Chad Holm

COVA CCI Cybersecurity Undergraduate Research

cholm017@odu.edu

Security Issues with Network Connected SCADA Systems

Security Issues with Network Connected SCADA Systems

Abstract:

The use of Supervisory Control and Data Acquisition (SCADA) systems has become common place and are being used in several different industries. These have evolved as the technology has progressed. The use of Internet of Things (IOT) devices makes for less human intervention to run daily operations in these industries. This can also allow hackers to gain access to these devices due to security holes that are overlooked. There have several different ways that have been exploited on SCADA networks and the goal is to recognize and secure them so hackers cannot gain access to them.

Introduction:

Large industrial facilities and infrastructures such as chemical and petrochemical factories, oil refineries, power generation plants, and water/sewage treatment plants are highly dependent on automatic control systems, among which SCADA systems are the most widely deployed. See figure 1. In this paper the 3rd generation of SCADA devices will mostly covered. This generation is still widely used and has flaws in it, when being hooked up to networks. These devices were released without the threat of security as the newer devices are, like Windows XP being released with a software firewall turned on by default. The use of these devices is increasing as manufacturing and monitoring is getting more advanced. There is an increase with these systems to be controlled remotely and use network protocols to relay the data. The 3rd generation systems are using TCP/IP protocol and use UNIX, Microsoft Windows, and other commercial software packages [1]. The software that controls them is more open source than in the past. In the past these devices used proprietary software which was only known to the people familiar with that certain device. With these systems, they have begun to use common operating systems and programs that can be used on multiple types of SCADA systems. This has allowed real time control and monitoring over the internet. This convenance of having remote access has made these systems more vulnerable to IP based attacks with more security holes in the system from using more complicated software packages [1]. There

are now documented cases of these systems being probed daily looking for vulnerabilities [2]. This had been on the rise significantly with more SCADA systems being connected to networks and controlled remotely. The earlier versions of SCADA systems were not IP based in connectivity. They were hooked up on a point-to-point basis so no remote access was available. This has changed with the 3rd generation systems, and now they are involved in a complex network to have communication between the central control unit and multiple control units on a common communication bus.

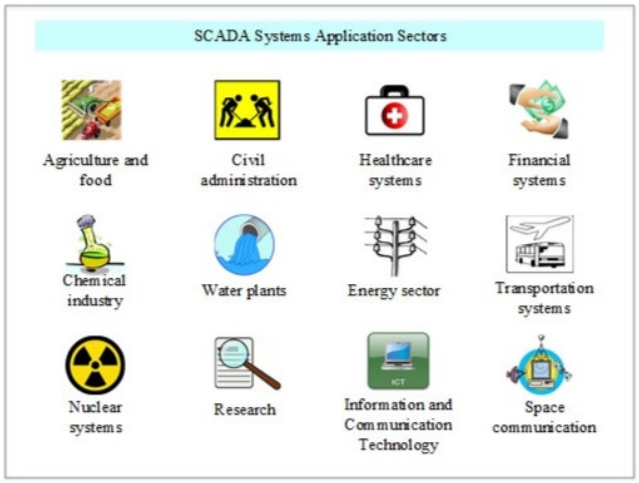

Figure 1. SCADA system application sectors

Interface and devices:

The architecture of SCADA devices is network based with a central control unit. This central control unit is the main control for the system with other devices connected to it by network cables. The devices that are connected to the main unit can vary in their function to serve different functions that need to be controlled or monitored. They are controlled over the SCADA network by either a PC or a programmable logic controller (PLC). In many locations the use of one central computer is common to control all the SCADA devices at that location [3]. The control unit does not need to be at the same location as the devices since many of these devices are controlled by the used of TCP/IP protocol. The more modern control centers us data servers called Human-Machine Interface (HMI) stations to aid in the operation of the SCADA network. This HMI is what allows the SCADA network to be hooked up to an external corporate

network for easier ese. A typical example of SCADA network is shown in Fig. 2. On a SCADA network, communications are exchanged by control messages going between the master and the devices. The master (PLC) is what controls the slave device (sensors, actuators). The PLC can also be a slave device if the SCADA network is large enough to need multiple PLC's on the SCADA network [3]. The system has other functions enabled to alert the operators of deviations in the normal use. This can include a simple alert, warnings an action to control the system if it is required. For example, this is the type of warning that was used to warn the operators of the water treatment plant in Florida. Hackers had found a way into the network that controls the SCADA system and were able to remotely control the unit. The hacker had control of the unit for 3-5 minutes, opening various functions on the screen. One of the functions that they were playing with was the control of the amount of sodium hydroxide (lye) that is added to the drinking water. The normal quantity of sodium hydroxide is 100 parts per million, the hacker raised those levels to 11,100 parts per million. They use this to control the acidity of the water and to remove metals. At the level the hacker set the controls to would have been deadly if the system had not detected the abnormal levels.

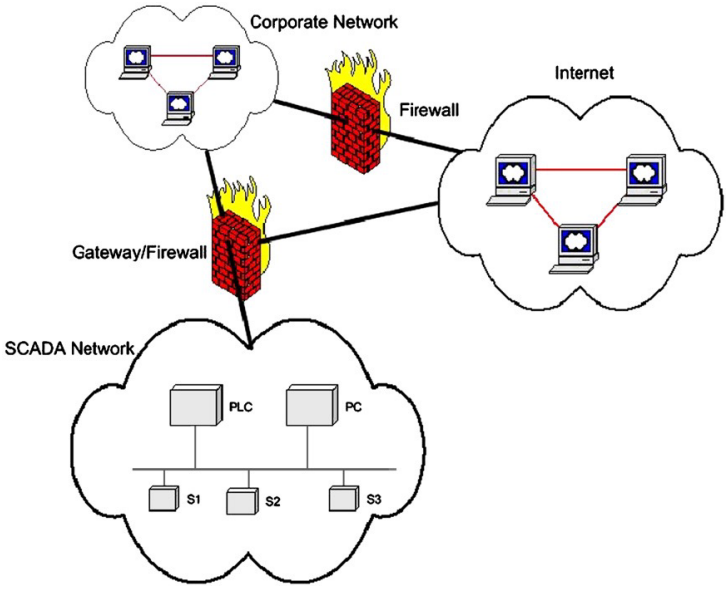

Figure 2, Typical SCADA network setup

Commercial Off the Shelf concerns:

The recent trend of SCADA networks is to use software that is proprietary. These Commercial Off the Shelf (COTS) software and hardware have reduced the cost and the time to design these systems. However, this has raised concerns in the industry with flaws in a certain system are more well known since they are more widely used. These new COTS systems use ethernet networks and a TCP/IP stack. This new way has begun to do away with the traditional master/ slave setup that older SCADA networks used [3]. Many of these new SCADA networks add an extra layer to the application layer for the SCADA messaging protocol. This is often setup in a web-based interface so the units can be controlled on the corporate networks. This is one of the problems with the newer networks since they are open to attacks from vulnerabilities in the TCP/IP stack [5].

Non-Network based attacks:

The vulnerably associated with SCADA networks is not only with the network. These networks are also vulnerable from a physical attack. SCADA networks need protection from access by unauthorized individuals. One of the most common ways is for a particular user to have a distinctive password. This can open the door for a hacker to social engineer an attack to trick an authorized user to give the hacker their password and in turn give the hacker the users credential to gain access to the system. There are new ways to avoid this, one way is using a smart card-based authentication mechanism. This will eliminate the problem with the user accidently giving the password to the hacker since there is a physical device that is required for access to the system.

Intrusion Detection Systems and Firewalls:

Firewalls are used to block unauthorized traffic from a network. These block traffic on certain ports and can also be setup to allow certain traffic on those ports to pass. They can also be setup to allow and block from certain devices and applications. These are widely used in networks and are highly configurable. SCADA networks also use these to block unauthorized traffic from gaining access to the system. The configuration can be setup to allow authorized users access to the system so they can monitor and configure the SCADA system. The National

Infrastructure Security Co- ordination Center (NISCC) has provided a good source on the configuration of external firewalls on networks that have SCADA systems. They published common guidelines on proper setup of these firewalls [7]. This report gives several recommendations to go by to ensure a secure network. They recommend a 3-zone architecture, which divide the network into 3 physical and logical zones. These three zones are the SCADA or process control network, the corporate network, and a demilitarized zone as a buffer between the other two zones. There are many benefits to using a firewall on these networks. One problem is that many of the commercially available firewalls are not capable of recognizing SCADA protocol traffic. This must be taken into consideration when selecting a firewall to secure a SCADA network.

Because traditional firewalls are not able to be used with most SCADA networks, the industry has started using micro-firewall. These smaller firewalls are directly connected to the devices. They are setup to protect critical devices on the SCADA networks. Another type of device that can be used to secure a SCADA network is an Intrusion Detection System (IDS). These are commonly used on corporate networks to monitor traffic and detect unwanted traffic. These same features can be used to protect SCADA networks with these devices. IDS's are commonly used along with firewalls when incorporated in SCADA networks. The setup is similar to a traditional network with the IDS being setup to detect abnormal behavior on the network [8].

4th Generation SCADA Cloud Based

The most current generation of SCADA, 4th generation, has taken security and accessibility to a new level. With the advancements in mobile technology and the Internet of Things (IoT) advancements, these systems are being integrated into the cloud to make them more secure and easier to use [9]. One new solution for the industrial systems is cyber physical system (CPS). This is integrated into the IoT and are considered a smart industrial system, with their most prevalent applications in smart transportation, smart grids, smart medical and eHealthcare systems, and many more. These industrial CPSs mostly utilize SCADA systems to

control and monitor their critical infrastructure (CI) [9]. Another innovation is WebSCADA, this is an application that is being used to communicate with smart medical technology.

Older SCADA systems were lacking in the proper security that these devices needed. The newer SCADA systems are integrated with complex new architectures for the new IoT, mobile wireless sensor networks, cloud computing concepts. However, there are new threats always emerging, so attention to the security of these devices must up to date.

Potential threats with 4th generation SCADA systems.

- Advanced Persistent Threats (APT)
- Unintended spillover of corporate network compromises
- Disruption of voice & data network services
- Coordinated physical & cyber-attack
- Hacktivist attacks
- Supply chain disruption or compromise
- Distributed Denial of Service (DDOS)

This transition to cloud-computing for SCADA systems has several advantages including scalability, cost efficiency, and flexibility. Even with the use of firewalls and VPN's, these are not enough to protect these systems. The current generation devices now use encryption to help secure them. Encryption methods such as Data Encryption Standards (DES), Triple DES, Advanced Encryption standards (AES), Blowfish, and others are being used. Another technique that has been proposed is the use of digital signature with the cloud-based computing for added security [10].

With the discovery of the Stuxnet attack, there is increasing attention to the threat that malware can do to modern SCADA systems. Like Stuxnet, malware can get into these systems and cause physical damage to them [11]. To counter such situations recently, there has been a trend towards the implementation of machine learning techniques for anomaly detection and prevention in the networks of the SCADA systems [12].

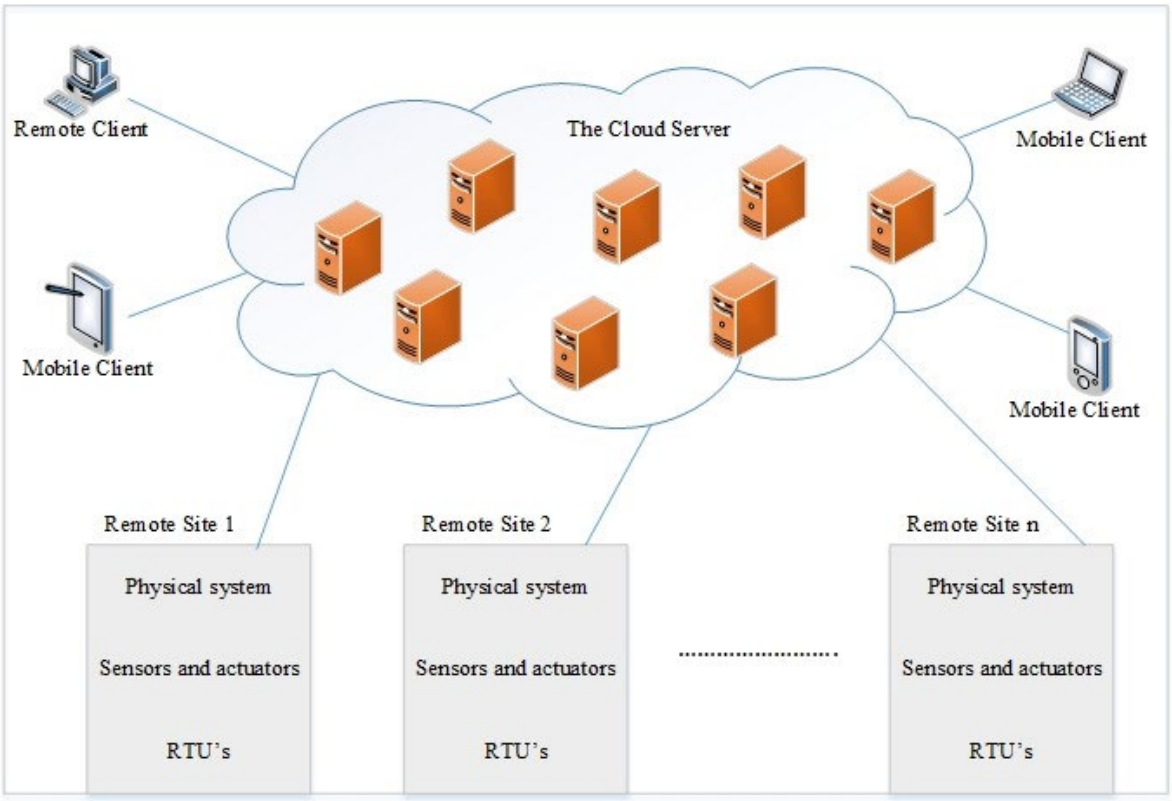

Figure 4. The general architecture of SCADA systems in an IoT-cloud environment.

There are several suggestions that the NIST has published for the proper security of these systems [13]. They have been published in the NIST SP. 800-82 r2.

Below is a short list of recommendations to secure ICS/SCADA systems: [14]

- Use virtual patching to help manage updates and patches. Patch management is critical in industrial systems where the deployment of an update could cause downtime. Virtual patching can help manage vulnerabilities and prevent cyberattacks when it is not possible to immediately apply the patches
- Implement network segmentation to prevent the spread of malware and lateral movements of the attackers once they have compromised the target network. By segmenting the network, it is possible to drastically minimize the exposure of sensitive information
- Separate the ICS network from the corporate network, using adequate security measures like firewalls to prevent the lateral movement of attacks from one to another
- Prevent the use of untrusted removable devices that could be used as attack vectors by threat actors

- Manage authorization and user accounts. Experts recommend monitoring and assessing the authorizations and accesses to SCADA systems. Monitor the creation of administrator accounts by third-party vendors
- Protect engineering workstations connected to SCADA for device programming and control adjustments with endpoint protection
- Employ strict policies to regulate how devices can connect to SCADA networks. Deploy secure remote access methods such as Virtual Private Networks (VPNs) for remote access
- Restrict the roles of transitory SCADA nodes to a single purpose. Having a single purpose for transitory nodes lowers the chances of unknowingly exposing these nodes or having them accessed by unauthorized users
- Using a web application firewall (WAF) to scan and patch vulnerable web applications
- Remove, disable, or rename any default system accounts

Conclusion:

SCADA systems are used to automate complex industrial processes where human control is difficult and to reduce the manpower required to operate them. They are used in all types of industry and have helped reduce costs and errors with the systems running off a bit of code. They have had their disadvantages when their security is taken for granted. With their wide use on critical infrastructure systems the security needs to be considered when they are being designed and not after the systems have been installed as they were in the past. The next generation of SCADA devices places security in the forefront and has fixed many network security flaws that the 3rd generation devices had.

[1] Cai, Ning & Wang, Jidong & Yu, Xinghuo. (2008). SCADA system security: Complexity, history and new developments. 569 - 574. 10.1109/INDIN.2008.4618165.

[2] PeterT.King,DanielE.Lungren,DaveG.Reichert,"SCADA Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems (Joint Hearing before the Subcommittee on Economic SECURITY, Infrastructure Protection, and Cybersecurity with the Subcomm

[3] Vinay M. Igure, Sean A. Laughter, Ronald D. Williams, Security issues in SCADA networks, Computers & Security, Volume 25, Issue 7, 2006, Pages 498-506, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2006.03.001.

[4] https://www.securitymagazine.com/articles/94552-hacker-breaks-into-florida-water-treatment-facility-changes-chemical-levels

[5] Byres EJ, Lowe J. The myths and facts behind cyber security risks for industrial control systems. In: VDE Congress, VDE Association for Electrical, Electronic & Information Technologies, Berlin; October 2004.

[6] Schwaiger C, Treytl A. Smart card based security for fieldbus systems. In: Emerging technologies and factory automation, proceedings ETFA '03. IEEE conference, 16–19 September 2003, vol. 1. p. 398–406.

[7] NISCC good practice guide on firewall deployment for SCADA and process control networks, February 2005.

[8] Pollet J. Developing a solid SCADA security strategy. In: Second ISA/IEEE sensors for industry conference, 19–21 November 2002. p. 148–56.

[9] Sajid, Anam & Abbas, Haider & Saleem, Kashif. (2016). Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. IEEE Access. 4. 1-1. 10.1109/ACCESS.2016.2549047.

[10] Rewagad, P., Pawar, Y., 2013. Use of digital signature with Diffie Hellman key ex- change and AES encryption algorithm to enhance data security in cloud computing. In: Proceedings of the International Conference on Communication Systems and Network Techno

[11] McLaughlin, S.E., 2011. On dynamic malware payloads aimed at programmable logic controllers. HotSec.

[12] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., Rajarajan, M., 2013. A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. 36, 42–57.

[13] Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, *34*, 100433.

[14] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf