Investigating Usable Indicators against Cyber-Attacks in Industrial Control Systems

Mohammed Asiri, Neetesh Saxena, and Pete Burnap
Cardiff University, UK

Abstract

Industrial control systems (ICSs) control and monitor industrial activities and physical processes. The attack of the ones and zeroes for a control system taught us that the physical world could be impacted remarkably by cyber-attacks. It is necessary to have capabilities of identifying footprints of the attacks in time when the system is under attack. This will help to mitigate the impact of cyber-attacks, especially when we are not able to prevent such attacks.

By monitoring indicators of compromise (IOCs), operators at utilities can recognize triggers of malicious activities and react quickly to similar compromise incidents in the earlier stages of such attacks. The purpose of this study is to examine how effective the IOCs used in IT systems are in detecting cyber-attacks in the ICS systems under operational technology (OT) environment. We run a questionnaire with ICS attack scenarios to the industry experts working on OT security. During our study and analysis, we found that there are some key indicators better recognized than others for indicating attack behavior.

1 Introduction

In the recent era of technology, hackers have diverted their attention towards the form of technology used in industrial control systems such as the smart grid. Security engineers and system operators work hard to protect these systems against cyber-attacks. It is quite essential to have awareness of cyber security risks for industrial control systems (ICSs) due to the rise in cyber incidents targeting these systems directly [8].

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Vancouver, B.C., Canada.

According to an IBM report [8], cyber incidents against ICS systems are increased by 2,000% in 2019 compared to 2018. Therefore, security experts in these facilities conduct post-incident analysis to determine if an intrusion has occurred, to what extent the system is compromised, what functional operations and assets are impacted, and how the intrusion or attack occurred [4]. ICSs need to be guarded against any threat because any compromise to the system can affect the immediate safety of people.

In general, Indicators of compromise (IOCs) include numerous types of indicators, such as IP address, URL, port numbers, MD5 hashes of malware, or filenames. These forensic artifacts can be used to detect execution traces of malware activity, which can be discovered during the initial analysis of the static and dynamic of the malware. Even though IOCs can effectively prevent further and future incidents, they can only be extracted when the incident is going on or has occurred. The complexity of networks and systems increased due to the convergence of the IT/OT network. This left frontline responders in critical infrastructure to struggling with identifying and responding to the new threat landscape." Frontline responders" is a metaphor we used for the professional who often deals with emerging security issues or obstacles resulting from the convergence.

For this reason, we conducted an observational study to investigate the effectiveness and usability of IOCs that exist in IT against in the OT environment. We aim to investigate the operators' perspective on this matter. Without such understanding, we can neither identify incident response capabilities nor develop usable solutions that empower employees such as operators in the OT environment to manage systems securely and effectively. In this study, we focus to answer the following questions:

- What are industry people's perceptions on how effective these IOCs are to detect cyber incidents in ICS systems?
- What additional IOCs that security experts find useful to indicate a compromised system in an ICS environment?

- What challenges do security experts encounter in terms of developing IOCs associated with the ICS system?

2 Related Work

Limited studies have explored IOCs associated with IT systems in the ICS domain, researchers have investigated ICS security and forensics more extensively after Stuxnet was discovered in 2010. Research studies have generally focused on how to define and express cyber-attacks such as threat modeling approaches. Other studies have examined threat information presented in public reports or open-source threat intelligence (OSCTI). Open Indicators of Compromise (OpenIOC) [11] and The Incident Object Description Exchange Format (IODEF) [16] are findings in the field of threat modeling, which expresses data relevant to cyber-attacks. These findings were later expanded to the data-sharing system for more advanced cyber threat intelligence (CTI) systems [10]. Trusted Automated Exchange of Intelligence Information (TAXII) [6] and Structured Threat Information Expression (STIX) [3] are becoming the de-facto industry standards that enable information sharing and expression for IOCs related to cyber incidents. Many commercial CTI platforms such as Anomali and IBM X-Force Exchange are currently using them as data management systems.

Besides existing threat intelligence-gathering tools and management systems (e.g., security incident and event management solutions (SIEMs), open-source intelligence feeds, reports, vulnerability and malware databases), researchers have made great progress to analyze threat intelligence sources and extract IOCs [10] [19], [20]. In terms of automated threat-related data collection and analysis, Rudman et al. [14] presented a framework for generating network-based indicators from captured packets automatically. Dridex malware was used in the dynamic sandbox to generate PCAP files and extracted low-level indicators such as IP address, suspicious domain names, and commonly used protocols and ports. These are useful indicators for analyzing the behavior of particular malware variants. Nevertheless, it failed to generate IOCs associated with ICS. Other works proposed iACE [10] that employs the natural language processing (NLP) technique to efficiently extract IOC data and use graph mining techniques to analyze the extracted IOCs data. iACE extracted IOCs data from 71,000 industry blogs and reports, with a classification accuracy rate of about 95%. Atluri et al. [2] applied machine learning (ML) models for network traffic classification and extraction of IOCs. The proposed models were verified by using the dataset of 5 different simulated attacks resulted from the ICS testbed. Some of the extracted IOCs, however, are overlapped among the different simulated attack traffic. To increase the timely detection of cyber threats, Noor et al. [12] proposed a machine learning-based framework through utilizing high-level IOCs that includes (tactics, techniques and procedures – TTP), where Deep Learning Neural Network (DLNN) showed the best results in comparison to the other ML models.

Several studies have focused on developing live acquisition frameworks to collect IOCs data using agents [1], [17] , [9]. However, the majority of existing frameworks lack practical evaluation, and they focus only on the supervision layer of the control system. Others have found that acquiring forensic data from Programmable Logic Controllers (PLCs) is useful. Rad-vanovsky et al. [13] have indicated the importance of acquiring hexadecimal dump from PLC memory. Wu et al. showed that it is possible to identify the attacker's intention by obtaining the program code on PLC using debugging tool [18]. The researchers have proven that modification of the memory address of the PLC can be considered as IOC.

Previous studies, however, did not discuss the IOCs used in the IT domain for detecting cyber threats against ICS systems. Our work specifically focuses on investigating these IOCs in the ICS context with respect to usability for detecting attacks. We observed that some IOCs are effective for indicating attack activity.

3 Approach

The goal of this work is to understand up to what extent IOCs utilized in IT systems are helpful in detecting attacks in ICS/OT systems from the experts' and industry people's points of view. IOCs are highly specific to the environments that adversaries target. We divided our approach into preparing a questionnaire and key scenarios, focus group participants, and identified IOC. To answer our research questions, we conducted a study with industry participants responding to an online questionnaire. This study was reviewed and received approval from the research ethics committee at our institution.

Questionnaire and key scenarios: We created a scenario-based questionnaire which includes four scenarios of cyber attacks: Stuxnet malware, Ukraine Power Grid attack, Man-in-the-Middle (MITM) attack, and Distributed Denial-of-Service (DDoS) attack. When considering a scenario, we ask participants to reflect on the potential IOCs that help to detect the attack based on their working experience and handling similar scenarios. We used the open-ended responses for each question to allow participants to add others IOCs based on their experience and knowledge.

Participants from the focus group: we have made contact with the industry people working on OT/ICS security. A total of nine participants' responses were collected to discuss these IOCs usability.

Ethical Consideration: This study was reviewed and received approval from the research ethics committee (at our institu-

tion). We obtained informed consent from all participants. Our study did not involve any personal information and the data collected will be kept entirely confidential for two years. The participants were informed about the usage of data collected from them and who will have access to it.

Identified IOC: In this regard, we determined potential IOCs based on similarities between traditional IT and ICS environments in terms of industry-standard and network protocols [15]. A key summary of these indicators is as follows.

Unusual Outbound Network Traffic.Unusual change in the network traffic provides operators with an overall view and specific information about particular traffic or attacks on the network. However, this Indicator can be ignored by the operator due many legacy protocols and devices often communicate in plain text. It is difficult for the operator to accurately distinguish normal from malicious network traffic.

Log-in Anomalies. Log-in failures and frequent irregularities when seeking to access an account are another indicator of an attacker seeking to access the account's control system. For instance, third-party vendors and operators are often given remote access to ICS/SCADA. The increasing of failed logins is the easiest IOC for the system operator to hunt by analyzing system logs. This is because login failures would trigger a log entry.

Communication with malicious CC server. Once the ICS system becomes compromised, the attacker starts maintaining persistent access by communicating with a malicious or unknown command and control (C2) server. However, complex attacks may use C2 infrastructure that can be notoriously difficult to detect by traditional network monitoring solutions. In this situation, the forensic investigator may manually inspect packet dumps to extract C2 artifacts.

Geographic Irregularities. This is a common indicator of a potential ICS-related attack in which there are frequent anomalous log-in requests from unusual geographic locations. For example, within a smart grid environment, this can be a red flag when it comes from countries where the domestic smart grid does not engage in any business.Therefore, it is important for a forensic analyst to take a deeper look at that activity by utilizing a tool such as IP lookup tool.

Anomalies in privileged user account activity. Once account credentials have been stolen, attackers often attempt to escalate the privileges of the account they have hacked. For example, In 2015, when BlackEnergy malware hit a Ukrainian power company, stolen credentials were used to access the ICS devices that controlled the power breakers [5]. From defender's perspective, watching changes (such as time of activity, systems accessed, and type data accessed) will help to hunt such indicator.

Applications Using the Wrong Port. This often occurs when communicating with an internal system which may involve inbound and outbound connections, which often take place over an open port. For example, Stuxnet malware sending C2 connections includes information about the compromised host over port 80 to bypass a firewall. Identifying this IOC enables investigators to build hypotheses about the covert tactics used by the adversary.

Response size. Many ICS network protocols are susceptible to various attacks due to the lack of authentication measures. This could allow attackers to modify, capture, or forward response packets. Abnormal increases in response size may indicate that the system is compromised. In such case, security investigator can observe such activity through an interactive visualization system which help to analyze traffic and detect massive amounts of packets in response.

Unexpected Resources Usage. Devices such as pumps, switches, and centrifuges in ICS perform nearly the same tasks during their lifespan. They most likely have a predictable usage. A sudden difference in resource load would provide the operator with visibility of a system if it is under attack or not. Nonetheless, considering abnormal resource usage as IOC depends on a defender situational awareness and ability to identify usage load changes in some significant way.

Port Scanning of Control devices. Port scanning is a technique used by security operators for troubleshooting or to check for vulnerabilities; however, it can also be used by attackers to identify the role and services of target systems or to bring system down. Consequently, this IOC may introduce a gap in security perception between security crew and operators. For example, the operator may ignore such scanning without regard for the fact that such scanning may be the result of cyber threat.

Control Logic Modification. In general, a programmable logic controller contains control logic and firmware. Any change to the firmware is protected by security measures such as hash algorithm and digital signatures, but the modification of control logic is not protected with any measures in most instances [7]. In a situation when the operator is dealing with a PLC connected to a physical device of the process, and the physical device has unusual damage, it may take a long time to understand that it could be affected by a remote attack.

4 Preliminary Results and Discussion

We analyze the responses from the participants obtained through the study based on grounded theory. Moreover, open-ended responses were analyzed to understand security workers' insights into defensive practices. Figure 1 summarises notable indicators suggested by experts as well as the key challenges that may hinder the development of effective IOCs in the ICS systems.

Perception of the effectiveness of IT's IOCs in the ICS domain: The experts highlighted that most cyber incidents against the ICS environment start from the IT network, so the security understanding of the people working in IT systems matters. As a result, these incidents share some IOCs that are related to the IT environment. Unusual outbound traffic activity, for example, is an effective IOC for detecting cyber-attacks against the ICS network. Since the ICS systems are unlikely to have outbound inter-net access, industry people have chosen this indicator for all attack scenarios.

P[1]: "*there is no one size fits all when talking about IOCs*".

Nonetheless, IOCs are highly specific to the environments that adversaries target. For instance, response size is a specific IOC for DDoS attack, while it might not be effective for detecting other cyber incidents. Some IOCs may provide valuable information with a high level of confidence that this is certainly malicious (e.g., communicating with a known malicious IP or finding a known-bad binary MD5/SHA1 hash).

P[2]: "*Sometimes the attack occurs at IT level and with current level of maturity in industrial networks design / security it is impossible to differentiate between legitimate use or attack*".

However, others are inconspicuous and equivocal such as log-in anomalies and geographic irregularities indicators might indicate abnormal activities that may not necessarily be high fidelity indicators. From an evidentiary perspective, cyber-crimes involves collecting artifacts of intrusion and linking it to a suspect. It requires building defender knowledge of attacker techniques to distinguish between abnormal behavior and malicious activity.

Usability of additional IOCs: The participants highlighted that identified IOCs are applicable for dealing with security incidents in the OT environment. However, in practice, IOCs are reduced to atomic indicators such as file names, domain names, and IP addresses. In real-time systems, anomaly detection is an important IOC to detect potential compromise. This is especially useful in situations where straightforward methods of detection are ineffective.

P[3]: "*physical / logical system access at unusual times*". P[7]: "*changes of traffic patterns through the firewall between business and control networks*".

Of course, exploitation of legitimate functionality should not be considered an IOC. Nevertheless, rising an alarm is important. These anomalies can be combined with one or more IOCs to indicate the system is being compromised.

P[5]: "*alarms generated by the PLC in combination with other IOCs can be a clear indication of compromise*".

Developing IOCs : Historically, maintenance of ICS was reasonably cheap due to control systems are bought with perpetual licenses. From a security point of view, developing defensive tools in control networks might be challenging due to the cost of having an OT security operation center (SOC). Operational costs of maintenance are a difficult pill to swallow for asset owners, especially given that the likelihood of a cyber attack is low compared to other risks such as equipment failure and safety.. However, the lack of personnel skill and ability to develop these tools are the barrier.

P[5]: "*Legacy equipment/software may not be generating logs that would be useful for security monitoring purposes*".

Another challenge comes from legacy systems that are poorly designed with security capabilities. These systems neither have valuable log capabilities nor tools necessary to extract forensic artifacts. Such log data in the ICS network does not provide an investigator with contextual knowledge of an event especially in an environment when something unusual occurs may consider'threat'.

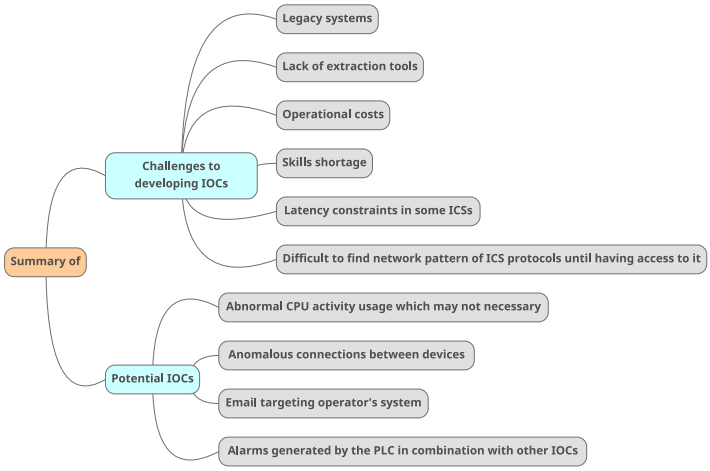

Figure 1: Tree map of open-ended response questions

5 Conclusion and Future Work

In this study, we presented the preliminary results of the study that gauged how usable that IOCs found in IT systems to detect cyber-attacks against ICSs from the security experts' viewpoints. This will help utility employees to better understand cyber behavior while working on ICS systems. Our discussion indicates that most of IOCs are applicable and effective in the ICS environment. Regardless of a positive or negative hit – it will be useful for detecting parts of adversaries activities in an OT environment. Furthermore, we have also highlighted the challenges faced by operators and other personnel when thinking of IOCs in ICS systems.

Future work will look at highlighting concrete approaches used by SOC in identifying IOCs associated with ICS systems. This involves recruiting more participants from industry along with researchers and security providers such as *Dragos* and *Fortinet*, extending questionnaire with more deep questions, managing collected data responses and the overall results.

References

[1] Irfan Ahmed, Sebastian Obermeier, Martin Naedele, and Golden G Richard III. Scada systems: Challenges for forensic investigators. *Computer*, 45(12):44–51, 2012.

[2] Venkata Atluri and Jeff Horne. A machine learning based threat intelligence framework for industrial control system network traffic indicators of compromise. In *SoutheastCon 2021*, pages 1–5. IEEE, 2021.

[3] Sean Barnum. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation*, 11:1–22, 2012.

[4] P Saskia Bayerl, Ruža Karlović, Babak Akhgar, and Garik Markarian. *Community Policing-A European Perspective*. Springer, 2017.

[5] Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388, 2016.

[6] Julie Connolly, Mark Davidson, and Charles Schmidt. The trusted automated exchange of indicator information (taxii). *The MITRE Corporation*, pages 1–20, 2014.

[7] Naman Govil, Anand Agrawal, and Nils Ole Tippenhauer. On ladder logic bombs in industrial control systems. In *Computer Security*, pages 110–126. Springer, 2017.

[8] IBM, Michelle Alvarez, Dave Bales, Joshua Chung, Scott Craig, Kristin Dahl, Charles DeBeck, Ari Eitan, Brady Faby, Rob Gates, Dirk Harz, Limor Kessem, Chenta Lee, Dave McMillen, Scott Moore, Georgia Prassinos, Camille Singleton, Mark Usher, Ashkan Vila, Hussain Virani, Claire Zaboeva, and John Zarabedian. X-force threat intelligence index 2020. *IBM X-Force Incident Response and Intelligence Services*, pages 1–49, 2020.

[9] Tim Kilpatrick, Jesus Gonzalez, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi. An architecture for scada network forensics. In *IFIP International Conference on Digital Forensics*, pages 273–285. Springer, 2006.

[10] Xiaojing Liao, Kan Yuan, XiaoFeng Wang, Zhou Li, Luyi Xing, and Raheem Beyah. Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 755–766, 2016.

[11] OpenIOC Mandiant. An open framework for sharing threat intelligence. *Alexandria, Virginia (www. openioc. org)*, 2014.

[12] Umara Noor, Zahid Anwar, Tehmina Amjad, and Kim-Kwang Raymond Choo. A machine learning-based fintech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, 96:227–242, 2019.

[13] Robert Radvanovsky and Jacob Brodsky. Scada/control systems security. *Boca Raton: CRC Press*, 31:33, 2013.

[14] Lauren Rudman and Barry Irwin. Dridex: Analysis of the traffic and automatic generation of iocs. In *2016 Information Security for South Africa (ISSA)*, pages 77–84. IEEE, 2016.

[15] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011.

[16] Takeshi Takahashi, Kent Landfield, Thomas Millar, and Youki Kadobayashi. Iodef-extension to support structured cybersecurity information. *IETF Internet Draft*, 2012.

[17] Pedro Taveras. Scada live forensics: real time data acquisition process to detect, prevent or evaluate critical situations. *European Scientific Journal*, 9(21), 2013.

[18] Tina Wu and Jason RC Nurse. Exploring the use of plc debugging tools for digital forensic investigations on scada systems. *Journal of Digital Forensics, Security and Law*, 10(4):7, 2015.

[19] Panpan Zhang, Jing Ya, Tingwen Liu, Quangang Li, Jinqiao Shi, and Zhaojun Gu. imcircle: Automatic mining of indicators of compromise from the web. In *2019 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6. IEEE, 2019.

[20] Jun Zhao, Qiben Yan, Jianxin Li, Minglai Shao, Zuti He, and Bo Li. Timiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. *Computers & Security*, 95:101867, 2020.