]* an attack for Siemens S7 Simatic Programmable Logic Controllers (PLCs) is presented, where the control logic of the PLC is modified while the source code which the PLC presents the engineering station is retained. As a result, the PLCs functionality is different from the control logic presented to the engineering station. Furthermore, steganographic techniques are frequently used to hide information in media files.

In *[2]* BlackBerry Threat Researchers discovered hidden malicious code in WAV audio files, where the files were coupled with a loader component for decoding and executing malicious content secretly. Additionally, image steganography is used in *[3]* to obfuscate network traffic. The article *[4]* shows how image steganography is used to hide malicious JavaScript code in PDF files. In addition, network traffic is a well-known carrier for steganography to embed hidden communication. The work *[5]* presents for example a technique which uses the DNS protocol as steganographic carrier. However, Industrial Control Systems (ICS) control essential process control functions in Nuclear Power Plants (NPP). They rely on sensors (collecting information about the physical process), computing units (PLCs) and actuators (implementing the commands issued by the computing units) and the communication between these components. These ICS form complex communication networks with differing security requirements. As computer systems, ICS are target of attacks *[10, 11, 12, 13]*. These attacks aim at data exfiltration (an attacker gaining unauthorized access to data) or data infiltration (an attacker manipulating digital assets). In previous work, we evaluated common protocols found in ICS environments, like Modbus/TCP and OPC UA in regards to steganographic channels. In *[27]* we take a deeper look at Modbus/TCP and describe various methods for hiding information in ICS networks. In *[26]* we propose a method for OPC UA based hidden channel attacks. In *[25]* we provide a broader view on how information hiding become a novel threat for nuclear security. Even though there are various common security measures like firewalls and IDS, which can detect and partially mitigate a broad range of attacks, they still lack the ability to detect attacks which rely on information hiding properly. Here, more complex detection measures are required. However, since ICS networks and the employed infrastructure is different from IT, this carries different implications for the detection of attacks as well. This paper aims at using the specific properties of ICS networks and protocols in order to improve the detection of attacks employing information hiding measures. After describing the basics of network information hiding in Chapter 2, we demonstrate in Chapter 3 how it can be generally applied to I&C environments and described and modeled as a kill chain. Chapter 3 concludes with details on how two common hiding patterns can be applied to ICS protocols. In Chapter 4 we briefly describe the shortcomings of common IDSs and apply recommendations for anomaly detection to a model factory in order to motivate further research in this field – especially the need for developing reliable detection methods regarding information hiding based attacks in this specific domain. Chapter 5 concludes our findings and gives an outlook on future research.

2 Network Information Hiding

Network Information Hiding is only one subtopic of many in the field of information hiding and steganography. Recent research, which also has implications for I&C communication, include the pattern based taxonomy of Wendzel et al. *[17]* and its later extension *[16]*, which we use in this paper to formally describe potential information hiding based attacks. A survey of network steganography and its techniques is presented in *[6]*. Information Hiding in the Internet Protocol has been shown for the Internet Protocol v4 (IPv4) *[19]* as well as the application of covert channels to IPv6 in real world scenarios *[18]*. In order to evaluate whether rule-based IDS systems are appropriate to detect covert channels in ICS protocols, we use the extended pattern based taxonomy by Mazurczyk et al. *[16]*, which is originally introduced by Wendzel et al. in 2015 *[17]*. Hidden channels in network communication can be differentiated in storage and timing channels. The pattern based taxonomy is an approach to define general patterns, which are used for information hiding. The extended taxonomy is based on the analysis of over one hundred information hiding techniques, and unifies them into 18 general patterns, of which are 8 based on packet or flow timings (timing channel), and 6 on modification of data of a packet or flow (storage channel). By this, it is possible to describe covert channels in different protocols in a unified way. We use these patterns in a reversed way to evaluate if those patterns can be detected in common configured rule-based IDS systems.

3 Information Hiding as a Novel Threat for I&C environments

In this chapter, we show how network information hiding can be applied to the specifics of ICS networks and describe an exemplary attack scenario as well as how two generic patterns can be applied to ICS protocols. In this paper we focus on information hiding by modification of existing communication in a given target network. As stated in Chapter 2, two categories of hidden channels can be distinguished for network information hiding: timing channels, which modulate the temporal behavior of a packet flow and storage channels which modify contents of specific packets to embed a secret message or information. To illustrate the purpose and functionality of information hiding a common scenario is the so-called Prisoners' Problem where a sender (usually called Alice) and a receiver (usually called Bob) are imprisoned in different cells. This scenario includes the possibility for Alice to send messages to Bob, with the limitation that a warden is able to see and read the communication. Therefore, the aim of Alice and Bob is to hide the actual information within the communication that is observed by the warden *[15]*. In the context of Industrial Control Systems, Alice and Bob are usually OT components, for example PLCs, Human-Machine-Interfaces (HMI) and Engineering Workstations, or network elements like switches, hubs and firewalls. Based on this assumption, we can differentiate between active, passive and hybrid information hiding (see *[27]*). When the embedding and retrieval takes place at the originating entities (e.g. a PLC and HMI) of the communication, this is considered as active hiding, whereas passive embedding and retrieval takes place on intermediaries, like switches and firewalls. The mix between those two are considered as hybrids. For the successful use of information hiding in (ICS) networks we can define three requirements that need to be addressed (see *[27]*): cover plausibility, protocol-compliance and warden-compliance. Cover plausibility refers to the use of cover channels or objects which are plausible within the usual, realistic and expected communication flow and behavior of the target system. A covert channel is considered protocol-compliant, when a modification of a packet or packet flow does not break the specified protocol in a way the recipient would not receive, accept or process the packet. The warden-compliance can be differentiated in three levels (based on probabilities): (1) the message is hidden in a way that a potential warden has no knowledge of the existence of a hidden message (inconspicuous), (2) the warden has a suspicion that there is a hidden message but cannot access it and (3) the warden can identify and access but not reconstruct the hidden message.

3.1 Kill Chain & Exemplary Attack Scenario

Unfortunately, current defense mechanisms lack effective measures against novel attack scenarios with steganographic techniques. In order to defend I&C environments an attack modeling can help to understand and comprehend attacks with steganographic techniques to elaborate protective security mechanisms. One way to do so, is to use the Lockheed Martin Cyber Kill Chain by Hutchings et al. *[7]*. The Kill Chain is a 7-stage-model (Reconnaissance (1), Weaponization (2), Delivery (3), Exploitation (4), Installation (5), Command & Control (6) and Action on Objectives (7)) developed by the U.S. company Lockheed Martin Corporation and is briefly described in *[7]*. It is developed to analyze cyber-attacks (especially advanced persistent threats) and to derive security mechanisms along all phases of the attack modeling. Furthermore, attack indicators can be elaborated based on the Kill Chain attack modeling. The Kill Chain is described as a "chain" because an interruption of the "chain" will stop the entire attack process. So, an attacker has to go through the entire Kill Chain to reach their goals and a defender can stop an attack on every phase.

3.1.1 Attack Scenario

In this work, we design a fictional and exemplary attack scenario which could take place in an I&C environment. We conduct Kill Chain attack modelling in order to demonstrate how the modelling works for attacks with steganographic techniques in I&C environments and how it could reveal security vulnerabilities. Furthermore, security mechanisms can be elaborated based on the attack modelling. The fictional attack scenario is based on the BSI-CS 005E Top 4 scenario *[8]* and the MITRE ATT&CK® Framework for ICS. For our exemplary scenario we assume that the firmware of a PLC is corrupted via a supply chain attack or modified by an inside threat (e.g. third-party contractors). The corrupted firmware enables the ability to embed hidden information into the data which is sent to the plant historian. The retrieval takes place on the workstation of the analyst who has access to the plant historian's data. By this procedure, it is possible to exfiltrate valuable information from higher security levels.

3.1.2 Kill Chain Attack Modelling

In this section, we model the introduced attack vector with the Kill Chain and propose security mechanisms and attack indicators based on the modelling. The modelling is visualized in **Figure 1**. In Phase 1 (Reconnaissance) the attacker has to gain information on the network infrastructure. Common scenarios are social engineering, insiders, and targeted attacks e.g. on document servers. To mitigate Phase 1 awareness for social engineering can be improved by special trainings of the employees. During Phase 2 (Weaponization) the development of the (manipulated) firmware and the receiving tool takes place. In Phase 2, defenders cannot directly prevent the attack, but comparable attacks which include steganographic techniques can be analyzed and evaluated. The 3rd Phase (Delivery) brings the malware developed in Phase 2 to the I&C environment. In this scenario, the PLC gets manipulated before it is delivered to the plant. The tool for receiving could be delivered by removable devices (e.g. by utilizing common steganographic methods to avoid detection) or developed in-situ by the employee which has access to the data historian. To stop the attack in Phase 3 all delivery vectors need to be monitored closely and mitigated by structural defensive measures. Phase 4 (Exploitation) takes place by delivery and installation of the infected PLC as well as the installation of the receiving tool via USB or in-situ development. To prevent the attack, defensive methods against supply chain attacks need to be implemented (e.g. code reviews). Phase 5 (Installation) is done with delivery of the PLC or triggered by time or certain events (logic bomb). The installation of the receiving tool takes place on the data analysts' workstation. The malware might be detected by anti-virus-software. During Phase 6 (Command & Control) the usual network traffic

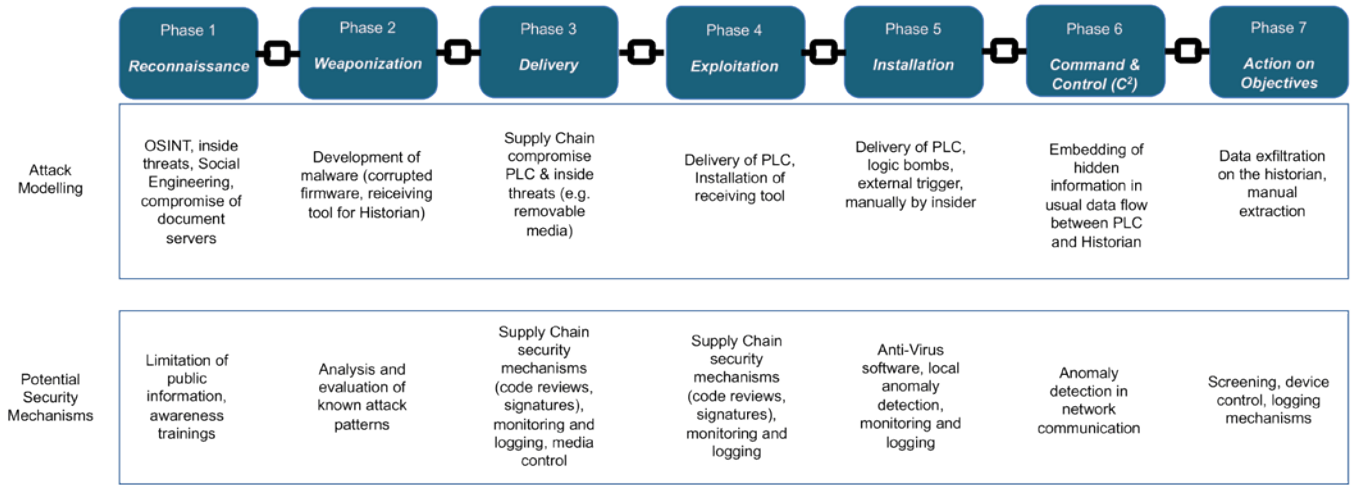

Fig. 1.
Kill Chain model of the exemplary attack scenario.

from the PLC to historian is misused to hide information within this data which is then stored on the historian. Detection approaches for Phase 6 are discussed in Chapter 4.2 and in Chapter 5. In Phase 7 the hidden information is extracted from the historian and exfiltrated by the data analyst. Screening, device control, and logging mechanisms might mitigate the exfiltration.

3.2 Exemplary Generic Hidden Channels in ICS protocols

To illustrate the threat and applicability of hidden communication we describe two hidden channel patterns that are applicable to most ICS protocols and could be part of the previously described attack scenario: (1) Payload Modulation and (2) Inter-Packet Timing Modulation. Even though there is a large variety of different protocols, that are used in ICS environments, most of them share certain inherent characteristics that can be (mis-)used for information hiding. A common example is the periodic transmission of sensor data of a PLC to another entity in a specific timing interval. Independently from the used protocol a potential adversary can encode a hidden message by manipulating those timings, e.g. by delaying certain packets for a given amount of time. This can be done in an active way (e.g. on the PLC and receiving entity), in a passive way by network elements or in a hybrid form. For example, a compromised PLC can delay responses to embed a single bit into one packet, whereas a network element (e.g. a switch) can observe and calculate those delays to decode the hidden message of the PLC. This pattern is called Inter-Packet Timing Modulation *[16]*. Another common scenario is the transmission of sensor data or high-resolution set points, e.g. temperatures. Depending on the resolution, the payload modulation pattern *[16]* can be used by altering the least significant bit (LSB) of sensor data to encode a hidden message. In high resolution readings, such modifications alter the sensor data only slightly, and therefore do not have impact on the controlled (physical) process while being unnoticeable for humans.

4 Strategic Preparation & Anomaly Detection

In this chapter we briefly describe the limitations of common IDS systems regarding the detectability of information hiding in ICS networks and apply, as a first step, measures of anomaly detection to a real-world ICS demonstrator.

4.1 Limitations of common IDS systems

Different security measures are in use in the domain of information technology. Some of these measures are also applied in the domain of ICS. Intrusion Detection Systems (IDS) collect data from either the network (network-based IDS) or from the computer systems within a network (host-based IDS). This data is checked for the signatures of known attacks or suspicious behavior patterns. Anomaly detection is the reversal of an IDS. While an IDS looks for known patterns of malicious behavior, an anomaly detection detects unusual behavior (see *[9]* for more details). In order to achieve this, an IDS needs to have a model of normal behavior. Usually, anomaly detection learns this usual behavior during a training phase.

Common Intrusion Detection Systems, like Snort *[20]* and Suricata *[21]* use signatures of known patterns or suspicious behavior patterns to detect potential attacks. For the example of Modbus/TCP there are several rulesets for Snort and Suricata *[22, 23]*. For example, the Quickdraw Rule Set *[22]* defines certain IP(-ranges), that are allowed to communicate with each other. The rule set also checks for known attack patterns, e.g. denial of service attacks. Other rule sets, e.g. *[23]* are built upon the Modbus/TCP specification and test against any violations. As described in Chapter 3, these procedures are mainly testing for protocol-compliance. Since many information hiding based attacks, e.g. the exemplary attacks of chapter 3.2, can be performed within the limits protocol-compliance, those IDS systems are not able to detect the hidden communication. Especially the category of timing-based channels are not detectable by those means without further extensions. However, certain storage channels, for example the use of unused fields, are detectable by those systems, if specific rules, that check against those known signatures, are available.

Due to these limitations, we are going in the opposite direction by using anomaly detection as a first step towards detecting information hiding in I&C environments. As a first starting point we use the BSI CS 134E recommendations *[9]* and evaluate how they could be applied to real world scenario.

4.2 Applying the BSI CS 134E two a real world scenario

For an anomaly detection it is important to filter data in a targeted and efficient way. This requires a selection of processes and procedures. For these analysis criteria are defined so that

the Security Information and Event Management (SIEM) can determine the normal state. This is used as a reference for future analyses. Over a longer period of time, an image of the normal state is generated during a training phase in an uncompromised I&C system. Thus, the SIEM can store data of events, such as cycle times of processes or DHCP requests from known devices in the network, in order to evaluate future events with this data. Therefore, a decision is made whether the event is categorized as an anomaly. In order to specifically detect anomalies, a SIEM system at the University of Applied Sciences Magdeburg-Stendal is integrated into a model factory to evaluate different attacks and their detection levels. The model factory represents the production process of a complete filling plant with different production sections including distillery. Various system data of the sections of the model factory are logged, then centrally analyzed and interpreted in SIEM. **Figure 2** shows an example of where and which data could be collected, based on the proposals of the BSI *[9]*. Three mechanisms shall be used: logging, network access control (NAC) and netflow analysis. Logging data can be collected directly at the PLCs of the individual sections of the model factory, such as at the distillery or during the filling process. Process data (sensor values, frequency, cycle times, ...), access to the PLCs (user, time, ...) and ICS protocol data (unusual error messages, faulty data packets, ...) are logged. Further information is available on intelligent, manageable switches. These provide logging data about network activities (device logins, DHCP requests, data packets from unknown devices, ...). Permanent communication between the switches and the NAC server automatically detects the devices currently connected to the network. Intruders can be immediately identified, moved to quarantine zones or logically separated from the network. In addition to this feature, the devices can also be checked for security guidelines for devices within the network, such as the latest firmware version, software installed on the devices and others. The investigation is rounded off by the integration of a netflow analysis. In addition to the possibilities of monitoring and optimized display, this offers network behavior anomaly detection, as well as real-time DDoS detections and application performance monitoring.

The presentation of the results can be user-specific, the spectrum ranges from a traffic light system to detailed reports. The difficulty with the detection of hidden channels lies in the fact that the data is hidden in usual user data and transported over normal network traffic and is not detected with the previous control routines because it does not appear to be an anomaly. The big challenge is to identify the right indicators and tools for hidden channel attacks or to develop them if necessary. In this way, an intelligent linking of the analysis mechanisms can contribute to a more efficient plausibility control of the transmitted data in I&C systems and thus improve IT security. Still, even by applying those measures, a reliable detection of previously unknown hidden channels remains a challenge.

5 Conclusion

Based on the findings of chapter 4 we have to adjust our detection approaches in future work. For future detection approaches, we are planning to design detection approaches based on machine learning. For our machine learning based detection approaches, we will design a comprehensible feature space with handcrafted features. Approaches based on machine learning have to be trained with representative training data of an I&C environment. Therefore, we will set up our own fictitious reference facility to acquire representative network traffic and consequently training and test data. When training and test data is available, we will extract the handcrafted feature spaces from the data and train a classifier which should be able to detect steganographic or abnormal network traffic. Therefore, One-Class-Classifier or Two-Class-Classifier could be trained. For a One-Class-Classifier we train only the target class with known-good network traffic to detect outliers of this class. For a Two-Class-Classifier we need to train one class with known-good network traffic and one class with abnormal or steganographic network traffic, then the classifier decides if test data belongs to known-good class or the class with abnormal network traffic. Thus, we need to generate steganographic network traffic to build a Two-Class-Classifier. In this paper, we showed the emergence of information hiding as a new threat for I&C environments and the limitations of common IDS systems against such attacks. Anomaly detection based systems need to be adapted and extended in

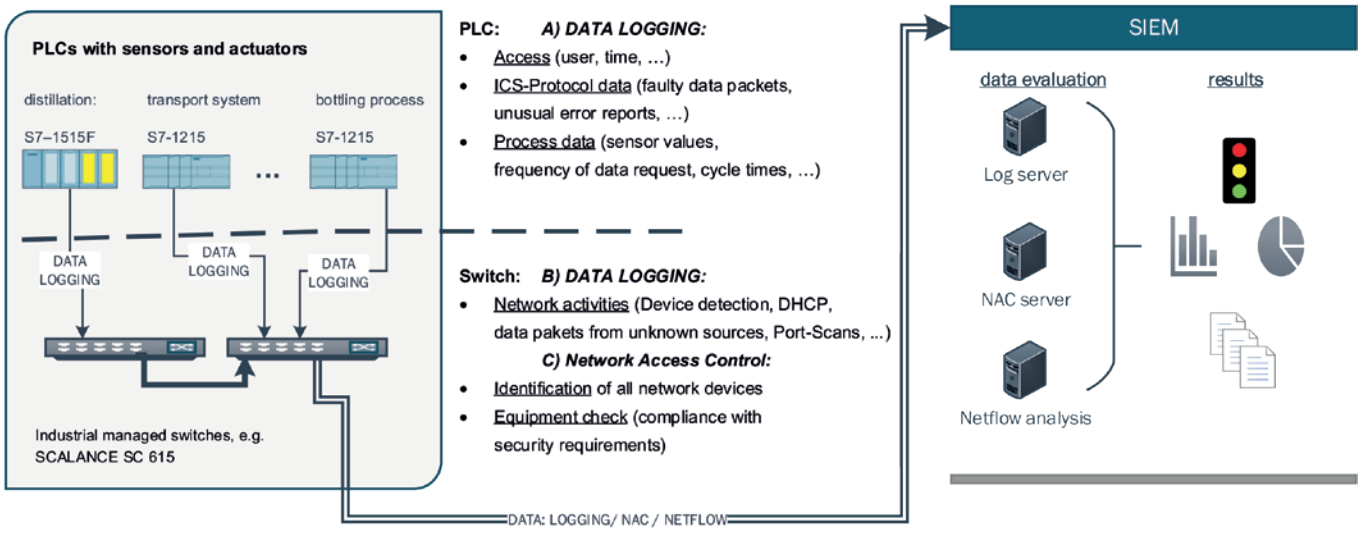

Fig. 2.
Presentation of data logging with inclusion of I&C components of the model factory at PLC level.

order to accurately and reliably detect such novel attack patterns for this specific domain. In the future, machine learning based approaches will be further investigated as a possible solution for the detection and mitigation of information hiding based attacks in I&C environments.

References

[1] Biham, E.; Bitan, S.; Carmel, A.; Dankner, A.; Malin, U.; Wool, A.: PPT: "Rogue7: Rogue Engineering-Station attacks on S7 Simatic PLCs" at Black Hat USA 2019; 2019 Aug 8 Mandalay Bay / Las Vegas. Online available from: https://i.blackhat.com/USA-19/Thursday/us-19-Bitan-Rogue7-Rogue-Engineering-Station-Attacks-On-S7-Simatic-PLCs-wp.pdf

[2] Soni, A.; Barth, J.; Marks, B.: "Malicous Payloads – Hiding Beneath the WAV" in Threatvector October 16, 2019 Online available from: https://threatvector.cylance.com/en_us/home/malicious-payloads-hiding-beneath-the-wav.html

[3] z3roTrust: "ScarCruft APT Malware Uses Image Steganography" in Medium Online available from: https://medium.com/@z3roTrust/scarcruft-apt-malware-uses-image-steganography-c69d51fa9bbb

[4] Arghire, I.: "Attackers Use Steganography to Obfuscate PDf Exploits" in SecurityWeek January 24, 2019, Online available from: https://www.securityweek.com/attackers-use-steganography-obfuscate-pdf-exploits

[5] Drzymala, M.; Szczypiorski, K.; Urbanski, M.: "Network Steganography in the DNS Protocol" in JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2016, VOL. 62, NO. 4, PP. 343-346, DOI: 10.1515/eletel-2016-0047

[6] Singh, N.; Bhardwaj, J.; Raghav, G.: "Network Steganography and its Techniques: A Survey." in International Journal of Computer Applications (0975 –8887) Volume 174 – No.2, September 2017

[7] Hutchings, E., Cloppert, M., and Amin, R. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lockheed Martin Corporation.

[8] Federal Office for Information Security (BSI), Recommendation: IT in Production, Industrial Control System Security, "Top 10 Threats and Countermeasures 2019", BSI Publications on Cyber-Security, BSI-CS 005E V1.30, 2019

[9] Federal Office for Information Security (BSI), Recommendation: IT in Production, "Monitoring and Anomaly Detection in Production Networks: Is this normal?", BSI Publications on Cyber-Security, BSI-CS 134E V1.00, 2019

[10] Neubert, T.; Vielhauer, C. : Kill Chain Attack Modeling for Hidden Channel Attack Scenarios in Industrial Control Systems. Manuscript 1475 accepted to 21st IFAC World Congress, 2020. (to be published)

[11] R. M. Lee, M. J. Assante, T. Conway: "Analysis of the Cyber Attack on the Ukrainian Power Grid", https://ics.sans.org/media/EISAC_SANS_Ukraine_DUC_5.pdf (23/05/2018), 2016.

[12] N. Falliere, L. O Murchu, E. Chien: "W32.Stuxnet Dossier", https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf(18/05/2018), 2011.

[13] Ralf Spenneberg, Maik Brüggemann, Hendrik Schwartke: "PLC-Blaster: A Worm Living Solely in the PLC", https://www.blackhat.com/docs/us-16/materials/us-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-ThePLC-wp.pdf (23/05/2018), 2016.

[14] S. Gallagher: "Vulnerable industrial controls directly connected to Internet? Why not?", https://arstechnica.com/information-technology/2018/01/theinternet-of-omg-vulnerable-factory-and-power-grid-controlson-internet/ (23/05/2018), 2018.

[15] Ker, Andrew: Information Hiding (complete), (2016), http://www.cs.ox.ac.uk/andrew.ker/docs/informationhiding-lecture-notes-ht2016.pdf

[16] Mazurczyk, Wojciech, Steffen Wendzel, and Krzysztof Cabaj. "Towards deriving insights into data hiding methods using pattern-based approach." Proceedings of the 13th International Conference on Availability, Reliability and Security. ACM, 2018.

[17] Wendzel, Steffen, et al. "Pattern-based survey and categorization of network covert channel techniques." ACM Computing Surveys (CSUR) 47.3 (2015): 50.

[18] Mazurczyk, Wojciech, Krystian Powójski, and Luca Caviglione. "IPv6 Covert Channels in the Wild." Proceedings of the Third Central European Cybersecurity Conference. ACM, 2019.

[19] Mazurczyk, Wojciech, et al. "Towards Reversible Storage Network Covert Channels." Proceedings of the 14th International Conference on Availability, Reliability and Security. ACM, 2019.

[20] Cisco, Snort, Network Intrusion Detection & Prevention System https://snort.org/, (16.12.2019)

[21] Open Information Security Systems, Suricata, Open Source IDS / IPS / Nsm engine, https://suricata-ids.org (16.12.2019)

[22] Digitalbond, Quickdraw-Snort, Github.com, https://github.com/digital bond/Quickdraw-Snort/blob/master/modbus.rules (16.12.2019)

[23] Luis Martin, Snort Rules for Modbus, Liras en la red, http://www.lirasen lared.xyz/2018/06/snort-rules-for-modbus.html (12.12.2019)

[24] The MITRE Corporation, MITRE ATT&CK® for Industrial Control Systems, https://collaborate.mitre.org/attackics/index.php/Main_Page (13.03.2020)

[25] Hildebrandt, Mario; Altschaffel, Robert; Lamshöft, Kevin; Lange, Matthias; Szemkus, Martin; Neubert, Tom; Vielhauer, Claus; Ding, Yongjian; Dittmann, Jana: Threat analysis of steganographic and covert communication in nuclear I&C systems: International Conference on Nuclear Security 2020: 10-14 February 2020 – Indico, 2020. – 2020; https://conferences.iaea.org/event/181/contributions/15608/attachments/8569/11404/CN278_478-stealth_v006.pdf ; [Konferenz: 3. International Conference on Nuclear Security, ICONS 2020, Vienna, Austria, 10 - 14 February 2020]: 2020

[26] Hildebrandt, Mario; Lamshöft, Kevin; Dittmann, Jana; Neubert, Tom; Vielhauer, Claus: Information hiding in industrial control systems – an OPC UA based supply chain attack and its detection: IH & MMSec '20: proceedings of the ACM Workshop on Information Hiding and Multimedia Security : Denver, CO, USA, June, 2020 – New York, NY: The Association for Computing Machinery, 2020. – 2020, S. 115-120; unter URL: http://dx.doi.org/10.1145/3369412.3395068; [Workshop: ACM Workshop on Information Hiding and Multimedia Security, IH & MMSec '20, Denver, USA, June 2020]:2020

[27] Kevin Lamshöft and Jana Dittmann. 2020. Assessment of Hidden Channel Attacks: Targetting Modbus/TCP. To appear in 21st IFAC World Congress, Elsevier ScienceDirect IFAC-PapersOnLine. Berlin, Germany.

Authors Kevin Lamshöft
kevin.lamshoeft@ovgu.de

Robert Altschaffel
Mario Hildebrandt
Jana Dittmann
Otto-von-Guericke University Magdeburg
ITI Research Group on Multimedia and Security
University Square 2
39106 Magdeburg, Germany

Tom Neubert
Claus Vielhauer
Brandenburg University of Applied Sciences
Department of Informatics & Media
Magdeburger Straße 50
14770 Brandenburg an der Havel, Germany

Mathias Lange
Yongdian Ding
Hochschule Magdeburg-Stendal
University of Applied Sciences
Institute for Electrical Engineering
Breitscheidstr. 2
39114 Magdeburg, Germany

nucmag.com

atw

International Journal
for Nuclear Power

Subscription

I would like to subscribe from now on to atw – International Journal for Nuclear Power.

☐ Mr ☐ Ms

Surname, First Name

Organization

Sector of your organisation
☐ Industry ☐ Utilities ☐ Research/Education
☐ Consulting/Services ☐ Expert organization ☐ Administration
☐ Association ☐ Other:

Order No.

Street

Postal Code City Country

Telephone, E-mail

VAT No. (EU countries except Germany)

Billing address (if different from subscription address):

☐ Mr ☐ Ms

Surname, First Name

Organization

Street

Postal Code City Country

Telephone, E-mail

You will receive atw for a price of:

- **Annual subscription – 9 issues 183.50 €**
  (20.38 € per issue/copy instead of
  23.55 € per single issue/copy)

Preferred payment method (please tick):

☐ By invoice

☐ By SEPA Direct Debit

Name of bank

IBAN

BIC

☐ **I agree to the terms and conditions below.**

Date Signature

Please send your order to:

INFORUM Verlags- und
Verwaltungsgesellschaft mbH
Petra Dinter-Tumtzak
Robert-Koch-Platz 4
10115 Berlin, Germany

Mail to: info@nucmag.com
or order online: www.nucmag.com/shop

Terms and conditions

Prices for annual subscription outside Germany and for single issues excluding postage.

Prices including 5 % VAT for Germany and all EU member states without VAT number. For EU member states with VAT number and all other countries the price for annual subscription will be reduced to 174.77 €.

The publisher must be notified of cancellation of the subscription no later than 4 weeks before the end of the subscription period. Unless terminated with a notice period of 4 weeks to the end of the subscription period, the subscription will be extended for a further year in each case under the subscription terms applicable at the time.

Right of cancellation: This order may be cancelled within 14 days of the order form being received at INFORUM Verlags- und Verwaltungsgesellschaft mbH, Robert-Koch-Platz 4, 10115 Berlin, Germany.

atw
International Journal
for Nuclear Power

Guideline for authors

publishing Technical Papers in atw

The technical and scientific reports in atw cover developments and trends in all major areas of nuclear power technology, as also related energy economics, law and energy politics.

Articles are presented by scientists and researchers, industry and suppliers, utilities, authorities and independent experts.

Manuscript

Technical papers are published free of charge.

E-mail-Address	editorial@nucmag.com
Language	English
File format	DOC or RTF document (no PDF)
Exclusion of promotion	Organisation, product and brand names are permitted as far as they contribute to the understanding of the paper.
External editorial deadline	6 weeks prior to the concerning issue.

Papers (text ad figures) are subject to review by the atw.

Publisher

INFORUM Verlags- und Verwaltungsgesellschaft mbH
Robert-Koch-Platz 4, 10115 Berlin, Germany
Phone +49 30 498555-33
E-mail info@nucmag.com
Web www.nucmag.com

Editorial

Christopher Weßelmann
(Editor in Chief)
Phone +49 2324 43977-23
E-mail christopher.wesselmann@nucmag.com

Nicole Koch
(Editor)
Phone +49 163 7772797
E-mail nicole.koch@nucmag.com

1. Main text

Languages English

Scope min. 13,000 characters
max. 35,000 characters
(incl. blanks)

Clear structure

1 Headline
all authors with academic title, first and surname, organisation, position and place
2 Introduction
(description of the problem)
3 Main part
4 Summary/result

2. Figures and tables

Number permitted max. 12 figures
max. 8 tables

Remark Please do not insert your figures into the text but in a separate file. Please integrate your tables in the text (Word table). Designate the position in the text with reference: (Figure 1) or (Table 1). Please list the captions to figures and tables at the referenced position in the text.

Files needed

Digital files with resolution > 300 dpi
or PowerPoint® presentation
with true-to-the-detail figures.

The author accepts the conditions of publication when providing the manuscript – atw has the right of publication and exploitation. The author assures that no third party right will be infringed when publishing his paper in atw. In such cases, the editorial office must be informed.

Please do not hesitate to contact us if you have further queries.
Thank you for your support.

Editorial Christopher Weßelmann
Editor in Chief

Nicole Koch
Editor

View publication stats