SCADA Cyber Attacks and Security Vulnerabilities: Review

Jinan Fiaidhi, Yvette E. Gelogo
Department of Computer Science, Lakehead University, Hannam University, Korea
jfiaidhi@lakeheadu.ca, vette_mis@yahoo.com

Abstract: SCADA plays a vital role in critical infrastructures. As the modern IT technology become very advanced, the threat on industrial control system (ICS) and SCADA security become a big concern of every critical infrastructures operator. With the recent cyber-attacks, the urge to secure the critical infrastructure is a big issue especially for those countries that uses critical infrastructures. In this paper, we discuss the recent cyber-attacks that became threat to SCADA systems. Give some updates with the vulnerabilities and security for SCADA system. The ANSI/ISA-99 Standards was also discussed to Improve Control System Security. We also discussed different aspects that need to be considered in securing SCADA systems.

Keywords: SCADA, ICS, ANSI/ISA99, Cryptosystem

1. Introduction

The term Supervisory Control and Data Acquisition (SCADA) usually refers to centralized systems which monitor and control entire sites, or complexes of systems spread out over large areas. SCADA systems are vital components of most nations’ critical infrastructures. They control pipelines, water and transportation systems, utilities, refineries, chemical plants, and a wide variety of manufacturing operations. Most control actions are performed automatically by RTUs or by PLCs. Host control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process, but the SCADA system may allow operators to change the set points for the flow, and enable alarm conditions, such as loss of flow and high temperature, to be displayed and recorded. The feedback control loop passes through the RTU or PLC, while the SCADA system monitors the overall performance of the loop. Data acquisition begins at the RTU or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a Historian, often built on a commodity Database Management System, to allow trending and other analytical auditing. In this paper we discussed the recent cyber-attacks that threatened the industrial control system (ICS) and SCADA system. We also discussed different aspects that need to be considered in securing SCADA systems.
2. Background

The following are the SCADA System Components:

1. **Operator**: Human operator who monitors the SCADA system and performs supervisory control functions for the remote plant operations.

2. **Human machine interface (HMI)**: Presents data to the operator and provides for control inputs in a variety of formats, including graphics, schematics, windows, pull down menus, touch-screens, and so on.

3. **Master terminal unit (MTU)**: The MTU presents data to the operator through the HMI, gathers data from the distant site, and transmits control signals to the remote site. The transmission rate of data between the MTU and the remote site is relatively low and the control method is usually open loop because of possible time delays or data flow interruptions.

4. **Communications means**: Communication method between the MTU and remote controllers. Communication can be through the Internet, wireless or wired networks, or the switched public telephone network.

5. **Remote terminal unit (RTU)**: Functions as a slave in the master/slave architecture. Sends control signals to the device under control, acquires data from these devices, and transmits the data to the MTU. An RTU may be a PLC. The data rate between the RTU and controlled device is relatively high and the control method is usually closed loop. A Remote Terminal Unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition system) by transmitting telemetry data to the system and/or altering the state of connected objects based on control messages received from the system. Another term that may be used for RTU is Remote Telemetry Unit, the common usage term varies with the application area generally. An RTU monitors the field digital and analog parameters and transmits all the data to the Central Monitoring Station.

SCADA systems are primarily control systems. A typical control system consists of one or more remote terminal units (RTU) connected to a variety of sensors and actuators, and relaying information to a master station [8]. For the most part, the brains of a SCADA system are performed by the Remote Terminal Units (sometimes referred to as the RTU). The Remote Terminal Units consist of a programmable logic converter. The RTU are usually set to specific requirements, however, most RTU allow human intervention, for instance, in a factory setting, the RTU might control the setting of a conveyor belt, and the speed can be changed or overridden at any time by human intervention. In addition, any changes or errors are usually automatically logged for and/or displayed. Most often, a SCADA system will monitor and make slight changes to function optimally; SCADA systems are considered closed loop systems and run with relatively little human intervention [8]. SCADA provides management with real-time data on production, operations, implementations more efficient control paradigms, improves plant and personnel safety, and reduces costs of operation. These benefits are made possible by the use of standard hardware and
software in SCADA systems combined with improved communication protocols and increased connectivity to outside networks, including the Internet. [10]. Modern SCADA architectures rely heavily on standard protocols and digital data transmission.

3. Units

Recently, there listed cyber-attacks that have been an issue to SCADA systems. The discovery of the Flame malware focused the cyber security world on the sophisticated strikes targeting energy companies in the Middle East. Although Flame’s goal was espionage rather than damaging operations as Stuxnet did, it has been seen as one more indication that the industrial world is now in the bull’s eye of clever attackers [11].

3.1 Stuxnet

The Stuxnet malware worm has been called an incident “that marks a new age of cyber warfare”. Stuxnet Central provides a hub for the information that Byres Security has created regarding Stuxnet, along with links to key industry material [1]. Stuxnet is an advanced malware worm that was discovered in July 2010 and that has attacked Siemens PCS7, S7 PLC and WinCC systems around the world. It has infected at least 22 manufacturing sites, and it appears to have impacted its possible target - Iran’s nuclear enrichment program [2]. Using human vectors, local area network communications or infected project files, Stuxnet reached its PLC targets. The business practices of today, which involve using remote contractors and support staff, links between the enterprise network and the control networks, and removable media for updates or support, all provide multiple pathways for infection. Even a simple PDF file could be a pathway into your control system [2]. A key to protecting your ICS from a potential “Son-of-Stuxnet” is to examine all possible infection pathways, not just a single pathway such as a USB key. Develop strategies for discovering, documenting and mitigating ALL transfer of electronic information, regardless of the technology or form of the transfer [2].

2.2 Flame

Flame appears to be a carefully crafted attack toolkit for industrial or political espionage [5]. Flame shares many characteristics with notorious cyber weapons Duqu and Stuxnet: while its features are different, the geography and careful targeting of attacks coupled with the usage of specific software vulnerabilities seems to put it alongside those familiar ‘super-weapons’ currently deployed in the Middle East by unknown perpetrators. Flame can easily be described as one of the most complex threats ever discovered. It’s big and incredibly sophisticated. It pretty much redefines the notion of cyberwar and cyberespionage [6].

Currently there are three known classes of players who develop malware and spyware: hacktivists, cybercriminals and nation states. Flame is not designed to steal money from bank accounts. It is also different from rather simple hack tools and malware used by the hacktivists. So by excluding cybercriminals and hacktivists, we
come to conclusion that it most likely belongs to the third group. In addition, the geography of the targets (certain states are in the Middle East) and also the complexity of the threat leaves no doubt about it being a nation state that sponsored the research that went into it [6].

From the initial analysis, it looks like the creators of Flame are simply looking for any kind of intelligence - e-mails, documents, messages, discussions inside sensitive locations, pretty much everything. We have not seen any specific signs indicating a particular target such as the energy industry - making us believe it’s a complete attack toolkit designed for general cyber-espionage purposes [5][6].

Of course, like we have seen in the past, such highly flexible malware can be used to deploy specific attack modules, which can target SCADA devices, ICS, critical infrastructure and so on [5][6].

![Fig.1. Flame Infection Methods. Source:Securelist.com, Tofino.com](image)

As illustrated in Figure 1, like Stuxnet, it has multiple propagation vectors – USB keys, printer sharing, and domain controller rights to name a few.

An analysis of the data from 1982 to 2010 found that the type of incidents affecting control systems breaks down as follows [2]:

- 50% of incidents were accidental in nature
- 30% of incidents were due to malware
- 11% of incidents were due to external attackers
- 9% of incidents were due to internal attackers

4. Using ANSI/ISA-99 Standards to Improve Control System Security

205
Security experts generally agree that the most effective way to prevent the rapid spreading is to make use of zone based defenses as described in the ANSI/ISA-99.02.01 and IEC-62443 standards. The concept is to break up the network into security zones. Between the zones, industrial firewalls are installed with rules that block the protocols that Stuxnet uses for infection and communications. This way, if a Stuxnet infection does accidentally occur, it is limited to a small number of machines in a single zone [12].

ANSI/ISA-99 is a complete security life-cycle program for industrial automation and control systems. It consists of 11 standards and technical reports on the subject, a number of which have been publicly released as American National Standards Institute (ANSI) documents. Work products from the ISA99 committee are also submitted to International Electrotechnical Commission (IEC) as standards and specifications in the IEC 62443 series [3]. ANSI/ISA-99 introduces the concepts of “zones” and “conduits” as a way to segment and isolate the various sub-systems in a control system. A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. Equipment in a zone has a security level capability. If that capability level is not equal to or higher than the requirement level, then extra security measures, such as implementing additional technology or policies, must be taken [3].

5. Choosing the Right Security Approach

There have been a lot of proposed security approaches for SCADA system. Every security provider uses different kinds of security strategies. The question now is how to choose the right security mechanism?

In order to improve the SCADA system security, the following aspect must be considered:

**Authentication:**
Authentication is the process of verifying a user or other entity’s identity. This is typically done to permit someone or something to perform a task. There is variety of authentication system, some are stronger than others. A strong authentication system ensures that the authenticators and messages of the actual authentication protocol are not exchanged in a manner that makes them vulnerable to being hijacked by an intermediate malicious node or person. That is, the information used to generate a proof of identity should not be exposed to anyone other than the person or machine it is intended for.

**Authorization:**
Authorization is when the system decides whether or not a certain entity be allowed to perform a requested task. This decision is made after authenticating the identity in question. When considering an authentication system for a particular application, it is crucial to understand the type of identifier required to provide a certain level of authorization.

**Confidentiality:**
Confidentiality is needed when the message sent contains sensitive material that should not be read by others and therefore must not be sent in a comprehensible format. A loss of confidentiality is the unauthorized disclosure of information.
Confidentiality, as it relates to security and encryption techniques can be obtained by encrypting messages such that only intended recipient are able to read them.

**Integrity:**

Integrity is ensuring that the data presented are true and valid master source of the data and includes guarding against improper information modification or destruction to ensure information non-repudiation and authenticity. A loss of integrity is the unauthorized modification, insertion, or destruction of information.

One way of ensuring of data integrity is by using simple checksums which prevent an attacker from forging or replaying messages. Checksum is usually implemented when the channel between communication parties is not secure and ensure that the data has reached its destination with all bits intact, if bits have been modified, that the modification will not go unobserved.

**Non-Repudiation:**

Non-repudiation is ensuring that a traceable legal record is kept and has not been changed by a malicious entity. A loss on non-repudiation would result in the questioning of the transaction that has occurred. A simple example of non-repudiation is signing a contract. The signer cannot claim they did not agree a contract because there is an evidence that they did agree. The difference is that a signature can be forger but good encryption cannot.

By considering the above aspects, we can now easily figure out the things that we need to consider.

**6 Conclusion and Future Works**

Cyber-attacks are now becoming a big threat in internet world. Being connected to internet, SCADA systems are vulnerable for cyber-attacks. The recent cyber-attacks urge to deploy more secure critical infrastructures. Using ANSI/ISA-99 standard to improved control system security is now being pursued by many security providers. We also discussed different aspects that we need to consider in designing a more secure SCADA system. Our future works is to study different an appropriate security mechanism for every “zones and conduits “described in ANSI/ISA-99 standards. Study an appropriate cryptosystems and other physical protection for network system.

**References**