2019 6th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)

Review of SCADA Systems and IoT Honeypots

MOHAMMED H. ALQUWATLI, MOHAMED HADI HABAEBI and SHEROZ KHAN
Department of Electrical and Computer Engineering, International Islamic University Malaysia,
Jalan Gombak, 53100 Kuala Lumpur, Malaysia Mohammedhadi15@gmail.com; habaebi@iium.edu.my; sheroz@iium.edu.my

Abstract— **Internet of Things (IoT) is a massive technology that is being improved day by day. It connects different types of devices to the internet so that they can interchange data. The most feild that has been improved by implementing IoT's technology is Supervisory Control and Data Acquisition (SCADA) Systems, or Industrial Control Systems (ICS). The application of these systems is to be used in controlling different elements that is connected to it (sensors, devices, and machines). However, connecting different types of devices of different physical circuitry and different communication technology, together raises various security issues that has been a place of concern for years. A famous technique that has been implemented in the field of security to further study Cyber Attacks, its causes, and effects is Honeypots. The Aim from this paper is to categorize Cyber -physical attacks and their effects, study SCADA/ICS systems' architecture, highlight its security weaknesses, and how Cyber/Physical attacks make use of these weaknesses. Finally, a break down Honeypots and understand its implementation and effectiveness in the Field of Cyber Security.**

Keywords— Supervisory Control and Data Acquisition, SCADA, Industrial Control Systems, ICS, Conpot, Honeypot, Cyber Security, Cyber Physical Attacks, Modbus TCP Protocol, S7comm Protocol.

I. INTRODUCTION

Internet of Things (IoT) is a massive technology that is being improved day by day. It connects different type of devices to the internet so that they can interchange data in between. Its impact in having certain activities monitored and recorded, and certain devices controlled is visible. It has been mentioned that by 2020, a number of 20 up to 50 billion devices will be acting as an IoT devices which is a number that cannot be taken for granted [1].

The largest field that has been improved by implementing IoT's technology is Supervisory Control and Data Acquisition (SCADA) Systems, or Industrial Control Systems (ICS). The application of these systems is to be used in controlling different elements that is connected to it (sensors, devices, and machines). It can be noticed in Gas and Oil Administration systems, Water Supply Administration systems, and factories and other major fields [2].

However, connecting different types of devices, each has its own physical circuitry and uses different communication technology, together raises various security issues that has been a place of concern for years. Some of its security issues are Confidentiality, Trust, Privacy, Authentication, and Cross-System security concerns. Researchers have been studying IoT Architecture over the last decade to better understand how it can be improved in terms of Security against various types of threats that faces this new technology [3, 4].

A famous technique that has been implemented in the field of security to further study Cyber Attacks, its causes, and effects are Honeypots. Honeypot is a fake interactive system (simulation) that is connected to the internet, which persuade attackers to believing that it is a real system and monitor their attacks. This is achieved by creating a simulation of the communication protocols that the system uses on an independent device and connecting that device to the internet where it will start interacting with attackers. The behavior of the attacker as well as its basic information will then be saved in order to be studied later [5].

The Aim from this paper is to categorize Cyber -physical attacks and their effects. In addition, study SCADA/ICS systems' architecture, understand its security weaknesses, and how Cyber/Physical attacks uncover and use these weaknesses. Finally, break down Honeypots and understand its implementation and effectiveness in the field of Cyber Security.

II. CYBER/PHYSICAL ATTACKS

[6, 7] defined Cyber-Physical attacks in which attacks that affect the Physical space by performing specific actions that jeopardize its Cyber Space. Looking on how IoT systems have its own unique architecture and its huge implementation in various fields, it became a primary target for cyber attackers and unauthorized users. As a result, their actions cost governments millions of dollars and put lives under threat. Due to the previously mentioned reasons, making sure that these systems are secure and immune to these attacks became a priority worldwide. Fig. 1 [6] shows Cyber Attacks impact on the Physical Space.

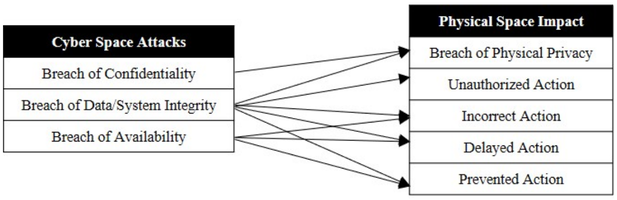

Fig. 1. Cyberattacks impact on the Physical space.

978-1-7281-4082-7 /19/$31.00 ©2019 IEEE

If a breach that effects the system integrity which is an element in the Cyber Space, it will also affect the physical privacy of the user. Which means that the attacker has the ability to perform an unauthorized action, an incorrect action, a delayed action, and prevent specific actions all together. Therefore, it is considered to be a breach in the Physical Space of the system. It was also mentioned that denying a breach in the Cyber Space doesn't necessary means that the Physical Space will be immune, since there will always be different ways for the system's security to be broken [6]. It was mentioned in [8] that there are 4 famous attacks that happen to IoT Systems, which are Denial of Service Attacks (DoS Attacks), Important Information Leakage, Device Replication, and Unauthorized System Control.

The main objective of DoS Attacks is to break the system down and disable it from performing its main job, by creating huge traffic on the system's network [9]. Important Information Leakage is a threat in which the system's crucial information is being transferred on the network without encryption. Device Replication is a threat caused when an unauthorized outsider device is replicating the behaviour of a device inside the network. This intruder may upload incorrect data to the servers, which will affect the integrity of the data. Furthermore, it might help in stealing data transmitted in between the network. With time it will create a problem of differentiating unauthorized replicas and real authorized nodes inside the network [10]. Unauthorized System Control is a threat in which unauthorized user gains control of the system. The user can control the system's behaviour and functionality, or shutdown the system entirely without any notice before hand [10].

III. SCADA/ICS SYSTEMS

Supervisory Control and Data Acquisition (SCADA) or Industrial Control Systems (ICS) are an autonomous data collecting, monitoring and controlling systems that are implemented in industrial fields. Its implementation is wide and huge, it can be noticed in controlling pipelines (gas, oil, and petrol), Water Supply Administration systems, and factories all around the world. It was reported that more than 128 countries from all around the world use SCADA and ICS Systems in their industrial fields [11]. Fig. 2 [2] shows an example of SCADA/ICS System Architecture.

[2] Mentioned that SCADA/ICS systems' Architecture is divided into 4 major elements:

- SCADA/ICS Master: It is the server (heart) of the system. It takes control of the systems as it holds the system's information and stores the data. In addition, the commands sent/received to/from the system acts through it.
- Remote Terminal: responsible of collecting and sending the data from its physical devices/sensors to the Master.
- Human Machine Interface (HMI): A platform that enables the engineer/operator on duty to control the system.
- Communication Infrastructure: The network infrastructure that connects system together.

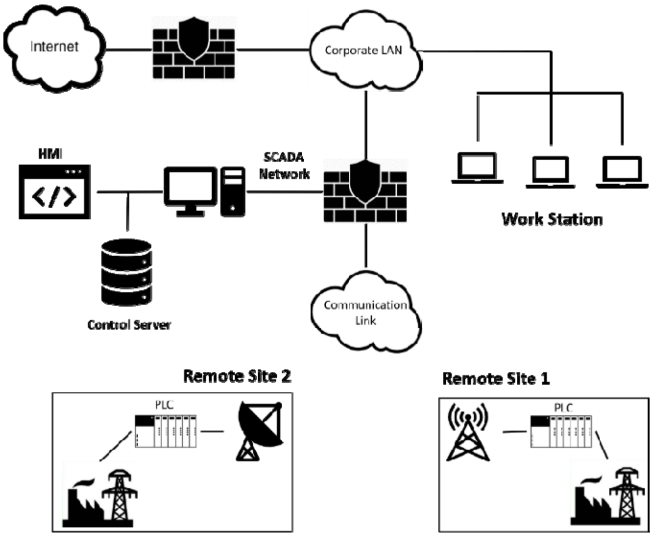

Fig. 2. SCADA/ICS System Architecture.

These systems use the internet to communicate, as most of them obtain IPv4 addresses to help in identify the sender and the receiver throughout the network. There are 17 Industrial control protocols that is being used as a medium for communication by these systems. It is shown in Table I [11].

TABLE I. INDUSTRIAL CONTROL PROTOCOLS.

Category	ICS Protocols
TCP-Based	OMRON FINS, HART-IP, Siemens S7, Modbus, IEC 104, DNP3, EtherNet/IP, Tridium Niagara Fox, PCWorx, ProConOS, CodeSys, Red Lion Crimson V3, General Electric SRTP, CSPV4, Automatic Tank Gauge
UDP-Based	BACnet, OMRON FINS, MELSEC-Q, HART-IP

ICS protocols usually operate under one of two categories, Transmission Control Protocols (TCP) based, or User Datagram Protocols (UDP) based. According to [12], TCP-based protocols will usually create a standard connection before transmitting data, this standard connection can help in getting authentication from the sender before transmitting data, which makes TCP protocol reliable and secure (Host-To-Host). On the other hand, UDP-Based protocols create the packet and send it to the host without the need for a standard connection, which means that there is no act of authentication involved (Process-To-Process).

A. *Modbus TCP Protocol:*

With a percentage of 50% as the most common protocol used in SCADA/ICS Systems [13], Modbus TCP showed a lot of effectiveness when it comes to sending and transmitting information in SCADA/ICS Systems. It is used to connect the controlling devices in the system between each other and the network that it is connected to it [14]. Since it is TCP based communication protocol, an authenticated connection is important to be established before transmitting data between the sender and the receiver. The packet structure of this protocol is shown in Fig. 3 [11].

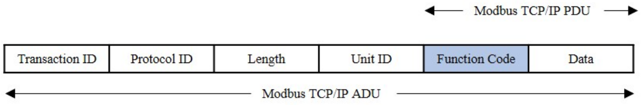

Fig. 3. Application Data Unit of Modbus TCP Protocol.

However, according to [14] Modbus TCP faces huge issues when it comes to its security characteristics, which are:

- Weakness in standard Connection: The attacker can set up a communication line with the device only by having the IP Address of the device.
- Weakness in Authority: Any user (which can be attackers) who is connected to the device can communicate with it with no authentication technique that identify the user's privilege.
- Weakness in Encryption Methods: The packets shared on the network can be seen and understood from anyone. There is no practical Encryption technique that has been implemented in Modbus TCP Protocol that can help in protecting the data shared.

B. *S7comm Protocol:*

One of the most common Programmable Logic Controllers (PLC) that is used in most systems is Siemen's S7 PLC. The PLC uses S7 Communication Protocol (S7comm) to act as a medium between it and the Human Machine Interface (HMI) that operators and engineers use to control the system [15]. Since The protocol is ISO-TSAP based, but when it uses TCP/IP to transfer data, there will be two connection establishments to be done before transferring data. TCP/IP will establish an authentication connection before sharing the packets on the network medium. Furthermore, ISO-TCAP itself is also a connection-oriented based protocol, that gives the result of having to establish another authentication connection before sending the results [15]. Fig. 4 [16] shows the connection establishment between the Engineer/Operator (HMI user) and the receiver (PLC Machine).

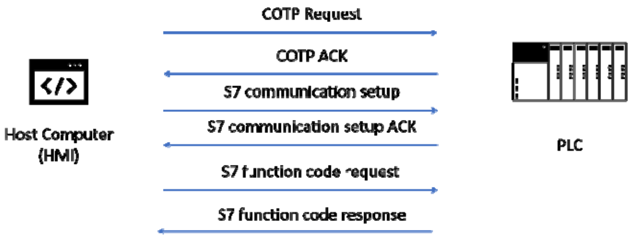

Fig. 4. Connection Establishment in S7comm Protocol.

Fig. 5 below shows the Header Structure in S7comm Protocol.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Protocol ID</td><td colspan="8">ROSCTR</td><td colspan="16">Reserved</td></tr>
<tr><td colspan="16">Request ID</td><td colspan="16">Parameter Length</td></tr>
<tr><td colspan="16">Data Length</td><td colspan="16">Error Code- only for ROSCTR 3</td></tr>
<tr><td colspan="8">Function Code</td><td colspan="8">Item Count</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Fig. 5. Header Structure of S7comm protocol.

C. *Security Issues in SCADA/ICS Systems:*

It was argued by [18] how SCADA/ICS Systems were closed systems that did not have the ability to connect to the internet, and because of that securing these systems was not a problem. This changed when the idea of IoT Systems came along, present SCADA/ICS Systems now have the ability to communicate over the internet. Thus, these ICS TCP/IP-based communication protocols were introduced from its Domain-specific fieldbus, i.e. Modbus TCP, ProfiNET, and OPC UA. Moreover, it was mentioned that the security breaches which SCADA/ICS Systems is facing is because of its weak and inherited security issues.

These security issues are PLCs Attacks, Fieldbus-level Attacks, Wireless Communication Systems Attacks, and Physical-Layer Attacks. Programmable Logic Controllers (PLCs) are the heart of SCADA/ICS Systems, they usually deal with the operating systems of the Physical Space. A well-designed successful attack on PLCs may fall under one of 4 categorizations. Executing unauthorized code, extracting vital information about the system, Denial of Service (DoS), or taking control over the entire system [18].

Fieldbus-level attacks refers to attacks that is performed on the communication bus between two devices, which leads to creating a trust issues in the connection between the destination and the source. Spammers can attack the bus, and steal information shared in the medium, and meddling with the commands sent/received to/from the system [19].

Some Wireless Communication Systems are still fresh when it comes to implementing it in SCADA/ICS Systems, such as Zigbee, Long Range Wide Area Network (LoRaWAN), and Wireless Local Area Network (WLAN). However, when these wireless systems are being implemented in the Industry, it carries a lot of security issues that threatens SCADA/ICS Systems security structure [18].

IV. HONEYPOTS AND ITS IMPLEMENTATION

Honeypot is a fake interactive system (simulation) that is connected to the internet, which persuade attackers to believing that it is a real system and monitor their attacks. This is achieved by creating a simulation of the communication protocols that the system uses on an independent device and connecting that device to the internet where it will start interacting with attackers. The behavior of the attacker as well as its basic information will then be saved in order to be studied later [5].

A. *Honeypot Classification:*

Honeypots can be classified in 3 main sub-classifications. Level of Interaction (High Interaction/Low Interaction), Design (Physical/Virtual), and purpose

(Industrial/Research). Level of interaction classification depends on how much the Honeypot interacts with attackers. Design classification depends on if the Honeypot is deployed on a physical machine or not. Purpose classification depends on the reason behind designing the Honeypot, if it was for research purposes or to implemented by the industry itself [20].

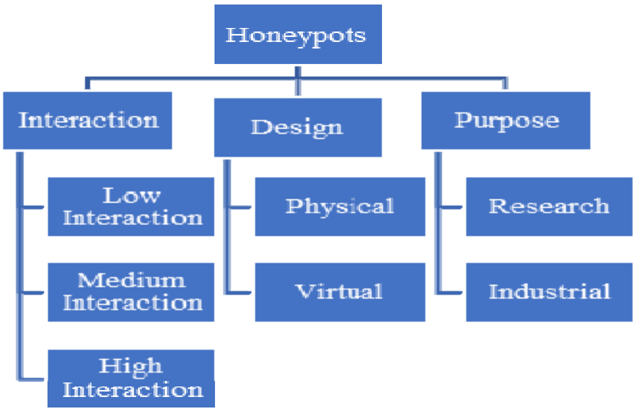

Fig. 6. Honeypots Classifications.

Level of Interaction based Classification:

There are 3 levels of interactions that can categorize Honeypots, Low Interaction Honeypots (LIH), Medium Interaction Honeypots (MIH), and High Interaction Honeypots (HIH). LIH emulate limited rather basic functionalities of a system, which helps in detecting significant thus low-level security breaches i.e. unwanted malwares or Viruses. MIH are an advanced LIH that can collect valid data about different intruders. HIH are fully functioned Honeypots that either simulate complete systems or there is a fully functioned system involved in the architecture of it. The mentioned type is the most advanced as it can interact with intruders a as areal system, which means capturing an essential information about the means used in hacking the system, and intruder's final goal behind attacking the system [5, 21].

Design based Classification:

According to [22], Honeypots can be categorized based on their Design into 2 main categories, Physical Honeypots, and Virtual Honeypots. Physical Honeypots are Honeypots that has been deployed on one physical machine, meaning that the computer will only contain one Honeypot with one address. On the far side, Virtual Honeypots are types of Honeypots that has been deployed on several virtual machines, meaning that one computer can have several Honeypots, each one has its own address. In addition, these Honeypots can be designed in way that they can interact and communicate with each other.

Purpose based Classification:

In [5], it has been mentioned that Honeypots fall under two types when their purpose is taken as a classification, Research Honeypots and Industrial Honeypots. Research Honeypots are designed to study the behavior of attackers, and the means used by them to attack a system. Furthermore, it doesn't help in protecting the system overall, instead it helps in gaining information about the attackers and their location and what tools they used to attack a system. Industrial Honeypots are a type of Honeypots that being implemented by a specific organization to understand the vulnerabilities of a specific system. As a result, it may help the organization to better study their security issues that exists in the system used, and to better improve it and make it immune to attacks.

B. *Honeypots Characteristics:*

In [21], It was mentioned Honeypots characteristics that makes it efficient in detecting attacks and monitoring attacks which are:

- Generated Attacking files: if the attacker had to download a file form the honeypot, the file can be programmed to act as a Trojan Virus, and it helps in collecting data about the attacker.
- Well designed and accurate to mimic well known targets: which is a vital feature that helps in luring attackers to Honeypot.
- Automated Shell Code Analysis: this feature helps in interacting with the attackers in which it takes the right action when there is a command given by the attacker.
- Safe Storage: this feature helps in separating and saving files that has been uploaded/modified by the attacker for further studies.
- Emulate Full Architecture Networks: in advanced HIH, it is possible to emulate a full architecture networks (Switches, Routers, WAN), which gives a better understanding about attackers and their methods to break firewalls and hack through any network.
- Redirects attackers when the traffic on the system is high, to another Honeypot that emulate the user's system.
- Able to create Virtual Access Points when connected to real systems, to copy the attacker's IP address and block it on the real Access point.

Since Honeypots demonstrated a sufficient and well-designed architecture that helps in detecting various types of attacks, the Hacking community started to develop techniques that helped in revealing Honeypots and showing its weaknesses. Attackers can check the Response Time of the Honeypot being attacked, Network Traffic Limitation that the Honeypot has, Unmaintained System Notifications may reveal the Honeypot, and Backend Devices Capabilities that might not be combatable to the Honeypot used. However, these techniques are a certain of concern for Honeypot developers, as it helps in making introducing Honeypots that sufficient, smarter and proactive with hackers [23, 21].

C. *Honeypots Implementation:*

In their Experiment, [21], they compared HIH and LIH using Anti-Honeypots features that has been discussed before as the parameters of the study. As a result of the mentioned study, it was shown that when implementing a HIH with an effective simulation of the functionalities of the system gives impression of being a real system with less downsides than a LIH. In addition, the techniques used by spammers to attack the system was not efficient enough to reveal the HIH.

[24] developed a LIH that helps in detecting Telnet Attacks performed on IoT Systems. The purpose behind development proposed is identifying Mirai Attacks as one of the main factors that helps in using IoT Systems to perform DDoS Attacks. The Honeypot created consisted of two major parts, Front-end which it was designed using Node.js programming language, and Back-end which it was designed using Python programming language. The Front-End's main purpose was to handle answers for the attacker's queries. It was divided to 2 scripts, MANUpot.js which handles the manual attacks that the system face, and MIRAIpot.js which deals with the Mirai Attacks. Both were connected to LOG.py script, which is the Back-end of the system. Its purpose was to collect data transformed from Front-end, makes it accessible to the monitor and saves it for further studies. The Back-end of the system was built behind a firewall to protect it from the attackers. The LIH developed was successful in detecting Mirai Attacks after testing it. One downside of the experiment is that the system proposed was not deployed online, it was tested using Mirai source code.

Researchers in [25] did an analyzation review of Conpot Honeypot, a SCADA/ICS LIH that was designed under non-profitable security organization, The Honeynet Project. The main objective of their analyzation was to minimize the gap between performing studies and conducting actual researches with real results on SCADA/ICS security issues using the Honeypot Technology. Moreover, their research manly focused on finding what type of communication ports is usually open when connecting more than 2 Conpots simulating different types of SCADA/ICS devices. It was deployed on multiple Amazon Web Services (AWS), so that it gives a better analysis of the Honeypot. Each of these images were given a specific template to simulate, along with an IP address of each of the images so that it becomes accessible on the Internet. Some images implemented Guardian AST gas pump, Siemens S7-200 ICS, IPMI-371, and Kamstrup-382 smart meter SCADA/ICS device, which are actual devices that has been used in the industry. Conpot Honeypot was online and running on a device that supports Ubuntu 12.04 operating system for 19 days. Two main tools have been used to scan the communication ports of the Honeypots after deployment, Nmap Scan Tool and Shodan Scan Tool. The results obtained from both Scan tools was different, as each scanning tool was focusing on different communication ports. However, it was clear that using Nmap Scan Tool gave better information about the system being scanned since the tool focused on more ports compared to Shodan Scan Tool.

In their research, [26] customized Conpot Honeypot to create an Intrusion Detection System (IDS) that detects attackers on Modbus TCP protocol. The system created relied on a log clustering sequence algorithm with consideration of three aspects that are essential when it comes to IDS and Modbus TCP. First aspect is using Sequential Attacking Patterns (SAPs), which takes in consideration the command sequence variations that the attacker may perform on the system for multiple times, each time with a different sequence. Second aspect is overcoming the challenge of detecting unexpected attacking patterns by the IDS. This was accomplished by implementing the Honeypot system for that simulates Modbus TCP attacks, and helping IDS in creating attacking conditions. The Final aspect was creating a user Interface representing SAPs. The functionality of the project proposed was, using Conpot Honeypot to log attacking information, creating a Clustering Algorithm that uses the information and represent the results using SAP Interface.

After deploying the Conpot Honeypot system on the Internet for 1 month, 98 collection interaction was collected, in which 70,000 logs of different IPs was included in these collections. The results were divided into 2 main categories, the outcome of the proposed method on categorizing Modbus TCP attacking patterns, the outcome of the proposed method on categorizing unexpected patterns. The first category identifies two types of attacks, DoS attack, and Scanning Attacks (queries about the devices and nodes). The second category was measured by choosing a random sequence that was collected from the Conpot Honeypot and re-emulate the sequence to check if it is going to be detected through the algorithm proposed. This method was repeated to get the True Positive Rate, while assuming the False Positive rate as an incorrect detection of a sequence of unexpected pattern.

[2] performed an analyzation of using Honeypots in identifying network attack vectors on SCADA/ICS Systems. The model proposed is to expose the methods used by unauthorized users to attack the SCADA/ICS Systems. Thus, gives suggestions for improving the security on these systems. The authors mimic 3 different protocols, HTTP, S7comm, and Modbus TCP, as they are well used in most Industrial Systems as we mentioned before. The Honeypot used was Target VM, and the machine that uses these protocols is Siemens S7-200 PLC, which also includes S7-comm (102), Modbus (502), and HTTP (80). To monitor the packets transmitted and received through the network, TCPDUMP was used as packet capture tool. To make the system believable by the attacker as a real system, Tarpit technique was used to delay replies coming from the system. 24 devices use Modbus TCP, were simulated and connected to different user interfaces that uses HTTP as a medium for sending commands to the devices. This mechanism gave the attacker the chance to control the machine, while all the controls used and sent was monitored. identify the attacks and its efficiency, a model was made by the authors, defining SNMP Attacks as Medium Risk, HTTP Attacks as High Risk, and Modbus TCP Attacks as Critical. After setting up the Honeypot and deploying for 30 days, the results of this research was collected and reported. HTTP Attackers were attacking php pages to reveal some information, but since the authors did not have any php based emulation, the attack was not successful. Modbus TCP Attackers used two types of function codes that are common in Modbus TCP, function code 43 which is used to gain critical data from the system (mostly PLC related information), and function code 17 Report Slave Identification, which means that attacker is gather information to perform another attack at a later time.

In [17] Conpot Honeypot was further improved to act as HIH and used in emitting a SCADA/ICS System that uses two protocols, HTTP and S7Comm (Used in SIEMENS S7-

400 PLCs). The HTTP protocol has been used by a Dynamic Graphical User Interface (DGUI) website that has been designed to look real for the attackers. Since most GUIs used in Conpot are Static, the website's design has been influenced by looking at Siemens' Human Machine Interface (HMI). The DGUI has Dynamic elements which are, Dynamic timestamp (To show date and time), Updated Login/Logout information, Page Identifier to show what page is open, a Print button to print the opened page, a Navigation Bar, and the Oage Content. The simulation of S7Comm has been improved by analyzing the structure of the header in S7Comm used in Conpot and improving it. [17] claimed "we improved the analytic method and the reply method of S7comm protocol for different function structures in the Conpot." (P.2938). The results have been divided into two parts, Before and After Improving Conpot Honeypot. However, some of the limitations that has been faced by [17] was only improving S7comm protocol due to the time limit. The DGUI which only simulates commands to S7-300/S7-400 and S7-1200 series. A reason for that was in order to simulate other Types of PLCs, separated webpages should be developed accordingly.

V. Conclusion

In conclusion, the objectives of this paper have been met, as an overview of Cyber/Physical Threats has been explained and Cyber/Physical attacks has been classified. In addition, SCADA/ICS systems' architecture, security issues and weaknesses has been elaborated on. Furthermore, it has been shown how Honeypots can be implemented in the field of SCADA/ICS Security to study the effects of Cyber/Physical attacks on these systems.

This paper can be extended by including an experiment on a SCADA/ICS Honeypot system. As it helps in inquiring extra input in the subject of study, as well as exploiting the practical weaknesses that SCADA/ICS systems holds to modern security issues.

VI. Acknowledgment

This work was conducted at the IOT and Wireless Communication Protocols Lab, and is partially funded by International Islamic University Malaysia (IIUM) Publication RIGS grant no. P-RIGS18-003-0003.

References

B. Chung, J. Kim and Y. Jeon, "On Demand Security Configuration for IoT Devices," *The 7th International Conference on Information and Communication Technology Convergence (ICTC), IEEE,* pp. 1082-1084, 2016.

R. S. Ramachandruni and P. Poornachandran, "Detecting the Network Attack Vectors on SCADA Systems," *IEEE, International Conference on Advances in Computing, Communications and Informatics (ICACCI),* pp. 707 - 712, 2015.

S. Pal, M. Hitchens and V. Varadharajan, "On the Design of Security Mechanisms for the Internet of Things," *11th International Conference on Sensing Technology (ICST), IEEE,* 2017.

S. Li, T. Tryfonas and H. Li, "The Internet of Things: A Security Point of View," *Emerlad,* 2016.

I. Mokube and M. Adams, "Honeypots: Concepts, Approaches, and Challenges," *The Annual ACM Southeast Conference ACMSE,* pp. 321-326, 2007.

G. Loukas, Cyber-Physical Attacks: A Growing Invisible Threat, Elsevier Inc., 2015.

D. Minoli, K. Sohraby and J. Kouns, "IoT Security (IoTSec) Considerations, Requirements,and Architecture," *IEEE Annual Consumer Communications & Networking Conference (CCNC),* pp. 1006-1007, 2017.

S. Naik and V. Maral, "Cyber Security - IoT," *IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT),* pp. 764-767, 2017.

L. Liang, K. Zheng, Q. Sheng and X. Huang, "A Denial of Service Attack Method for an IoT System," *IEEE 8th International Conference on Information Technology in Medicine and Education,* pp. 360-364, 2016.

J. Deogirikar and A. Vidhate, "Security Attacks inIoT: A Survey," *International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud),* pp. 32-37, 2017.

Q. Li, X. Feng, H. Wang and L. Sun, "Understanding the Usage of Industrial Control System Devices on the Internet," *IEEE Internet of Thing Journal,* pp. 2178-2189, 2018.

B. A. Forouzan, Data Communication and Networking, McGraw-Hill, 2013.

E. IRMAK and I. Erkek , "An Overview of Cyber-Attack Vectors on SCADA Systems," *6th International Symposium on Digital Forensic and Security (ISDFS),* 2018.

Q. Wanying, W. Weimin, Z. Surong and Z. Yan, "The Study of Security Issues for the Industrial Control Systems Communication Protocols," *Joint International Mechanical, Electronic and Information Technology Conference (JIMET),* 2015.

A. Kleinmann and A. Wool, "Accurate Modeling of the Siemens S7 SCADA Protocol for Intrusion Detection and Digital Forensics," *Journal of Digital Forensics, Security and Law,* pp. 37-50, 2014.

F. Xiao, E. Chen and Q. Xu, "S7commTrace: A High Interactive Honeypot for Industrial Control System Based on S7 Protocol," *Information and Communications Security, 19th International Conference,* pp. 412-423, 2017.

C. Zhao and S. Qin, "A Research for High Interactive Honepot Based on Industrial Service," *3rd IEEE International Conference on Computer and Communications (ICCC),* pp. 2935-2939, 2017.

S. D. Ant´on, D. Fraunholz, C. Lipps, F. Pohl, M. Zimmermann and H. D. Schotten, "Two Decades of SCADA Exploitation: A Brief History," *IEEE Conference on Application, Information and Network Security (AINS),* pp. 97-104, 2017.

A. Porros and S. Villanueva, "Nuking and defending SCADA networks," *No cON Name,* 2010.

N. F. Zulkurnain, A. F. Rebitanim and N. Abdul Malik, "Analysis of THUG: A Low-Interaction Client Honeypot to Identify Malicious Websites and Malwares," *7th International Conference on Computer and Communication Engineering (ICCCE),IEEE,* pp. 135-140, 2017.

J. Pagna, K. Jones and S. Bailey, "A Plausible Solution to SCADA Security Honeypot Systems," *IEEE, Eighth International Conference on Broadband, Wireless Computing, Communication and Applications,* pp. 443-448, 2013.

N. Provos and T. Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley Professional, 2007.

N. Krawetz, "Anti-Honeypot Technology," *IEEE Security & Privecy,* pp. 76-79, 2004.

H. ˇSemi´ and S. Mrdovic, "IoT Honeypot: A multi-Component Solution for Handling Manual and Mirai-Based Attacks," *IEEE, 25th Telecommunication Forum,* 2017.

A. Jicha, M. Patton and H. Chen, "SCADA Honeypots: An In-depth Analysis of Conpot," *IEEE Conference on Intelligence and Security Informatics (ISI),* pp. 196-198, 2016.

Ahmed, Syed Faiz, et al. "Remote access of SCADA with online video streaming." 2013 8th International Conference on Computer Science & Education. IEEE, 2013..