International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 1, Mar-Apr 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Protection Trends in Scada Cyber Threats

Anusha H S[1], Amulya C T[2], Annapoorneshwari M R[3], Monisha Krishna D S[4], Mohammed Elahi[5]

[1, 2, 3, &4]Students, Dept of ECE, Ghousia College of Engineering, Ramanagaram, Karnataka

[5]Asst. Professor, Dept. of ECE, Ghousia College of Engineering, Ramanagaram, Karnataka

Abstract:

The answer to the existing threat issues in SCADA is that these types of threats are becoming more likely, as current SCADA systems and networks increasingly utilize commercially off-the-shelf (COTS) software, connect to the enterprise layer and move toward IP connectivity. These recent changes have contributed to higher threat levels and increased vulnerability. A few short years ago, the chances of someone finding these vulnerabilities and exploiting them were very slim. This was due to the fact that process control systems and SCADA networks were unheard of by the general population and systems were based on specialized platforms that were segregated from the enterprise layer. In recent years, industrial systems have begun to take a front seat in the spot light, due to the focus by the Department of Homeland Security on national critical infrastructure and some unfortunate media coverage. Despite current efforts, there is a high probability that something bad is eventually going to happen. In addition, the number of "SCADA hacking" presentations is increasing at security and "hacker" conventions, with the number of vulnerabilities discovered within these systems increasing. Bottom line, our little corner of industry is no longer isolated and the word is now out. While cyber security is being given the lion's share of attention, with "hackers" already attracting premature blame from a few recently publicized incidents, the widespread disregard for physical and operational security within many organizations has become a huge concern. Many companies are heavily focused on shoring up their cyber security, with little or no regard for physical security.

Index Term: Commercially off the shelf (COTS), SCADA hacking

I. INTRODUCTION

SCADA stands for *Supervisory Control And Data Acquisition*. It generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility based as described below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, and large communication systems.
- Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control HVAC, access, and energy consumption.

SCADA systems are used to control and monitor physical processes, examples of which are transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights, and other systems used as the basis of modern society. The security of these SCADA systems is important because compromise or destruction of these systems would impact multiple areas of society far removed from the original

 ©IJSRED: All Rights are Reserved

compromise. For example, a blackout caused by a compromised electrical SCADA system would cause financial losses to all the customers that received electricity from that source. How security will affect legacy SCADA and new deployments remains to be seen.

Many vendors of SCADA and control products have begun to address these risks by developing lines of specialized industrial firewall and VPN solutions for TCP/IP-based SCADA networks. Additionally, application white listing solutions are being implemented because of their ability to prevent malware and unauthorized application changes without the performance impacts of traditional antivirus scans. Also, the ISA Security Compliance Institute (ISCI) is emerging to formalize SCADA security testing starting as soon as 2009. ISCI is conceptually similar to private testing and certification that has been performed by vendors since 2007. The increased interest in SCADA vulnerabilities has resulted in vulnerability researchers discovering vulnerabilities in commercial SCADA software and more general offensive SCADA techniques presented to the general security community.

II. PROBLEM STATEMENT

The move from proprietary technologies to more standardized and open solutions together with the increased number of connections between SCADA systems and office networks and the Internet has made them more vulnerable to attacks. Consequently, the security of SCADA-based systems has come into question as they are increasingly seen as extremely vulnerable to cyberwarfare/cyberterrorism attacks.

In particular, security researchers are concerned about:

- The lack of concern about security and authentication in the design, deployment and operation of existing SCADA networks.
- The mistaken belief that SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces.
- The mistaken belief that SCADA networks are secure because they are purportedly physically secured.
- The mistaken belief that SCADA networks are secure because they are supposedly disconnected from the Internet.

III. METODOLOGY

1. Systems concepts

The term SCADA usually refers to centralized systems which monitor and control entire sites, or complexes of systems spread out over large areas (anything between an industrial plant and a country). Most control actions are performed automatically by remote terminal units ("RTUs") or by programmable logic controllers ("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.

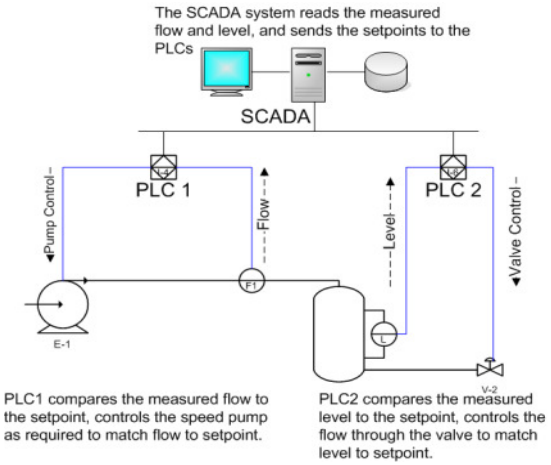

Fig. Basic SCADA System

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.

 ©IJSRED: All Rights are Reserved

SCADA systems typically implement a distributed database, commonly referred to as a *tag database*, which contains data elements called *tags* or *points*. A point represents a single input or output value monitored or controlled by the system. Points can be either "hard" or "soft". A hard point represents an actual input or output within the system, while a soft point results from logic and math operations applied to other points. (Most implementations conceptually remove the distinction by making every property a "soft" point expression, which may, in the simplest case, equal a single hard point.) Points are normally stored as value-timestamp pairs: a value, and the timestamp when it was recorded or calculated. A series of value-timestamp pairs gives the history of that point. It's also common to store additional metadata with tags, such as the path to a field device or PLC register, design time comments, and alarm information.

A SCADA System usually consists of the following subsystems:

- A Human-Machine Interface or HMI is the apparatus which presents process data to a human operator, and through this, the human operator, monitors and controls the process.
- A supervisory (computer) system, gathering (acquiring) data on the process and sending commands (control) to the process.
- Remote Terminal Units (RTUs) connecting to sensors in the process, converting sensor signals to digital data and sending digital data to the supervisory system.
- Programmable Logic Controller (PLCs) used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
- Communication infrastructure connecting the supervisory system to the Remote Terminal Units.

2. Human Machine Interface

A Human-Machine Interface or HMI is the apparatus which presents process data to a human operator, and through which the human operator controls the process.

The HMI system usually presents the information to the operating personnel graphically, in the form of a mimic diagram. This means that the operator can see a schematic representation of the plant being controlled. For example, a picture of a pump connected to a pipe can show the operator that the pump is running and how much fluid it is pumping through the pipe at the moment. The operator can then switch the pump off. The HMI software will show the flow rate of the fluid in the pipe decrease in real time. Mimic diagrams may consist of line graphics and schematic symbols to represent process elements, or may consist of digital photographs of the process equipment overlain with animated symbols.

An important part of most SCADA implementations are alarms. An alarm is a digital status point that has either the value NORMAL or ALARM. Alarms can be created in such a way that when their requirements are met, they are activated. An example of an alarm is the "fuel tank empty" light in a car. The SCADA operator's attention is drawn to the part of the system requiring attention by the alarm. Emails and text messages are often sent along with an alarm activation alerting managers along with the SCADA operator.

3. Hardware solutions

SCADA solutions often have Distributed Control System (DCS) components. Use of "smart" RTUs or PLCs, which are capable of autonomously executing simple logic processes without involving the master computer, is increasing. A functional block programming language, IEC 61131-3 (Ladder Logic), is frequently used to create programs which run on these RTUs and PLCs. Unlike a procedural language such as the C programming language or FORTRAN, IEC 61131-3 has minimal training requirements by virtue of resembling historic physical control arrays. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC. Since about 1998, virtually all major PLC manufacturers have offered integrated HMI/SCADA systems, many of them using open and non-proprietary communications protocols.

 ©IJSRED: All Rights are Reserved

4. Remote Terminal Unit (RTU)

The RTU connects to physical equipment. Typically, an RTU converts the electrical signals from the equipment to digital values such as the open/closed status from a switch or a valve, or measurements such as pressure, flow, voltage or current. By converting and sending these electrical signals out to equipment the RTU can control equipment, such as opening or closing a switch or a valve, or setting the speed of a pump.

IV. DISTRIBUTED CONTROL SYSTEM

A **distributed control system** (DCS) refers to a control system usually of a manufacturing system, process or any kind of dynamic system, in which the controller elements are not central in location (like the brain) but are distributed throughout the system with each component sub-system controlled by one or more controllers. The entire system of controllers is connected by networks for communication and monitoring.

DCS is a very broad term used in a variety of industries, to monitor and control distributed equipment.

- Chemical plants
- Pharmaceutical manufacturing
- Sensor networks
- Dry cargo and bulk oil carrier ships
- Electrical power grids and electrical generation plants
- Environmental control systems
- Traffic signals
- Water management systems
- Oil refining plants

The preceding discussion does not constitute a formal threat assessment. It merely presents a listing of trends affecting CS development and a number of factors requiring monitoring and research. On the other hand, this discussion does project that the operational environment in 2010-2015 will likely see an increase in Capability and Opportunity available to threat sources. Coupled with the broader presence and exposure of control systems, this suggests the future operational environment will be bothmore congested and more vulnerable. Should a threat actor emerge that has the Intent the equation Threat = Capability + Intent+ Opportunity will be complete.

V.CONCLUSION

REFERENCES

1. SONG X P, LIAO M F.design of internet based scada System frame for wind power plant[J]. automation of electric power system 2006.

2. CHONG C Y, KUMAR S P.sensor networks: Proceedings of the IEEE,2003.

3. C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA Cyber Security Testbed Development", Power Symposium, 2006. NAPS 2006.

4. Ronald L. Krutz,Securing SCADA systems,Willey,2006.

5. Josh Siegle, Motorola Solutions. "Cyber Security for SCADA and ICS Systems", in Entelec Fall eminar Series, 2014.

6. T. Paukatong,SCADA Security: A New Concerning Issue of an In-house EGAT-SCADA 2005 IEEE/PES Transmission and Distribution Conference & Exhibition:Asia and Pacific Dalian,China.

7. American Petroleum Institute, API 1164:SCADA Security, Washington,DC,2004.

8. D. Kilman and J. Stamp, Framework for SCADA security policy, Technical Repot SAND2005-1002C, Sandia National Laboratories, Albuquerque, New Mexico, 2005.

9. K. Stouffer, J. Falco and K. Kent, Guide to Supervisory Control and Industrial Control Systems Security-Initial Public Draft, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

10. Pollet J. Developing a solid SCADA security strategy. In: Second ISA/IEEE sensors for industry conference, 19-21 November 2002.

 ©IJSRED: All Rights are Reserved