# A Review of Cyber Security Techniques for Critical Infrastructure Protection

Raghav Gupta
Department of Cyber Law & Information Tech
NLIU, Bhopal (M.P.), India
raghav.seth18@hotmail.com

Ratish Agarwal
Department of Information Technology
UIT, RGPV, Bhopal (M.P.), India
ratish@rgtu.net

Sachin Goyal
Department of Information Technology
UIT, RGPV, Bhopal (M.P.), India
sachingoyal@rgtu.net

**Abstract— Security is the most important aspect of any infrastructure. Infrastructure may be of private organization or government organization and the economy of the nation depends on this infrastructure.**

**A no. of approaches have been developed and proposed of researcher to ensure the security of critical infrastructure. This paper surveys the existing techniques for critical infrastructure protection. SCADA is defined as Supervisory Control and Data Acquisition. SCADA is considering as critical infrastructure. This paper also provides some important techniques for protection of SCADA.**

**Keywords**— Cyber-security, Critical infrastructure, SCADA,

## I. INTRODUCTION

Critical Infrastructure is defined as those infrastructures which would have a serious impact on national security, economic, public health; safety, etc belong to critical infrastructure. Every nation have critical infrastructure and it varies nation to nation. It is combination of distinguish sectors like;

- Energy, including oil, natural gas, and electric power
- Banking and finance
- Transportation (Including air, surface, and water transportation)
- Information and Communications Technology (ICT)
- Water systems
- Government and private emergency services
- facilities that produce, use, store, or dispose of nuclear material

Now Cyber Infrastructure is also considering as a critical infrastructure. Those assets and system which belong to cyber is very vital to the Nation. Cyber infrastructure comprise of computing systems, data storage systems, advanced instruments and data repositories, etc.

Critical infrastructure covers a wide variety of infrastructure. There is another sector which is considered as a critical infrastructure in cyber space called SCADA system. SCADA system is a control system. SCADA system has been implementing within most of the critical infrastructure, so that can operate the infrastructure automatically over long distance by simply given the command. To achieve this goal, SCADA system is using public network or internet. It increases its vulnerability which has been exploiting by the attacker. It causes cyber-attack. To defend from cyber-attack, we have to implement or increase the cyber-security of the critical infrastructure or in SCADA by using different techniques.

## II. LITERATURE REVIEW

A number of papers have been presented by distinguish authors in this area. Some important contributions are given below.

A. Shahzad, et al. in [1] have discussed, SCADA deployment in cloud computing to minimized the cost. During communication security will be the major issue. Since SCADA has deployed within cloud infrastructure without any security consideration. SCADA system connectivity with non-proprietary network and protocol affects the real time infrastructure. Few researchers proposed security implementation include SSL, TLS, IPSec, but all these have also limitation and mostly based on digital signature and cryptography. Some other solution

has been suggested and deployed to firewall protection, Intrusion detection system and prevention system. Cryptography solution has been implemented successfully during test-bed communication.

Yogge Wang, in [2] have discussed to design cryptographic standard to protect SCADA communication link. This paper proposed a suite of security protocols optimized for SCADA/DCS system, these protocol works for specific task or security that is the challenge for SCADA. Different type of standard like IEEE P1711, IEEE P711, and IEC are discussed to provide the security protocols. These standards try to define security protocols. sSCADA term is used in this paper, its means secure SCADA. sSCADA protocol is proposed to overcome the security challenges.

Giovanni A Cagalaban, in [3] have discussed in this paper about the testing of vulnerability of a software system. To test the vulnerability, it refers fault injection. Fault injection based on software technique called SWIFI (software implementation fault injection). Researcher also discuss about the SCADA device test-bed for vulnerability testing and assessment. In this paper, describe the vulnerability that is of two types. It is bug at implementation level and flaw at the design level. There is also some advantages of these models are to emulate the system vulnerability without concern, how they could occur in actual simulation. It also provides automating testing procedure, so the use of these vulnerability models in SCADA communication reduces the vulnerability of these critical systems to malicious cyber attack.

Vinay M. Igure, et al. in [4] have discussed, general architecture of SCADA network and properties of communication protocols. Also discuss the ongoing work in SCADA security areas such as firewall, Intrusion detection system, protocol analyses, cryptography. Most of the protocols of SCADA are of proprietary standard and total number of SCADA protocol is 150-200. Many of these protocols doesn't support any kind of cryptography, sniffing communication on the network, that's why security is compromised easily by attacker. Researcher also discusses the challenges to improve the access control, security, security management of the SCADA network. To overcome these challenges, proposed some methods such as linux based firewall, cryptographic models. This also highlight some of the threats and vulnerability that SCADA network face. Also present some of the ongoing work in this field and technical problem that should be addressed to improve overall security of SCADA network.

Rosslin John Robles, et al. in [5] highlight SCADA system act as a critical infrastructure. Also discuss the vulnerability in the SCADA system and difference between common computer system and SCADA system. SCADA is the combination of telemetry and data acquisition. Telemetry is used to connect system and equipment by long distance. Acquisition is to acquire the information from the devices/ network. SCADA system is now connects to the public network or internet. So SCADA security is SCADA network. SCADA system is already not secure and now it connects to the internet, so vulnerability is increase. COT can be use to overcome the security issues. COT is hardware and software; develop for operating in the network to decrease the risk. "HoneyPot" is another solution to secure the SCADA network. It is a technique to trap, detect, and deflect, to an unauthorized access to the network. Most critical infrastructure are controlled by control system like SCADA. If the vulnerability will not attend, it will cause great effect to the society.

AAmir Shahzad, et al. in [6] have discussed in this paper, the implementation of SCADA within cloud infrastructure. It is beneficial for real time infrastructure. Conception model is proposed to implement SCADA within cloud computing. Cryptographic solution is implementing in SCADA communication with/without the cloud infrastructure to achieve security services. Researcher also discusses SCADA generations. EPA (Enhanced performance architecture) mode, it is three layer models which use DNP3 protocol, and setup the relation with OSI model for communication. In this paper researcher also discuss about the three basic model of cloud computing like IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS(Software as a Service). Current paper provides research direction to secure real time infrastructure and way to implement SCADA within clud computing environment.

Aine MacDerMott, et al. in [7] have discussed, the current research direction in protecting critical infrastructure and the role of intrusion detection. It also represents research direction and proposed framework for critical infrastructure protection. Researcher found there is a weakness in the creation of critical infrastructures. The project aim to develop a framework for the protection of critical infrastructure based on anomaly based network intrusion detection. The frame work will be applied as a separate component from the SCADA network, as previous work has attempted to add IDSs as middleware. Our aim is to use network based sensors to collect and analysis the network traffic and provide real time monitoring of the network. An initial idea is that the framework will be implemented as a layer that runs above the SCADA network and does not alter the network in any way.

Thomas, et al. in [8] have discussed about the test-bed which enable a research process so that cyber-security vulnerabilities may be discovered. Test-bed is used as platform, so that researcher may develop solution for cyber-security. Test-bed includes wireless test-bed facility, cyber test-bed, for the testing of firewalls and virtual private network. SCADA test-bed provides real world testing facilities for SCADA manufacturer, academic

researcher. In this paper test-bed is used to provide live demonstration of control systems under cyber attack and to understand the implication of the vulnerability.

Bonnie Zhu, et al, in [9] have discussed highlight difference of SCADA from standard IT systems. Also focus on cyber attack including cyber-physical attack on SCADA system. SCADA attacks including cyber-physical attack on SCADA system. SCADA are widely involved in the constitution of vital enterprises. SCADA have many characteristic of vital traditional IT system in terms of risks and operation priorities. These difference adjust goal of desirable security set like confidentiality, integrity, availability. Cyber attacks on SCADA system take routes through internet connection, business or enterprise network connection and connection to other network. Cyber attack on hardware is to gain unauthenticated access to remote device. The main issues in preventing cyber attack on hardware are access control. During attack, attacker tries to penetrate the layer of the network mainly network layer, application layer, and also on the protocol.

Irfan Ahmed, et al. in [10] have discussed the challenges and to investigate the possible solutions. SCADA term in this paper stands for all kinds of control system. The reach-ability of SCADA system toward wider network brings threats. In this paper, researcher also highlights the forensics of SCADA network. If any security breach happens then digital forensics of SCADA network will be the essential part of cyber defense. Digital forensic investigation will play important role in the SCADA network security. Another word which is used by researcher is “Live Forensics”. Since SCADA utility for 24/7 hours, that’s why SCADA system can’t stop for any type of digital forensic. Live forensic have to perform on SCADA network. During live forensic it acquire volatile and non-volatile both. It arise some challenges in forensic of SCADA network such as customize operating system kernel, inadequate logging and so on. For forensics they use tools for testing of data acquisition. It will not affect the availability of the SCADA system.

## III. CYBER-SECURITY APPROACHES

SCADA system which is now considered as critical infrastructure is not designed for the general IT environment. It run as isolated network, not connect to the Internet. Now it adopts technology and evolved to communicate over public IP network or through internet, that’s why it needs cyber-security.

So there are following techniques which can provide cyber-security to the critical infrastructure like SCADA from the cyber-attack by attacker. Most of the sectors which implement SCADA in their organization, implement one of these techniques which we discuss below.

### *A. Network Intrusion Detection Sensor (NIDS)*

It is a device put on the network to evaluate the data which is transferring over the network. NIDS are connecting to the ports on switch and router which collect data and compare with the signature. There are four techniques which is used during to detect and analyze the attack signature are; matching, frequency crossing, correlation of lesser events, and statistical anomaly detection [11]. Through such type of device we can provide security to the communication links. These current devices are excellent against kiddies hackers who get exploit easily through internet because hackers use http protocol for attack and these devices have no knowledge or intelligence of SCADA application and protocol. [12]

The use of NIDS may be beneficial to some extent such as the implementation of IDS is comparatively having low cost. NIDS can implement at the interface to the internal network. There is no need to deploy at every machine for protection. The main feature of NIDS is to analyze the live data of network for detection of any type of attack. [13]

### *B. Host Intrusion Detection Sensor (HIDS)*

HIDS is software installed on a host computer system. It monitors the activities of the users and the process whether it involves in malicious activity or not. Mainly it analyzes the internal data, and if it find any intrusion it reconfigure itself automatically. The feature of reconfigure automatically prevents it from exploitation. [14]

Some benefits of HIDS such as it do not require any extra hardware and have ability; to handle encrypted data, to detect file access activity such as changing, permission, or attempt to install new software, to monitor administrative activities such as adding, and deleting. [15]

### C. *Cryptography*

Cryptography provides encryption facility for the communication between clients. To maintain the authenticity, integrity, confidentiality of the message over the network is very important because attacker can attack on the network by which CIP of the message or data can compromise. That’s why SCADA system also adopts cryptography to secure its communication among different sector which implement SCADA. SCADA system adopts famous cryptographic approach which is commercially available such as secure socket layer (SSL), internet protocol security (IPSec), transport layer security (TLS) framework. SSL also use symmetric algorithm like; DES, triple DES, to validate data integrity. These frameworks are used throughout the internet and less expensive than those which are particularly made for SCADA networks. [16]

*D. Honey-pot*

Honey-pot is the trap in an IT system that is used to distract the attacker from critical resources. Honey-pot is a technique which is used to detect ongoing attack, to obtain attack data detail, to identify new threats and hacking approaches. Honey-pot is currently testing in the SCADA system, so that can know, honey-pot is capable to protect the SCADA system or not. SCADA honey-pot gathers the information about the attack which is performed by the attacker and their approaches. It is much similar like honey-pot deploy in non-SCADA applications. [17]

Above we discuss four techniques which provide security to SCADA system. If we compare these techniques to find, which one can provide more security to SCADA system, then it will be cryptography. Cryptographic technique has number of algorithm which is used for encryption. If these entire algorithms are used together, it provides strong encryption for message and increase security of SCADA communication.

## IV. CONCLUSION

As we know that human life is totally depend on the technology. Every critical infrastructure accepts technology and they connect to each other through internet. If anyone of them is stop to work, it can impact serious damage to the nation economy, public life, safety and so on. That is the reason, critical infrastructure also need cyber-security than physical security or any type of security.

Every sector use different type of techniques to provide cyber-security to an organization as we discussed above. But none of them can provide better security, that's why we have to need another new technology, new tool, and new algorithm, to increase the security which previous one can't provide.

In future, Critical infrastructure use more advance technologies to secure its infrastructure from cyber attack. At present it use one of them and try to implement those which is growing in this field.

## REFERENCE

[1] A. SHAHZAD, et al, "A New Cloud Based Supervisory Control and Data Acquisition Implementation to Enhance the Level of Security Using Testbed", Journal of Computer Science 10 (4): 652-659, (Science Publication, 2014).
[2] YONGGE WANG, et al, "sSCADA: Securing SCADA Infrastructure Communications", airXiv: 1207.5434v1 [cs. IT], July 2012.
[3] GIOVANNI A. CAGALABAN, et al, "Software Vulnerability Design and Approaches for Securing SCADA Control Systems", Vol. 3, No. 1, International Journal of Smart Home, 2009.
[4] Vinay M. Igure, Sean A. Laughter, Ronald D. Williams, Security issues in SCADA networks, ELSEVIER, Computers & Security 25 (2006) 498 – 506
[5] ROSSLIN JOHN ROBLES, et al, "Vulnerability in SCADA and Critical Infrastructure System", International Journal of Future Generation Communication and Networking.
[6] AAMIR SHAHZAD, et al, "Cryptography and Authentication Placement to Provide Secure Channel for SCADA Communication", International Journal of Security, Volume (6): Issue (3): 2012.
[7] AINE MACDERMOTT, et al, "Intrusion Detection for Critical Infrastructure Protection", ISBN: 978-1-902560-26-7, 2012.
[8] THOMAS MORRIS, et al, "A Testbed for SCADA Control System Cybersecurity Research and Pedagogy".
[9] BONNIE ZHU, et al, "A Taxonomy of Cyber Attacks on SCADA Systems".
[10] IRFAN AHMEN, et al, "SCADA System: Challenges for Forensic Investigators".
[11] DALE PETERSON, "Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks", 2004
[12] SINCLAIR HANSEN, "An Intrusion Detection System for Supervisory Control and Data Acquisition Systems", 2008
[13] SINCLAIR HANSEN, "An Intrusion Detection System for Supervisory Control and Data Acquisition Systems", 2008
[14] DALE PETERSON, "Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks", 2004
[15] SINCLAIR HANSEN, "An Intrusion Detection System for Supervisory Control and Data Acquisition Systems" 2008.
[16] WALEED H. ELSAID, "Enhanced Cryptographic Approaches for SCADA Network Security" 2010.
[17] Wade, Susan Marie, "SCADA Honey-nets: The Attractiveness of Honey-pots as Critical Infrastructure Security Tools for the Detection and Analysis of Advanced Threats" (2011). Graduate Theses and Dissertations, Paper 12138.