International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

SCADA for National Critical Infrastructures: Review of the Security Threats, Vulnerabilities and Countermeasures

Fidelis Chukwujekwu Obodoeze
Department of Computer Engineering Technology,
Akanu Ibiam Federal Polytechnic, Unwana,
Ebonyi State, Nigeria

Ifeyinwa Nkemdilim Obiokafor
Department of Computer Science Technology,
Anambra State Polytechnic, Mgbakwu,
Anambra State, Nigeria

Tochukwu Chijindu Asogwa
Department of Computer Engineering Enugu State University of
Science and Technology (ESUT), Enugu, Nigeria

ABSTRACT

The Supervisory Control And Data Acquisition (SCADA) networks contain computers and applications that perform key functions in providing essential services and commodities to citizens such as electricity, natural gas, crude oil and refined petroleum products, waste-water treatment and transportation. This paper looks at SCADA, its architecture and functions to industrial control system (ICS) as well its security threats, vulnerabilities and attacks that could prevent SCADA from delivering these functions especially in Nigeria. This paper finally recommended far-reaching holistic solutions to the various SCADA's security challenges.

Keywords : *SCADA, RTU, threats, ICS, vulnerabilities, attack, control, HMI, PLC, sensors, instruments, telemetry, PLC, plant, Nigeria.*

1.0 Introduction

Supervisory control and data acquisition (SCADA) networks contain computers and applications that perform key functions in providing essential services and commodities (e.g., electricity, natural gas, crude oil, refined petroleum products such as gasoline, gas oil, water, waste. treatment, transportation) to citizens of a country. SCADA is a type of control system that is used to manage and control network of computers and applications that perform these essential services. SCADA is data-gathering oriented. SCADA systems are used to monitor or to control chemical, physical or transport processes.

SCADA performs about four functions [1]. They include - data acquisition, networked data communication, data presentation and control.

These four functions are performed by several kinds of SCADA components such as 1.) sensors (either digital or analog) and control relays. These directly interface with the managed system ; 2.) remote telemetry units (RTUs) are small-computerized units deployed in the field at single sites and locations. RTUs serve as local collection points for gathering reports from sensors and delivering commands to control relays. 3.) SCADA master units are larger computer consoles that serve as the central processor for the SCADA system. Master units provide a human interface to the system and automatically regulate the managed system in response to sensor inputs. 4.) The communications network connects the SCADA master unit to the RTUs in the field monitor at your remote sites.

In Nigeria, SCADA is used majorly in power (electricity) and oil and gas industry to control and manage distribution of power (electricity) and petroleum products respectively across the nooks and crannies of the country. Attacking SCADA or its sub-systems can cause adverse effects to a nation's economy and security. Already, Nigeria has had her own share of both physical and SCADA attacks targeting oil and gas industry in recent times. SCADA and its sub-systems can be monitored and attacked by criminal-minded individuals or even terrorists. Cyber criminals often "infect" systems and silently monitor traffic, observe activity, and wait for months or even years before taking any action. This allows them to strike when they can cause the most damage.

In recent years, numerous forms of malware targeting SCADA systems have been identified, including Stuxnet, Havex, and BlackEnergy3 [2]. What these three forms of malware have in common is their ability to sneak through Industrial Control Systems (ICS) undetected by exploiting the weakest link in the cyber defense network (people) and posing as a legitimate e-mail or by finding a back door in the SCADA system. The power sector has already demonstrated itself to be particularly vulnerable and must dedicate substantially more resources to closing back doors and training employees to avoid clicking on malicious files.

While the majority of the equipment that comprises a SCADA system resides in the control center network behind firewalls, localized SCADA communication equipment directly connected to the ICS can be as vulnerable as the ICS themselves. A digital attack or intrusion on these localized communication systems can have a greater effect on the overall system and allow the attacker access to all ICS connected to them. This gives the attacker the ability to operate all ICS, creating broader systemic impact.

Understanding common SCADA system threats and vulnerabilities allow us to develop a clear, actionable framework for overcoming these security issues.

1.1 Objectives of the research

1. To investigate the security architecture, threats, attacks and vulnerabilities of SCADA systems and

2. To proffer solutions on how these security threats, attacks and vulnerabilities of SCADA system can be mitigated, overcome and prevented in order to protect critical national infrastructure from abuse, sabotage and attack of hackers and malwares.

1.2 Research Questions

To be able to do justice to the stated research objectives in section 1.1, there is need to answer the following research questions concerning SCADA, its architecture and its vulnerabilities.

1. *What is SCADA and its architecture?*
2. *What are the functions of SCADA?*
3. *What are the security holes or flaws or vulnerabilities in SCADA?*
4. *What are the attack types of SCADA?*
5. *What are the measures that can be taken to prevent or protect SCADA and its sub- systems from attacks?*

1.3 SCADA Basics [3]

The block diagram of SCADA system as shown in Fig.1 consists of different blocks, namely Human-machine Interface (HMI), Supervisory system, Remote terminal units (RTUs), PLCs, Communication infrastructure and SCADA Programming [3].

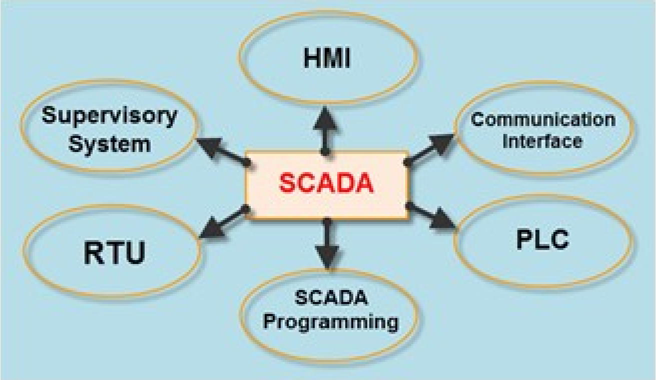

Fig 1: *Basics of SCADA [3].*

1. Human-machine Interface (HMI)

It is an input-output device that presents the process data to be controlled by a human operator. It is used by linking to the SCADA system's software programs and databases for providing the management information, including the scheduled maintenance procedures, detailed schematics, logistic information, trending and diagnostic data for a specific sensor or machine. HMI systems facilitate the operating personnel to see the information graphically. Fig.2 depicts HMI.

Fig 2: *Human-Machine Interface (HMI)[3].*

2. Supervisory System

Supervisory system is used as server for communicating between the equipment of the SCADA system such as RTUs, PLCs and sensors, etc., and the HMI software used in the control room workstations. Master station or supervisory station comprises a single PC in smaller SCADA systems and, in case of larger SCADA systems, supervisory system comprises distributed software applications, disaster recovery sites and multiple servers. These multiple servers are configured in a hot-standby formation or dual-redundant, which continuously controls and monitors in case of a server failure for increasing the integrity of the system.

3. Remote Terminal Units

Physical objects in the SCADA systems are interfaced with the microprocessor controlled electronic devices called as Remote Terminal Units (RTUs). These units are used to transmit telemetry data to the supervisory system and receive the messages from the master system for controlling the connected objects. Hence, these are also called as Remote Telemetry Units.

4. Programmable Logic Controllers

In SCADA systems, PLCs, as depicted in Fig.3, are connected to the sensors for collecting the sensor output signals in order to convert the sensor signals into digital data. PLCs are used instead of RTUs because of the advantages of PLCs like flexibility, configuration, versatile and affordability compared to RTUs.

Fig 3: *Programmable Logic Controllers [3].*

5. Communication Infrastructure

Generally the combination of radio and direct wired connections is used for SCADA systems, but in case of large systems like power stations and railways SONET/SDH are frequently used. Among the very compact SCADA protocols used in SCADA systems – a few communication protocols, which are standardized and recognized by SCADA vendors – send information only when the supervisory station polls the RTUs.

6. SCADA Programming

SCADA programming in a master or HMI is used for creating maps and diagrams which will give important situational information in case of an event failure or process failure. Standard interfaces are used for programming most commercial SCADA systems. SCADA programming can be done using derived programming language or C language.

1.4 Architecture OF SCADA

Generally the SCADA system architecture includes the following major components:

1. Local processors. These communicate with the site's instruments and operating equipment such as the Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED) and Process Automation Controller (PAC).
2. Operating equipments such as pumps, valves, switches, conveyors and substation breakers that can be controlled by energizing actuators or relays,

3. Programmable Logic Controller (PLCs),
4. Sensors, detectors or Instruments in the field or in a facility that sense conditions such as pH, temperature, pressure, power level, flow rate, presence or motion, etc.
5. Remote Terminal Unit (RTU),
6. Intelligent Electronic Device (IED),
7. Short range communications backbones between the local processors and the instruments and operating equipment. These relatively short cables or wireless connections carry analog and discrete signals using electrical characteristics such as voltage and current, or using other established industrial communications protocols.
8. Master Terminal Unit or Host computers and a PC with human machine interface (HMI). Host computers that act as the central point of monitoring and control. The host computer is where a human operator can supervise the process; receive alarms, review data and exercise control.

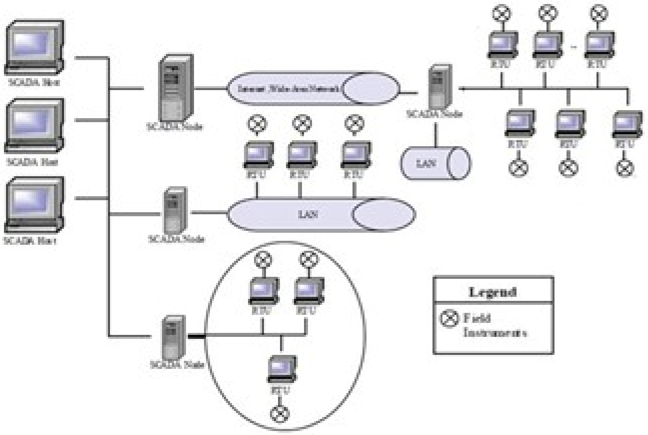

Fig 4:*. Architecture of SCADA [3]*

The block diagram of SCADA system as shown in Fig.4 represents the basic SCADA architecture. The SCADA (supervisory control and data acquisition) systems are different from distributed control systems that are commonly found in plant sites. When distributed control systems cover the plant site, SCADA system cover much larger geographic areas.

Fig.4 depicts an integrated SCADA architecture which supports TCP/IP, UDP and other IP based communication protocols as well as industrial protocols like Modbus TCP, Modbus over TCP or Modbus over UDP. These all work over cellular, private radio or satellite networks.

In complex SCADA architectures, there are a variety of wired and wireless media & protocols involved in getting data back to the monitoring site. This allows implementation of powerful IP based SCADA networks over landline, mixed cellular and satellite systems. SCADA communications can utilize a diverse range of wired and wireless media.

The choice of the existing communication depends on the characterization of a number of factors. The factors are remoteness, available communications at the remote sites, existing communications infrastructure, polling frequency and data rates. These factors impact the final decision for SCADA architecture. Therefore, a review of SCADA systems evolution allows us to better understand many security concerns.

Figs.5 and 6 depicts typical examples of SCADA applications in real-time environmental and industrial monitoring and control. Fig.5 depicts a SCADA system monitoring the environment using a temperature sensor, which sends the data via an RTU which forwards the data to the SCADA Server at the Control Room. SCADA now controls industrial plant using the data it obtains from the RTU and sensor. Fig.6 shows how SCADA can use readings from flow and liquid level sensors together with two PLCs to control the pump and valve using preset setpoints.

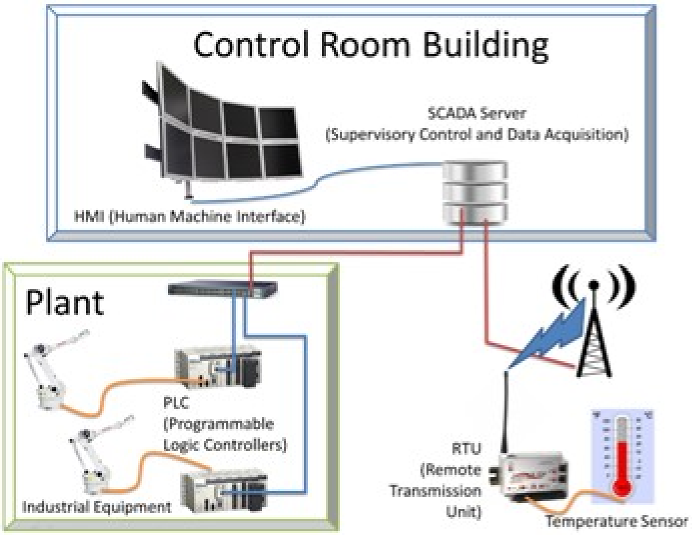

Fig 5: *Typical example of SCADA monitoring temperature of the environment [3].*

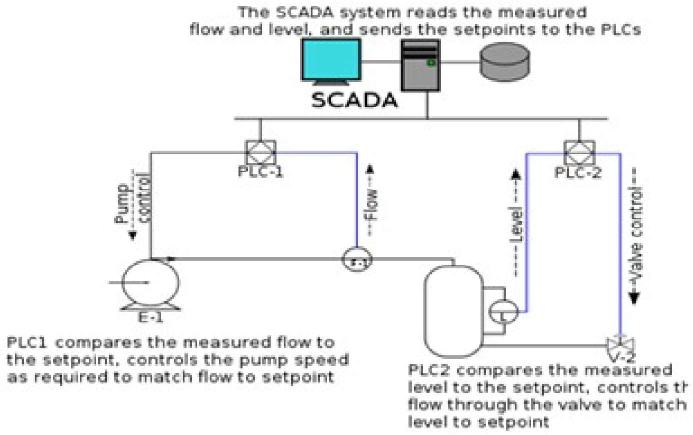
The SCADA system reads the measured flow and level, and sends the setpoints to the PLCs
SCADA
PLC-1
PLC-2
Pump control
Flow
Level
Valve control
E-1
F-1
V-2
PLC1 compares the measured flow to the setpoint, controls the pump speed as required to match flow to setpoint
PLC2 compares the measured level to the setpoint, controls the flow through the valve to match level to setpoint

***Fig 6:** Typical example of SCADA monitoring and controlling liquid flow and level.*

In general, for controlling and monitoring a substation in real time (PLCs) Programmable Logic Controllers, Circuit breakers and Power monitors are used. Data is transmitted from the PLCs and other devices to a computer-based-SCADA node located at each substation. One or more computers are located at different centralized control and monitoring points.

SCADA system usage has become popular from the 1960s with the increase in need of monitoring and controlling the equipment. Early systems built using mainframe computers were expensive as they were manually operated and monitored. But the recent advancements in technology have made-advanced, automated SCADA systems with maximum efficiency at reduced cost, according to the alarming requirements of the company [3].

1.4 SCADA and its role to critical infrastructure systems

Critical infrastructures are those that are so vital that their incapacity or destruction would have a debilitating impact or effect on the defense or economic security of a country. For example, important public buildings, bridges, telecommunication networks, oil and gas pipelines that supply petroleum products nationwide, gas pipelines that supply critical gas to electricity/power plants, pipeline distributing portable or drinking water, chemical plant, nuclear plant, etc. Disrupting or attacking these infrastructures will harm the economy or security of the nation.

According to [4], telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue) and continuity of government. Fig.7 shows the infrastructures that were commonly pointed out as “critical”.

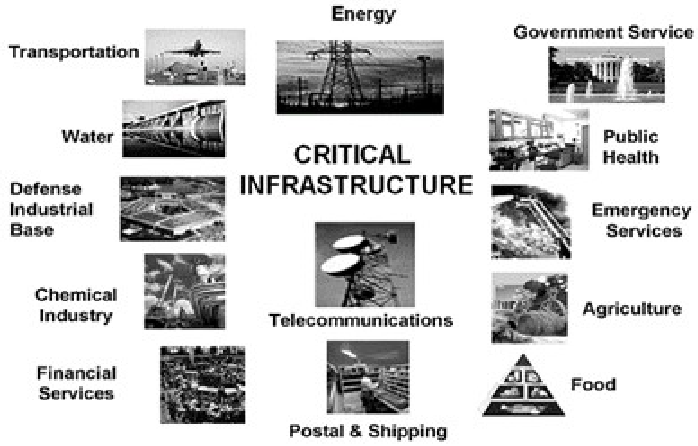

***Fig 7:** Critical infrastructures [4]*

Most of these so-called critical infrastructures nowadays are controlled by controlled systems, SCADA in particular. So if the SCADA will malfunction, it will cause debilitating impact to the community and society at large; there will loss on revenue, loss of life and degradation of the environment.

1.5 Types of SCADA attack

Criminal-minded individuals or terrorists can have unauthorized access into a SCADA system in order to cause harm or sabotage to a national economy. For instance, pumps and motors are made to run faster than normal, equipment is turned on and off, and valves and controls are switched erroneously, all of which are designed to make the machinery run out of control in a prescribed sequence. Attacks on SCADA can either be physical attack (this is largely done by vandalizing the physical infrastructure of SCADA) or Denial-of-Service (DoS) attack to disrupt SCADA services, or attack on sensitive data of SCADA in order to steal or modify it.

1.6 SCADA System Threats and Vulnerabilities

According to [5], many, if not most, SCADA systems are currently vulnerable to cyber-attacks due to the following:

- **Lack of network monitoring.** Without active network monitoring, it is impossible to detect suspicious activity, identify potential threats, and quickly react to cyber-attacks.

- **Slow updates of software.** As SCADA systems become more advanced, they also become more vulnerable to new attacks. Maintaining firmware and software updates may be inconvenient (without the proper systems in place), but they're necessary for maximum protection.
- **Lack of knowledge about devices**. Connecting devices to a SCADA System allows for remote monitoring and updates, but not all devices have equal reporting capabilities. Since most SCADA systems have been developed gradually over time, it's not uncommon to see technology that's 5 years old paired with technology that's 20 years old. This means the knowledge about network connected devices is often incomplete.
- **Inability to understand traffic.** Managers need to know what type of traffic is going through their networks. Only then they can make informed decisions about how to respond to potential threats. With advanced data analysis, managers can get a big picture view of data gathered from traffic monitoring, and translate that into actionable intelligence. For example, an infiltrated system might check with a foreign server once every 30, 45, or 180 days.
- **Authentication holes**. Authentication solutions are designed to keep the wrong people from accessing the SCADA system. However, this can easily be defeated due to common unsafe practices such as poor passwords, username sharing, and weak authentication.
- **Unsecure credential management**—Lack of encryption or the use of default passwords—is a common problem, as is default settings in systems that were never designed to be secure.

1.7 Incidences Caused by SCADA attacks around the world

SCADA attacks were documented by [5] according to the year and the corporations that witnessed the attacks around the world. The author highlighted the attacks according to the year they took place. The authors classified the attacks as either *unintentional* or *intentional. Unintentional attacks* are the ones not really targeting a particular corporation but they still got to them *accidentally* or *unintentionally* while intentional attacks are the ones that are specifically targeted at a particular corporation(s) by hackers using malwares like virus, trojan horse, worms, botnets and logic bombs. SCADA attacks are meant to compromise SCADA systems of critical assets such as oil and gas pipelines and installations, airways control, military equipment control, electricity and power installation, nuclear systems etc. In most of the attacks, the malwares were able to gain backdoor or unauthorized access they created illegal access to the hackers. The victims of the attacks underwent a lot of devastations, security and economic loss.

Fig.8, as exemplified by [5], shows an example of a Security compromised SCADA Network. Here the RTUs have been compromised and this gives room for Denial-of-Service (DoS) attack and malicious control of the network.

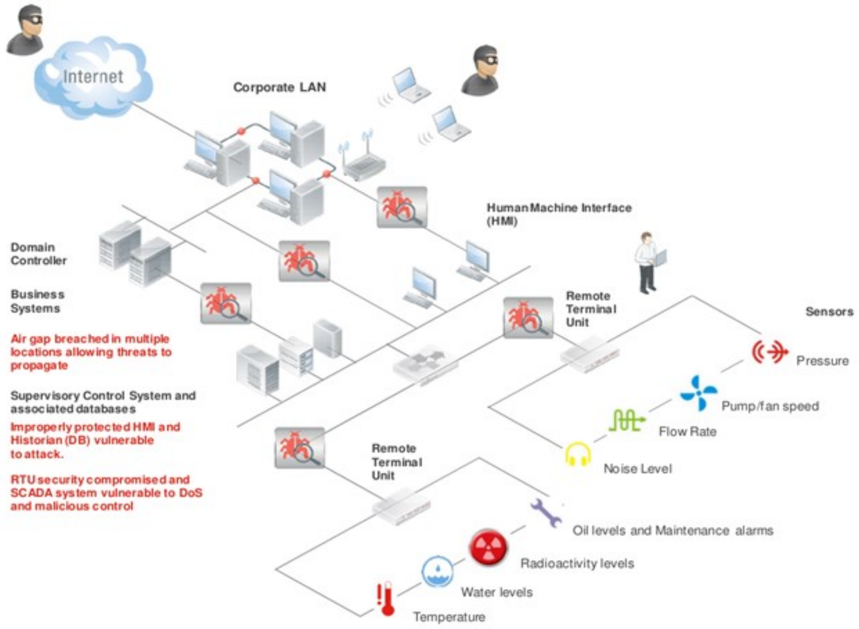
Internet
Corporate LAN
Human Machine Interface (HMI)
Domain Controller
Business Systems
Air gap breached in multiple locations allowing threats to propagate
Supervisory Control System and associated databases
Improperly protected HMI and Historian (DB) vulnerable to attack.
RTU security compromised and SCADA system vulnerable to DoS and malicious control
Remote Terminal Unit
Remote Terminal Unit
Sensors
Pressure
Pump/fan speed
Flow Rate
Noise Level
Oil levels and Maintenance alarms
Radioactivity levels
Water levels
Temperature

Fig 8: *An example of how SCADA can be compromised security-wise*

2.0 Recommended Strategies to Secure and Protect SCADA from Attacks

The following strategies or approaches can be employed to safeguard SCADA and its sub-systems from attacks and compromises in Nigeria.

- Install 24-hour intrusion detection systems to detect external and internal physical security breaches. This needs to be connected to mobile phone numbers to send alerts to designated personnel whenever any incident is detected. This will help protect SCADA infrastructure from physical attack and vandalisation. Examples include intrusion detection systems such as perimeter fencing and alarms, fences, doors, motion detection sensors, hotspot detectors, CCTV cameras etc. Additionally incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

Fig 7: *CCTV cameras with motion detection and night vision*

- Carry out routine physical security audit to testrun security controls such as guard mechanisms, fences, doors, alarms, CCTV, and other aspects including security management systems and reporting mechanisms, and production of reports for clients highlighting shortfalls and what should be done with respect to security improvements.
- Implement encryption of hash keys, passwords etc. to authenticate users that uses the SCADA system
- Establish system backups and disaster recovery plans. Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from exercises.
- Installation of firewalls and DeMilitarized Zones (DMZ) around SCADA network infrastructure to protect the SCADA network from malwares and hackers.

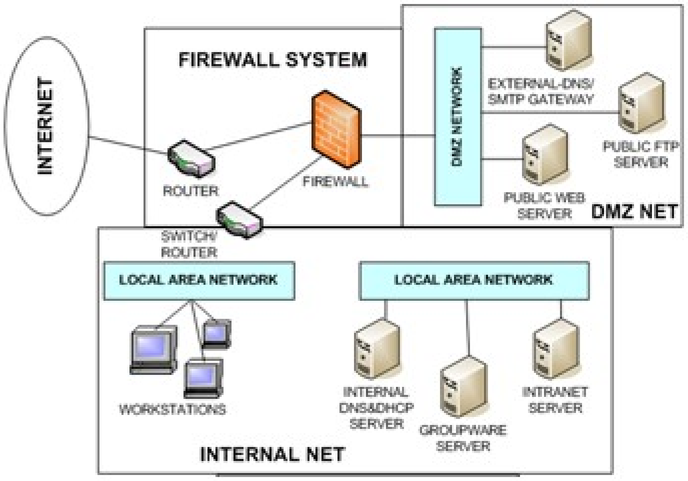

Fig 8: *Multi-homed Host Firewall with Demilitarized Zone (DMZ)*

- Install and update Good Anti-malware software such as Anti-Virus, Anti-Spyware, Anti-botnet etc.
- Conduct routine self-assessments from time to time. Robust performance evaluation processes are needed to provide organizations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organization is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organizational and individual performance.
- Carry out comprehensive risk analysis to ascertain weakness in the SCADA system and sub-systems so as to identify the security holes or vulnerabilities in order to fix it.

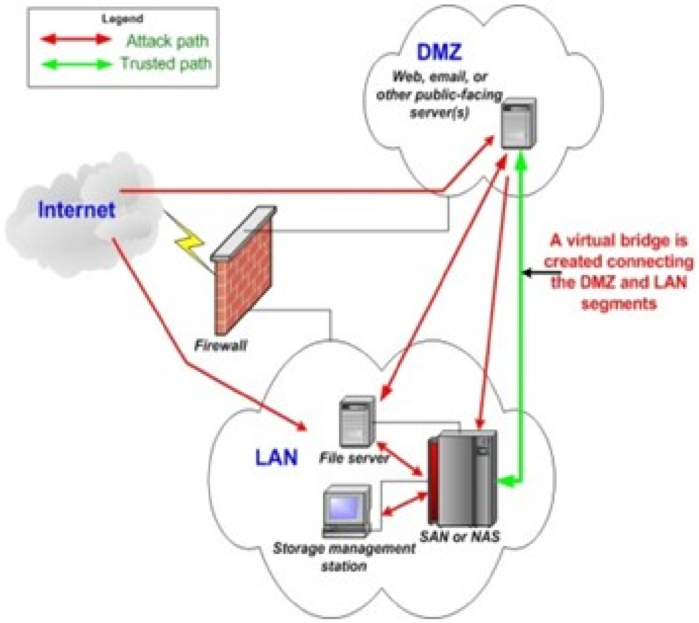
Legend
Attack path
Trusted path
DMZ
Web, email, or other public-facing server(s)
Internet
A virtual bridge is created connecting the DMZ and LAN segments
Firewall
LAN
File server
SAN or NAS
Storage management station

Fig 9: *Firewall with Demilitarized Zone (DMZ) to protect SCADA's network and File Server*

- Encrypt all communications links and data associated with SCADA system to protect the data from hacker's or malware's eavesdropping

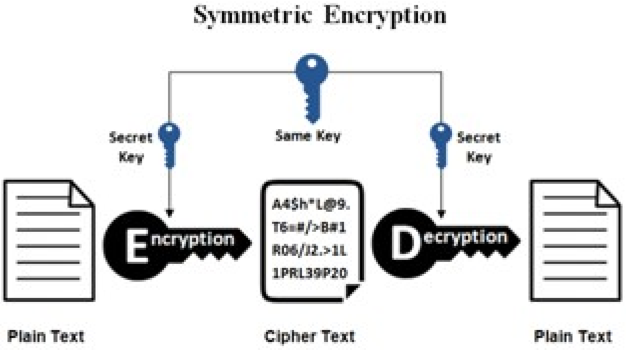

Fig 10: *Symmetric and encryption scheme to protect plain text data from eavesdropping and modification using secret key*

- Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

Release data related to the SCADA network only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. "Social engineering," the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks. The more information revealed about a computer or computer network, the more vulnerable the computer/ network is. Never divulge data related to a SCADA network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfillment. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

3.0 Summary and Conclusion

A SCADA is used to manage and control critical infrastructures which perform essential services to the citizenry of a country. Most critical infrastructures are controlled by control systems such as SCADA. Critical Infrastructures are vital and very important to the society. If SCADA is compromised security wise, there will be catastrophic consequences on the life of the society. The economy will be affected. The environment will be affected and ultimately life will be affected. This paper presented different aspects or types of vulnerabilities or threats that SCADA are prone to and its operations. These vulnerabilities or threats need to be identified and fixed otherwise it may leads to attacks which will have catastrophic effects on the society. This paper identified different strategies to tackle the threats to SCADA so that the SCADA and its sub-systems will be secure and attack-proof so as to deliver on its mandate of rendering reliable essential control services.

References

1. DPS Telecom, "What is SCADA?" Available: http://www.dpstele.com/scada/what-is.php
2. Daniel Wagner (September 8, 2017). "The Threat of Virtual Terrorism against Infrastructure is growing". Available:
3. https://intpolicydigest.org/2017/09/08/threat-virtual-terrorism-infrastructure-growing/
4. Tarun Agarwal, "Know all about SCADA Systems Architecture and Types with Applications. Available: http://www.edgefxkits.com/blog/scada-system-architecture-types-applications/
5. Rosslin John Robles , Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park, Sang-

Soo Yeo, “Vulnerabilities in SCADA and Critical Infrastructure Systems”, International Journal of Future Generation Communication and Networking, pp.99-104.

6. Ruchna Nigam (Feb 12, 2015). “(Known) SCADA Attacks Over The Years”, Fortinet. , Available: https://blog.fortinet.com/2015/02/12/known-scada-attacks-over-the-years
7. Aaron Hand (April 19, 2015), “SCADA Attacks Double in 2014”, Available: https://www.automationworld.com/scada-attacks-double-2014