Network and Industrial Control Systems (SCADA) Security in the Oil and Gas Industry

Ali Abdollahi, Kamyar Abedi

***Abstract*— one of the main causes of attacks on oil industry is the use of vulnerable industrial control systems (SCADA) and the lack of implementation of security requirements in dependent companies. This leads to an increase in attacks against this industry in recent years. The purpose of this paper is at first, a report of vulnerabilities on the industrial control systems on oil and gas industries like SIEMENS, ABB and…, attacks statistics on oil companies in the Middle East like Iran and Qatar Oil Companies; and at the following we study on motivation of attacks that are political agenda, Causeless or done for fun.**

Finally, we provide secure solutions in different layers of SCADA systems, Communications and related networks, Members security and physical security of Gas and Oil Networks.

***Index Terms*— SCADA Security, Cyber Attacks, Hardening, Security in Gas and Oil**

I. INTRODUCTION

At the present time, whenever weaknesses or vulnerabilities are discovered in the system, hardware and software manufacturers quickly analyze it and try to update and introduce security patches. Using this process is not enough to deal with vulnerabilities in communication infrastructure of critical industries [1]. Hardware and software components used in the most sensitive industries such as oil, gas, and petrochemical industries play an important role in their industrial control systems and should be designed and used safely. As this equipment is mainly supplied as a complete package to the customer by manufacturers and customers do not know the internal structure and its possible vulnerabilities, there is the possibility of threats that result in huge losses.

One industrial control system is SCADA that is widely used today in most oil and gas industries [2]. SCADA systems are offered as a package to clients and the level of knowledge about their performance is generally low, so in case of any problems, the consumers of these systems will not be able to fix them [3]. In recent years, some attacks have been made on the industrial control systems of which the attack made to ABB product in 2013 can be noted [4].

In the attack, three products of ABB Company were influenced by the attack of execution of vulnerability using a remote code. This vulnerabilities allows attackers to exploit and penetrate into the system, causing malfunctions. In 2011, a serious vulnerability was discovered in SCADA control system (S7-1200PLC) of Siemens [5]. The vulnerability allowed the hacker to disable CPU, removing and adding programming code in memory, eliminating the security controls and complete remote control over all PLC. Another attack was reported from two very dangerous vulnerabilities in SIMANTIC WinCC and TIA Portal SIMANTIC PCS7 [6]. The first vulnerability with CVE-2014-8551 code has damage intensity 10 of 10 that allows the attacker to execute remote code. The second vulnerability with CVE-2014-8552 code has damage intensity 7.8 of 10 that allows the attacker to have access to send-receive packages of the system and therefore has the ability to read the files and batch numbers stolen remotely. In 2015, a serious vulnerability among several other vulnerabilities was discovered on systems of Honeywell Company that had 10 of 10-destruction intensity. This security leak on Web SCADA allowed the hacker to have full access to the system [7]. Thus, the attacker can access some information and privacy settings and even edit them.

In 2012, and just two years after the attack on the Iranian Natanz nuclear site SCADA systems, release of computer malware known as Viper with cutting the link of the central sever server and several subsidiary of oil, gas and petrochemical companies became a headline [8].

This malware is of Remote Access Trojan (RAT) type and has the ability to transfer from one system to another. The malware gives a lot of functionality to the hackers remotely, of which sending or receiving a variety of files, access to browsers, and data stored on the victim's system can be noted. After the attack, the Ministry of Petroleum of the Islamic Republic of Iran started to clean all target systems.

In 2012, this time, the second major oil company of Qatar called RasGas was targeted by an unknown virus. The malware created a serious disorder by turning off email servers and website of the company in domestic and international economic affairs [9].

II. SECURE COMMUNICATION PLATFORM

Securing communications platform includes links LAN, WAN, wireless networks, MPLS platform and all network equipment such as routers and switches. It should be noted that the use of security devices such as firewalls, intrusion detection and prevention systems.

III. SECURITY IN INDUSTRIAL CONTROL SYSTEMS

In general, the motivation of hackers from infiltrating and disrupting oil and gas companies is divided into two categories [10]:

1. The first category consists of politically-governmentally motivated hackers who carry out such acts. In these cases, attack intensity is much higher than that of other types.
2. The second category of hackers is not affiliated with any government and attack as socio-cultural groups

Manuscript received October 05, 2019
Ali Abdollahi, Senior Security Consultant Tehran, Iran
Kamyar Abedi, Senior Security Consultant Tehran, Iran

and with the aim of awakening and objecting to governments and politicians.

3. The third category is the attackers who do such dangerous acts with no intention nor support and just for curiosity. Sometimes these people even do not know to whom and what institution the targets they are attacking and destroying belong.

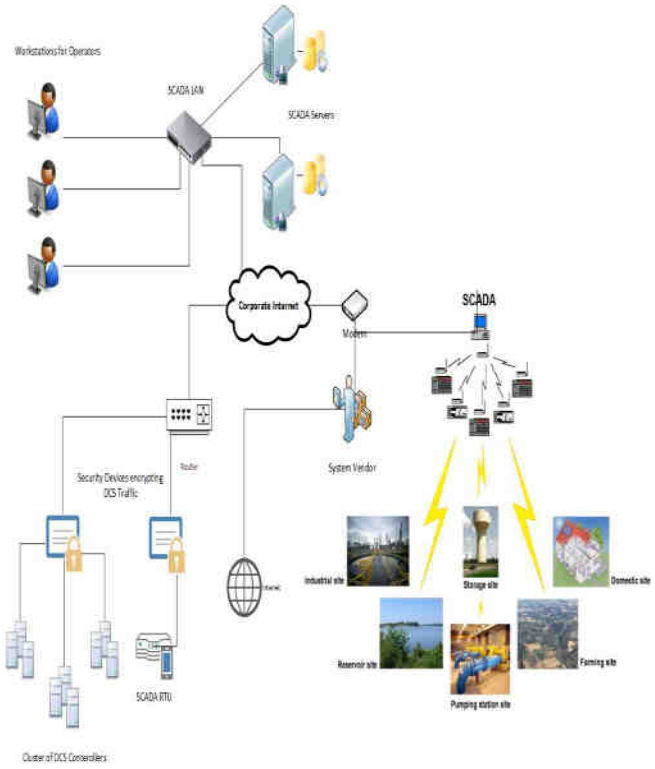

Figure 1. The security model for industrial control systems

IV. A MODEL TO SECURE

In this section, a model is presented for securing SCADA industrial control systems. Figure 1 is the model based on multi-layered defense that includes the following:

A. Multi-Layered defense

In this layer, security includes the security of network and security management. In network security, both hardware and software must be considered. To consider security in these sectors, network can be secured in the following three perspectives:

- Core network security:

This can be done by securing the communication and protocols used by Network Equipment (It should be noted that should, of the security features of this equipment like port security and Dynamic ARP Inspection) as well as the use of safety equipment such as firewalls, detection systems, and intrusion prevention and honeypot.

- Network Management:

Network management should be comprehensive and vendor less i.e. management software and hardware systems must be compatible with all the different products.

- Security in application programs

Security in applications includes the following ranges:

1. Web-based applications:

These programs include web mail service, ERP systems, internal automation and so on that are very sensitive and important points are for hackers.

2. Operational programs:

The application range of these applications is very broad and in general includes all the applications that organization users work with them locally and offline: such as monitoring software and so on.

However, securing solutions for the mentioned applications is listed below:

- Security review of source codes
- Implementing security in security testing laboratory for behavior
- Access control

B. Security Management

In security management, standard rules should be implemented under organization [11], including the following:

- security policy
- monitor and log
- Password
- Human resources security
- Physical and environmental security
- Communication Management and Operations
- Access Control
- control, storage and backup

V. SECURING PROCESS

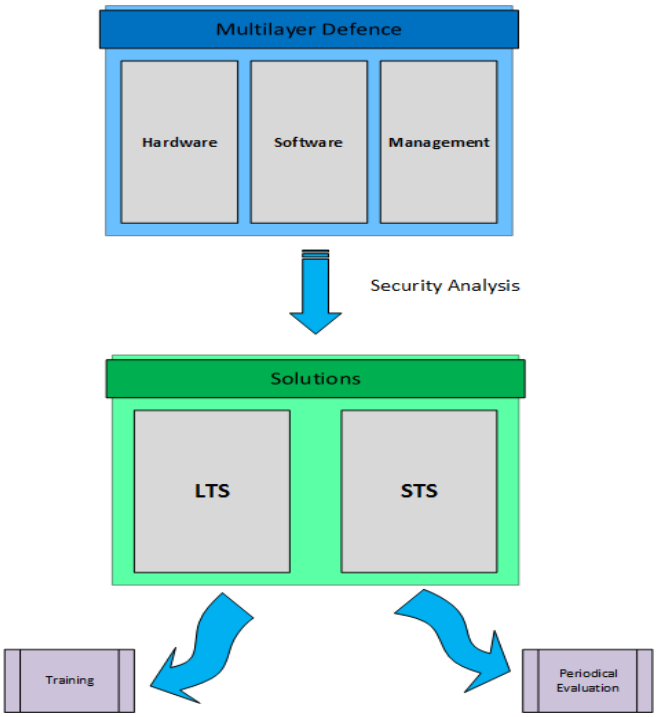

Figure 2. The process of securing industrial control systems

Security assessment is done on hardware, software and management part according to Figure 2. The result of this assessment leads to providing short-term and long-term solutions. These solutions leads to SCADA industrial control

systems security. To continue security in SCADA industrial control systems, training every individual personnel, managers, and professionals involved in the network is essential. Periodic evaluation, implementation, and running short-term and long-term solutions should be carried out regularly.

Security is divided into several layers not only in oil, gas and petrochemical sector but in all industries and organizations as follows:

- Securing industrial control systems
- Implementing Security Operations Center
- Implementing ISO 27001 standard
- In this section, we examine the items listed.

A. Securing in industrial control systems

This section should be secured in two layers. First, protocols and the communications between them must be secured, and second is that security systems is used to verify package (TCP Packet) and appeals sent to the SCADA system.

B. Implementation of Security Operations Center (SOC)

Implementation of security operations at oil companies play a significant role in detecting and preventing attacks, because at this center all the events and any suspicious behaviors are identified and followed. Thus, by using SOC, can quickly react and prevent the occurrence of infiltration and disruption of networks against cyber threats.

C. Implementing ISO 27001 standard

With the implementation of security requirements for information security-management system, one can cover all macro-policy and security policy of the organization that include in all areas of an oil and gas a company.

CONCLUSION

Industrial companies generally, to control their processes, need control systems and defects in them can cause them significant losses. One of the things that can affect their control in the industry of the performance of their control systems is the existence of security vulnerabilities in control networks that by creating security threats allows vandals to have access to different sources, to disrupt the network performance under load.

Given the importance of this issue, in this paper, by reviewing past attacks and vulnerabilities in industrial control systems, the security model to secure industrial control systems was developed that includes hardware, software and management parts (Figure 2). With this model (Figure 1), one can take effective steps to secure industrial control systems.

REFERENCES

[1] Impact Of Network Infrastructure Parameters To The Effectiveness Of Cyber Attacks Against Industrial Control Systems Béla Genge, Christos Siaterlis, Marc Hohenadel, 2014.

[2] Research on the Integrated Attack-Defense Simulation Platform Architecture of the large-scale oil and gas gather-transferring SCADA system Jie Li1, a, Xiedong Cao 2, b, Li Yang 3, c, 2015.

[3] Global and initiative safety mechanism in industrial control system Xinguo Xu, Wei Kang, Zhiqi Fang, Baohui Sun, Yan Wang, Tingshao Zhu, 2015.

[4] Cyber Security of Smart Grid Infrastructure Adnan Anwar, Abdun Naser Mahmood, 2014.

[5] PLC Monitoring and Protection for SCADA Framework an AlShemeili, CY Yeun, J Baek, 2014.

[6] Siemens Security Advisory by Siemens ProductCERT SSA-134508: Vulnerabilities in SIMATIC WinCC, PCS 7 and WinCC in TIA Portal, 2014.

[7] Acknowledging the Threat: Securing United States Pipeline Scada Systems Hellmann, Hillary, 2015.

[8] Security and privacy challenges in industrial internet of things Ahmad-Reza Sadeghi, Christian Wachsmann, Michael Waidner, 2015.

[9] Conflict in Cyberspace: The Case of the Middle East O Danino, 2015.

[10] Sean Atkinson, Christopher Walker, Psychology and the hacker – Psychological Incident Handling GIAC (GCIH) Gold Certification, June 20, 2015

[11] ISO/IEC 27001