ijournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 1/ January 2014

A Survey: An Advanced Key Management Technique with Enhanced Security SCADA System

Author: Manoj B C[1]

Affiliation: Department of Computer Science, Assistant Professor, SCT college of Engineering[1];

ABSTRACT

Modern industrial facilities have command and control systems. These industrial command and control systems are commonly called supervisory control and data acquisition (SCADA).In this paper, we analyze several security issues in SCADA systems. We classify these issues based on key management, vulnerability and survivability. Using this standardized security techniques we can easily compare & contrast, current & future SCADA systems.

General Terms

Network, data

Keywords

Supervisory Control and Data Acquisition (SCADA)

1. INTRODUCTION

Supervisory control and data-acquisition (SCADA) systems are control systems for any national infrastructures. The term SCADA usually refers to centralized systems which monitor and control entire sites, or complexes of systems spread out over large areas. **Supervisory Control and Data Acquisition (SCADA)** offers the ease of monitoring of sensors placed at distances, from one central location. A SCADA system is a common process automation system which is used to gather data from sensors and instruments located at remote sites and to transmit and display this data at a central site for either control or monitoring purposes. The collected data is usually viewed on one or more SCADA Host computers located at the central or master site.

The SCADA Host is usually an industrial PC running sophisticated SCADA Man Machine Interface or Human Machine Interface software. 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. SCADA is not a specific technology, but a type of application. **SCADA** gets data about a system in order to control that system is a SCADA application. A SCADA application has two elements: 1. the process/system/machinery you want to monitor a control - this can be a power plant, a water system, a network, a system of traffic lights, or anything else. 2. A network of intelligent devices that interfaces with the first system through sensors and control outputs. This network, which is the SCADA system, gives you the ability to measure and control specific elements of the first system.

Historically, SCADA systems were designed without security functionality because of the closed operating environment. However, the security of SCADA Systems has become an issue with connection to open networks becoming more common. 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. Any damage to the SCADA system can have a widespread negative effect to society. SCADA system performs four functions: Data acquisition, Networked data communication, Data presentation &Control. Sensors (either digital or analog) and control relays that directly interface with the managed system. Remote telemetry units (RTUs) are small computerized units deployed in the field at specific sites and locations. RTUs (Remote Telemetry Units) serve as local collection points for gathering reports from sensors and delivering commands to control relays. SCADA master units. These 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. The communications network that connects the SCADA master unit to the RTUs in the field.

SCADA systems are also generally fault-tolerant (redundant), and major pipelines may even have a physically separated, alternate-site SCADA system, intended to assume control if the primary SCADA system were disabled. A major pipeline might have field-based personnel who can take local manual

control of booster stations and storage terminals, as long as voice communications are available. Thus the SCADA systems can be vulnerable to a variety of attacks. These changes have made SCADA systems more available for attackers to target from anywhere in the world. SCADA systems are capable of communicating using a wide variety of media such as fiber optics, dial-up, or dedicated voice grade telephone lines, or radio. Recently, some utilities have employed Integrated Services Digital Network (ISDN). Typically, SCADA systems are used to automate complex industrial processes where human control is impractical - systems where there are more control factors, and more fast- moving control factors, than human beings can comfortably manage.

For the first time, vulnerability assessment framework [1] is made to systematically evaluate the vulnerabilities of SCADA systems at three levels: system, scenarios, and access points. Since 2009, the existing key-management [2] schemes for SCADA systems provide the secure unicast communications but these schemes do not support the secure message broadcasting. Increasing the security dependence, the trust system [3] was implemented to increase its flexibility, and demonstrates the trust system using TCP traffic with precautions including closing unnecessary communication ports & keeping system patches up to date. A recent report comparing different security guideline has been provided to emphasize, the number of keys [4] to be stored in a remote terminal unit (RTU) that decreases the computational cost for multicast communication. Reference [5] proposes a novel approach using a critical state based filtering method for securing SCADA network protocols. SCADA applications require a more flexible approach to achieving reliability. There are [6] probabilistic models to predict survivability of SCADA systems. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time. Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be performed by operator commands. In this paper, several security techniques of SCADA are compared for providing both multicast and broadcast communication for efficient and stable operation of SCADA systems.

2. SURVEY OF SECURITY ISSUES IN SCADA

SCADA offers intercommunication between applications, standardization of the communications with the field devices and adoption of the communication surroundings. Supervisory control and data acquisition allows a utility operator to monitor and control processes that are distributed among various remote sites. SCADA can be traced to the development of telemetry from the first half of the century. The technology of rockets and aircraft afforded man with the opportunity to investigate weather and planetary data. This required a simple way to get data that observers could not normally achieve from space (Boyer 1993). Manned stations on the surface of the Earth such as lighthouses, post offices, weather stations, etc., were able to collect and monitor data on weather. However, for accurate weather prediction, more detailed information was needed from the atmosphere. SCADA is used for gathering, analyzing and to storage real time data. SCADA systems are usually designed to be fault-tolerant systems with significant redundancy built into the system architecture. The following are an analysis of several security issues in yearly order.

2.1 Vulnerability assessment of Cybersecurity for SCADA systems.

Vulnerability refers to the inability to withstand the effects of a hostile environment. In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Firewall & password model [1], regulates the packets flowing between two networks & evaluates penetration attempts based on repeatedly failed logons without establishing authentication credentials respectively. The mechanism for storing these failed logon trials, or other security-relevant events, is embedded in the computer system for analysis. Vulnerability assessment is a critical task to ensure that power infrastructure Cybersecurity is systematically evaluated. The impact of a potential electronic intrusion is evaluated by its potential loss of load in the power system. The proposed framework can be used as a planning tool that assists security analysts to identify the bottleneck of the system where improvements are most effective.The advantage is that it quantifies the potential impact of cyber power system attack. The main disadvantage is that it is computationally inefficient for large systems & lack of statistical information about intrusion attempts.

2.2 Advanced key management architecture for secure SCADA communication

Logical Key Hierarchy is based on constructing a logical tree of keys. Each member knows the entire symmetric keys from its leaf to the root. If a new node joins the group, logical key hierarchy updates the entire symmetric keys from its leaf to the root. A key-management protocol [2] is proposed to support both the message broadcasting and secure communications. . Each RTU knows all keys which are on the path from leaf to the root. The contributions are of two-fold. First, the scheme supports both the message broadcasting and the secure communications. Secondly, evenly spreading much of the total amount of computation across high power nodes (MTU or SUB-MTU) is made. It supports multicast & broadcast communication, no key translations needed, avoids performance bottleneck by keeping RTU minimal. The demerits are SUB MTU overhead increases, number of keys to be stored is increased, newly joining keys are not encrypted, key

hacking is easier; performance of broadcast communication is very low.

2.3 A trust system architecture for SCADA network security

A trust system [3] is a communication security device with firewall & intrusion detection capabilities designed for use with time- critical network system. The concept of trust system is to provide a non-proprietary system, system of systems, or software agents that plug into an existing network, somewhat transparently, to perform the functions of correlating data &identifying risk levels for corresponding events & status updates that point to negative impacts on utility services. The major goal of the trust system is to increase security with minimal impact on existing utility communication systems. Trust-management engines avoid the need to resolve identities in an authorization decision. The trust system enforces access restrictions between IP addresses that should not be allowed to communicate with one another via specific message types and interfaces. It blocks incoming packets for open port without communication, secure for power grids. The disadvantage is that protection to the power grid is not effective, tunneling between trust systems adds overhead & delay for packet encryption & decryption.

2.4 Efficient secure group communications for SCADA

ASKMA [3] is a more efficient key-management scheme supporting efficient multicast communication by considering the number of keys to be stored in a remote terminal unit (RTU). The key structure is divided into two classes: applying the lolus framework [3] & constructing each class as a logical key hierarchy. The MTU or SUB-MTU is able to multicast messages efficiently through the key structure between SUB-MTU and RTU organized as a logical key hierarchy structure. ASKMA provides direct communication between RTU's. No key translations are needed so that this architecture can be used for real time applications. The computational cost of the key-management scheme occurring when a member is added and left is not important or may be ignorable, since the addition and deletion of a member rarely occurs. ASKMA provides the number of keys to be stored and provides multicast and broadcast communication for efficient and stable operation of SCADA systems. It reduces the number of keys in the remote terminal unit & provides multicast &broadcast communications. The disadvantage is that less efficient during the multicast process.

2.5 Critical state based filtering system for securing SCADA network protocols

Critical State Based Firewall [5] is based on monitoring the evolution of the state of the protected system and on the analysis of the command packets between master and slaves of SCADA architecture. A critical state detector is used to check whether the state of the system is evolving toward a defined critical state. A critical state distance metric computes how close any state is with respect to the critical states. Critical State Based Firewall also detects attacks composed of a set of SCADA commands which disrupt the correct behavior of the system when executed in particular operating states. These will co-ordinate the evolution of target systems with the analysis of command packets flowing between the master and the slave of SCADA system. The key elements of this technique are the concept of critical state and the observation that an attacker, in order to damage an industrial system, will have to modify its state from secure to critical. It blocks attacks based on unknown techniques on the basis of the system evolution, the number of false positives results are limited. If the real system and its virtual image are desynchronized an error in the configuration of the auto synchronization time between the real system and the virtual system, cannot protect SCADA from traditional ICT attacks such as virus attacks.

2.6 A probabilistic model to predict the survivability of SCADA systems

Probabilistic model [6] offers a new direction in measuring survivability & solves the issues with current models by combining the formalism of Bayesian networks with information diversity. Survivability focuses on provisioning of an acceptable level of services even in the presence of malicious attack. Service independencies are properly taken into account and information diversity metric is used to represent the service behavior. New metric, called information diversity, analyzes system's behavior that takes a different approach from the current models based on performance metrics. By using the formalism of Bayesian networks, the proposed model is suitable to perform both prediction and diagnosis. Survivability is defined as the capability of the system to exist, function, and recover in spite of adversity. The survivability assessment is performed based on information diversity, interdependencies, heterogeneity. For survivability evaluation, a usage model for a system must embody essential and nonessential service workflows, as well as intrusion workflows, all of which are interwoven according to usage probabilities to represent the spectrum of expected system usage by both legitimate users and attackers. The model uses this information to perform the overall survivability. Services of part of the system are evaluated individually; analytical analysis on survivability is effective. It does not handle systems with feedback loop, & does not handle disconnected graphs. Limitation also occurs when too many parents generate huge CPT's.

3. PROPOSED METHOD

3.1 Firewall & password model

Firewall & password model assess the vulnerability to ensure Cybersecurity. But there is a lack of statistical information about intrusion attempts towards the

power infrastructure. This limitation can be partially increased, newly joining keys are not encrypted, key hacking is easier; performance of broadcast communication is very low.

3.2 Logical Key Hierarchy

A trust system Logical key hierarchy is used for secure SCADA communications. The contributions are of two-folds. First, the scheme supports both the message broadcasting and the secure communications. Second, by evenly spreading much of the total amount of computation across high power nodes (MTU or SUB-MTU), the protocol avoids any potential performance bottleneck of the system while keeping the burden on low power nodes (RTU) at minimal. The LKH+++ protocol used has greater advantages. It generates a new logical key hierarchy, such that the performance of broadcasting can be improved by this tree structure.

3.3 Trust Systems

A communications network security device, called a trust system, is used to enhance supervisory control and data-acquisition (SCADA) security. The major goal of the trust system is to increase security with minimal impact on existing utility communication systems. The trust system is augmented by routers to protect User Datagram Protocol (UDP)-based traffic. The trust system implementations increase flexibility, in TCP traffic & can be made in order to strengthen existing security. Strict access controls should be enforced and only the minimum rights should be granted to an individual to accomplish their jobs. Passwords should be robust. Transmissions from RTU's, PLC's, and IED's should be protected by digital certificates and digital signatures to prevent unauthorized users from intercepting the information or introducing false data into the SCADA system. Finally, Cybersecurity needs to be a priority for system administrators. SCADA systems are of increasing interest to hackers and other unauthorized users. Increasing levels of communication and protocol standardization will only increase the seriousness of this threat. Administrators should take precautions including closing unnecessary communication ports, keeping system patches up to date, and should keep up to date on current computer security practices. The elements inside the trust system should be inspected every day.

3.4 Advanced SCADA Key Management Architecture (ASKMA)

Advanced SCADA Key Management Architecture provides direct communication between Remote Terminal units. ASKMA++ is more efficient and secure compared to existing schemes. ASKMA++ reduces the number of keys to be stored and provides multicast and broadcast communication for efficient and stable operation of SCADA systems. This key management technique will increase the performance of the entire network .Using this key management technique we can able to increase the performance of the encryption algorithms like DES, RSA etc.

removed through future development of the test beds

3.5 Critical State Based Firewall

Critical state based firewall will monitors the commands between master & slave. The scenario in which an attacker is able to inject malicious packets directly in the network segment between the proxy and the remote terminal unit, and the scenario in which both the proxy and the master have been corrupted and collaborate in order to damage the process network are the problems facing. These two can be eliminated by using advanced security enhancement. Additional passwords should be introduced between proxy and network terminal.

3.7 Probabilistic Model

The probabilistic model provides a better measure of stability. Currently, it does not handle systems that provide some type of feedback loop, as regular Bayesian networks do not support cycles. This issue will be fixed by replacing regular Bayesian networks with Dynamic Bayesian networkswhich can handle cyclic graphs through temporal discretization. It does not handle disconnected graphs, in cases that the communication between services generates disconnected network structures. To overcome this issue a heuristic that connects the network structures will be proposed. And the limitation when a node (service) has too many parents, consequently generating huge CPTs also needs to be addressed. To address this issue a network traffic similarity heuristic will be used to combine parent nodes with similar traffic into one parent node, consequently decreasing the number of parents of the node. Another possible way that will be investigated is to replace the conditional probability tables with functions that represent the same distributions defined by the original probability tables .Introducing another efficient dynamic network rather than Bayesian networks to handle feedback loops cycles etc.

4. FUTURE WORK

4.1 Performance Enhanced trust system for broadcast communication

A SCADA system is a common process automation system which is used to gather data from sensors and instruments located at remote sites and to transmit and display this data at a central site for either control or monitoring purposes. The trust system intercepts & reaches to status messages & commands from network nodes destined for the master control station and other nodes in the network. In tunnel mode the trust system routers provide firewall & other security features for the nodes between them. They also create an encryption gateway between themselves to protect communication between trust systems. In order to avoid overhead and delay for packet encryption and decryption an efficient DES algorithm can be provided. DES uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. Although key

management is essential for secure SCADA communications. The trust system can be added to the advanced SCADA key management architecture to support message broadcasting and secure communications.

5. CONCLUSIONS

A trust system Logical key hierarchy is used for SCADA systems have become common place in national infrastructures such as electric grids, water supplies, and pipelines. SCADA (supervisory control and data acquisition) is a category of software application program for process control, the gathering of data in real time from remote locations in order to control equipment and conditions. SCADA systems include hardware and software components. The hardware gathers and feeds data into a computer that has SCADA software installed. The computer then processes this data and presents it in a timely manner. SCADA also records and logs all events into a file stored on a hard disk or sends them to a printer. SCADA warns when conditions become hazardous by sounding alarms.

6. ACKNOWLEDGMENTS

Our thanks to all the anonymous experts who have contributed towards development of the paper.

7. REFERENCES

[1] Donghyun ,Choi Efficient Secure Group Communications For Scada Inf. Security Group, Sungkyunkwan Univ., Suwon, South Korea

[2] D Choi, H Kim, D Won, S Kim Advanced Key-Management Architecture For Secure Scada Communications. - Power Delivery, Ieee, 2009 - Ieeexplore.Ieee.Org.

[3] Cw Ten, Cc Liu, G Manimaran Vulnerability Assessment Of Cybersecurity For Scada Systems - Power **Systems**, Ieee 2008 - Ieeexplore.Ieee.Org

[4] Cc Liu, Critical State- Based Filtering System For Securing Scada Network Protocols G Manimaran - Power **Systems**, Ieee ..., 2008 - Ieeexplore.Ieee.Org.

[5] Carlos Queiroz, Abdun Mahmood, Zahir Tari A Probabilistic Model To Predict The Survivability Of Scada Systems

[6] D. P. Bertsekas, "Dynamic Behavior Of Shortest Path Routing Algorithms For Communication Networks", Ieee Trans. Auto. Control, Pp. 60-74, 1982.

[7] M. Kafai And B. Bhanu, "Dynamic Bayesian Networks For Vehicle Classification In Video," *Ieee Trans. Ind. Inf.*, Vol. 8, No. 1, Pp. 100–109,Feb. 2012.

[8] G. Ericsson, "Toward A Framework For Managing Information Security For An Electric Power Utility—Cigré Experiences," *Ieee Trans. Power Del.*, Vol. 22, No. 3, Pp. 1461–1469, Jul. 2007.

[9] G. Ericsson, "Toward A Framework For Managing Information Security For An Electric Power Utility—Cigré Experiences," *Ieee Trans. Power Del.*, Vol. 22, No. 3, Pp. 1461–1469, Jul. 2007.