ISSN:0975-9646

Secure Data Acquisition System

Ajay[1], Ajey B S[1], B C Steaven[1], Naveen Deshpande[1], Anitha C[2]

[1]*UG Students, Dept. of CSE, NIE, Mysuru.*

[2]*Assistant Professor, Dept. of CSE, NIE, Mysuru.*

***Abstract*— Data acquisition is the process of sampling signals that measure real world physical conditions and converting the resulting samples into digital numeric values that can be manipulated by a computer. Data acquisition systems, abbreviated by the acronyms *DAS* or *DAQ,* typically convert analog waveforms into digital values for processing. A Data Acquisition System (DA system) is used for acquiring real time data. In our project we use vibrations, which will be produced by an Android device as the real time data and this data from the android device will be transmitted to the DA systems from where the data will be transmitted to the Admin in a secured manner. The Admin can send remote signals to these DA systems through a remote terminal unit. Whenever an intruder tries to hack the network, he will be provided with decoy information using a honeypot system and an alert in the form of an e-mail will be sent to the admin so that he can take suitable actions.**

Keywords*— Supervisory Control and Data Acquisition, Remote Terminal Unit, Honeypot System, RSA cryptography

I. Introduction

Security is a major concern in any network and the fact that data acquisition systems use real time data, providing security to such systems becomes that much more important. Also we require a system which not only tells us that an attack has occurred but it should also give a clear picture on which part of the data was compromised so that such attacks may be stopped in the coming future. Transmission of data across the network in a secured manner is also a major problem[1] .

One possible solution would be the use of Honeypot system. These security systems would be embedded into the DA system which will provide false data to an intruder and also maintain a log file about the intruders various actions and send this log to the admin.

II. Existing System

Currently DA systems are used in Nuclear power plants, gas and oil pipelines to collect and monitor data in real time. In the existing system data is sent from the DA system to the admin without even checking whether the data is from a valid source or not. There is also a security system present which will intimate about the intruder but it is incapable of specifying what the intruder wanted to access which could be used to prevent future attacks from happening.

There are three different kinds of threats to the SCADA systems. They are Attack on the SCADA systems, Attack by the SCADA system and Attacks through the SCADA systems. Further threats to the SCADA systems are Authorization violation, Bypassing Controls, Data Modification, Denial-of-Service, Eavesdropping, Physical Intrusion, Replay, Traffic Analysis, Trojan Horse, Virus and Worms. A Researcher classified Attackers Goals into various categories.[2]

1) Gain SCADA system access with severity as Low.
2) Identify Mod bus device with severity as Low.
3) Compromise Master with severity as Extreme. [2]

The SCADA incidents were categorized based on the severity levels, consequences and entry point, etc. The two main observations noticed were there are more frequent attacks and are becoming more external than Internal oriented. The attacks were categorized into two types, the Attacks on the PLC and the Attacks on the HMI. Both the attacks divided into four sections: Cryptographic attacks, replay attacks, DoS attacks and Fragmentation attacks. [2]

III. Proposed System

In our system there exists four major components they are

- Admin
- SCADA
- Android Device
- Intruder

The Admin creates a shared key with the DA systems for secure transmission of data. The Admin can also send remote signals to the DA systems.

The DA system receives the encrypted data from the android device and sends the encrypted data to the Admin. RTU system sniffs the data packets to ensure that it is coming from a reliable source. Android device is used to collect and send vibrations to the DA systems.

The intruder attacks the network and sends commands to the DA system which is responded by the honeypot system with a false data.

An intimation will be provided to the Admin about the attack through an e-mail so that he can decide on future actions.

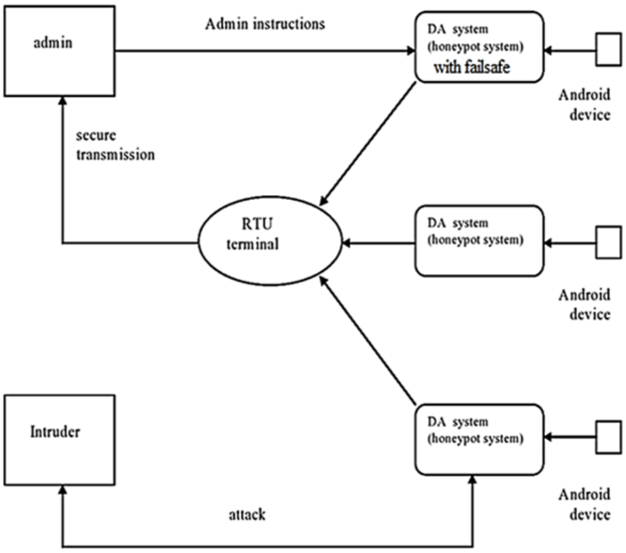

Fig 1: Basic architecture of the system

IV. ADVANTAGES OF PROPOSED SYSTEM

- It provides secure transmission of data through encrypting it in various sections.
- It includes a honeypot system which removes the vulnerability from different types of attacks.
- It includes a remote terminal unit for processing encrypted commands.
- It also includes a fail-safe in-case there is a transmission error between SCADA and admin.

We propose a three-tier architecture with the following specifications:

USER INTERFACE : JAVA AND .NET

MIDDLEWARE : MOBILE VIEW CONTROLLER (MVC) AND C#

STORAGE : XML

V. DESIGN

Sequence diagram is a kind of interaction diagram that shows how components among system interact with each other and in what order.

Admin:

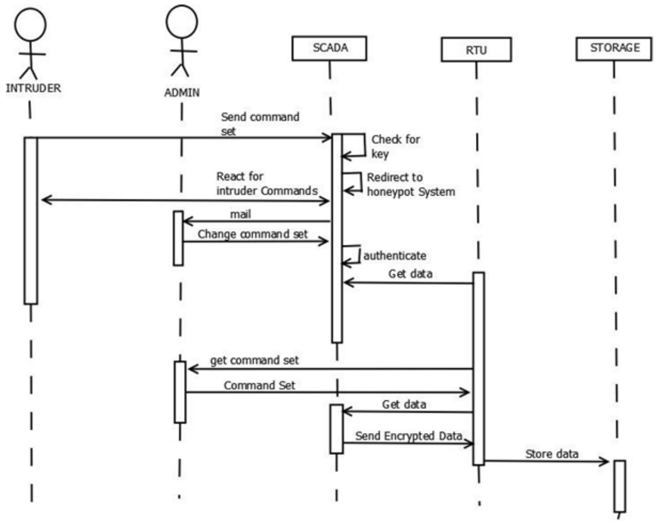

Fig 2(a): Sequence diagram of the system(ADMIN)

In figure 2(a), SCADA interacts with Admin by sending request to admin. Admin then generates credentials which are sent to SCADA. After the SCADA has been authenticated, Admin sends the instruction set to SCADA. After that SCADA starts pumping the data to RTU continuously based on instruction set and RTU stores the data. Whenever the Admin wants data he sends an instruction set to RTU and the RTU checks whether he is a valid admin or not and after he is a valid admin, based on the instruction set RTU retrieves the data and the same data is sent to Admin where it is decrypted.

Intruder:

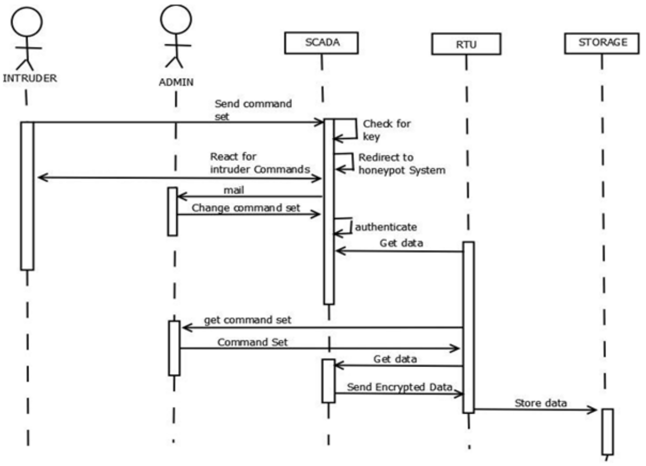

Figure 2(b): Sequence diagram of the system(INTRUDER)

In case of Intruder, intruder interacts with SCADA system with sole purpose of taking control of the entire system by compromising it. He sends Instruction set to the SCADA machine. The SCADA machine then redirects the intruder to Honeypot System since the intruders IP Address is not registered with SCADA machine. The intruder is then provided with false data and the intruder's activities are mailed to Admin and Admin can take preventive measures by changing command set.

VI. Results And Discussion

The Security Strategy need to implement to protect SCADA systems are use of Administrative and Technical Controls and Defense-in-depth.

It includes Authentication method, Encryption Technology, securing Application protocols, implementing Access Control Lists. Understanding how are internal systems connected to the rest of the SCADA Infrastructure, are External and Internal systems updated with the latest Anti-virus signatures and latest Operating systems patches and Measures to take if security is breached. The Countermeasures i.e., Line of Defense techniques suggested are Setting up Multiple VLANs for various types of traffic, Implementing Access Control Listto dictate traffic flow and administrators suggested to use SSH(encrypted Communication) instead of Telnet for Management and Configuration of network devices.

The Security measures for SCADA systems, suggested by author are understand the risk, protection and necessity of every connection to the SCADA network, make the network as isolated as possible and use safe methods for data transfer, remove or disable unused services provided by non-proprietary operating systems, Secure Back-doors and vendor connections, clearly define roles and responsibilities for all organization personnel. Identify risks and vulnerabilities and create an ongoing Risk Management process, base protection strategy on defense-in-depth strategy, Training personnel to prevent disclosure of sensitive Information about the SCADA System. Therefore there is secured data transmission between the SCADA system and the admin. The real time data is encrypted and transmitted so that no one can get the data except the admin.

VII. Conclusion

We have designed a system similar to the real time system SCADA, which helps in acquisition of the real time data. There is secured data transmission between the SCADA system and the admin. The real time data is encrypted and transmitted so that no one can get the data except the admin.

When an intruder tries to get the real time data from SCADA, it redirects him to the honey pot system thereby creating an illusion that intruder is interacting with the SCADA and creates a log file about the intruder.

VIII. Future Enhancements

In the future, we can ensure that network should be configured on threat by changing the network protocol and listen ports to avoid further network data damage.

We can enhance our system and include other functions like identifying intruder country, zone and service provider to reach intruder physical location.

References

[1] A SCADA Intermediate Simulation Platform to Enhance the System Security by Aamir Shahzad , Naixue Xiong(IEEE Member), Muhammad Irfan , Malrey Lee , Shahid Hussain(IEEE Member), Khaltar.

[2] Detecting the Network Attack Vectors on SCADA Systems by Ram Sandesh Ramachandruni,Prabaharan Poornachandran