Issue 1 vol 4 ISSN: 2321-8134

IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

SCADA SYSTEMS-THREATS And ANALYSIS

Pallavi S. Sabal[1], Ashish S. Chopade[2], Digambar S. Dayma[3,] Dhiraj D. Shirbhate[4]

[1]*Computer Science and Engineering, J.D.I.E.T.,Maharashtra,India,**sabalpallavi1@gmail.com***
[2]*Computer Science and Engineering, J.D.I.E.T.,Maharashtra,India,**ashishchopade18@gmail.com***
[3]*Computer Science and Engineering, J.D.I.E.T.,Maharashtra,India,**daymadigambar@gmail.com***
[4]*Asst. Professor, Computer Science and Engineering,J.D.I.E.T.,Maharashtra,India,**shirbhate.dhiraj@gmail.com***

Abstract

SCADA stands for Supervisory Control and Data Acquisition, which is a communication technology scheme for collecting data from distant facilities and also controlling them on control systems. SCADA enables operating the facilities without assigning operators to remote locations. As the information and technology is evolving the SCADA is being applied to wide scale industries for their ease.Starting from the locally independent network system to being connected to communication infrastructure,SCADA system expanded.In this era of Internet,where all different kinds of communication networks have been being integrated into the Internet for both technological and economic efficiencies,The major problem that is arising is cyber attacks on the SCADA systems.Since many of the large scale industries are dependent on SCADA for their remote access,it is very critical to prevent SCADA systems from various kinds of Cyber Threats, therefore it should be considered to take countermeasures against the threats.

Index Terms: *SCADA, wide-area control system, cyber security, vulnerabilities, encryption, security device.*

---------- *** ----------

1. INTRODUCTION

SCADA stands for Supervisory Control And Data Acquisition. SCADA refers to a system that collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data.SCADA focuses on gathering and circulating the right amount of system information to the right person or computer within the right amount of time so that creative solutions are made possible. SCADA system mainly focuses on the gathering and circulating information from the sensors in the industries to the right person.

SCADA systems enable the operator to open and close valves, switches and to make set point changes from remote locations. This facility of SCADA makes it useful in the oil or gas field, Industries using pipelines and hydroelectric generating complex. SCADA started as local to site to control the system however it has extended towide-area for supervisory control and monitor as the information technology evolves, which requires the interconnection between systems and networks both on economic and technological aspects.

2. COMPONENTS OF SCADA

2.1 SCADA HMI

SCADA system has a user interface which is usually called Human Machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by a human operator. HMI gives the power to an individual to control the interface with the SCADA System. HMI's are an easy way to standardize the facilitation of monitoring multiple RTU's or PLC's.[1]

2.2 Remote Terminal Unit (RTU)

The RTU is used to connect the physical equipments. Typically, an RTU converts the electrical signals from the equipment to digital values. The examples can be open/closed status from a switch or a valve, or for 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 orclosing a switch or a valve, or setting the speed of a pump.

2.3 SCADA Software

SCADA software is usually related to the SCADA system's databases and Human Machine Interface, for providing trending, diagnostic data, and management information. This information includes scheduled maintenance procedures, logistic information, detailed schematics for a particular sensor or machine, and expert-system troubleshooting guides. SCADA software is mainly divided

into two types-open type or proprietary type. The main problem faced by these systems is overwhelming reliance on the supplier of the system.

2.4 SCADA Hardware

Distributed Control System components are mainly included in SCADA. The main hardware components are IEDs, RTUs or PLCs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. The hardware parts play a vital role in the SCADA system.

2.5 Supervisory Station

Supervisory Station includes the servers and software responsible for communicating with the field equipment such as RTUs, PLCsand then to the HMI software running on workstations in the control room, or somewhere else. In smaller SCADA systems, the master station may include a single PC. But in larger SCADA systems, the master station may expand to multiple servers, distributed software applications, and disaster recovery sites. To increase the integrity of the system the multiple servers will often be configured in a dual redundant or hot-standby formation providing continuous control and monitoring in the event of a server failure.[1]

2.6 Threats to SCADA system

The most famous threats now-a-days are the threats posed by terroristic groups and hostile nation states. These are organized groups with a clear goal and some level of sophistication. There is also some of the threat posed by a company's own employees. Employees of the companies have access to internal controls and data, and either by accident or malicious intent can cause equipment outages. A third category of threat is the threat posed by casual hackers, known as "script kiddies". When considering the closed characteristics of SCADA system in electric power industry compared to others, the threats of insiders i.e. employees of the company and of hackers are comparatively probable threats. But the SCADA systems connected to the Internet in the States already have had experiences of being threatened by script kiddies.[2]

"Threat" is commonly, although not consistently, defined as: Threat = Capability + Intent + Opportunity. From the analytic perspective, the definition assumes the existence of a threat "source" – an actor or agent posing the threat. For many reasons, the vulnerability assessment process is developing at a faster pace than the threat assessment process due to some serious issues. While vulnerability assessment helps in estimate the capability factor in the threat equation, satisfactory assessment of Intent and Opportunity is more difficult .Because of these difficulties it is very important and necessary to define and classify the possible threats and vulnerabilities for building security countermeasures for protecting the SCADA system from them for safe SCADA Systems.[3]

There are three categories related to the cyber security- Attack that is upon the power system, Attacks that are caused by the system, Attacks that are occurred through the system. In the First attack, the primary target is Electricity infrastructure. The point of attack can be simply a Transmission tower. Since the power systems are highly vulnerable, the countermeasures should be made to prevent these systems from these attacks. In the second attack, the ultimate target is the population using parts of the electricity infrastructure as a weapon. In the third attack, the target is civil infrastructure.

2.7 Common RT Computer Threats

The common threats to the SCADA systems can be illustrated by the following table.

Table-2.1: Common RT Computer Threats

1.Authorization Violation	9.Information leakage	17.Sabotage	25.Traffic Analysis
2.Bombs (Logic or Time)	10.Intercept/ Alter	18.Scavenging	26.Trap Door/ Back Door
3.Browsing	11.Interference Database Query Analysis	19.Spying	27.Trojan Horse
4.Bypassing Controls	12.Masquerade	20.Service Spoofing	28.Tunneling
5.Data Modifications	13.Physical Intrusion	21.Sniffers	29.Unauthorized Access Violations of Permission
6.Denial of Service	14.Replay	22.Substitution	30.Unauthorized Access Piggybacking
7.Eavesdropping	15.Repudiation	23.Terrorism	31.Virus
8.Illegitimate Use	16.Resource Exhaustion	24.Theft	32.Worm

The treats elaborated in table 1 could be mapped into Fig.1

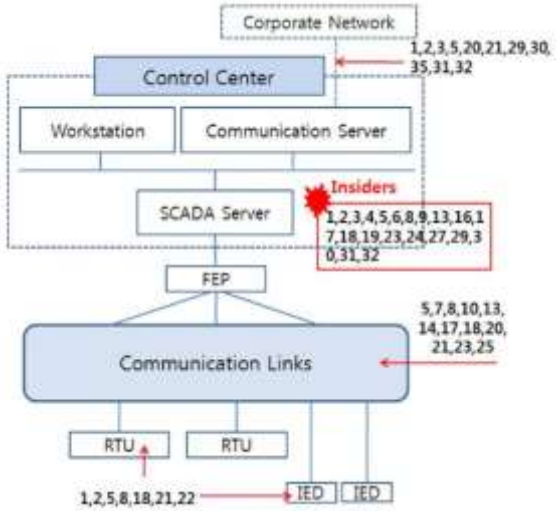

Fig-2.1:Attack types mapped into SCADA

3. CONCLUSION

Vulnerability assessment is a critical task to ensure that power infrastructure cyber security is systematically evaluated. The proposed analytical framework provides a measure to quantify the system vulnerability. SCADA system is a kind of new changeable having started to be connected into the internet according to the network integration. It is strongly related to our daily life, therefore the normal operation of the system is very critical and that is the reason why the system should be strongly secured. The recent movie "Diehard4.0" also dealt with the cyber security issues on SCADA systems and its impacts when it fails by hostile hackers' attack. However, the study is still in the beginning stage although people started to pay attention to the issue. There are several reasons for the slow progress on the study.

ACKNOWLEDGEMENT

We are indebted to our proactive **guide Prof. D. D. Shirbhate**, Professor and HOD of CSE department because without his valuable guidance this work would not have a success. His constructive, useful, timely suggestions and encouragement in every stem immensely helped us to carry out my paper work. His invaluable presence was a great boost for us in achieving our goal.

REFERENCES

[1]. Dong-Joo Kang; Jong-Joo Lee; Seog-Joo Kim, Jong-Hyuk Park," Analysis on Cyber Threats to SCADA systems" IEEE T&D Asia 2009.

[2].Rosslin John Robles; Min-kyu Choi," Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems" International Journal of of Grid and Distributed Computing Vol.2, No.2, June 2009

[3].Chee-Wooi Ten; Chen-Ching Liu; GovindarasuManimaran,"Vulnerability Assessment of Cybersecurity for SCADA Systems" IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 23, NO. 4, NOVEMBER 2008