Cyber Security Threats Targeting CPS Systems: A Novel Approach Using Honeypots

Conference Paper · August 2018

CITATIONS
0

READS
302

3 authors:

Sameera Almulla
University of Dubai
13 PUBLICATIONS **177** CITATIONS
SEE PROFILE

Claude Fachkha
University of Dubai
20 PUBLICATIONS **276** CITATIONS
SEE PROFILE

Elias Bou-Harb
University of Texas at San Antonio
72 PUBLICATIONS **525** CITATIONS
SEE PROFILE

Cyber Security Threats Targeting CPS Systems: A Novel Approach Using Honeypots

Sameera Almulla[1], Elias Bou-Harb[2], Claude Fachkha[1,3]

College of IT and Engineering
[1] University of Dubai, Dubai, United Arab Emirates
[2] Cyber Threat Intelligence Laboratory, Florida Atlantic University, Florida, United States
[3] Steppa Cyber Inc., Canada
e-mail: {salmulla,cfachkha}@ud.ac.ae, ebouharb@fau.edu

***Abstract*—Supervisory Control and Data Acquisition (SCADA) systems are quite prominent for use in industrial, utility, and facility-based processes. While such technology continues to evolve in the context of Cyber-Physical Systems (CPS), and new paradigms such as the Internet-of-Things (IoT) arise, the threat of such systems remains relatively obscure, especially from the operational cyber security perspective. Various obstacles hinder the cyber security analysis of such systems, including the lack of (malicious) empirical data in addition to numerous logistic, privacy and reputation concerns. In this paper, we draw upon large-scale empirical data that was uniquely captured and analyzed from a recently deployed, Internet-scale CPS-specific honeynet. The aim is to shed light on misdemeanors and malicious activities targeting such CPS honeypots for threat inference, characterization and attribution. In addition, this aims at (1) collecting rare empirical data targeting such systems for further forensic investigations and sharing with the research community and (2) contributing to generating CPS-tailored empirical attack models to aid in effective CPS resiliency. The results identify and attribute the top sources of such suspicious and unauthorized SCADA activities and highlight a number of targeted threats. Furthermore, we uncover undocumented abuse against CPS services operating in building automation systems as well as factory environments.**

Keywords–SCADA System; CPS Security; CPS honeypots; Threat characterization.

I. INTRODUCTION

The Internet today continues to experience constant attacks targeting Cyber-Physical System (CPS). Such systems are defined by the National Institute of Standard and Technology (NIST) [1] as a set of inter-connected and distributed physical processes which control and monitor industrial control sectors such as utilities (i.e., electric, water, oil, natural gas), transportation, and building automation systems.

Several factors are affecting CPS security. First, in an ideal situation, the isolation of a CPS network from the external unsecured network (e.g., Internet) is a common practice. However, this is not the case, as there is a necessity to access such systems remotely using external devices. Second, support, consultants and vendors who connect their devices to the CPS network for various purposes create potential CPS security risks [2]. Third, replacing original parts in the CPS network with low-quality equipment to reduce the cost has recently triggered critical security against CPS systems by generating a plethora of 0-day vulnerabilities [3] [4]. Last but not least, the modernization of smart cities, inter-connected devices and IoT will obviously scale the threat vector against SCADA systems. According to the Industrial Control System Computer Emergency Response Team (ICS-CERT) [5], the assessment teams have identified hundreds of vulnerabilities within CPS architectural design. The rise of attacks on CPS compared to 2016 was attributed to the widespread adoption of the IoT technology.

Given the scarcity of CPS-specific tailored cyber threat intelligence, the contributions of this paper could be summarized as follows:

- deploying distributed SCADA monitors (i.e., honeypots) in various countries,
- analyzing and characterizing one month of unsolicited and suspicious SCADA communications, and
- measuring and validating the severity impact of such SCADA activities.

The remainder of this paper is organized as follows. Section II provides an overview of the related work. Section III presents the approach used to profile CPS cyber activities. Section IV elaborates the derived results based on the analyzed one-month period of SCADA data. Section V puts forward a few limitation points and its limitation. Finally, Section VI summaries and concludes this paper.

II. RELATED WORK

The literature review could be divided into mainly two parts, namely, probing analysis and CPS analysis.

A. Probing Analysis

Since probing activities is an important topic in cyber security and Internet measurements, it has been the focus of attention in many contributions. In [6], the authors provided an extensive survey in which they categorize the scanning topics based on their nature, strategy, and approach. Leonard *et al.* [7] performed stochastic derivation of a number of relations in order to propose an optimal stealth distribution scanning activity based on the probability of detection. The authors undertook the attackers' perspective (and not the measurement point of view) in order to significantly minimize the probability of detection. In [8] [9], the authors studied probing

activities towards a large campus network using netflow data. They attempted to find different probing strategies and study their harmfulness. They analyzed the scanning behaviors by introducing the notion of gray IP space and techniques to detect potential scanners. Pryadkin *et al.* [10] performed an empirical evaluation of cyber space to infer the occupancy of IP addresses. In addition, J. Heidemann *et al.* [11] was one of the first works to survey the edge hosts in the public Internet. Cui *et al.* [12] analyzed a wide-area scan and presented a quantitative lower bound on the number of vulnerable embedded devices on a global scale. Further, in [13], the authors analyzed data from a large darknet composed of 5.5 million addresses to study Internet-wide probing activities. They detected probing events as large spikes generated by unique sources.

Furthermore, in [14], we have proposed a hybrid approach based on time-series analysis and context triggered piecewise hashing as applied to passive darknet dataset to infer, characterize and cluster probing activities targeting CPS protocols. Our work is complementary to the aforementioned contributions by focusing only on probes targeting CPS honeypots.

B. CPS Traffic Analysis

CPS network traffic monitoring and analysis can be divided in two main categories, namely, interactive monitoring and passive monitoring. On one hand, honeypots are an example of low- to high-interactive trap-based monitoring systems [2]. The first CPS honeypot, known as the SCADA HoneyNet Project, was designed and deployed in 2004 by Cisco Systems [15]. Digital Bond, a company that specializes in CPS cyber-security, deployed two SCADA honeypots in 2006 [16]. The release of Conpot in 2013 has greatly facilitated the deployment and management of CPS honeypots [17]. In order to evaluate the strength of a given honeypot in deceiving the attackers, Sysman *et al.* [18] introduced the notion of "Indicators of Deception", where some of the most popular low and medium interaction honeypots were examined. An indicator of deception is an action performed by the honeypot that may alert the attackers to identify that they are interacting with a honeypot. For example, Artillery [19] honeypot, by default blocks any malicious activities trying to connect with the services they emulate. Therefore, such honeypot is easy to be identified only due to their default action. Therefore, the deployed conpot was carefully configured to deceive the intruders without being noticed.

On the other hand, in terms of passive analysis, such methods include the study of network telescope traffic to generate statistics and trends related to various inferred CPS misdemeanors. The first limited reported network telescope study which addressed the security of CPS protocols was conducted in 2008 by Team Cymru [20]. Their report included coarse statistics on scans targeting commonly used CPS protocols, such as Distributed Network Protocol (DNP3) [21], Modbus [22] and Rockwell-encap [23]. Vasilomanolakis *et al.* [24] propsed a multi-stage attack detection system based on the attack signature analysis with CPS honeypot. The authors introduced a mobile device based CPS honeypot that monitors incoming probing activities, in general. Unlike the work presented in [24], our proposed methodology presents the first large-scale experimentation of the deployment and operation of a CPS-specific attacks by leveraging existing CPS honeypot that performs the essential analytics on attacks targeting CPS services on a darknet.

In contrast to current practices, in this work, we intend to establish a large-scale honeynet infrastructure to collect and curate CPS data from a plethora of systems and configurations. While the utilization of honeypots in cyber security tasks is definitely not new, their use cases tended to be ad hoc, independent and non-CPS focused. Thus, we propose a systematic and collaborative approach to harvest Internet-scale CPS honeypot data in a planned/staged manner.

III. Methodology

The proposed methodology consists of three phases: (1) data monitoring, which includes data collection; (2) data analytics, which provides statistics and information on the collected data; and (3) result's validation, which proves and affirms the obtained results.

In a nutshell, the monitored Internet activities are amalgamated into a centralized database for analysis and insights generation. Finally, the results are validated via trusted third party data-sets. Figure 1 provides an overview of our methodology. The deployed infrastructure is composed of 32 hosts distributed in 8 countries. In this setup, we were able to monitor activities originating from more than 40 countries targeting countries where the monitors are deployed.

First, in the data monitoring phase, every host is assigned an Internet public IP address to attract any unauthorized SCADA activity. Subsequently, we leverage three types of sensors that run simultaneously on the incoming traffic. We describe each of the sensors below:

- Generic sensors, which are configured to collect data from various communication protocols, SCADA and non-SCADA. Such sensors aim at (1) collecting all activities for through network investigation; and 2) helping in differentiating between random and focused SCADA activities. Please note that the deployed infrastructure mimics the internal dynamics of CPS systems, where the external vantage point has been protected by basic configuration of iptables.
- Network Intrusion Detection System (NIDS) sensors, which are Network based Intrusion Detection System, are used to identify threats that target the generic sensors as well as SCADA sensors. Such sensors provide more insights on the intention of the captured network activity. In this work, we have leveraged Snort [25] engine, an open-source NIDS, to detect and classify intrusions.
- SCADA sensors, which are typical SCADA honeypots which have been setup in interactive mode. SCADA sensors have been configured to monitor incoming traffic targeting SCADA protocols, namely, Modbus and Distributed Network Protocol (DNP3) as per their default setup [2]. Typical CPS dynamics (i.e., control and communications) provided by Modbus on port TCP 502 and Siemens on port TCP 102 have been emulated. Please note that the honeypots have been configured with public IP addresses but have not been advertised publically to prevent their immediate exploitation.

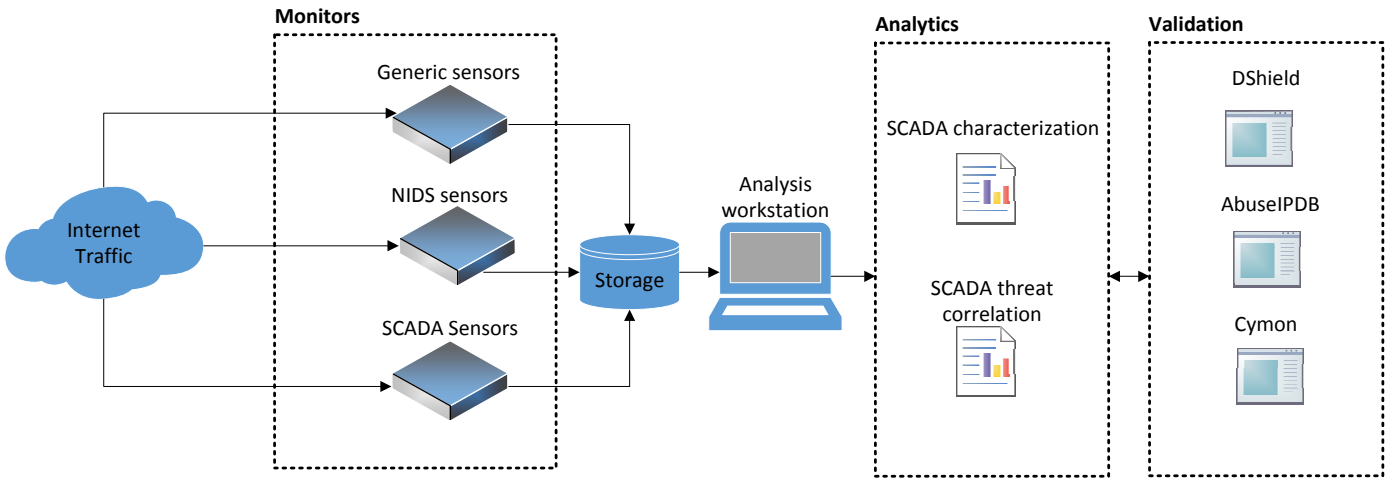

Figure 1. Methodology Overview

Second, in the analysis phase, the collected data from the monitors are pushed into an un-relational database for further analysis. In this context, we leverage several open source tools (e.g., whois [26]) to characterize the SCADA activities and identify the countries, cities, and Autonomous System (AS) names involved. Furthermore, the amalgamation in the previous phase allows us to correlate between the generic sensors and NIDS sensors data with the SCADA sensors data. For instance, we were able to tell the percentage of SCADA communication compared to generic ones and the types of threats affiliated to SCADA activities.

Last but not least, in order to validate our findings, reduce false positives and assess our methodology in identifying unreported (potential 0-days) attempts, we leverage three other trusted third-party datasets, namely, DShield [27], AbuseIPDB [28] and Cymon [29]. Such datasets provide rich insights on suspicious Internet activities such as types of threats and reputations of IP addresses. In the next section, we list our results based on this proposed multi-phase approach.

IV. Preliminary Results

The aim of this section is to provide an overview of our results based on our proposed approach. This section is divided into three parts. On one hand, the first part provides a characterization based on the overall data collected from our generic sensors. The latter collects generic network flow information which might include conventional Internet communications including SCADA activities. In fact, even if we setup a SCADA sensor, as long as it is publicly available, adversaries' activities can target SCADA services, in addition to any other services (ports) available on this sensor. On the other hand, the second part provides more detailed analysis based on SCADA sensors only. These sensors are dedicated to imitate SCADA hosts.

We have setup the SCADA sensor as per the open source deployment in [2]. We run the sensor in default mode, which emulates the basic SCADA host on the following services: Siemens S7-200 [30] Central Processing Unit (CPU) with 2 slaves, Modbus on port 502 Transmission Control Protocol (TCP), S7 Communication (S7Comm) [31] on port 102 TCP, HTTP on port 80 TCP, and Simple Network Management Protocol (SNMP) on port 161 User Datagram Protocol (UDP). Finally, the last part provides an overview of the threats associated to such SCADA activities. Such inference can help us understand the impact of these activities and the intention of the user, who is originating the cyber activity.

A. Data Overview

As mentioned earlier, this section provides an overview of any Internet activities or network traffic targeting the deployed sensors.

Overall, Figure 2 provides an overview of: 1) the number of identified flows, where a flow is defined as a collection of packets originating from one source IP address to one or multiple destination IP addresses; 2) total unique IP counts; 3) total number of scanning activities in all flows; and 4) alerts and intrusions associated to these flows.

The number of alerts and intrusions identified via network-based monitoring systems [25] is relatively high due to the fact that one source IP address within a flow might generate multiple threats on multiple sensors. Further discussion will be elaborated in Section IV-B. It is important to mention that our data is based on one-month period, namely, March 2018.

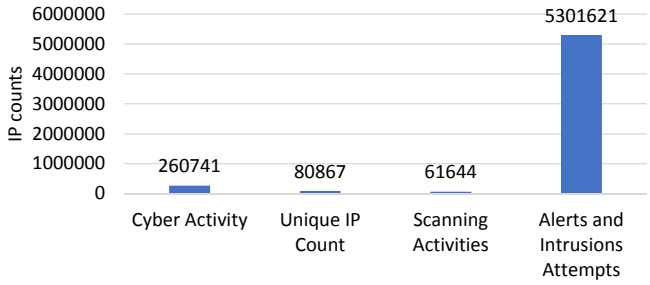

Figure 2. CPS Traffic Behavior Characterization

We have proceeded with the process of data characterization by identifying the top source countries, which initiated unsolicited cyber activities targeting our sensors. Figure 3

provides the top 10 source countries. United States is leading in terms of activities, followed by China then Brazil and Russia. Note that the United States generated around 44,500 flows, which is almost 38% of the global top countries. It is noteworthy to mention the surprising appearance of small countries in Asia, such as Vietnam and Indonesia, which have generated a relatively large number (almost 30%) of activities.

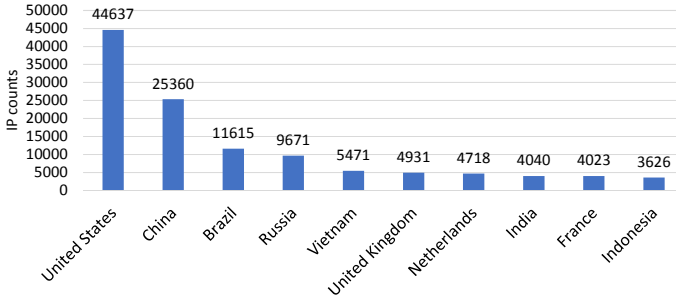

Figure 3. Top 10 Source Countries - Generic Sensors

We further classify the network traffic based on the initiating Autonomous Systems (AS). An AS number can uniquely identify Internet Service Providers (ISPs).

In Figure 4, we list the top 10 AS numbers, as per the traffic targeting our generic sensors. It is worth mentioning that, given that United States is identified as the highest country generating Internet traffic, however, based on AS classifications, Brazil is identified as the highest with 22.6% of the total traffic. This means that more network flows are originated from one single Brazilian AS number as compared to the United States, where more distributed flows are originated from various AS numbers. It is noteworthy to mention that Chinese ASes, which are ranked second and third, have generated together around 35% of the top ASes' traffic.

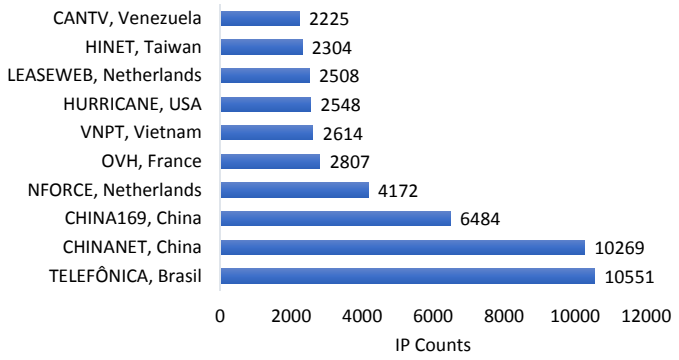

Figure 4. Top 10 Source AS Numbers - Generic Sensors

B. SCADA-Specific Cyber Activities

In this section, we aim at inferring probing events targeting main SCADA communication and control protocols as per the deployment of sensors in [2]. Using this deployment, we identified 54,511 SCADA cyber activities, in which 1,173 unique IP address are involved. This number of activities represents almost 21% of the total 260,741 generic cyber events, which were identified in the previous section (IV-A).

As shown in Figure 5, almost half (48.4%) of the top SCADA activities is generated from the United States. Furthermore, as per the AS name representation in Figure 6, the United States ASes are dominating with CariNet on top of the list. In light of the findings in Figure 6, we can further categorize probing events based on ASes associated services. For example, the purpose of probing can be to conduct scientific research [32] such as University of Michigan (UMICH in US), or the malicious probing activities got generated using a leased host from external service providers such as Linode [33] and Leasweb [34].

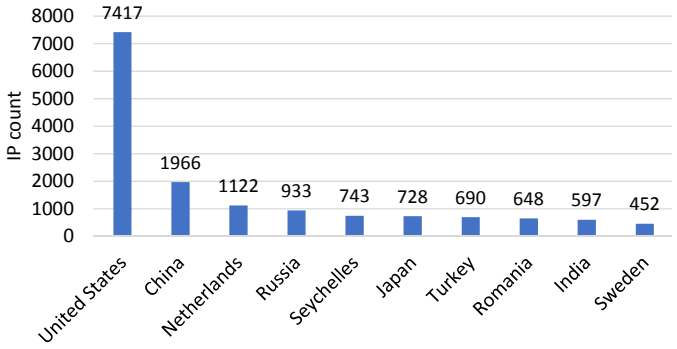

Figure 5. Top Source Countries - SCADA Activities

It is noteworthy to mention Seychelles among the top 5 source countries with 743 activities. Note that Seychelles, among many other islands, is a good location for abusers who find countries with weak or absent cyber security policies. In general, such islands can be easily set for botnet, Command and Control C&C servers and repositories of stolen information.

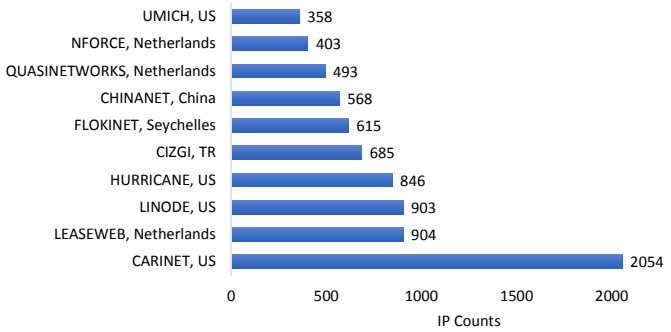

Figure 6. Top Source AS Names - SCADA Activities

In order to assess the severity of such SCADA activities, we have classified the traffic as per Table I. In a nutshell, our classification, which is motivated by [2], flags the network severity as medium, once a session is created, high if a request or response is generated, and critical if messages are transferred or communicated among the deployed monitors and the source IP addresses. Since the monitoring sensors are set on unused IP addresses, any traffic targeting them is deemed to be suspicious and/or unauthorized, or at least misconfigured.

As per the aforementioned approach, the investigation revealed that 13% of SCADA cyber activities are of medium severity, 64% of highly severity and 23% of critical severity.

TABLE I. CPS Probing Activities Severity Rating

Probing Activity Type	Severity Level
Session	Medium
Request/Response	High
Traffic/Connection	Critical

This result is shown in Figure 7.

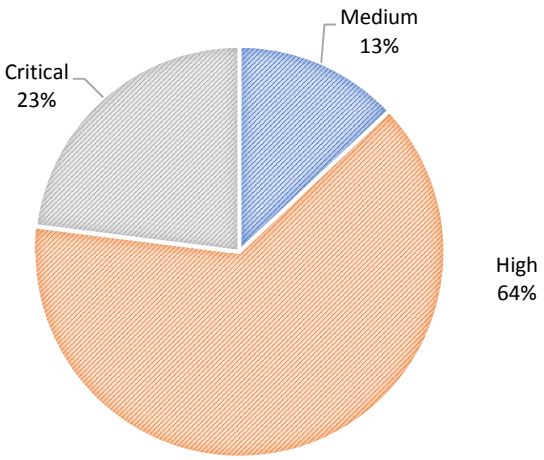

Figure 7. The Severity of SCADA Cyber Activities

In order to achieve a better accuracy and understanding as per the abused services, next, we characterize the communication per the targeted ports, which represent specific operated services. Figure 8 visualizes the distribution of abused services for those of critical severity only. This means that such activities have not just probed requested connection or a session to the deployed monitors, but also have shared data, after the connection setup.

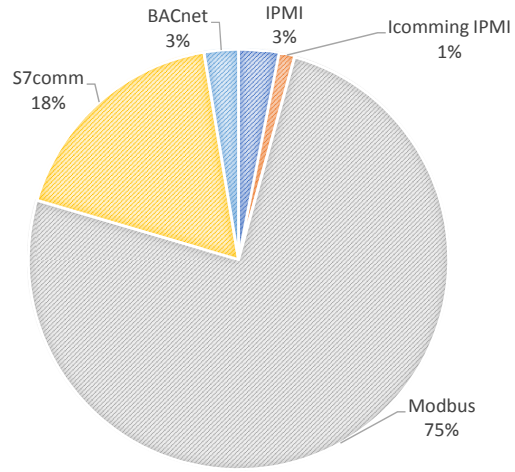

Figure 8. Top Critical Abused SCADA Services

It is not very surprising to identify that Modbus is the most (75%) critically abused SCADA service. Such result is not new for security researchers [14], who have already found similar results based on the analysis of passive monitoring sensors. It is also important to mention that Modbus is the most widely used SCADA service today. In addition to S7comm and BACnet, which came second and third after Modbus respectively, the Intelligent Platform Management Interface (IPMI) has been also found but with very minimal numbers (total of 4%).

C. Validation

In an attempt to validate our findings, we adopt the approach used in [14], where publicly available online databases namely DShield, AbuseIPDB, and Cymon are used. Undoubtedly, the integration and synergy of the findings from multiple online databases will lead to better validation of the obtained results.

DShield is a community-based firewall log correlation system that holds records on reported suspicious IP addresses. Furthermore, the online database returns the risk scale, targeted attacks and a total number of the report counts. DShield reports the speciousness of a reported IP address on a scale from 0% (lowest) to 100% (highest)

As stated earlier, we validated the source IP addresses of the SCADA network communication activities. Our findings revealed that 100% of the worldwide source IP addresses were found in DShield, with an average risk scale of 53%. Among the highly risky malicious sources of SCADA communication, where the risk scale was either 90% or 100%, the maximum attack counts are 2,946 and 53,215 report counts. Overall, the average attack counts of the detected source IP addresses is 1,199, while the average reported malicious IP addresses were 22,016. DShield findings summary are listed in Table II.

TABLE II. Validation Summary

	Dshield			AbuseIPDB
	Risk Scale	Attacks Count	Report Count	Abuse Confidence Rate
Minimum	0%	133	3000	15%
Maximum	100%	2946	65158	100 %
Average	53%	1199	22016	67%

To measure the abuse confidence rate of the detected SCADA activities, we used the AbuseIPDB's online repository which indexes Internet-scale specious IP addresses as reported by the service providers and backbone network operators. Our investigation revealed that the average abuse confidence rate of the unsolicited interaction is 67.4%, with a maximum of 100% abuse confidence rate and the minimum of 15%. A summary of the validation results are listed in Table II.

In an effort to map the results obtained from AbuseIPDB to DShield, we observed that despite the high-risk scale of the source of SCADA traffic, the abuse confidence rate varied from 15% to 57%. This implies that there are abuse cases reported for those IP addresses in DShield and that have not been reported in AbuseIPDB.

Next, we will correlate threats generated from such activities. To identify the type of the network traffic activities, we levereged Cymon's [29] online repository. Cymon is a largest

open source tracker of malware, botnets, spams, etc. Based on our findings, 6 6.6% o f m alicious a ctivities w ere e-mail attacks, and 50% of the following types: WEB attacks, Internet Message Access Protocol (IMAP) attacks, Secure Shell (SSH) attacks, and File Transfer Protocol (FTP) attacks. In addition to the attacks, 16.6% of scanning activities were detected, such as Domain Name Service (DNS) attacks, password disclosure attempts, telnet scans and Remote Desktop Protocol (RDP) scans.

V. Discussion

In this section, we interpret and describe the significance of our findings i n l ight o f t he p roposed methodology.

Vantage Points: Our contribution is limited to the number of deployed monitors. Although this study covers 32 monitors across 8 countries, we cannot identify SCADA activities targeting networks beyond such vantage points. However, we believe that this work is a step forward for building a more distributed network of monitors at large-scale.

Internal SCADA Dynamics: Our model covers the CPS communication targeting SCADA hosts from an Internet perspective. However, this contribution does not cover the security or monitoring of communications within SCADA systems (e.g., inside a power plant), neither hardware devices (e.g., physical smart grid). Our approach complements on-site SCADA security mechanisms such as network isolation SCADA security systems.

VI. Conclusion and Future Work

Conducting research on SCADA data is challenging due to the restrictions on physically accessing critical infrastructure sites. In this paper, we have analyzed SCADA data independently of the infrastructure, via SCADA sensors deployed on the Internet. Our contribution is unique in terms of the following items: 1) our dataset which is collected from more than 32 deployments in 8 countries and (2) our analysis which correlates conventional data with SCADA data and associated threats. Our analysis uncovers unsolicited traffic originating from various countries and AS names. Our future work involves fully-automating the detection and analysis models at a large scale and in real-time. Furthermore, we are developing algorithms to provide insights on the intention of the scans (i.e., benign vs malicious). The purpose is to produce threat intelligence data and sharing in addition to generating notifications f or a wareness a nd m itigation o f t hreats against SCADA systems.

Acknowledgment

The dataset used in this research was provided by Steppa Cyber Inc (steppa.ca). The authors would like to thank all the research team at Steppa. Furthermore, the authors would like to thank our colleagues from Dubai Electronic Security Center (DESC), who provided insight and expertise that assisted this research.

References

[1] S. Keith, P. Victoria, L. Suzanne, A. Marshall, and H. Adam, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security," [Online]: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, 2015, retrieved: August, 2018.

[2] C. Scott and R. Carbone, "Designing and implementing a honeypot for a scada network," The SANS Institute Reading Room., vol. 22, 2014, p. 2016.

[3] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Modeling security in cyber–physical systems," International journal of critical infrastructure protection, vol. 5, no. 3-4, 2012, pp. 118–126.

[4] E. Bou-Harb, M. Debbabi, and C. Assi, "A statistical approach for fingerprinting probing activities," in Availability, Reliability and Security (ARES), 2013 Eighth International Conference on. IEEE, 2013, pp. 21–30.

[5] Department of Homeland Security (DHS), "ICS-CERT Monitor Newsletter," [Online]: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2017_S508C.pdf, 2017, retrieved: August, 2018.

[6] E. Bou-Harb, M. Debbabi, and C. Assi, "Cyber scanning: a comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, 2014, pp. 1496–1519.

[7] X. W. D. Leonard, Z. Yao and D. Loguinov, "Stochastic analysis of horizontal ip scanning," in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 2077–2085.

[8] Y. Jin, Z.-L. Zhang, K. Xu, F. Cao, and S. Sahu, "Identifying and tracking suspicious activities through ip gray space analysis," in Proceedings of the 3rd annual ACM workshop on Mining network data. ACM, 2007, pp. 7–12.

[9] Y. Jin, G. Simon, K. Xu, Z. Zhang, and V. Kumar, "Grays anatomy: Dissecting scanning activities using ip gray space analysis," SysML07, 2007.

[10] Y. Pryadkin, R. Lindell, J. Bannister, and R. Govindan, "An empirical evaluation of ip address space occupancy," USC/ISI, Tech. Rep. ISI-TR-2004-598, 2004.

[11] J. Heidemann, Y. Pradkin, R. Govindan, C. Papadopoulos, G. Bartlett, and J. Bannister, "Census and survey of the visible internet," in Proceedings of the 8th ACM SIGCOMM conference on Internet measurement. ACM, 2008, pp. 169–182.

[12] A. Cui and S. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan," in Proceedings of the 26th Annual Computer Security Applications Conference. ACM, 2010, pp. 97–106.

[13] Z. Durumeric, M. Bailey, and J. A. Halderman, "An internet-wide view of internet-wide scanning." in USENIX Security Symposium, 2014, pp. 65–78.

[14] C. Fachkha, E. Bou-Harb, A. Keliris, N. Memon, and M. Ahamad, "Internet-scale probing of CPS: Inference, characterization and orchestration analysis," in Network and Distributed System Security Symposium (NDSS), 2017.

[15] V. Pothamsetty and M. Franz, "Scada honeynet project: Building honeypots for industrial networks," 2008.

[16] Digital Bond, "SCADA Honeynet," [Online]: http://www.digitalbond.com/tools/scada-honeynet/, retrieved: August, 2018.

[17] HoneyNet Project, "CONPOT ICS/SCADA Honeypot," [Online]: http://conpot.org/, retrieved: August, 2018.

[18] D. Sysman, G. Evron, and I. Sher, "Breaking honeypots for fun and profit," in BLACKHAT, 2015.

[19] Project Artillery, "SCADA Honeynet," [Online]: https://blog.binarydefense.com/project-artillery-now-a-binary-defense-project, retrieved: August, 2018.

[20] Team CYMRU, "Who is looking for your SCADA infrastructure?" [Online]: https://www.team-cymru.com/ReadingRoom/Whitepapers/2009/scada.pdf, 2008, retrieved: August, 2018.

[21] DNP, "Overview of the DNP3 Protocol," [Online]: https://www.dnp.org/Pages/AboutDefault.aspx, 2011, retrieved: August, 2018.

[22] Modicon, "Modbus," [Online]: http://www.modbus.org/, 2018, retrieved: August, 2018.

[23] Rockwell, "Rockwell Automation," [Online]: https://www.rockwellautomation.com/site-selection.html, 2018, retrieved: August, 2018.

[24] E. Vasilomanolakis, S. Srinivasa, C. G. Cordero, and M. Mhlhuser, "Multi-stage attack detection and signature generation with ics hon-

eypots," in NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 1227–1232.

[25] M. Roesch, "Snort: Lightweight intrusion detection for networks." in Lisa, vol. 99, no. 1, 1999, pp. 229–238.

[26] "Whois," [Online]: https://www.whois.net/, 2018, retrieved: August, 2018.

[27] Internet Storm Center, "DShield," [Online]: https://www.dshield.org/, retrieved: August, 2018.

[28] Digital Ocean, "AbuseIP DB," [Online]: https://www.abuseipdb.com/, retrieved: August, 2018.

[29] Open Threat Intelligence, "Cymon," [Online]: https://cymon.io/, retrieved: August, 2018.

[30] Siemens, "Programmable Controller System Manual," [Online]: https://cache.industry.siemens.com/dl/files/582/1109582/att_22063/v1/s7200_system_manual_en-US.pdf, 2018, retrieved: August, 2018.

[31] ——, "S7 Communication (S7comm)," [Online]: https://wiki.wireshark.org/S7comm, 2018, retrieved: August, 2018.

[32] M. Bailey, E. Cooke, F. Jahanian, A. Myrick, and S. Sinha, "Practical darknet measurement," in Information Sciences and Systems, 2006 40th Annual Conference on, 2006, pp. 1496–1501.

[33] Linode, "Linode Cloud Hosting Service," [Online]: https://welcome.linode.com/features-1gb/?gclid=EAIaIQobChMIt_2Rgbym3QIVVTPTCh1ACALZEAAYASAAEgLH2_D_BwE, 2018, retrieved: August, 2018.

[34] Leaseweb, "Global Hosted Infrastructure (IaaS) and Cloud Solutions," [Online]: https://www.leaseweb.com/, 2018, retrieved: August, 2018.