Data Acquisition System Security by Honeypot

Ranjana H

Abstract— The SCADA System attacks is been increasing and some security must be provided to prevent system attacks. There are few solutions present to overcome this problem. So there is a great need to address this problem. In this paper we have introduced new methodology for providing security to SCADA systems. Honeypot system will be embedded into SCADA which mimic the services of an ICS. These systems are exposed to internet to attract the unauthorized logins. The main purpose this model is to track the user activities and to prevent the system from future attacks.

Index Terms—Honeypot, ICS, IDS, SCADA

1. INTRODUCTION

THE monitoring and control systems are used in critical industrial processes. The system acquiring real time data and has a controlling ability is termed as SCADA (Supervisory Control and Data Acquisition System). Data acquisition is reading the information from devices or field instruments through sensors. SCADA system fetches the data from various fields such as power plants, water management system and others. These data is used to monitor the current temperature, pressure or environment where field instruments are present. SCADA can be set up within the corporate and access remotely by master terminal unit. Earlier system where designed using protocols own by private organization were in no much importance was given to the security of the data as well as system.

1.1 SCADA System

The system consists of major components

1) SCADA Server or Master Terminal Unit (MTU): This master set up commands for SCADA.

2) Remote Terminal Units: It collects large amount of data and those data must be protect by attack.

3) Human Machine Interface: Human operator role is to configure set points or display process status information in the event of an emergency.

4) Communication Infrastructure: It is used to connect various components of the SCADA system together. This infrastructure consists of multiplexed fiber-optic, satellite network and Internet.

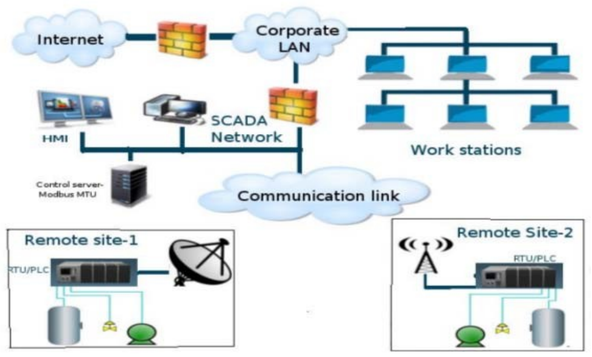

Fig1. SCADA System Architecture

1.2 Major functionalities of the SCADA

1) Acquisition of data: Sensors are used to acquire real time data such as temperature in power plants and in water management systems pressure at the valves are sensed.

2) Controller: Human play a role of control operator. Trigger of control alert to operator in case of emergency situations.

Data storage: Remote end unit stores the data obtained from sensors.

Alarm: When some problem occurs an alert is provided to the SCADA system.

Reporting: History of logs maintained and sent to the master of SCADA.

Tagging: Unauthorized operations are to be prevented.

1.3 Security areas of ICS

Defense in depth strategy used as a good security strategy throughout organization without relying on one thing we need to have many layers of protection. Different layers can be put in to the organization environment. Firewall can be put at the edge of the organization. Organization put firewall on inside for protecting floors of a building or protecting devices inside data center because people go in & out to the internet. Only the data required by organization flows inside the network.

Another methodology associated with many firewall is a demilitarized zone or DMZ. DMZ is the middle ground between inside and outside so that people who need to access resources in organization don't come all the way to internal parts of network. They go to middle ground called DMZ. Authentication is taken granted as a security strategy. Authenticate people by using a username and password.

Intrusion detection system is able to watch all the traffic travelling in the network. If somebody is trying to take advantage of vulnerability on a server or workstation stop the bad traffic flow. If we are coming in to network from outside then we will be using virtual private network. VPN access encrypts data going through the internet. Decrypt the traffic when it comes inside the network of the organization. Running anti-virus and anti-malware software in all over workstation stop malicious activities.

2. LITERATURE SURVEY

Attack can be made on the SCADA systems or by SCADA system and Attacks through the SCADA systems.

Organizations like NERC or NIIST going a step ahead to provide security to such systems by deploying of critical infrastructure. Proper guidelines, test beds, new technology, encryption methods are developed. SCADA facing several threats and risk must be secured.

Author suggested the measures to provide security at top level by high analyses of threads and risks. Solution was formulated by creating SCADA specific IDS and metrics for security. These security measures are under high risk of attack. Safe method need to be developed to achieve secure authentication.

Researcher Further threats to the SCADA systems are Authorization violation, Bypassing Controls, Data Modification. SCADA system is lacking Unrealistic testing environments, poorly Analyzed threat models, IDS implementations specific to different SCADA environments and Lack of analysis of false positive/ false negative of IDS's. And the author suggested a solution of creating SCADA specific IDS and Security Metrics.

A Researcher presented a novel SCADA Firmware technique and analysis that compared altered firmware to a known good firmware of a particular PLC and report a static analysis of differences. Research goals were to detect modifications and characterize nature and behavior of modification.

The Security measures for SCADA systems are understand the risk this can be overcome by isolating network so much as possible, using secure protocol applications, understanding internal structure of system, updating latest versions of protection software. Services that are not frequently used or completely out of order are to be disabled.

3. HONEYPOT SYSTEM

A honeypot is in the form of physical or virtual system that attracts the attackers. Honeypot helps in studying the behavior of attackers. It also helps researches to analyze how the real world attacks are taking place so that we can defend against future attacks or helps in writing signatures for IDS for identification of future attack. Honeypot categorized based on degree of interaction and extend of detecting attacks.

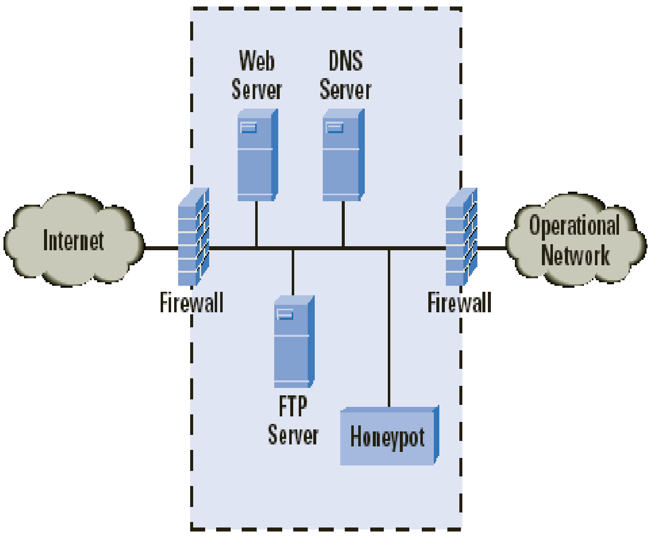

Fig2. Deployment of Honeypot System

3.1 Benefits of Honeypots in Supervisory Systems

The honeypot system is embedded on to Supervisory systems as several benefits in compared security measures such as firewall or IDS. Security devices specific to SCADA networks are very few in number. Addition of honeypot actually do not modify the existing network configuration but help in tracking the attackers movement & what the intention behind such attacks can be investigated by authority. Honeypot acts as plug-in tracking the methodology of attack which in turn helps in changing the system commands by administrator.

4. PROPOSED SYSTEM

In our system there exist 5 major components they are

1. Admin: Creates a security key secure transmission of data and sends remote signals to supervisory systems.
2 SCADA System: This system receives the encrypted data from the sensor and sends the encrypted data to the Admin.
3 RTU: Data from SCADA system is sent to RTU. RTU stores encrypted data.
4 Attacker: The attacker attacks the network and sends commands to the SCADA system which is responded by the honeypot system with a false data.
5 Sensor: used to collect & send pressure, temperature to supervisory systems.

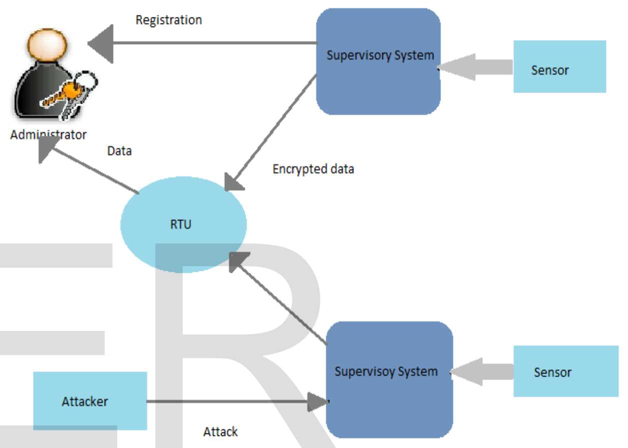

Fig3. System Architecture

5. CONCLUSION

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 that prevents future attacks. So honeypot system is embedded on to supervisory systems. Transmission of data in secure manner is taken care by RTU. Thus ensure reliable transmission of data.

REFERENCES

[1] Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST special publication (2011): 800-82.

[2] Igure, Vinay M., Sean A. Laughter, and Ronald D. Williams. "Security issues in SCADA networks." Computers & Security 25.7 (2006): 498-506.

[4] Matrosov, Aleksandr, et al. "Stuxnet under the microscope." ESET LLC (September 2010).

[5] Provos, Niels, and Thorsten Holz. Virtual honeypots: from botnet tracking to intrusion detection. Pearson Education, 2007

[6] Charlie Scott, “Designing and Implementing a Honeypot for a SCADA Network”, Sans Institute, June 7, 2014.

[7] Dong-Joo Kang ; Jong-Joo Lee ; Seog-Joo Kim ; Jong-Hyuk Park “Analysis on Cyber Threats to SCADA systems ” Transmission & Distribution Conference & Exposition: Asia and Pacific, 2009.

[8] Gunnar Björkman; Diana Koshy; “SCADA Security Measures”; Expository; Systems and Internet Infrastructure Security (SIIS) Laboratory, Pennsylvania State University, June, 2011

[9] Dong-Joo Kang ; Jong-Joo Lee ; Seog-Joo Kim ; Jong-Hyuk Park “Analysis on Cyber Threats to SCADA systems ” Transmission & Distribution Conference & Exposition: Asia and Pacific, 2009.

[10] Haji.F; Lindsay, L ; Shaowen Song; “ Practical Security strategy for SCADA automation system and Networks” Saskatoon, Sask, 1-4 May 2005.

[11] Naoum Sayegh ; Ali Chehab ; Imad H. Elhajj ; Ayman Kayssi; Internal Security Attacks on SCADA Systems.