ANNALS OF THE ORADEA UNIVERSITY
Fascicle of Management and Technological Engineering
ISSUE #1, MAY 2014, http://www.imtuoradea.ro/auo.fmte/

DEPENDABILITY AND VULNERABILITY OF SCADA SYSTEMS

Nicoleta IGNAT
University Politehnica of Bucharest, nicoleta_ignat@yahoo.com

***Abstract*—**In the last years, the security of critical infrastructures followed a decreasing trend due to the apparition of new cyber threats against Supervisory Control and Data Acquisition (SCADA) systems. As the increasing interconnections have made SCADA systems more vulnerable to attacks and risks, an emergent need to mitigate these risks appeared. While SCADA systems protection is extremely poor and needs to be upgraded to withstand cyber attacks of all forms, cyber security problem requires multidirectional approach considering many different aspects of vulnerabilities in the system. This paper analyzes the SCADA network vulnerabilities with respect to cyber security and tries to find countermeasures for the most common attacks.

***Keywords*—**attack, measures, risks, SCADA systems, vulnerability

I. Introduction

SUPERVISORY Control and Data Acquisition (SCADA) have been commonly used to monitor and control continuously processes of Critical infrastructures (CIs). CIs involve multi-dimensional, highly complex collections of technologies, processes and people, and as such, they are vulnerable to potentially catastrophic failures at many levels. Moreover, cross-infrastructure dependencies can give rise to cascading and escalating failures across multiple infrastructures [1].

SCADA systems are the largest subgroup of Industrial Control Systems (ICSs). ICSs are command and control networks and systems designed to support industrial processes [2], such as gas and electricity distribution, water treatment or railway transportation.

The infrastructure of the electricity sector consists of several facilities such as generating units, transmission lines, substations, transmission and distribution substation, control centers, remote terminal units (RTUs), intelligent electronic devices (IEDs) and communication links.

Each national, regional or local control centers contains one or several workstations, connected via Local Area Network (LAN), which is running different applications. These control centers interact with the supervisory and control systems, named Supervisory Control and Data Acquisition (SCADA) systems which interface with the hardware units (RTUs and IEDs), that in their turn monitor sensors and interface with the various physical devices (circuit breakers, transformers, breakers, switches, relays) [3].

SCADA systems form the backbone of industries in the areas of electric power, oil and gas, water and rail transportation [4]. They have been identified by the EU Commission as a core component of most critical infrastructures.

SCADA systems monitor and control many critical installations around the world, by providing with real-time centralized monitoring and control of industrial processes through a combined use of data acquisition and transmission systems and Human-Machine Interfaces (HMIs) and interpreting the information gathered from a multitude of resources in order to drive the physical processes to a desired state. As for the system to react correctly, the collected data from the sensors must be reliable, accurate and timely, regardless of distance and environmental conditions.

During the recent years, continued SCADA modernization and increased interconnection have determined a transition from closed, isolated networks to open, IP-based networks. Accordingly, SCADA systems are now considered to be part of the cyber infrastructure [5].

II. SCADA System Structure

SCADA systems are used to collect data from sensors and instruments located in remote locations and transmit them to a control center for supervision.

The components of a SCADA system include:

1) *data field devices such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) that interface with local sensors and actuators;*
2) *the communication network between the SCADA master and the field devices (slaves);*
3) *the SCADA master station located in the control center;*
4) *the Human Machine Interface (HMI) devices.*

The SCADA system is located in an industrial PC or workstation containing the HMI software that reads the remote stations and collect data in a database.

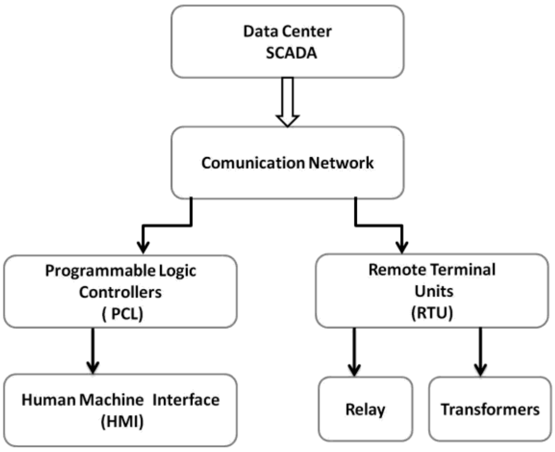
Data Center SCADA
Comunication Network
Programmable Logic Controllers (PCL)
Remote Terminal Units (RTU)
Human Machine Interface (HMI)
Relay
Transformers

Fig. 1. The components of a SCADA system.

The data acquisition is initiated first by RTUs and PLCs located between the remote sensors and control center. After reading the input connected to RTUs and PLCs, they transmit the data to the workstation in order to be processed. The components of the SCADA systems are represented graphically in the Fig. 1.

III. Risc And Vulnerability In Scada Systems

A major problem in SCADA systems security is related to the fact that many SCADA protocols in use today are still operating in unauthenticated clear text.

As SCADA communication networks need to be monitored in order to provide accurate and timely information about the network devices and their interactions, a considerable effort to improve SCADA protocols with security functionality is being put.

Another problem is related to the data collected by SCADA systems that are, in most cases, incomplete and corrupted. Data can be vulnerable to the cyber attacks of terrorists, hackers, hostile nations, but also there is a threat from natural phenomena and catastrophic events.

According to “Guide of Supervisory Control Data Acquisition (SCADA) and Industrial Control Systems Security” [6], there are three board categories of SCADA incidents: intentional attacks, unintentional consequences or collateral damage from viruses or control systems failures and unintentional internal security consequences: inappropriate testing or unauthorized system configuration changes.

Because of the complexity of this system, it is necessary to have a much more integrated and comprehensive methodology to identify where weaknesses might occur.

Many threats in the communication networks can be also applied to SCADA systems as they are connected to each other directly or indirectly. It is strongly believed that many SCADA systems are exclusive to other networks, but it has been proved many times that they are indirectly connected to the Internet through the facilities for on-line maintenance.

Threats to SCADA systems are classified into many kinds: authorization violation, unauthorized access violations of permission, bombs (logic or time, bypassing controls, browsing, illegitimate use, information leakage, data modifications, substitutions, intercept, replay, sabotage, spying, physical intrusion, trap door/ back door, trojan horse, tunnelling, virus, worms).

The possible attacks to SCADA systems can be grouped into the following categories:

1) *delaying or interrupting the data flow through corporate or control networks (denial of service);*
2) *changing programmed instructions in PLCs, RTUs or SCADA controllers;*
3) *sending false information to control system operations;*
4) *modifying control system software or configuration settings;*
5) *introducing malicious software into the system.*

Considering the different types of common cyber attacks [7], the following distribution is proposed.

The first category of attacks - backdoors and holes in network perimeter includes the following items.

Diagnostic Server Attacks through UDP port: Adversaries have access to the same debugging tools that any RTOS developers do. They can read symbol tables, step through the assembly, etc., considering also that many attackers don’t even need code-level knowledge

Smurf: is a type of address spoofing, in general, by sending a continuous stream of modified Internet Control message Protocol (ICMP) packets to the target network with the sending address is identical to one of the target computer addresses.

In the context of SCADA systems, if a PLC acts on the modified message, it may either crash or dangerously send out wrong commands to actuators.

The ARP is primarily used to translate IP addresses to Ethernet Medium Access Control (MAC) addresses and to discover other connected interfaced device on the LAN. The ARP spoofing attack is to modify the cached address pair information. By sending fake ARP messages which contain false MAC addresses in SCADA systems, an adversary can confuse network devices, such as network switches.

When these frames are falsefully sent to another node, packets can be sniffed; or to an unreachable host, DoS is launched; or intentionally to an host connected to different actuators, then physical disasters of different scales are initiated. Static MAC address is one of the counter measures for networks allowing this. Segmentation of the network may also be a method to alleviate the problem.

The second category includes the vulnerabilities in common protocols. Protocol vulnerabilities can turn themselves into segmentation faults, stack, heap or buffer overflows, etc., all of which can cause the protocol implementation to fail resulting in a potential exploit.

There are several attacks that specifically exploit the implementation of TCP/IP protocols in Windows. Although there are patches available, restrained to be on-line continuously, it's very likely that these machines do not have up-to-dated patches. Here, we only name a few well known ones are mentioned: WinNuke that takes advantage of the absence of status flag URG in handling the TCP protocol; TearDrop/NearTear and Ssping that utilize implementation error of fragmentation handling in TCP/IP protocol.

A nightmare scenario can be that one company's network is compromised and a polymorphic worm takes down most servers and any un-patched SCADA servers running Windows. Secondly, these protocol stacks can and do suffer from various vulnerabilities commonly found due to poor software design and coding practices

ICCP - The most serious and exposed SCADA protocol stacks are those that are used to exchange information with business partners, such as ICCP, or those used to exchange information between the corporate network and control center network.

The third category is dedicated to communications hijacking and Man-in-the-middle (MittM) attacks. One of the most dangerously attacks is MittM attack that gives the attacker long time and absolute control over the control system.

The attacker could insert an invisible malware in the SCADA systems. In this way the attacker can operate the system and control software, egress through the network firewall and establish a connection with his platform. In the time the MittM devastate the system, the users think that everything is operating normally.

The only way to clear this out is to turf the control system and restore to an early backup if wasn't itself infected.

Another category includes cyber-attacks on hardware, and the most common attack is the doorknob-rattling attack. In this case, the adversary performs a very few common username and password combinations on several computers that results in very few failed login attempts.

This attack can go undetected unless the data related to login failures from all the hosts are collected and aggregated to check for doorknob-rattling from any remote destination.

The last category includes database attacks and my example is Structured Query Language (SQL) Injection. This attack occurs when an adversary is able to manipulate data input into a Web application, which fails properly sanitize user-supplied input, and to insert a series of unexpected SQL statements into a query.

Moreover, if a "command shell" store procedure is enabled, an attacker can move further to prompt level. The process will run with the same permissions as the component that executed the command. The impact of this attack can allow attackers to gain total control of the database or even execute commands on the system.

IV. An Optimization Of Security Function In SCADA Systems

One of the important difficulties encountered in monitoring the electric power systems is the nonlinear characteristic of its behaviour, forcing the use of numerical methods which are not suitable for the on-line monitoring because consume time and resources consuming.

These problems require developing security standards (to ensure interoperability representing obstacles for anyone attempting to establish secure communication) and regulations (to define what information must be included in a standard and how to react to a given set of conditions).

The increased use of control center databases in recent years has made control systems become more vulnerable to attackers.

There are several attack routes where internal and external attackers could use to gain access to the station power equipment or collected measures such as the corporate network, the wireless network.

The ultimate target of an attack is the control of workstations, specifically the HMI because there are the important bits including RTUs, IEDs, PLCs, Process control rules and Data.

In order to improve the security of industrial control systems, several measures can be taken including the use of firewalls, control accesses, encryption or intrusion detection systems (IDS).

IDS is defined as the process of monitoring events in a computer system or network and the analysis of such events looking for intrusion traces.

IDS helps in identifying corrupted information by attacks and foult injection from a malicious source. These systems can be characterised by different proposals for monitoring and analysis.

The IDS monitoring has three levels: network, host and application. The host-based level analyzes the information related to the host activities and states such as file-system modifications, applications logs and so on. Network intrusion detection systems (NIDS) analyze the traffic generated by a set of devices.

NIDS is frequently used in SCADA system unlike the host-based intrusion detection systems (HIDS) sensors who cannot be instaled in SCADA systems due to the limited resources of the components.

The analysis of events has two sections: detection by abuse or signature and anomaly detection. The first type investigates network activities that describe a type of attack. The second type determines attacks by identifying the system deviant behaviour. This model is preferred because anomaly detector has the ability to adapt to new types of attacks due to its dynamic behaviour.

The use of authentication and encryption in securing SCADA systems helps in proving the identity of users, access control and pad messages with random data to prevent an attacker from estimating the size or type of the transmission.

There are two main open standards for enforcing SCADA communication with security mechanisms. Cryptography Working Group (CWG) uses encryption to protect the data from SCADA networks as to authenticate the senders and receivers of the messages and to ensure data integrity.

The second mechanism is the IEC 62351 standard that enhances the security of the IEC 60870-5 protocol, widely used in Europe for SCADA masters to RTUs communications. This standard allow the receiver to verify the source of the message (an authorized user) and if the message was tempered during the transit.

Another solution to prevent cyber-attacks over ICS is to completely separate the two networks that exist in any organization: the Enterprise network running the business and the ICS network running the control system and processes.

In this way, nothing like malware from the business network can cross over into the control system and damage controllers. This measure helps in protecting the control system from any damage from an attack on the enterprise network or vice versa.

This is a difficult task because there are too many shared systems between both networks but applying appropriate configuration like perimeter-in or control system-out approaches could harden the control system network.

The ideal ICS security should include the following topics [8]:

1) *Early anomaly detection;*
2) *Methodologies to manage and integrate logic and physic threats;*
3) *Improved forensic techniques to support criminal law enforcement;*
4) *Patching and updating equipment without disruptions;*
5) *Making contact with the existing security programmes at European Union and National level, such as the European Framework Programme.*

V. Conclusion

SCADA systems are vulnerable to attacks and threats due to the vast number of resources and functions to be controlled, the increasingly automated manner of controlling of such and because they use old technologies. Although new software upgrades and secure equipment are available, it is difficult to adopt them in order to protect the systems from vulnerabilities. The resistance to change is based on the desire not to break anything.

It is considered that the slow progress of the SCADA systems is mostly caused by the lack of recognition on cyber security. The managers and workers in the field think the system is isolated and thereby it is safe while the reality is different. However the risk is real and many hacking incidents already happened on SCADA network. Therefore it is very critical to build the countermeasures against potential threats. The priority is to analyze and define the vulnerability points of the system and possible attack types. This paper specifies the threats to SCADA system and proposes generally accepted solutions in order to improve the security of SCADA systems in particular and ICS in general.

References

[1] W. Tolone, D. Wilson, A. Raja, W. N. Xiang, H. Hao, S. Phelps and E. Johnson, "*Critical infrastructure integration modeling and simulation: Inteligence and security informatics*", H. Chen, R. Moore, D. Zeng and J. Leavitt (Eds.), Germany: Springer, 2004, vol. 3073, pp. 214-225.

[2] V. M. Igure, S. A. Laughter and R. D. Williams, *"Security issues in SCADA networks"*, Computer & Security, 25 (7), pp. 498-506, 2006.

[3] M. P. Coutinho, G. Lambert-Torres, L. E. Silva, H. Lazarek and E. Franz, *"Detecting Cyber Attacks on SCADA and Other Critical Infrastructures"* In C. Laing, A. Badii and P. Vickers "Securing Critical Infrastructure and Critical Control Systems", IGI Global, 2013.

[4] NCS, *Supervisory control and data acquisition (SCADA) systems,* technical information bulletin NCS TIP 04-1, Arlington, VA, 2004.

[5] DHS and DoE, *Energy: Critical infrastructure and key resources, sector-specific plan as input to the national infrastructure protection plan*. Departament of Energy, 2007.

[6] K. Stouffer, J. Falco and K. Kent, *Guide to supervisory control and data acquisition (SCADA) and industrial control systems security,* Recommandations of the National Institute of Standards and Technology Special Publication, 2006.

[7] D. J. Kang, J.J, Lee, S. J. Kim and J. H. Park, "*Analysis on Cyber Threats to SCADA systems"*, IEEE T&D Asia, 2009

[8] P. H. Jenney, "*ICS Software Protection"* In C. Laing, A. Badii and P. Vickers "Securing Critical Infrastructure and Critical Control Systems", IGI Global, 2013.