Security Issues of SCADA Systems

Emily Ciaravino, Md Minhaz Chowdhury and Mike Jochen

Computer Science Department

East Stroudsburg University

East Stroudsburg, PA 1830

Eciaravino@live.esu.edu,
Mchowdhur1@esu.edu,
Mjochen@esu.edu

Krishna Kambhampaty

Computer Science Department

North Dakota State University

Fargo, ND 58102

K.kambhampaty@ndsu.edu

Abstract

The supervisory control and data acquisition systems allow people to monitor, collect, and analyze real-time data, giving them the flexibility to interact with devices on a detailed level. These systems rely more on the Internet and automation of tasks compared to those with more human decision making. Such reliance has enabled these systems to incorporate hundreds of thousands of devices connected via the internet, resulting more room for security holes. Hence, these systems are becoming subject to growing security threats, necessitating a major revision in these systems security tactics. This paper delves into the current common security holes of the supervisory control and data acquisition systems. The security holes are characterized from three aspects: physical, social, and policy-enacted level. This paper also presents specific techniques that can patch these holes to make each system as safe as possible. This paper concludes that the supervisory control and data acquisition systems in a critical environment must enact and display the specified security measures to prevent historic mishaps from the past and possible zero-day attacks.

Index Terms—Access Controls, Computer Security, Policy, SCADA, Vulnerabilities.

1 Introduction

Supervisory control and data acquisition (SCADA) systems are systems comprising of hardware and software components that make up many industrial organizations including health facilities, power generation plants, and manufacturing companies. For example, SCADA systems can be set up to determine a leak on a pipeline and either send an alert or close the valve entirely [1]. The systems allow people to monitor, collect, and analyze real-time data, giving them the flexibility to interact with devices on a detailed level [2]. Based on the detail provided, the operator(s) of the systems can make informed decisions to continue running each facility to its fullest. Additionally, these processes reduce human error, improve productivity, and can aid in monitoring a building that is geographically isolated [1]. People can interface with these systems through a variety of elements, and the infrastructure has evolved in such a way that there are usually connections and links to the Internet to provide an upper hand for the system. Since isolation of these infrastructures is virtually obsolete, it is critical to consider the security revolving around these systems [3].

People in the network/computer security field must keep up with preventive measures, access controls, and emergency preparedness plans for these structures, given the frequent and extensive occurrence of attacks [4]. Creating an awareness of potential threats to SCADA systems will allow for effective risk management tools, with the hopes that should an attack occur, it can be denied or downtime in general can be minimized. Because cyber-attacks have become more frequent and extensive within SCADA systems, professionals need to ensure the architecture of their system is secure, as it will help to prevent mishaps that have occurred in the past, prevent future exploitations, and guarantee that the people and businesses serviced by SCADA systems will remain functional. This topic will always remain relevant in computer security field as multiple security compromises have already occurred in the past and will continue to increase as terrorists, for example, look to take down critical systems.

Because these systems are connected to the Internet, it is imperative that as the infrastructure advances, so does the deterrent measures that come with it. SCADA systems allow automation of many industrial processes with minimal human interaction [5]. Five essential components comprise a SCADA system: human machine interface (HMI), supervisory system, remote terminal units (RTUs), programmable logic controllers (PLCs), and communication infrastructures. The HMI processes data and forwards it to a human operator in a readable format. The supervisory system takes this same data and sends commands to the process occurring. The RTUs connect sensors and convert the signals received to a digital format to send to the supervisory system and

store in a database. PLCs are used as field devices for various and specific tasks, for I/O, and for measuring of certain scenarios/events. The communication infrastructure is what allows connectivity between the supervisory system, RTUs, and PLCs [6]. Every component is connected to create a larger umbrella that powers the SCADA system as a whole.

This paper will delve into current security techniques on a physical, social, and policy-enacted level to showcase common vulnerabilities and how specific techniques can patch these holes. Threats in each of these three categories will also be discussed so that workers in these types of environments know what to keep their eye on. After reading this paper, users should be able to determine where vulnerabilities in a SCADA system lie and what can be implemented to make each system as safe as possible.

The remainder of this paper is organized as follows: Section 2 will delve into a background of vulnerabilities for this system. Section 3 discusses all relevant categories that must be addressed to maintain a secure SCADA system. Section 4 details major SCADA mishaps to show real-life examples of security importance. In section 5, we will conclude and present the future of SCADA security.

2 Background

The world connected to the internet is still vulnerable to existing and new threats. Threats are not limited to physical attacks and cyber-attacks; it has many forms e.g. fraud, deception etc. For example, cloud service provider can fraud its consumers to meet a specific goal [7-10]. To deal with these threats, by preventing or minimizing the adverse effect of threats, many scientific methodologies emerged. Examples of such methodologies or sub-disciplines are, but not limited to, machine learning, data mining, artificial immune systems. Machine learning techniques has the capability to learn from the nature of a given problem [11-12]. Similarly, data mining can summarize necessary concise information from a vast amount of data [13-14]. On the other hand, evolutionary computation algorithms, e.g. artificial immune system, can mimic the nature to solve a given problem [15]. In this paper, the security issues of a sensor based system, the SCADA system, has been presented.

The SCADA system is exposed to security threats, just like any other internet based devices. For example, access to just one computer is all it takes to give someone with malicious intent free rein to the physical machinery in a SCADA system. This is especially important with many systems being connected to the Internet, as it allows for an “in” from any remote location. That being said, this leaves many methods for attack, as more vulnerabilities can be leveraged. To understand how a system administrator can

protect their SCADA system, they must first understand what vulnerabilities they need to protect against.

The first category that must be addressed is the physical securing of all equipment, the building itself, and the perimeter. This can and should be accomplished in multiple ways, in order to provide redundancy, should something fail. One team of white hat hackers show how easy it can be to gain physical access to a building given the right tools. To see how this is done, refer to the video [16] created by a team of penetration testers. Their first tactic was to use social engineering and though it failed, they show how easy it is to toy with human emotions. However, within three days, the team is able to gain an extensive amount of access to the facility and network itself. The team enters the property through a fenceless side of the building, break open the door using a shove-it tool, and in turn, gain access to the vehicles and offices inside that are already unlocked [16].

In general, these systems do not have built-in security mechanisms, which is "considered a low hanging fruit" for those with lower skill levels, but also those who know how to cover their tracks [17-18]. One of the main attack scenarios that do occur are Man-In-The-Middle (MITM) attacks, due to the lack of authentication and encryption with protocols used [8]. Another main entry point for remote attacks are any vulnerabilities found in installed software or in the operating system itself [19]. This can allow an attacker to gain all the information he or she needs through reconnaissance, including power usage, breaker information, or mapping of the network to carry out their initial exploit [18]. Based on data collected, any hijacker can then use a replay attack to gain the access they want, all without being detected [18, 20]. By taking the necessary precautions to understand and pay attention to anomalies, professionals can implement access controls and additional security measures on the network to prevent attacks from occurring.

One of the final categories to pay attention to is the policies in place for a SCADA system. It is important for the users and overseers of these critical systems to understand the regulations and follow them. For example, a recent exploit due to a phishing email was successfully carried out due to a user's negligence at a Ukrainian power plant [2]. This was done by providing their username and password combination to the social engineer. Should a SCADA system not have a security plan in place, unnecessary human error could lead to exploits of the system. Policies and a security plan tie together the physical, technical, and social necessities needed to ensure the security of a SCADA system.

A combination of mitigation techniques is needed to effectively manage against various attacks. Diversity and redundancy are key, and effective strategies will be discussed in depth in the upcoming sections. There will always be zero-day attacks and other breaches that cannot be protected against, but prevention can certainly defend against past events that have happened and future attacks in the making.

3 Security Tactics

As a security measure, the physical measures needed to secure the perimeter and inside access controls are extremely important for SCADA systems. Also effective mitigation and prevention techniques need to be implemented on a network level to protect these systems from cyber-attacks. On the other hand, the administration and policy for SCADA need to reviewed, to find out if there are any flaws in the policy that prevents to take actions against threats and attacks. The following subsections describes these security tactics for SCADA system.

3.1 Physical Access Controls

The physical measures needed to secure the perimeter and inside access controls are extremely important. Securing all main and connecting sites with authorization and access controls is vital in allowing the permitted personnel access into the buildings, especially in environments where multiple vendors coincide [4]. Physical precautions should be implemented in locations where systems, applications, and segments of the network are critical and vital to the process at hand. Physical controls to include at a glance follow: network segmentation, the use of video monitoring, keeping all secure areas locked, giving access only to those authorized, and having outer perimeter security like fencing or guards.

While network segmentation should occur at a logical level, it is also important to ensure this is implemented physically. For example, with air gapping (which is a subset of granular network segmentation), a portion of this physical level of security can be achieved. Air gapping involves the isolation of a computer or network from any external connection, wired or wirelessly [4]. Along with this infrastructure, employees need to understand this is a secure network, and external devices are not allowed to be connected under any circumstances. Otherwise, this defeats the purpose of keeping portions of the network separate. Air gapping, however, can only truly work for systems that can stand alone, must be totally secure, and do not relay on the Internet, such as high-risk nuclear plants [21].

Looking at the topology of a network (physically and logically in this case), specific research [4] shows granular network segmentation is one of the most effective ways of securing a SCADA system. This was displayed with a tool called securiCAD, which

models an IT environment (focusing on the SCADA portion) and uses attack graphs to display weakness and pitfalls for potential attacks [4, 22]. A baseline using this tool allows users to visualize and prioritize what vulnerabilities are easiest to control. The team using this tool had input public information from published scientific journals, etc. to get the results they did. Because the results of this tool show "the SCADA server, application server and front end" have a "higher degree of vulnerability than most other systems in the SCADA network," [4] it is important to implement this network segmentation with regards to these areas, as it is possible to eliminate half the attacks that did occur, especially against those with little to no attacking skills.

Additionally, access controls play a huge part in the physical security. According to Korman et. al [4], "a well-aligned and properly functioning authorization and access control system drastically increases an enterprise's cyber security." Different levels of access should be given to the machines and networks themselves, the rooms where these systems are housed, and the perimeter of all facilities. Identification and authentication of people into a facility is extremely important. For instance, recording who comes into the building at what time, and ensuring he/she does not have access to secure portions of a building with locks, passcodes, etc. is vital. Users need to be authenticated and authorized to get to certain portions of a facility. In many cases, companies should also look into multi-factor authentication, depending on the criticality of their process. This can be c combination of swipe access and knowing a PIN or answering a security questions with the use of biometrics to verify.

3.2 Networking Access Controls

Since it is now commonplace for SCADA systems to be connected to the Internet, effective mitigation and prevention techniques need to be implemented on a network level. It was found that some companies with critical infrastructures have not updated the operating system (OS) running their systems in 30 years, leaving holes for those wishing to attack [19]. With the proper tools and configurations in place for SCADA systems, these setups can greatly aid the people acting upon all alerts received. While MITM and denial of service (DOS) attacks are common, exploits that now occur are becoming robust than this, making it even more important to address these problems [3].

Being that most networks are connected to the Internet in some way, a consistent patch management schedule should be in place [4], especially for companies who fail to update any of their systems. Patching is also important because systems are usually assembled from third party programs and hardware found from various parts of the world [3]. Unbeknownst to the people in control of the SCADA system, backdoors could be wide open. This is especially dangerous for those who monitor open-source code to determine

holes in software, giving them an advantage to “crack the system” days or months before a vulnerability is even publicly released [23]. A patching schedule should be created and followed on a regular basis and must have documentation that supports its development (which will be discussed in section 3.2).

Centralizing and segmenting important parts of the network on a logical level by using a demilitarized zone (DMZ) is an effective way to reduce harm from intrusions [4]. Ideally, in a DMZ, public facing servers are separated from the private network, where untrusted activity is to be kept out. The most common way to achieve this is with two firewalls, one facing the incoming public traffic, and another protecting the trusted network. If someone were to try to break through, they would need to get through not one, but two security features, making it a much harder task for the attacker to overtake.

Additionally, ensuring the SCADA system is self-autonomic to detect anomalous activity can greatly increase security with machine learning [3]. In essence, an autonomic system is “self-healing, self-regulating, self-optimizing and self-protecting” [3]. Through the collection of data from the processes occurring within the SCADA system, monitoring and control by users can be completed. The system needs to be able to allocate memory dynamically, be able to isolate an infected portion of the network, and should alert a user should the system deviate from its baseline. In order to gain traction towards autonomic systems, there needs to be a way to create a central database from logged user activity, process related activities, and the analysis of system commands to categorize which are threats [3]. While this is not seen in many SCADA systems today, it is something to consider implementing moving forward so unnecessary human error can be eliminated.

It is also good practice to install and configure an intrusion detection system (IDS) for a SCADA system. The IDS should pay attention to any anomalies in the registers within the programmable logic controllers [24]. Specifically, a group has designed their own IDS called PT-IDS [24]. This specific system, at a high-level, uses telemetry data to send an alert should something differ from the pre-programmed and known information. PT-IDS works to spot activity in conjunction with any traces of reconnaissance, injections, or DOS attacks [24].

As mentioned, access controls should be in place, however, it has been found the enforcement of port security, keeping static ARP tables, and implementing a strong password policy are some of the least effective ways to keep a SCADA system secure. These should not be the bare minimum of security implemented for SCADA systems though [4], as they have shown little improvement in overall security. A combination of the access controls listed so far can provide the most safety for a SCADA system.

3.3 SCADA Framework and Policy

The final category that we will delve into relates to administration and policy. Policies and training must be administered, as human error within a SCADA system could result in huge downfalls. In a 2015 Ukrainian attack on an electrical distribution plant, it was found intruders were given access via a successful phishing attack for username and password combinations [2]. Humans possess the abilities to determine patterns within events and can hone these skills even more with the proper training and awareness [2]. It is possible with the correct user awareness; the Ukrainian attack could have been avoided. Automated tools provide humans with data, however; it is up to them to interpret and decide their next course of action.

By developing a set of rules for a SCADA system, a logical baseline is created to follow and compare information to in a timely manner. For example, with an ethernet-connected field device and a remote terminal unit (RTU) used to transfer telemetry data to a master system, all initial traffic should start from the RTU given it is configured in a polling scheme [2]. If this is not the case, humans should be able to recognize the error and correct the problem.

A security framework needs to be set in place to cater to the specific SCADA system at hand. Information included in this should cover the purpose, scope, personnel involved, audit/access control assessments, physical securities, etc. [25]. However, an exact IT plan cannot be directly used to protect a SCADA system because it will be so distorted and vague to even be applicable at that point.

All documents/security policies that are created need to be enforced, detailing the who, when, why, and how evaluations of this plan will be conducted [25]. That being said, these must align with the goals of the organization. Multiple sections should come together at the end to create a customized framework for the companies' SCADA system. Audits and assessments should also be conducted for the system based on the documentation. The policies are part of a living framework, and as such, should be changed and updated when needed. Employees must know, understand, and follow these rules based on training and awareness events, as well as anything else the company finds fit to instill this information.

In summary, SCADA security can be enhanced by confirming physical security, effective mitigation and prevention techniques implemented on a network level and by revising and rewriting the administration and policy for SCADA usage.

4 Past SCADA Security Incidents

SCADA systems are used in many industries and as such, have had their own fair share of mishaps. Because of some of the flaws previously mentioned, unfortunate events occurred as a result. Stuxnet is one example and the first known worm to attack SCADA systems [19]. The worm is initially installed and spread via a USB drive, targeting Windows machines, Siemens Step7 software, and ultimately compromising logic controllers. In the case of Iran's plant, Stuxnet was able to take over centrifuges, and spin them to failure. Additionally, false feedback is given to reliant controllers, making any problems invisible until it is too late.

The malfunctioning of real-time systems can have fatal consequences if not tested before deploying, as seen with Therac-25, a computerized radiation therapy device. Due to the ineffectiveness of time-critical events from lack of testing and failure to remove fatal flaws, patients were subject to massive radiation overdoses [26]. That being said, if a third party were to tamper with a SCADA system in a harmful way, the results could be permanent.

Most recently, the power outage in Ukraine shows the seriousness of securing and preventing attacks. This attack was undergone by unauthorized commands to open circuit breakers via PLCs, resulting in power outages for an estimated 255,000 customers [27]. A fifth of the total power was taken out for about an hour, not a long time, but enough to show the potential consequences and importance of security [28]. The code that executed was purposely built to create the chaos it did. According to researchers from the Greenberg article, the "new malware can automate mass power outages, like the one in Ukraine's capital, and includes swappable, plug-in components that could allow it to be adapted to different electric utilities" [28].

5 Conclusion

In conclusion, the presented study in this paper confirms that all SCADA systems, new or old, need a major rehauling in their security tactics. The SCADA systems must maintain a consistent schedule to keep this information current and up-to-date. There are numerous tactics in defending against threats, but it is important to implement a variety of security controls on a physical, social, and networking level. Security administrators need to take a good look at the physical environment of their SCADA system to make sure people only have access to rooms and systems they are authorized to be in. On a social level, policies must be implemented and followed, while employees must be trained and adhere

to the guidelines. Finally, access controls such as an IDS and network segmentation are just the minimum of what should be protecting the SCADA system at a lower level. This will ensure redundancy should one or more of the access controls fail. Each implementation will vary among SCADA systems depending on the individual goals of each company. One tactic does not fit all.

People within this field should pay close attention to any new vulnerabilities in these systems, as failure could cause catastrophic failure on multiple levels. This has been seen in a few of the past events mentioned. Depending on the agreed upon schedule, policies and rules should be looked at and changed on an as-needed basis.

As SCADA systems evolve to incorporate hundreds of thousands of devices, more room for holes are created. Many researchers have been looking for ways to create specialized security software for SCADA systems. This is especially true with systems that rely more on the Internet and automation of tasks compared to those with more human decision making. Hopefully in the future, this is something that gains more momentum, as there will continue to be growing threats to these systems.

References

[1] "What is SCADA? " OleumTech. [Online]. Available: https://oleumtech.com/what-is-scada. [Accessed 26 October 2018].

[2] J. Pack, Situational awareness for SCADA systems, *The Fifth Cybersecurity Symposium*, Article no 6, Coeur d' Alene, Idaho, April 9-11, 2018.

[3] S. Nazir, S. Patel and D. Patel, Autonomic Computing Meets SCADA Security, *The 16th International Conference on Cognitive Informatics & Cognitive Computing*, London, UK, July 26-28, 2017.

[4] M. Korman, M. Välja, G. Björkman, M. Ekstedt, A. Vernotte and R. Lagerström, Analyzing the Effectiveness of Attack Countermeasures in a SCADA System, *The 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*, Pages 73-78, Pittsburgh, Pennsylvania, USA, April 18-21, 2017.

[5] J. Moos, Cyber Forensics in a Post Stuxnet World, *ITNOW*, Volume 57, Issue 4, Pages 32–33, November 6, 2015.

[6] D. Krambeck, ‘All About Circuits’, August 31, 2015. [Online]. Available: https://www.allaboutcircuits.com/author/donald-krambeck [Accessed October 2018].

[7] Md Minhaz Chowdhury and Kendall Nygard, Machine Learning within a Con Resistant Trust Model, *The 33rd International Conference on Computers and their Applications (CATA 2018),* Flamingo Hotel, Las Vegas, Nevada, USA, March 19-21, 2018.

[8] Md Minhaz Chowdhury, Kendall E. Nygard, Krishna Kambhampaty and Maryam Alruwaythi, Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm, *The 4th Annual Conference on Computational Science & Computational Intelligence*, Las Vegas, NV, USA, December, 2017.

[9] Md Minhaz Chowdhury and Kendall E. Nygard, An Empirical Study on Con Resistant Trust Algorithm for Cyberspace, *The 2017 World Congress in Computer Science, Computer Engineering, & Applied Computing*, Athens, Greece, July 17-20, 2017.

[10] Md Minhaz Chowdhury and Kendall E. Nygard, Deception in Cyberspace: An Empirical Study on a Con Man Attack, *The 16th Annual IEEE International Conference on Electro Information Technology,* Lincoln, Nebraska, U.S.A, May 14-17, 2017.

[11] Rahul Gomes, Mostofa Ahsan and Anne Denton, Random Forest Classifier in SDN Framework for User-Based Indoor Localization, *The 2018 IEEE International Conference on Electro/Information Technology,* Rochester, Michigan, USA, 3-5 May 2018.

[12] Mostofa Ahsan, Rahul Gomes and Anne Denton, SMOTE Implementation on Phishing Data to Enhance Cybersecurity, *The 2018 IEEE International Conference on Electro/Information Technology,* Rochester, Michigan, USA, 3-5 May 2018.

[13] I. Jahan and S. Z. Sajal, Stock Price Prediction using Recurrent Neural Network (RNN) Algorithm on Time-Series Data, *The Midwest Instruction and Computing Symposium (MICS 2018),* Duluth MN, USA, April 6-7, 2018.

[14] I. Jahan and S. Z. Sajal, Prediction on Oscar Winners Based on Twitter Sentiment Analysis Using R, *The 2018 SDSU Data Science Symposium,* Brookings SD, USA, February 11-12, 2018.

[15] Md Minhaz Chowdhury, Jingpeng Tang and Kendall E. Nygard, An Artificial Immune System Heuristic in a Smart Grid, *The 28th International Conference on Computers and Their Applications,* Waikiki, Honolulu, Hawaii, USA, December 2013.

[16] Watch hackers break into the US power grid, C. Snyder and P. Szoldra, USA, Tech Insider, 2016.

[17] B. Green, M. Krotofil and A. Abbasi, Significance of Process Comprehension for Conducting Targeted ICS Attacks, *The 2017 Workshop on Cyber-Physical Systems Security and Privacy*, Dallas, Texas, USA, November 03-03, 2017.

[18] H. Lin, A. Slagell, Z. Kalbarczyk and R. K. Iyer, Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids, *The 7th*

International Conference on Security of Information and Networks, Glasgow, Scotland, UK, September 09-11, 2014.

[19] D. Kushner, The real story of stuxnet, *IEEE Spectrum*, Volume 50, Issue 3, Pages 48-53, March 7, 2013.

[20] J. Dong, S. M. Djouadi, J. J. Nutaro and T. Kuruganti, Secure control systems with application to cyber-physical systems, *The 9th Annual Cyber and Information Security Research Conference*, Pages 9-12, Tennessee, USA, April 08 - 10, 2014.

[21] E. Byres, The Air Gap: SCADA's Enduring Security Myth, *Communications of the ACM*, Volume 56, Pages 29-31, August, 2013.

[22] M. Ekstedt, P. Johnson, R. Lagerstrom, D. Gorton, J. Nydren and K. Shahzad, Securi CAD by Foreseeti: A CAD Tool for Enterprise Cyber Security Management, *The IEEE 19th International Enterprise Distributed Object Computing Workshop*, Adelaide, SA, Australia, September 21-25, 2015.

[23] F. Li and V. Paxson, A Large-Scale Empirical Study of Security Patches, *The 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas, 2017.

[24] J. Zhang, S. Gan, X. Liu and P. Zhu, Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis, *IEEE Symposium on Computers and Communication (ISCC)*, Messina, June 27-30, 2016.

[25] D. Kilman and J. Stamp, Framework for SCADA Security Policy, 2005.

[26] D. Mandrioli, S. Morasca and A. Morzenti, Generating Test Cases for Real-time Systems from Logic Specifications, *ACM Transactions on Computer Systems*, Volume 13, Issue 4, pages 365-398, 1995.

[27] Z. Zheng and A. N. Reddy, Towards Improving Data Validity of Cyber-Physical Systems Through Path Redundancy, *The 3rd ACM Workshop on Cyber-Physical System Security*, Abu Dhabi, 2017.

[28] A. Greenberg, Crash Override: The Malware That Took Down a Power Grid, *Wired*, 12 June 2017. [Online]. Available: https://www.wired.com/story/crash-override-malware/. [Accessed November 2018].