This is a pre-print version of the paper entitled: "Protecting IEC 60870-5-104 ICS/SCADA Systems with Honeypots". The public version is available in IEEE Xplore: "https://ieeexplore.ieee.org/document/9850329" - E. Grigoriou et al., "Protecting IEC 60870-5-104 ICS/SCADA Systems with Honeypots", 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022. Available: 10.1109/csr54599.2022.9850329.

Protecting IEC 60870-5-104 ICS/SCADA Systems with Honeypots

Elisavet Grigoriou
Sidroco Holdings Ltd
Nicosia, Cyprus
egrigoriou@sidroco.com

Athanasios Liatifis
University of Western Macedonia,
Kozani, Greece
aliatifis@uowm.gr

Panagiotis Radoglou Grammatikis
University of Western Macedonia,
Kozani, Greece,
pradoglou@uowm.gr

Thomas Lagkas
International Hellenic
University, Kavala, Greece
tlagkas@cs.ihu.gr

Ioannis Moscholios
University of Peloponnese,
Greece, idm@uop.gr

Evangelos Markakis
Hellenic Mediterranean University,
Greece, emarkakis@hmu.gr

Panagiotis Sarigiannidis
University of Western Macedonia,
Kozani, Greece, psarigiannidis@uowm.gr

***Abstract*—Both signature-based and anomaly-based Intrusion Detection and Prevention System (IDPS) have already demonstrated their efficiency towards recognising and mitigating various intrusions. However, the first category cannot detect zero-day attacks, while the second one lacks the presence of appropriate datasets. Therefore, the presence of additional cybersecurity mechanisms is necessary, especially in the area of the Industrial Internet of Things (IIoT), including critical infrastructures, such as the smart electrical grid. Thus, honeypots are used to hide and protect critical assets. IEC 60870-5-104 (IEC104) is a widely used telemetry protocol in Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA). However, IEC104 lacks critical security features, such as encryption, integrity protection and authentication. This work presents the IEC104 honeypot, which is capable of hiding the actual IEC104 assets and detecting potential intrusions and anomalies. The experimental results demonstrate the effectiveness of our work.**

***Index Terms*—Cybersecurity, Honeypots, IEC 60870-5-104, ICS, SCADA, Smart Electrical Grid**

I. Introduction

As the use of internet-connected energy elements increases, allowing for remote monitoring of elements, both cyberattackers and cybercriminals are seeking new ways to compromise the security of critical Internet of Things (IoT) and Industrial IoT (IIoT) environments such as the smart electrical grid. In this paper, we focus our attention on the security of IEC 60870-5-104 (IEC-104) Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems. IEC-104 is a telemetry protocol widely used in European EPES. However, it suffers from severe cybersecurity issues since it does incorporate essential security mechanisms, such as encryption, authentication and authorisation. Therefore, the presence of extra protection mechanisms are necessary.

Although both signature-based and anomaly Intrusion Detection and Prevention Systems (IDPS) are efficient with respect to detecting malicious activities, the former cannot recognise unknown anomalies and zero-day attacks, while the second are characterised by False Positives (FP) and False Negatives (FN) depending on the available datasets adopted. Therefore, in this paper we focus our attention on another cybertrap mechanism, called *honeypots*. The main goals of a honeypot is to (a) hide and protect the actual assets, (b) to decoy the cyberattackers and (c) to collect useful information about the malicious activities. Therefore, based on the aforementioned remarks, in this paper, we present an IEC-104 related honeypot capable of hiding and protecting the IEC-104 EPES entities, collecting in parallel valuable logs related to the misuse of the IEC104 commands.

Based on the aforementioned remarks, the reminder of this paper is organised as follows. Section II present similar works in this field. Section III discusses the role of honeypots and their main categories. Section IV presents an overview of the IEC-104 protocol. Section V provides the proposed IEC-104 honeypot. Finally, section VI shows the experimental results of this work, while section VII concludes this work.

II. Related work

Several papers investigate the usage of honeypots for protecting both IoT and IIoT environments. Some of them are listed in [1], [2], [3], [4], [5]. In [1], J. Franco et al. provide a detailed survey regarding the use of honeypots in IoT and Cyber-Physical Systems (CPS). Similarly, in [2], the authors present a survey on honeypot software, paying special attention to a relevant data analysis. In [3] S. Sharma and A. Kaul provide a comprehensive study about honeypots in Vehicular Ad hoc Networks (VANETs). In [4], J. Uitto et al. discuss anti-honeypot strategies. Finally, in [5], the authors investigate the use of honeypots concerning the Machine Learning (ML)-based intrusion detection. Next, we analyse further some similar works.

`MimePot` [6] uses a model-based methodology, allowing it to imitate procedures in order to entice skilled attackers targeting industrial installations. Furthermore, `MimePot` takes full advantage of Software Defined Networking (SDN) technology to ensure a stable and future-proof security strategy. In a simulated water distribution system, the authors show the effectiveness of `MimePot` with respect to the detection of data integrity attacks.

In [7], the authors present TRUSTY, a strategic honeypot deployment and analysis platform. First, with respect to the strategic honeypot deployment, the authors provide an antagonistic game model between the attacker and the defender, utilizing honeypots. The goal of the defender is to deploy the optimal number of honeypots, taking into account the behaviour of the attacker and the available computing resources. The proposed model is solved through a Reinforcement Learning (RL) method called $e - Greedy$. Moreover, $TRUSTY$ is capable of processing and analysing the honeypots' data through a user-friendly environment. The evaluation results demonstrate the efficiency of TRUSTY.

In [8], the authors introduce the use of wireless honeypots in ultra-dense Beyond 5G (B5G) networks. Moreover, the authors model and discuss the strategic deployment of honeypots in ultra-dense B5G networks. This problem is solved with $Q - Learning$. The simulated results demonstrate the efficiency of the proposed method.

In [9], the authors proposed a network industrial honeypot system named *DiPot* for monitoring Internet scanning and attack patterns against industrial control systems. *DiPot* provides attack clustering and visualization services to customers and could assist users in understanding the present state of ICS security. Two advantages distinguish *DiPot* from existing Honeypot systems: high-level modelling and comprehensive data analysis. Additionally, *DiPot* is equipped with a sophisticated visualization frontend and could provide consumers with a positive experience. *DiPot* has amassed an abundance of data for six consecutive months and captured actual Internet assault samples. The experimental results suggest that *DiPot* is effective and efficient.

HoneyPLC [10] was offered as a high-interaction, flexible, malware-collecting honeypot that supports a wide range of PLC models and suppliers. Experiments indicate that *HoneyPLC* demonstrates a high level of camouflage: it is detected as an actual device with high confidence by various widely used reconnaissance tools, such as Nmap, Shodan Honeyscore and PLCScan. By locating *HoneyPLC* on Amazon Amazon Web Services (AWS), it was observed that a significant number of intriguing interactions over the Internet was recorded, demonstrating that attackers are indeed targeting ICS systems and *HoneyPLC* can successfully engage and fool them while gathering data samples for future analysis.

HoneyVP [11] is a revolutionary honeypot architecture that supports a semi-virtual and semi-physical honeypot design to provide cost-effective performance. There was initially an investigation of cyberattacks on ICS devices in terms of interaction levels. In order to combat these threats, *HoneyVP*'s design defines three core independent and cooperating components: the virtual component, the physical component and the coordinator. Finally, a unified local-remote ICS honeypot system is constructed to test its viability and efficacy. The experimental results demonstrate the superiority of the proposed architecture over previous honeypot systems. *HoneyVP* provides a cost-effective solution for ICS security researchers, increasing the allure of ICS honeypots and enabling the collection of physical interactions.

III. Honeypots Overview

Honeypots are frequently used by security personnel to obtain information about an attacker. Attackers vary their strategies frequently to take advantage of various types of attacks. In rare instances, attackers use zero-day attacks against honeypot servers. If the security operator or administrator fails to configure the honeypot correctly, an experienced attacker may view it as suspicious and avoid it. The honeypot enables the security team to comprehend the techniques of attackers, learn more about known and new assaults, and so safeguard the actual production systems more effectively. On the basis of this information, advantages and disadvantages of honeypots can be recognized. (1) Attackers can be watched in action and get insight into their behavior. (2) Knowing the sorts of assaults in use assists the security team in implementing the necessary defenses to safeguard your actual systems and data from attack. (3) An attack on a honeypot is likely to discourage intruders and prevent them from breaking into the actual computer systems. (1) Only when an attacker is actively attacking the system may data be captured. (2) If an attack occurs on a different system, the honeypot will be unable to detect it. (3) An attacker may utilize the victim's own honeypots as a bot to distract the victim. Thus granting them the ability to attack and compromise additional systems within the network. Depending on the sort of honeypots employed, the advantages and disadvantages described above may or may not appear. As shown in Figure 1, honeypots can be categorized based on their physicality, operating field, location, and interaction level.

- **Operation Field**. Honeypots can be utilized for two distinct goals[12]: production and research. A production honeypot helps reduce risk by enhancing security procedures. When a honeypot is used for research, it gathers useful information for the community to develop intelligence on risks and assaults, enhancing the protection of companies' systems. Lack of opponent knowledge, such as who the danger is, why they attack, how they attack, and when they attack, is a major security concern. The security community can't always answer these issues. To defeat a threat, first identify it. Information security lacks such data. Honeypots boost research value by allowing threat study [7]. Honeypots provide full attack information but are hard to deploy. The goal is to keep them at high risk so they may be attacked and compromised more easily. Researchers and network forensic scientists utilize them to evaluate assaults and build countermeasures. These honeypots collect statistics and event data for research purposes. They don't directly safeguard a company, but they assist assess dangers, devise countermeasures, and remediate exploitable breaches. Research honeypots capture automated attacks. Research honeypots can swiftly catch and analyze these network-wide attacks. Honeypots can increase attack prevention, detection, and response. Research honeypots don't improve company

security. If a company wants to increase the security of its production environment, it may choose to use production honeypots. Honeypots are useful research tools for universities, governments, and large companies engaged in threat research. Honeypots have 3 basic functions to execute their role: 1) Understand threats, build countermeasures, and remediate exploitable breaches. 2) Capture automated attacks.

- **Physicality**. The honeypots can be classified by their physicality [7]: **Virtual Honeypots**: A host system simulates a virtual honeypot by forwarding network traffic to it. These honeypots are adaptable and cost-effective, with high interactivity. They're used in this project. **Physical honeypots**: This honeypot has a real IP address on the network. Physical honeypots cost more than virtual ones, but they're more reliable and harder to distinguish.
- **Location**.Location-based categories for honeypots: [13]: (1) **Client honeypots** detect attacks, vulnerabilities, and rogue webservers. A browser that visits several websites to exploit vulnerabilities is a typical example. (2) **Server honeypots** act as network decoys for attackers. Mirroring production servers and services protects production settings. All attacks on a server honeypot are recorded. Administrators can be better prepared for future threats. (3) **Hybrid honeypots** add client honeypot modules to server honeypots to interface with webservers and expose server honeypot services.
- **Level of interaction** Honeypot deployment and decoy attack vector complexity vary. Classify honeypots by their level of interaction with host systems [14]. Interaction level determines hostile actor's system penetration. Malicious actors can interact more significantly with a system if a honeypot and host system interact more. A bad actor can't interact critically with a lower-level system. There are three levels of interaction for honeypots [15]:**(1) low-interaction honeypots; (2) medium-interaction honeypots [16], and (3) high-interaction honeypots** [17].

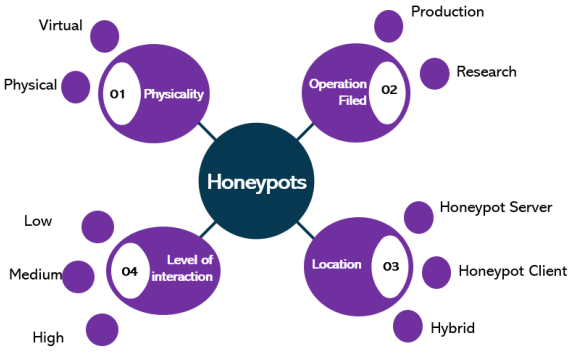

Figure 1: Honeypots classification

The honeypots can be incorportated into a Risk assessment methodology in order to act as a decoy device for would-be attackers, allowing for the quicker identification of threats and attack patterns and the consequent reduction of risk. Production, medium interaction, virtual, and server honeypots are the four categories into which the proposed IEC104 honeypot falls.

EPES and related ecosystems that manage energy generation, transmission, and metering have been a prime focus of sophisticated cyberattacks. Cyberattacks on the Industrial Control Systems (ICS) infrastructure of EPES are becoming more sophisticated as a result of the convergence of information technology (IT) and operational technology (OT). Management, regulation, and control of the behavior of other devices and control systems utilized in the processes of a certain industry (nuclear, electrical, chemical, oil and gas, water, etc.) fall under the purview of ICS (Industrial Control Systems). They incorporate a wide variety of parts, including electronics, mechanics, electricity, and hydraulics. Modbus, DNP3, and CIP are just a few of ICS's many communication protocols. Control systems such as DCS, PCS, SCADA, RTUs, HMIs, PLCs, etc., are the building blocks of ICSs. EPES systems with industrial processes comprise a corporate network (web services, email, etc.), supervision (SCADA, workstations, etc.), and control systems that utilize ICS, SCADA, PLC, RTU, HMI, and other industrial control devices (HMI, PLC, RTU etc). Industrial devices that can open or close breakers and connectors, obtain temperature, release pressure, etc., are supervised and controlled from a control network that allows sending and receiving information using industrial communication protocols to the PLCs and RTUs via a wired or wireless HMI.

Some commonly used honeypots are listed below:

- **Conpot** [18] is a low interaction open source honeypot geared toward industrial control systems (ICS / SCADA). This program provides a variety of popular industrial protocols, such as s7comm, capable of simulating vast infrastructures, and so on, to convince and fool the attacker that he is targeting a massive industrial complex. Conpot can also use a human-machine interface to broaden the attack surface.
- **Dionaea** [19] (formerly known as Nephentes) is a low contact honeypot designed to trap malware that exploits vulnerabilities disclosed by network services. It is intended to simulate vulnerabilities in order to intercept the code of malicious software such as worms that use them to spread. This honeypot may launch several services such as FTP, HTTP, MSSQL, SMB, and others. The utility may capture and log binary files used by attackers. For example, shell-codes in HTTP or payloads in SMB. DionaeaFR, an online interface, is accessible to analyze the acquired data.
- **Cowrie** [20] (Kippo fork) is a python-based medium interaction SSH and Telnet honeypot designed to log brute force attacks and the shell interaction conducted by the attacker. It may simulate a synthetic filesystem mimicking a Debian 5.0 installation. Files and session logs can be watched and stored in UML compliant format,

and binaries can be captured.

- **Glastopf** [21] is a honeypot for web applications with low/medium interactivity. Instead of vulnerability emulation, use vulnerability type emulation. Glastopf can handle unknown attacks of the same type once a vulnerability type has been simulated. It has the advantage of a modular design, which facilitates the installation of new logging capabilities or attack type handlers. Several database capabilities are already in place. HPFeeds logging is supported for centralized data collection. Emulation of popular assault types is already in place: Remote File Inclusion via a built-in PHP sandbox, Local File Inclusion via a virtual file system, and HTML injection via POST requests are all supported. It also supports Docker deployment.
- **HoneyD** [22] is an approach that may be adopted and deployed in medium to large-scale businesses, particularly those that have implemented computer-based systems and technology, to prevent, anticipate, and respond quickly when negative consequences arise. Because honeyd positions itself as a bait or a shadow server that is actively attacked, the consequences of the attack may be known and evaluated. In this study, a honeyd honeypot is a shadow server that looks like a genuine server and has various services as well as ports that are intentionally left exposed for attack.
- **GridPot** [23], an open-source conceptual cyber-physical honeynet framework, will be used to replicate actual protocols used in industrial control systems.

IV. IEC 60870-5-104 Protocol

IEC104 is an expansion of the IEC 60870-5 network protocol standard that allows for TCP/IP connection. The protocol is a remote control and communication standard designed specifically for electric power installations and power grids. IEC104 allows for both master/slave and station-to-station communication. There are no security procedures in IEC104. TCP port 2404 is used by the protocol [24]. The IEC 101/104 interaction between the controlled station and the controlling station [25] can be one the following:

- A ”RTU Master” or ”Controlling Station” monitors or commands a ”RTU Slave” or ”Controlled Station”.
- Controlling station or ”RTU Master” is a station at which controlled stations are regulated (SCADA).

IEC 101/104 provides three direction modes:

1) Monitor Direction is the transmission direction from the controlled station (RTU) to the controlling station unit (CTU).
2) Control Direction is the transmission direction from a controlling station, typically a SCADA system, to a controlled station, such as an RTU.
3) When the monitored station is sending commands and the controlling station is sending data in monitor direction, the direction is reversed.

Figure 2 [26] depicts the topology of an IEC104 router connected to a IEC104 SCADA monitoring system through IEC104 protocol over TCP/IP and an IEC 101 RTU. IEC104

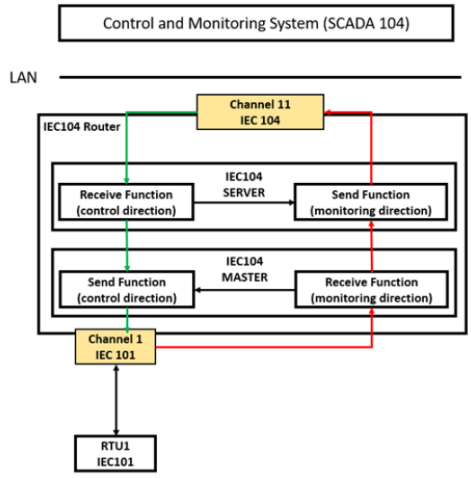

Figure 2: Network topology of SCADA monitoring system

is implemented in the TCP/IP stack’s application layer via the Application Protocol Data Unit (APDU) and Application Service Data Unit (ASDU). Three APDU formats are established based on the APDU Control field as shown in Figure 3:

- Use an i-frame to send data. It is divided into two sections: a fixed-length ASDU header and a variable-length list of information objects.
- The s-frame is used for supervisory tasks.
- u-frame for transmitting uncounted control functions (test frame, start transfer, stop transfer)

The ASDU header contains the following information: (a) the ASDU type (TypeID), (b) the number of transferred items, (c) the Cause of Transmission (COT), and (d) an ASDU address (station address). TypeID (ASDU Type Identification Field): For standard definitions from the IEC 60870-5-101 standard, the numerals 1 to 127 are utilized. The number range 128 to 135 is designated for message routing. The numbers 136 through 255 are reserved for special purposes. There are currently 58 particular types described in the range of standard type definitions. These are grouped, and each group of processes comprises the TypeID range, the name of the Group, the TypeID, and the Code [26].

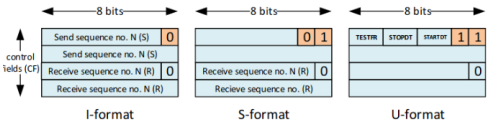

Figure 3: The frame formats

V. Proposed IEC 60870-5-104 Honeypot

In this work the Conpot honeypot is extended to support more IEC-104 commands compared to the original Conpot. Specifically, the source code of the IEC-104 module is modified and enhanced to support more commands as shown in Figure 4. This leads to support of a wider ranged of IEC-104

Table I: IEC104 Honeypot existing and newly added commands

Existing commands	Newly added commands
M_SP_NA_1, M_SP_TA_1,	C_CI_NA_1
M_DP_NA_1, M_DP_TA_1	C_RD_NA_1
M_DP_NA_1, M_DP_TA_1	C_CS_NA_1
M_ME_NB_1, M_ME_TB_1	C_TS_NB_1
M_ME_NC_1, M_ME_TC_1	C_RP_NC_1
M_SP_TB_1, M_DP_TB_1	C_CD_NA_1
M_ME_TE_1, M_ME_TF_1	
C_SC_NA_1, C_DC_NA_1	
C_SE_NB_1, C_SE_NC_1	
C_IC_NA_1	

based devices like RTUs and PLCs deployed in substation sites. Table I includes existing and newly added commands that IEC-104 honeypot supports.

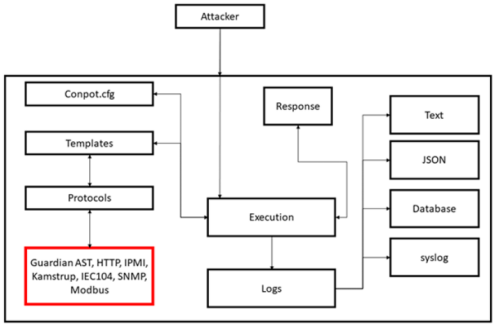

Figure 4: Conpot functionality

VI. Experimental Results

According to IEC104 specification, authentication of the data transfer is not provided, hence IEC-104 devices are vulnerable to unauthorized connection or data manipulation attacks and man-in-the-middle attacks in general. The following two scenarios demonstrate how the IEC-104 honeypot was upgraded to enhance the security to the remote control communications implementing six new commands. The first scenario involves the master sending a Counter Interrogation (CI) command to RTU (i.e. IEC104 honeypot) in an I-format and the RTU device freezes at common time while the second scenario involves the master sending Read Command (C_RD_NA_1) to the RTU in I-format ad the RTU device responds by sending the appropriate register values. In the following subsections the two scenarios are explained in detail.

A. Test scenario 1

Description: To execute information transfer, the Master sends a Counter Interrogation (CI) command to RTU (i.e. IEC104 honeypot) in an I-format. The RTU is compatible with Counter Interrogation Mode A ”Counter freeze without reset”. In this case the totals are frozen at common time using the CI command. **Procedure steps:** (1) An IEC104 client (Slave) seeks to establish a connection with the Master. (2) Determine whether the Master delivers a ”Activation” instruction with IOA=0. The element contains data for the CI command. (3) Then, it determines whether the RTU gets the Master’s CI command. Note that, the APDU is 20 characters long (in decimal). The ”C_CI_NA_1” is the ”Type identification” for the CI command. In this case, the total number of objects is one. The related ”Counter interrogation request qualifiers” setting is set to 5 (universal counter interrogation), which refers to all counters in the RTU. It should be noted that the Counter’s initial value is 0. (4) Then a check is realized to observe if the RTU responds with ”Activation Confirmation” and if the IOA’s Sequence number (SQ) is increased. The RTU resets the counter to 1. In response to the Master, the RTU provides the CI value. (5) Determine whether the RTU delivers the ”Activation termination” command in response to the CI command. (6) In the end, there is a check to observe if the IEC104 honeypot recorded this occurrence in the ”iec104_logs.log” file. The result is shown in Figure 5

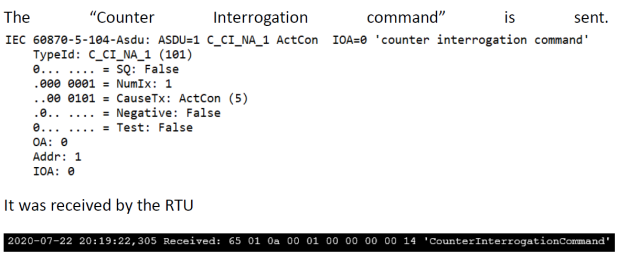

Figure 5: Results from the testing function 1

B. Test Scenario 2

Description: To transfer information, the Master sends a Read Command (C RD NA 1) to the RTU in I-format. In order to obtain each value of a register, the ”Read command” is invoked with an IOA address. It responds with the corresponding IEC104 register/bit value. **Procedure steps:** (1) An IEC104 client (Slave) seeks to establish a connection with the Master. (2) It determines, whether the Master delivers a ”Activation” instruction with IOA=0. The element contains data for the ”Read command” (RD command). (3) Determine whether or not the RTU receives the ”RD command” from the Master. (4) If more than one value is requested, the meter answers with an ASDU sequence with the SQ bit set to ”1”. (5) If a single value is requested, the meter replies to a read request with an ASDU sequence with the SQ bit in the variable structure qualifier set to ”0”. (6) Then, we check if the RTU sends the ”Activation Termination” message for the ”RD Command”, (7) In the end, there is a check to observe if the IEC104 honeypot recorded this occurrence in the ”iec104_logs.log” file. The result is shown in Figure 6

VII. Conclusions

Today, a large number of ICS devices are exposed on the Internet, frequently without any security measures, leaving them open and vulnerable to assaults with potentially catastrophic outcomes. These systems will invariably attract the notice of curious and even hostile actors. In this dissertation, we enhanced and implemented low-interaction honeypots to collect unsolicited traffic aimed at ICS devices, analyzing

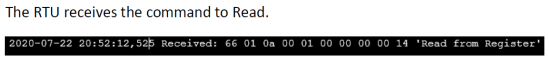

Figure 6: Results from the testing function 2

and characterizing the received traffic to determine who is engaged in vulnerable ICS devices and how they engage with them. This work aims to describe the IEC104 honeypot that mimic an industrial protocol. Honeypots in the realm of industrial protocols are intended to act as a distraction for would-be hackers, allowing for the rapid identification of threats and attack patterns and the consequent reduction of risks. As an increasing number of industrial control systems are interconnected and exposed to the Internet, an increasing number of systems are also subject to risks posed by malicious actors. With our study, we intend to encourage the industry to strengthen its efforts to secure ICSs and to continue monitoring new risks as they emerge. In future we aim to extend IEC-104 by producing replies artificially that are indistinguishable leveraging Artificial Intelligence, dynamically adjust the behaviour profile of the honeypot to match a certain environment state (e.g. the substation is under a heavy load). Finally, an interesting extension would be to design an open repository where stakeholders can upload industrial device profiles and behaviour models.

ACKNOWLEDGMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936 (ELECTRON).

REFERENCES

[1] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021.

[2] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, "A survey on honeypot software and data analysis," *arXiv preprint arXiv:1608.06249*, 2016.

[3] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud," *Vehicular communications*, vol. 12, pp. 138–164, 2018.

[4] J. Uitto, S. Rauti, S. Laurén, and V. Leppänen, "A survey on anti-honeypot and anti-introspection methods," in *World Conference on Information Systems and Technologies*. Springer, 2017, pp. 125–134.

[5] I. M. M. Matin and B. Rahardjo, "The use of honeypot in machine learning based on malware detection: A review," in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2020, pp. 1–6.

[6] G. Bernieri, M. Conti, and F. Pascucci, "Mimepot: A model-based honeypot for industrial control networks," in *2019 ieee international conference on systems, man and cybernetics (smc)*. IEEE, 2019, pp. 433–438.

[7] P. Radoglou-Grammatikis, A. Liatifis, E. Grigoriou, T. Saoulidis, A. Sarigiannidis, T. Lagkas, and P. Sarigiannidis, "Trusty: A solution for threat hunting using data analysis in critical infrastructures," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2021, pp. 485–490.

[8] P. Radoglou-Grammatikis, P. Sarigiannidis, P. Diamantoulakis, T. Lagkas, T. Saoulidis, E. Fountoukidis, and G. Karagiannidis, "Strategic honeypot deployment in ultra-dense beyond 5g networks: A reinforcement learning approach," *IEEE Transactions on Emerging Topics in Computing*, 2022.

[9] J. Cao, W. Li, J. Li, and B. Li, "Dipot: A distributed industrial honeypot system," in *International Conference on Smart Computing and Communication*. Springer, 2017, pp. 300–309.

[10] E. López-Morales, C. Rubio-Medrano, A. Doupé, Y. Shoshitaishvili, R. Wang, T. Bao, and G.-J. Ahn, "Honeyplc: A next-generation honeypot for industrial control systems," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 279–291.

[11] J. You, S. Lv, Y. Sun, H. Wen, and L. Sun, "Honeyvp: A cost-effective hybrid honeypot architecture for industrial control systems," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[12] D. Mashima, B. Chen, P. Gunathilaka, and E. L. Tjiong, "Towards a grid-wide, high-fidelity electrical substation honeynet," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2017, pp. 89–95.

[13] M. Mansoori, O. Zakaria, and A. Gani, "Improving exposure of intrusion deception system through implementation of hybrid honeypot," *The International Arab Journal of Information Technology*, vol. 9, no. 5, pp. 436–444, 2012.

[14] H. Wang and B. Wu, "Sdn-based hybrid honeypot for attack capture," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. IEEE, 2019, pp. 1602–1606.

[15] R. Karthikeyan, D. T. Geetha, S. Vijayalakshmi, and R. Sumitha, "Honeypots for network security," *International journal for Research & Development in Technology*, vol. 7, no. 2, pp. 62–66, 2017.

[16] G. Wicherski, "Medium interaction honeypots," *German Honeynet Project*, 2006.

[17] T. Kaur, V. Malhotra, and D. Singh, "Comparison of network security tools-firewall, intrusion detection system and honeypot," *Int. J. Enhanced Res. Sci. Technol. Eng*, vol. 200204, 2014.

[18] S. Maesschalck, V. Giotsas, and N. Race, "World wide ics honeypots: A study into the deployment of conpot honeypots," 2021.

[19] V. Sethia and A. Jeyasekar, "Malware capturing and analysis using dionaea honeypot," in *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2019, pp. 1–4.

[20] W. Cabral, C. Valli, L. Sikos, and S. Wakeling, "Review and analysis of cowrie artefacts and their potential to be used deceptively," in *2019 International Conference on computational science and computational intelligence (CSCI)*. IEEE, 2019, pp. 166–171.

[21] A. Kyriakou and N. Sklavos, "Container-based honeypot deployment for the analysis of malicious activity," in *2018 Global Information Infrastructure and Networking Symposium (GIIS)*. IEEE, 2018, pp. 1–4.

[22] A. M. Nasution, M. Zarlis, and S. Suherman, "Analysis and implementation of honeyd as a low-interaction honeypot in enhancing security systems," *Randwick International of Social Science Journal*, vol. 2, no. 1, pp. 124–135, 2021.

[23] N. Dutta, N. Jadav, N. Dutiya, and D. Joshi, "Using honeypots for ics threats evaluation," in *Recent developments on industrial control systems resilience*. Springer, 2020, pp. 175–196.

[24] P. R. Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis, A. Tsiakalos, and G. Efstathopoulos, "An anomaly detection mechanism for iec 60870-5-104," in *2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST)*. IEEE, 2020, pp. 1–4.

[25] G. Yadav and K. Paul, "Architecture and security of scada systems: A review," *International Journal of Critical Infrastructure Protection*, vol. 34, p. 100433, 2021.

[26] P. Matoušek, "Description and analysis of iec 104 protocol," *Faculty of Information Technology, Brno University o Technology, Tech. Rep*, 2017.