Forensic Analysis of SCADA/ICS System with Security and Vulnerability Assessment

Dr. Umit Karabiyik, Sam Houston State University

Umit Karabiyik is an Assistant Professor in the Department of Computer Science at Sam Houston University, in Huntsville, TX. Dr. Karabiyik completed his Ph.D. and M.S. degrees at Florida State University in 2015 and 2010 respectively. His research interests mainly lie in the area of Digital Forensics and Cybersecurity ranging from developing tools for forensic investigations to creating new models for forensic data analysis in various environments. He also has broad research interests in Expert Systems, Knowledge Representation, Encrypted File Analysis, Computer and Network Security. Dr. Karabiyik is the creator of open source digital forensics tool called Automated Disk Investigation Toolkit (AUDIT). Dr. Karabiyik is a recipient of NIJ Grant on Targeted Data Extraction from Mobile Devices. One of his recent work has received the ”Best Paper Award” at the IEEE 4th International Symposium on Digital Forensic and Security (ISDF). In addition, Dr. Karabiyik is leading the Mobile Forensics and SCADA Forensics Labs at SHSU.

Naciye Celebi
Dr. Faruk Yildiz, Sam Houston State University

Faruk Yildiz is currently an Associate Professor of Engineering Technology at Sam Houston State University. His primary teaching areas are in Electronics, Computer Aided Design (CAD), and Alternative Energy Systems. Research interests include: low power energy harvesting systems, renewable energy technologies and education.

James Holekamp, Sam Houston State University
Dr. Khaled Rabieh, Sam Houston State University

Forensic Analysis of SCADA/ICS System with Security and Vulnerability Assessment

Umit Karabiyik, Naciye Celebi
[umit, nxc038]@shsu.edu
Department of Computer Science
Sam Houston State University

Faruk Yildiz, James Holekamp
[fxy001, jwh042]@shsu.edu
Department of Engineering Technology
Sam Houston State University

Khaled Rabieh
rabieh@shsu.edu
Department of Computer Science
Sam Houston State University

Abstract

Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS) have achieved rapid growth within the competitive technology market. As a result, it has encountered serious security problems. Hence, security methods are needed to secure ICS from targeted attacks. The information security vulnerabilities of ICS have been studied extensively, and the vulnerable nature of these systems is well-known. However, in the case of a security incident (e.g. system failure, security breach, or denial of service attack), it is important to understand what the digital forensics consequences of such incidents are, what procedures or protocols are needed to be used during an investigation, what tools and techniques are appropriate to be used by an investigator, and where the forensic data can be collected from and how. Taking into these questions consideration, there is a serious gap in the literature as forensic attack analysis is commonly guided by experience and by intuition rather than by a systematic or scientific process. Therefore, in this study, we aim to close this gap by developing fairly complex SCADA/ICS laboratory at Sam Houston State University. During the course of our studies, several students (graduate and undergraduate) worked under the supervision of faculty members to understand the forensic aspects of real world attacks on SCADA hardware as well as the network used by the system. This new laboratory is intended to be used for Computer Science, Digital and Cyber Forensic Engineering Technology, and Engineering Technology programs at our university. With the availability of this laboratory we have a realistic SCADA/ICS system which can be used to study real-life experiments such as penetration assessment and testing, vulnerability assessment and testing, and the SCADA forensics research. In addition to aforementioned research activities, the laboratory will also serve to develop and support both undergraduate and graduate level computer science courses as well as undergraduate engineering technology courses. In this paper

we will discuss the digital forensics and security challenges in SCADA/ICS, system infrastructure, forensic attack scenarios and results, student and faculty involvement in this research, laboratory related future course development objectives, student assessments, and the industry support.

Introduction

SCADA (Supervisory Control and Data Acquisition) is mainly used in Industrial Control Systems (ICS) in order to remotely collect real time data to automate and control networked equipment such as Programmable Logic Controllers (PLC). SCADA/ICS systems are used to support and monitor the types of critical infrastructures that serve as pillars for many industrialized areas, such as municipal services, oil, and other types of large-scale energy industries [3, 19].

The significance of SCADA system is based on the data acquired from a remote location in order to control the environment conditions. For instance, SCADA collects data regarding where the leaks have occurred in a pipeline infrastructure. The SCADA system analyzes the real-time data and alerts the system about the detection of such incident. In the earlier design of the SCADA, it did not require internet connection therefore the system was isolated from the public network. In recent years, the system evolved with the technology and SCADA started to use the public network and become exposed to possible cyberattacks [12].

SCADA/ICS have achieved rapid growth within the competitive technology market as well. As a result, it has encountered serious security problems. Possible intrusion attacks may cause not only the financial loses, it may also be endangerment of public safety. Hence, security methods are needed to secure ICS from such targeted attacks. The information security vulnerabilities of ICS have been studied extensively, and the vulnerable nature of these systems is well known [6, 15]. However, in the case of a security incident (e.g. IP flooding attack), it is important to understand what are the digital forensics consequences of such attack? What procedures or protocols are needed to be used during an investigation? What tools and techniques are appropriate to use by the investigator? Where can forensic data be collected and how? In this area, there is a serious gap in the literature as forensic attack analysis is commonly guided by experience and by intuition rather than by a systematic or scientific process [10]. Therefore, we would like to close this gap in this study by performing specific attacks and presenting our observations in the system.

As an example, let's take one of the most serirous cyberattacks such as Stuxnet since it was an additional eye-opener for SCADA operators and vendors [16]. In July 2010, Stuxnet cyberattack caused substantial damage to Iran's nuclear program. The Stuxnet was known as the first discovered malware which specifically against an automation system and has infected estimated 50,000 to 100,000 computer worldwide [6, 3]. The Stuxnet attack has shown that the isolation of the SCADA system from the internet is not an ultimately effective defense method. Existing technologies would have difficulty defending against this attack [16, 8]. There are two main components of the SCADA system; control center and field sites. Field sites are based on Remote Terminal Unit (RTU) and Programmable Logic Controllers (PLC) and field sites send field equipment information to the control center. The control center is the hub of the SCADA system. Also, it has three components such as Human Machine Interface (HMI), database management

system (Historian) and Master Terminal Unit (MTU). The MTU has initiated all communication and receives the data sent from the field device [3]. The main aim of this paper is analyzing the SCADA and addressing the security threats and vulnerabilities in SCADA system.

This paper discusses the need for a SCADA laboratory at the Sam Houston State University specifically designed for Cybersecurity (penetration assessment and testing, SCADA protocols analysis, vulnerability assessment and testing) and SCADA forensics research. The need for cybersecurity increases each day and the known gaps of such expertise in the industrial automation world has given the much needed reason to undertake this work. Hence, we also would like to provide education infrastructure for both Computer Science and Engineering Technology students in our institution. This paper touches upon the existing attempts at building such a near-world lab for academic research and teaching purposes and their challenges. The SCADA laboratory we designed and the research findings we present will be either used to develop new courses or supplement the existing courses in the undergraduate and graduate curriculum with fairly enough number of hands-on activities. Moreover, our paper highlights the challenges, limitations and the methodologies in the project to achieve these goals. The cross-disciplinary design of the lab allows students from various programs with specific goals to use the lab for their studies.

Related Work

The SCADA systems have been target of attacks particularly in the last two decades with the advancements in technology. As part of the the growing awareness of the security issues in SCADA systems, researchers have analyzed series of attacks and vulnerabilities on the SCADA systems. In [24], Bonnie et al. classify the cyber attacks into two categories namely cyberattack in hardware and cyberattack on software. In this research paper, we examined the cyber attacks on SCADA hardware. In the case of cyberattack in hardware, the attacker can change the dataset point by gaining unauthenticated remote access to the hardware device. When the attacker obtains remote access then he/she could change the operator display values. For instance, if the alarm for mission-critical system is maliciously turned off, the human operator will not be aware of the malfunctioning system.

In order to meet the accountability requirement of the data security objectives, analysis of forensic attacks on SCADA system is essential. Forensic attacks are performed to identify possible weaknesses before they are exploited by malicious entities. As stated by Chris et al. in [11], the first step in preparing for any forensic attack is to identify and exploit weaknesses. In order to provide forensic readiness, the authors proposed a four-stage approach which helps performing forensic attacks targeting the SCADA systems and their countermeasures.

- *Stage one - Identify Vulnerabilities:* In this first stage of forensic attack analysis we identify the vulnerabilities in SCADA system.
- *Stage two: Identify Attack Methods:* In this stage, we identify the ways in which attacker may exploit the vulnerability.
- *Stage three: Implement Immediate Risk Reduction:* The goal in this stage is to identify the

need for increasing the SCADA system's defense mechanism.

- *Stage four: Implement Long-term Solutions:* Once the attacks have been identified, it is important to find long-term solutions. It is also important to find a way to provide a security plan for the systems.

During the course of this research project, we have focused on these four stages to attack and analyze the SCADA system. As the SCADA system is a real-time system, forensic analysis we perform must be live analysis according to [3, 16, 4, 17].

According to Ahmed et al. in [3, 16], state of the art digital forensic toolkits do not support the unique features of SCADA system protocols and system' log formats. Therefore, forensic tools particularly designed and developed for SCADA systems are needed. Because of this need, we studied some of the tools discussed in [18]. Sutherland et al. present the study of live forensics within the Windows operating system in [18]. The authors also mention the need of necessary tools which allow the investigator to access the network information, system activity, and memory.

In order to carry out the forensic investigation, we utilized 7-step forensic investigation model stated by Tina et al. in [23]. Identification and Preparation, Identifying data sources, Preservation, Prioritizing, and Collection, Examination, Analysis, Reporting, and Presentation and Reviewing Results. We further explain how the proposed model is adapted to our research in the upcoming sections.

Digital Forensics and Security Challenges in SCADA/ICS

Forensic Examination of SCADA/ICS

Digital forensics is a process of acquisition, examination, analysis and reporting of the evidence. Digital forensics is one of the key disciplines of cyber defense for accountability particularly when there has been a security breech occurred. It is important to carry out the investigation right after the incident to prevent loss of forensic data (evidence). In addition, proper forensic investigation helps to understand what the causes and effects of the intrusion attacks are. Recent attacks against to the SCADA systems demonstrate that forensic investigations become essential and need to be carried out for improved cyber defense on SCADA systems. As the investigator mainly focuses on gathering the evidence data from a device or network, the main goal of an investigation is to explore what exactly happened, how the system got affected, and who performed the attack. In this paper, we have utilized certain attacks in order to perform forensic analysis on the SCADA/ICS system.

Security Challenges in SCADA/ICS

As discussed earlier, SCADA is traditionally developed in a non-network environment, however due to the increasing demand for connectivity through the Internet; the SCADA system has started to use the public network and hence became exposed to the cyberattacks. The connected

system simply leave an open window if not many to various vulnerabilities. For instance, SQL injection, cross-site scripting, malware attacks, and buffer overflow attacks are only some of the attacks can be utilized against to SCADA/ICS systems. On the other hand, the growing awareness of the security issues in SCADA/ICS, researchers have been studying these attacks and vulnerabilities on the SCADA/ICS systems. The cyberattacks on the SCADA/ICS system have potential to damage mission critical operation in cyber and physical infrastructures, cause economic losses of companies, and even affect human and ecological lives.

Digital Forensic Process

Digital forensics is essential for incident response strategy and provide an adequate response in a forensic manner [8]. Radranovosky et al. provide a forensic investigation model for SCADA/ICS in [5]. These investigative steps are: Examination, Identification, Collection, and Documentation. In [23], Tina et al. propose a new forensic model which allows the investigator to carry out a full forensic investigation on a SCADA/ICS by using the combination of cyber forensic and incident response models. The forensic process given in [23] consists of the following phases:

Phase 1- Identification and Preparation: This is the initial phase of the proposed forensic process and its purpose is to understand how the SCADA/ICS operates.

Phase 2- Identifying data sources: This phase is one of the most important phases of the process because it deals with identifying controllers of the system, the type of data can be collected, and where the data can be collected. Data sources need to be identified when any type of attack performed to the system. Needless to say, documentation of the actions taken during this phase is critical and essential for a forensically sound investigation.

Phase 3- Preservation, Prioritizing, and Collection: In this phase, the identified data is collected from the known locations, and it is preserved and prioritized for the purpose of repeatability and presentation. In this phase, it is also critical to collect volatile data as it might be destroyed easily. For instance, data can be collected from databases, computer workstation(s), PLC, etc.

Phase 4- Examination: The purpose of this phase is the forensic examination of the collected evidence. In this phase, possible data filtering techniques can be used to reduce the unrelated data. In this phase, the evidence data is simply surfaced using recovery techniques and tools for forensic analysis.

Phase 5- Analysis: This phase includes recovered forensic artifacts and collected evidential data in order to develop a timeline of the events/incidents. The actual analysis of the data is performed in this phase.

Phase 6- Reporting and Presentation This phase is the collection of findings during the examination and analysis phases. It should include chain of custody documents to protect the admissibility and reliability of the evidence.

Phase 7- Review Results In this phase, all the investigative process is reviewed for comprehensive look to identify inculpatory or exculpatory data. The investigator may prove or disprove certain explanations made earlier.

SCADA/ICS Infrastructure at Sam Houston State University

SCADA systems are often viewed as a specialty subject of industrial engineers and technicians rather than IT engineers. As cyber threats against industrial systems grow and have no defined patterns, the need for understanding and defending these systems at the university study levels have increased. The security industry has stepped up to address cyber threats and are usually staffed with personnel from IT who are often unfamiliar with core SCADA/ICS operations. This lab at the university has been designed with these skill gaps in mind and aims to cover industrial cyber security and forensics. The main aim of the lab is analyzing the SCADA/ICS for vulnerabilities, testing and exploiting the system' weaknesses using penetration testing tools, and analyzing the system for forensic artifacts.

Design of the SCADA Forensics Laboratory

General SCADA/ICS systems composed of some significant units and these are Network Infrastructure, Programmable Logic Controllers (PLC), Supervisory Computers, Human Machine Interface (HMI) and Alarm Systems. Also, Allen Bradly, Automation Direct, Eaton, and Schneider implemented to the system. As we look from a research perspective, needs for an appropriate SCADA Lab consist of these terms above. Therefore, SCADA Lab designed carefully enough to keep these in mind. Lab design is also essential for digital forensic perspective. The SCADA forensics lab consists of both physical and logical components. Physical components are the hardware equipment installed in the system and the logical component is simply the simulations we created and deployed using InduSoft simulation software. We have successfully implemented the hardware and software environment their operations are tested for proper performances. In this paper, we performed and presented cyberattacks to particular PLCs and their connected hardware environments. This hardware is given in Table 1. Additional hardware such as wireless IP camera, red lion DSPLE protocol converter, wireless access point are also installed to the lab. To ensure compatibility between devices, a protocol converter is also included.

The Software

In order to create simulation of critical infrastructure, we have obtained InduSoft Web Studio [9] by Wonderware. InduSoft is a SCADA software platform that provides data acquisition

Table 1: Hardware environments used during the attack experiments

PLC Model	**Attached Hardware**
Eaton XC-CPU202	Buzzer, LED Lights
DirectLogic 06 Koyo	Tower Light, Buzzer, Rotary Encoder
Automation Direct Productivity 3000	Humidity Sensor, Picking Sensor, LED Light
Allen Bradly MicroLogix 1100	Photoelectric Proximity Sensor, LED Light
Schneider M221	Air Velocity Sensor, LED Light

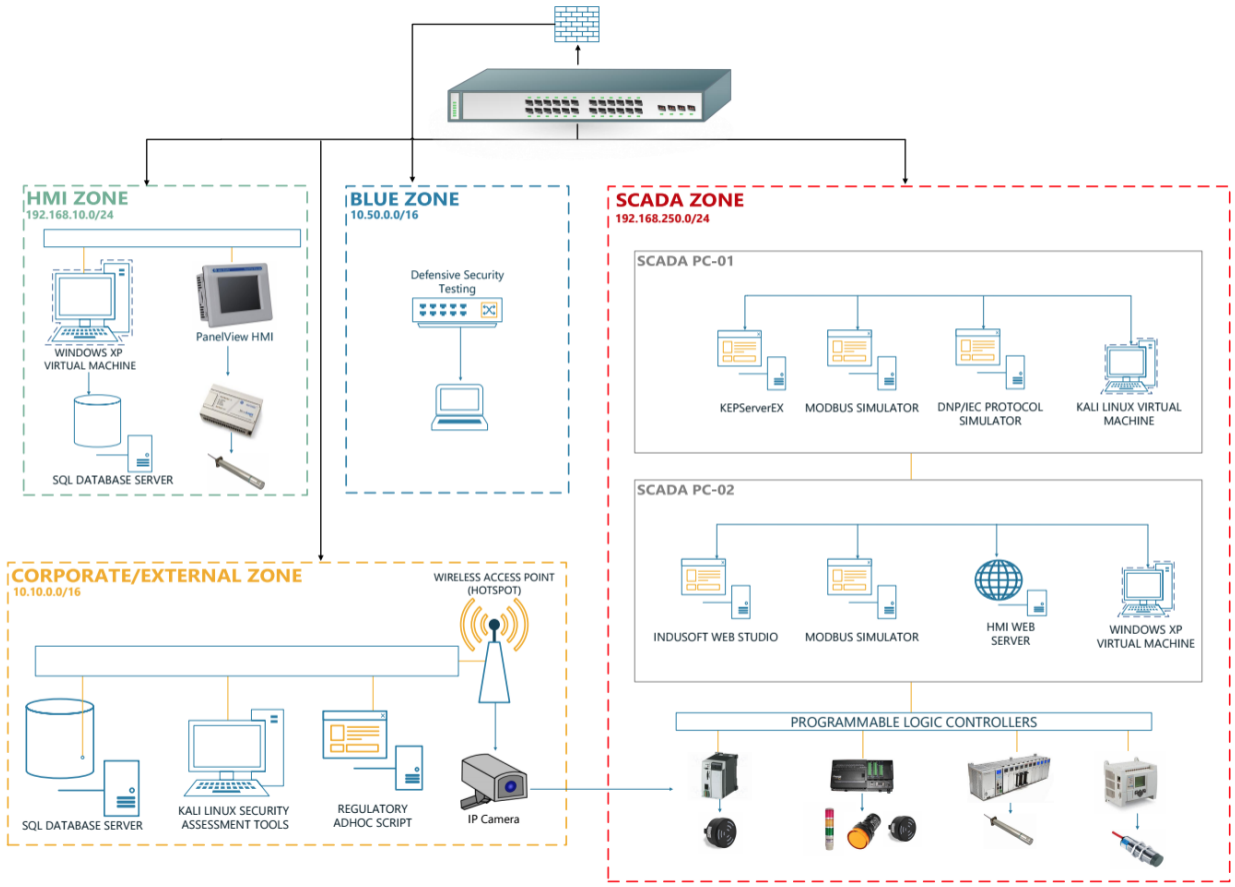

Figure 1: SCADA Lab Design

application. It also allows us to control the live runtime of the SCADA system. The operation of the HMI software and SCADA server are controlled from the InduSoft Web Studio. The InduSoft can be run on the Windows operating system. In our SCADA Lab, we have four Windows 7 desktops. In order to enable access to the InduSoft HMI screen, an Apache web server is also installed. While the InduSoft runtime is live, the Microsoft SQL Server Studio is used for recording all the PLC events, sensor data, and alarm information. KEPServerEX is deployed as an OPC (Object Process Control) server to enable network traffic for the OPC protocol and to provide communications across vendors with limited compatibility. By our design, the Microsoft SQL Server database directly communicates with InduSoft. In addition, the Modbus protocol simulator is also installed on the system. Fig. 1 shows the the core infrastructure of our SCADA lab.

InduSoft HMI Screen

In order to develop the InduSoft HMI screen, tags and VBScript are used. The HMI screen shows the interface with all PLC communications. Status indicators, measurement of the sensor' readings displayed on the HMI screen of the InduSoft (see Fig. 2). There is also automatic

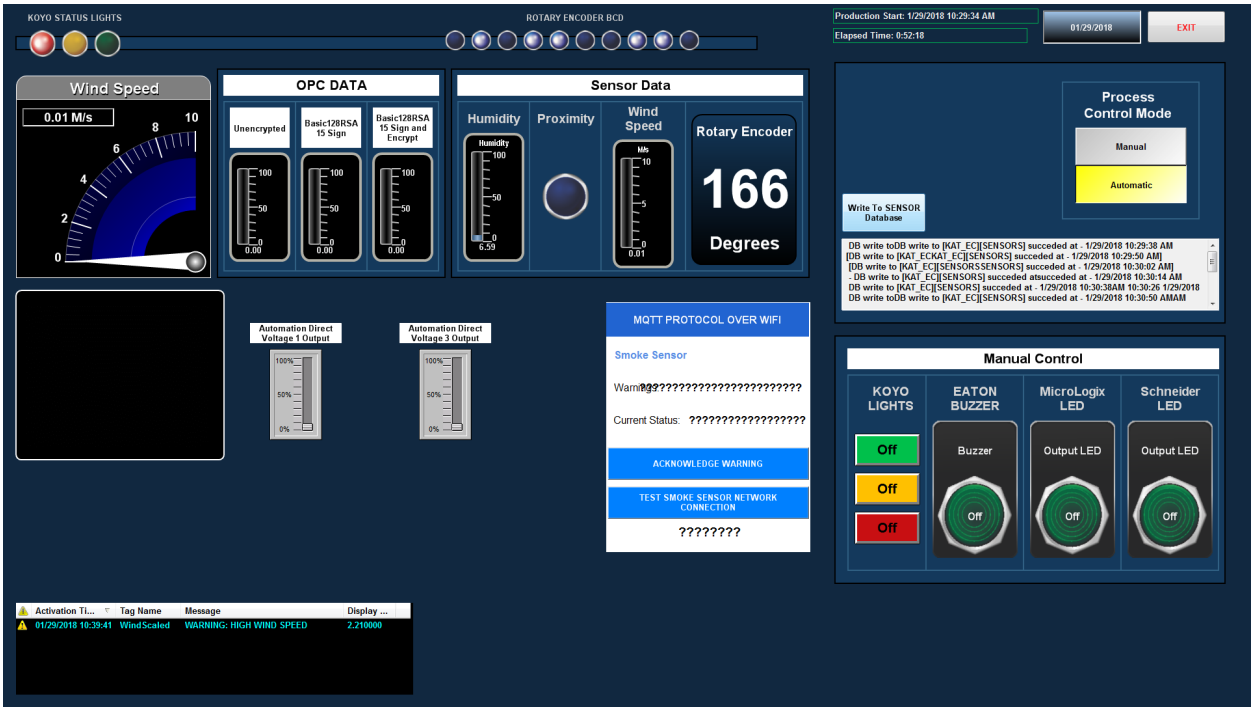

Figure 2: InduSoft HMI Screen

process control simulation located on the HMI screen. In the automatic process, all input data sent to the Microsoft SQL Server and this is set to repeat every 12 seconds. There is also manual input option allows us to write the data whenever it is desired. As the data is directly sent to the database through the network, each cycle of the automatic process generates a network traffic.

As shown in Fig. 2, users are able to observe and analyze the changes in the HMI screen. This screen also allows the users to determine if there is an ongoing attack being performed to the system. By using the Manual Control section in HMI screen a user can control and activate the KOYO lights, Buzzer, Output Led on MicroLogix LED and Schneider LED. The availability of written data to the SENSOR database shows that the data is successfully transferred. The Process Control Mode allows the user to send the data anytime to the database. In Sensor Data section, the user can analyze the change in the humidity sensor, proximity sensor, wind speed sensor, and rotary encoder.

Vulnerability Assessment, Penetration Testing, and Forensic Analysis

Our goal is to perform possible security attacks and identify the weaknesses of the SCADA system and analyze the system's behavior by collecting the evidential data. In order to do this, many forensic tools are installed in our attacker system. As we mentioned earlier, our SCADA lab consists of four Windows 7 workstations and a Linux (Kali/Linux was installed) workstation. The Kali/Linux operating system is used to run series of penetration testing tools such as Nmap [22], Zmap [14], Miranda [21], jSQL Injection [20]. Additionally, Low Orbit Ion Cannon (LOIC) [1]

tool installed on one of the Windows desktops and used to perform IP (Internet Protocol) flooding attack. Low Orbit Ion Cannon is a tool that performs denial of service attack (DoS) in the form of UDP (User Datagram Protocol) flood attack, the effects of these attacks will be explained later in detail. Moreover, Wireshark [7] network packet analysis is also installed and utilized to detect and filter the network traffic in SCADA and the database protocols.

As discussed earlier, in our attack scenarios the four-step approach proposed by Chris et al. in [11] is adapted to our experiments. Here we discuss how we adapted this model in this research.

Stage one- Identify vulnerabilities: After performing the attacks on the SCADA system's hardware, we identified the system's vulnerabilities and analyzed the collected data.

Stage two- Identify attack methods: We identified the attack types and how these attacks cause malfunctioning (stopping) the SCADA system's operations.

Stage three- Implement immediate risk reduction: We implemented some risk reduction scenarios, these scenarios will be detailed later.

Stage four- Implement long-term solutions: We leave this stage as our future work. We plan to implement a long-term solution to prevent the SCADA system from such attacks.

Forensics analysis of SCADA system constitutes different process than conventional forensic procedures. In SCADA forensics the analysis of data, presentation of data, and acquisition of data is performed [17]. There are mainly two types of data acquisition methods namely static and live acquisition. The former is the traditional approach in which the system needs to be shut down before the acquisition. In the latter data is gathered and analyzed while the system is running. Volatile (perishable data in memory) and non-volatile data can be acquired during the live acquisition. The forensic investigator simply cannot turn off the SCADA system for data acquisition [13] because of the availability of volatile data. If the system is turned off it is possible that the volatile data will be destroyed. Hence, live forensic [2] is a viable solution particularly for forensic analysis of SCADA system.

Experiments and Preliminary Results

During course of our experiments we have utilized series of attacks in order to present strengths and weaknesses of the SCADA Lab. In this section we will present the attacks we performed and the their consequences if there is any. Our experiments show that, our SCADA lab is not vulnerable against to significant number of attacks we have performed. Table 2 shows these attacks on the corresponding hardware and the result of the attacks.

Considering all of our experiments, the only test case that we were able to maliciously affect the SCADA system's operation was a type of Denial of Service Attack called IP flooding on the UDP. In order to perform the IP flooding attack, Low Orbit Ion Cannon tool is used to against to the SCADA system's sensors as shown in Fig. 3. Particularly, the attacks are successfully performed on Humidity Sensor, Wind Sensor, Rotary Encoder, Proximity Sensor, KOYO Led Lights and the Buzzer. All the sensor values along with associated timestamps are given in Table 3 for both regular working and attacked conditions.

Table 2: Unsuccessful attack cases and their corresponding results

Case #	Test Cases	Software Tool Used	Test Result
1	Test for MODBUS protocol traffic	Wireshark	Pass
2	Test for OPC DA protocol traffic	Simulator logs	Pass
3	Test for OPC UA protocol traffic	Wireshark	Pass
4	Test for KOYO protocol traffic (KOYO is transmitted as UDP packets)	Wireshark	Pass
5	Test for EATON's Code SYS ARTI protocol traffic	Simulator logs	Pass
6	Test for DNP 3.0 protocol traffic	Wireshark	Pass
7	Verify network for IE104 (IEC 60870-5-104) protocol traffic	Simulator logs	Pass
8	Verify if Direct 06 PLC is configured to respond via HMI(Indusoft) interface	HMI alarms and logs	Pass
9	Verify if Eaton PLC is configured to respond via HMI(Indusoft) interface	HMI alarms and logs	Pass
10	Test for password strength using password cracker tools	John the Ripper	Pass
11	Perform a penetration test using any known exploit against the lab network	Metasploit	Pass
12	Test for Windows security patches to expose backdoors	Microsoft Baseline Security Analyzer	Pass
13	Test for open and vulnerable ports against lab network	NMap	Pass
14	Test for SQL Injection against lab network	jSQL Map	Pass

The effects on KOYO LED Lights: In our SCADA Lab, we have three led lights (Green, Yellow, Red) which are connected to the InduSoft and can be controlled manually via the HMI screen (see Fig. 2). According to the proper operations of the KOYO LED Lights, when the "ON" button is pressed for any color, its appropriate light turns on. Before attack is performed on KOYO Led lights, the lights' IP addresses are recorded on the LOIC tool as '19.168.240.2'. While the attack is performed on the system, the LOIC tool prevented any associated lights being turned on. This was also observed on the HMI screen.

The effects on Humidity Sensor: Humidity sensor is connected to the Automation Direct Productivity 3000, and it communicates directly with InduSoft. Any instant changes in humidity can be observed on the HMI screen. Before performing the IP flooding attack on the Humidity Sensor, we tested the sensor and its data transfer to the database. Every 12 seconds cycle, the InduSoft was able to write the data to the database. The UDP flooding attack started with LOIC tool on sensor's IP address '19.168.250.10'. As shown in Table 3, at 11:53:58 we started the system and increased the humidity level. After the increase can be seen through the HMI screen, we collected the current data at that time. The humidity level was 23.023 on the database, and

Figure 3: Overview of SCADA Lab and its hardware

Table 3: Attack Results Analysis on Database (bold values represent turning-off caused by the attack

	Timestamp	KOYO_Humidity	MODBUS_Wind	KOYO_encoder
Regular	11:53:58	23.023	0.01	180
Attacked	11:55:47	**6.513**	0.01	204
Regular	11:55:22	6.29	0.16	204
Attacked	11:55:34	6.29	**0.01**	204
Regular	11:56:23	6.257	0.01	204
Attacked	11:56:47	6.15	0.18	**178**

while increasing the humidity, we started to perform the attack to analyze the sensor's operation. The attack stopped the sensor' operation at 11:55:47 and the humidity level decreased immediately. The changes on the data can be analyzed both the HMI screen and the database.

The effects on Wind Sensor: Similarly, wind sensor is connected with PLC and communicates directly with InduSoft. The wind changes can be watched and analyzed via the HMI screen. Users can increase the wind level by blowing out to the sensor. Before performing the flood attack on the wind sensor, we tested the sensor and its data transfer to the database. The UDP attack started using LOIC tool on the sensor's IP address '19.168.250.3'. As shown in Table 3, the system is started and the wind level is increased at 11:55:22. As soon as the the increase is observed on the HMI screen, the data in the database is collected. Regularly, the Lab's wind level is 0.01, and after increasing the wind level manually, the wind level became 0.16 in the database. While the humidity is increased, the same attack is launched to analyze the changes in sensor's

operation. The attack stopped the sensor's operation at 11:55:34 and the wind level decreased to 0.01 immediately.

The effects on Rotary Encoder: Rotary Encoder sensor is connected to Direct Logic 06 KOYO and communicates directly with InduSoft. The Rotary changes can be observed on the HMI screen. Users can change the degrees by rotating the sensor and the rotation and the rotation can be maximized at 360-degree and minimized at 1-degree. Before performing the flooding attack on the rotary encoder sensor, we tested the sensor and its data transfered to the database. The successful data transfer was observed in the database. The UDP attack started with LOIC tool on the sensor's IP address '19.168.250.2'. As shown in Table 3, at 11:56:23 we have started the system and rotated the rotary encoder to change the degrees. As we observe the changes in degree through the HMI screen, we also collected the related data from the database. The rotation degree was 204 before we launched the attack. After the attack, the sensor's operation has stopped at 11:56:47 and the rotation changes in the degree stopped at 178. Even though the rotation made manually while the attack was performed, the rotary degree changes stopped at both the HMI screen and the database.

The effects on Buzzer: Buzzer sensor is connected to EATON XC-CPU202 and communicates directly with InduSoft. The changes on the Buzzer can be observed on the HMI screen. Users can activate Buzzer manually by pressing the Buzzer button on the HMI screen. The UDP attack started with LOIC tool on the Buzzer's IP address '19.168.250.3'. After launching the attack, the buzzer's operation stopped. It took few minutes to reactivate Buzzer's operation after the UDP attack.

After performing the attacks on our SCADA system, we have forensically analyzed the SCADA system. In order to carry out forensically sound investigation, we used 7-step forensic investigation model stated by Tina et al. in [23].

Phase 1- Identification and Preparation: Phase 1 is the preparation part of the investigation. Before starting the investigation, we have analyzed the SCADA system's architecture and their hardware and software components.

Phase 2- Identifying data sources: In this phase, we have analyzed the system in detail. As we performed Denial of Service attack to the SCADA system we identified the ways of accessing the system which means how the attacker stopped the SCADA environment's operations.

Phase 3- Preservation, Prioritizing, and Collection: This phase consists of the collection of data from the SCADA system. We have collected volatile data from the database while the system is running and sending their data to the Microsoft SQL Server.

Phase 4- Examination: In this phase we have grouped the collected data into categories. As shown in the Table 3 the sonsors' data examined to observe the changes in values.

Phase 5- Analysis: In this phase, we have gathered the evidential data and developed a timeline for the evidence.

Phase 6- Reporting and Presentation: In this phase, we have examined and analyzed all collected data and created a report.

Phase 7 Reviewing Results: The final report is made available with considering all the results and put together as this paper.

Summary of Student Involvement

This project started with the announcement of Enhancing Undergraduate Research Experiences & Creative Activities (EURECA)'s Faculty and Student Team (FAST) project/grant announcements where undergraduate students work under one or more faculty supervisors for a summer project. This internal grant project provides summer stipend for the students and faculty. It is also a very competitive grant due to many applications received by the committee to review. Two students volunteered to be part of the project and filled out the application. The project was not among those applications were approved for the summer studies. However, office research and sponsored programs (ORSP) funded two students to work on the project. Both students were electronics and computer engineering technology (ECET) majors and then one computer science (CS) graduate student joined to team to help on the cyber security part of the project. The project was supervised by an CS and ECET faculty who are experts in digital forensics and industrial automation & control fields. In the fall of 2017, two of the students were graduated and three new students are identified to take over the project for the future expansion of the project. The Table 4 shows the student information and major fields who contributed to this project.

Educational Activities, Outcomes and Industry Support

During the course of this research, we have developed, deployed, tested, and analyzed our SCADA forensics laboratory. The current state of the lab is fully functional and yet to be improved with new equipment. This lab is an indispensable resource for both undergraduate and graduate students for both research and coursework. Students who were in Network & Cyber Security, Information Security, and Digital Forensic Investigation course have already shown interests working on research project using this facility as a group and individually. Moreover, students who have participated in this research have gained enormous knowledge on the SCADA system as well as penetration testing, vulnerability assessment and forensic investigation. Last but not least, both CS and ECET faculty members have started developing special topic courses on SCADA/ICS structure and its forensic analysis in their programs. As part of the industry support, we are considering

As part of out industry reach out and support activities, we have contact with InduSoft for their education support programs. We are giving the free education version of their software that we have utilized in our design and experiments. We share our finding and experiments with InduSoft engineers for future product development. We will be also reaching out to industry partners for collaborations and internship opportunities that our students can benefit the most.

Table 4: Student Involvement in SCADA Laboratory

Name	Major	Contribution/Length	Duty	Active/Graduated
Student A	ECET	Started the project Sp, Su, Fa 2017	Hardware/Software, report presentation, purchasing, data collection and analyzing	Fall 2017
Student B	ECET	Worked on the project Sp, Su 2017	Hardware, purchasing, manual preparation	Summer 2017
Student C	CS	Worked on the project Sp, Su 2017	Software (Cyberattacks, digital forensics), data collection and analyzing	Summer 2017
Student D	ECET	Working on the project, Sp 2018	Hardware (implementation, improvement), Software	Active
Student E	Engineering Technology (Electronics)	Working on the project, Sp 2018	Hardware (implementation, improvement), Software	Active
Student F	CS	Working on the project, Fa 2017, Sp 2018	Software (Cyberattacks, digital forensics), data collection and analyzing, report preparation	Active
Student G	ECET	Working on the project, Sp 2018	Hardware (implementation, improvement), Software	Active

Future Work and Conclusion

The SCADA system profoundly ingrained and being used in industries such as transportation, oil and gas refining, and telecommunication. In recent years, the system evolved with the technology and SCADA started to use the public network and exposed to the cyberattacks. These cyberattacks leave breadcrumbs behind and therefore needs to be analyzed forensically. Recent attacks to SCADA system demonstrate that forensic investigation becomes essential and needs to be carried out for improving the cyber defense on SCADA system. In this paper, we have presented the newly developed and deployed SCADA forensics lab, performed attacks on SCADA system, and performed digital forensic analysis of those attacks. Our future goal is to implement a long-term solution to SCADA/ICS system by creating an investigation tool as well as targeted data acquisition tool from the SCADA system and its network.

References

[1] abatishchev. Low orbit ion cannon — penetration testing tools, 2018. Accessed: 2018-02-01.

[2] Frank Adelstein. Live forensics: diagnosing your system without killing it first. *Communications of the ACM*, 49(2):63–66, 2006.

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

[4] David Bailey and Edwin Wright. *Practical SCADA for industry*. Elsevier, 2003.

[5] Jacob Brodscky and Robert Radvanovsky. Control systems security. *Corporate hacking and technology-driven crime: Social dynamics and implications*, pages 187–203, 2010.

[6] Thomas M Chen and Saeed Abu-Nimeh. Lessons from stuxnet. *Computer*, 44(4):91–93, 2011.

[7] Gerald Combs et al. Wireshark-network protocol analyzer. *Version 0.99*, 5, 2008.

[8] Fahmid Imtiaz. Enterprise computer forensics: A defensive and offensive strategy to fight computer crime. 2006.

[9] Indusoft. Indusoft web studio 8.1, 2018. Accessed: 2018-02-01.

[10] Chris W Johnson, Rob Harkness, and Maria Evangelopoulou. Forensic attacks analysis and the cyber security of safety-critical industrial control systems. 2016.

[11] Chris W Johnson, Rob Harkness, and Maria Evangelopoulou. Forensic attacks analysis and the cyber security of safety-critical industrial control systems. 2016.

[12] Rao Kalapatapu. Scada protocols and communication trends. *ISA2004*, pages 5–7, 2004.

[13] Martin Naedele. Addressing it security for critical control systems. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 115–115. IEEE, 2007.

[14] University of Michigan. Zmap — penetration testing tools, 2018. Accessed: 2018-02-01.

[15] Heiko Patzlaff. D7. 1 preliminary report on forensic analysis for industrial systems. *CRISALIS Consortium, Symantec, Sophia Antipolis, France*, 2013.

[16] H Vincent Poor. *An introduction to signal detection and estimation*. Springer Science & Business Media, 2013.

[17] Mamoona Rafique and MNA Khan. Exploring static and live digital forensics: Methods, practices and tools. *International Journal of Scientific & Engineering Research*, 4(10):1048–1056, 2013.

[18] Iain Sutherland, Jon Evans, Theodore Tryfonas, and Andrew Blyth. Acquiring volatile operating system data tools and techniques. *ACM SIGOPS Operating Systems Review*, 42(3):65–73, 2008.

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

[20] Tools.kali.org. jsql tool — penetration testing tools, 2018. Accessed: 2018-02-01.

[21] Tools.kali.org. Miranda — penetration testing tools, 2018. Accessed: 2018-02-01.

[22] Tools.kali.org. Nmap — penetration testing tools, 2018. Accessed: 2018-02-01.

[23] Tina Wu, Jules Ferdinand Pagna Disso, Kevin Jones, and Adrian Campos. Towards a scada forensics architecture. In *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*, volume 12, 2013.

[24] Bonnie Zhu, Anthony Joseph, and Shankar Sastry. A taxonomy of cyber attacks on scada systems. In *Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*, pages 380–388. IEEE, 2011.