The 12th International Conference on Business Information Security

(BISEC-2021), 3rd December 2021, Belgrade, Serbia

SECURITY OF GOVERNMENT CRITICAL INFRASRUCTURES WITH SCADA

MILOŠ JOVANOVIĆ

Belgrade Metropolitan University, Faculty of Information Technologies, milos.jovanovic@metropolitan.ac.rs

IGOR FRANC

Belgrade Metropolitan University, Faculty of Information Technologies, igor.franc@metropolitan.ac.rs

MILOŠ S. DRAŽIĆ

Belgrade Metropolitan University, Faculty of Information Technologies, milos.drazic@metropolitan.ac.rs

NENAD BIGA

Graduate School of Business, La Salle University, Philadelphia, United States, nenadbig@gmail.com

BOJANA TOMAŠEVIĆ DRAŽIĆ

Belgrade Metropolitan University, Faculty of Information Technologies, bojana.tomasevic@metropolitan.ac.rs

Abstract: *In a world where speed, efficiency, as well as access to an ever-growing amount of information and services are of strategic importance, the digital environment is what provides the necessary level of functionality that can meet the needs of society as a whole today. In that sense, the digital environment represents a paradigm and a necessary assumption on which the functioning of a wide range of data and services that are part of the so-callled critical infrastructures. As an interdependent, networked system, critical infrastructures provide fundamental services that are important for security, economic growth and prosperity, as well as social welfare and well-being. Critical infrastructures are based on services and related technologies that cover the production and distribution of energy, agriculture, banking and finance, transport and telecommunications, etc. Successful monitoring and control of these resources are widely implemented globally through the SCADA system service. The priority given to the robustness and operability of SCADA services often results in an insufficient level of security and network security problems, which will be addressed in this paper.*

Keywords: *Information Security, Critical Infrastructure Systems, SCADA*

1. INTRODUCTION

Awareness of the scale of the threats that cyber-attacks can have on critical infrastructures has grown significantly in recent years. Today, it can be said that practically every sector is endangered by cyber-attacks, with a special emphasis on the field of public health, energy production and telecommunications. In that sense, special attention must be paid to the monitoring and control systems, which are vital for their functioning. Efficient operation and functioning of critical infrastructure, as well as timely optimization, through real-time data collection and analysis, has been achieved globally through the implementation of the SCADA system. Weaknesses of SCADA systems and their vulnerability to cyber-attacks, could potentially lead to a violation of the integrity of critical infrastructure resources with unforeseeable consequences for society globally. SCADA control systems typically include sensors, actuators, and associated control software, which are deployed in widely dispersed locations. Due to the high exposure of these devices, it is necessary to use the best safety practices by the personnel who have access to them. The importance of SCADA devices is all the greater if we take into account that not only critical infrastructure, but also systems such as HVAC, traffic control and building automation rely on their proper functioning [1]. In order to best prevent cyber-attacks, it is necessary to identify the weaknesses and

potential vulnerabilities of the SCADA system. The current status requires the establishment of security countermeasures, which is something that the governments of Western countries were the first to recognize.

2. BACKROUND

The importance of critical infrastructure can be seen through the global, generally accepted practice of a well-run state and socio-economic order. The key indicators by which this is measured are voice and accountability, political stability, the absence of violence, government efficiency and quality regulation, rules of law and control of corruption. It is information and communication technologies (ICT) that have helped develop transparency, government accountability and reducing corruption, through the direct participation of citizens in government, the avoidance of mediation and the development of democracy [2]. The mentioned progress is being achieved to a great extent by achieving the goals set by the security of an informational system, which are integrity, confidentiality, secrecy, availability, accountability and information assurance [3]. Data, as a fundamental element of any information architecture, is sampled, exchanged, presented and stored with the help of adequate equipment, and it is the security of the system that is applied in order to preserve the attributes of the data. These include availability (access to information uninterrupted by malicious denials of service or unauthorized deletions), integrity (guaranteeing the protection of information from any kind of modifications) and confidentiality (access to information is allowed only to authorized personnel). All these are prerequisites for the reliable functioning of the entire information system. Through the proper functioning of the critical infrastructure, a reliable flow of products and services that are crucial for the defence and economic security of the country is enabled, as well as the uninterrupted work of governance at all levels and society as a whole [4]. All critical infrastructures are complex in the sense that they are interacting components in which change occurs through the learning process. This allows us to define general appearance of multiple infrastructure and to take into account interdependencies and multiple connection points accordingly [5]. Initially, SCADA systems relied on primitive serial protocols and communication infrastructures to link SCADA components and to transport control and data messages. This was accompanied by the absence of security mechanisms. Therefore, standards have been created that adopt security solutions to mitigate risk in industrial control environment. Applied to critical infrastructure installations, SCADA systems must meet specific security requirements and develop appropriate security mechanisms and strategies [6], [7]. The consequences that cyber-attacks can have on critical infrastructure are so devastating that at the level of state sovereignty and integrity they can be considered a terrorist attack or even an open act of aggression and declaration of war in the same way traditionally seen, through engagement. army and military resources. The problem, however, is that the very nature of cyber-attacks, through the relatively easy manipulation of forensic evidence, does not allow the individual or nation-state behind such activity to be easily identified.

3. THE CURRENT ROLE

Today, cyber-attacks have become so complex that they can cause systems shutdown, disrupting operations or even remote control over the attacked systems. Attacks of this kind on critical infrastructure have dramatic consequences on economic security, public health, safety, and even physical survival itself. SCADA systems, as vital elements of critical infrastructure, control pipe lines, refineries, chemical plants, utilities, water and transportation systems, as well as manufacturing operations, etc. SCADA functionalities include:

- Access control: users are divided among groups who are given different, well-defined privileges to the process parameters of the system and to specific product functionality.
- Multimedia interface: supports multiple screens, displaying combinations of diagrams and text.
- Trending: provides trending facilities, summarizing common capabilities through a chart or image.
- Alarm handling: Information exists only in one place, all users see the same status, i.e. acknowledgment, and priority levels of multiple alarms are supported. It is possible to group alarms and manage them as aggregation.
- Logging/archiving: logging, as a medium-term storage of data on a disk, is typically performed when the appropriate file size, period, or multiple points have been reached, and the existing data is overwritten. Archiving, like long-term storage of data on a disk or some other permanent medium, can also mean the transfer of logged data once the log is full.
- Report generation: reports can be sent using SQL type queries to the archive, real-time databases, or logs.
- Automation: the action is triggered automatically after the observed event [8].

SCADA provides real-time management, effectively implements control, raises the level of security of the supervised structure and its employees and reduces costs. All these benefits are possible due to the use of standard hardware and software in SCADA systems, as well as improved communication protocols and increased connectivity to outside networks, including the Internet. The price for these benefits is increased vulnerability to attacks or errors coming from both external and internal sources.

Typically, SCADA systems include human-machine interface (HMI) that is responsible for presenting data to the operator, remote terminal units (RTUs) used for connecting sensors in the plants, converting signals to digital data and sending this data to the supervisory system, the monitoring system responsible for data acquisition and

process activity control, programmable logic controllers (PLCs) which are final actuators used as field devices as they are more economical, flexible and configurable than, for this purpose designed RTU, communication infrastructure that connects the supervisory system to the RTUs and/or PLCs, various processes and analytical instrumentation [9]. The traditional SCADA system consists of a host computer, some RTUs, the operator terminals and PLCs. In addition to the components already mentioned, it also includes a SCADA meter used for gathering data from (acquiring) and sending commands (control) to a plant [10].

In order to better understand the threats, it is necessary to have a good understanding of the functioning of the SCADA system, and for that purpose it is good to look at the schematic SCADA architecture in a modern power plant (Image 1). As a central master system, SCADA controls RTUs which consist of relay devices, actuators and sensors, circuit power breakers, voltage regulators, etc. Higher-level units are the so-called master level units (MTUs), including supporting applications, HMIs, data storage and acquisition systems. RTUs and sensors control goes via PLCs, while programmable automation controllers are used as the basic controlling unit.

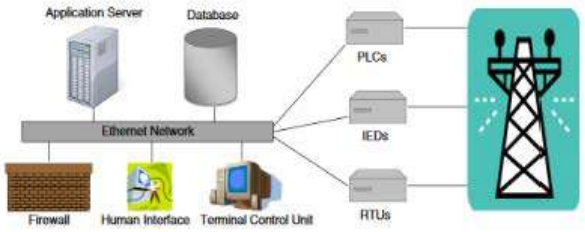

Image 1: SCADA architecture in modern power grids

There are three generations of SCADA system architecture, which rely on different solutions in the sense of communication between MTUs and RTUs. The first generation uses wide area networks (WAN), the second generation relies on local area networks (LAN), while the third generation uses WAN and Internet Protocol (IP). The communication component of the SCADA architecture, for example, includes Ethernet, wireless networks and Modbus and DNP3 protocols. Devices that are part of the SCADA architecture are generally controlling and controlled devices, which are run on embedded operating systems to communicate data primarily using protocols such as Modbus or DNP3. Attacks on the SCADA system pose a threat to human security, loss of productivity and environmental damage [11].

4. CHALLENGES, IMPACT AND SECURITY

Vulnerabilities in critical infrastructure have increased by 600% in the last decade, based on data presented in NSS Labs' Vulnerability Threat Report. This report pointed to an increase in hardware and software vulnerabilities related to the industry, as well as the obsolescence of a large number of SCADA systems. Main issues are:

- Increased exposure, as smart devices and systems create many access points;
- Inter-connectivity as a consequence of communication networks, which makes the system more exposed;
- Complexity of the electric system due to the interconnection of a large number of subsystems;
- Common computing technologies, because smart grid systems will increasingly use commercially available technologies and thus be subject to their weaknesses;
- Increased automation, because smart grid technology will automate many functions, and improper use of this data poses a new risk.

During 2012, The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) monitored 171 unique vulnerabilities affecting ICT products, coordinating the vulnerabilities with 55 vendors. The results of this tracking can be seen in Table 1.

Vulnerability type	**No.**
Buffer overflow	44
Input validation	13
Resource exhaustion	8
Cross-site scripting	8
Path traversal	8
Resource management	8
Access control	7
Hard-coded password	7
DLL hijacking	6
Other	39
Miscellaneous	15

Table 1: Vulnerabilities by type ICS-CERT 2012.

Key infrastructure challenges include:

- Secure interoperability between systems from different agencies;
- Development of methods and measurements of civic participation in democratic processes;
- Encouraging public and private partnerships and other networked organizational forms;
- Archiving and management of electronic records;
- Developing better methods for managing IT resources;
- Ensuring the availability and equality of access to data.

The overall security of critical infrastructure must be audited throughout the life cycle of its components. Authentication, access control and audit form the basis of information systems security. These three elements are interrelated: authentication, as an identification process, is a prerequisite for access control, while access control

places restrictions on the actions performed by the authenticated user. Finally, possible security breaches can be identified through an audit process that collects data on activities and actions. In this sense, audit and monitoring logs are of the utmost importance. While in the case of an audit, information is obtained when the event has already passed, monitoring provides real-time information. The application of these two techniques should bring similar benefits to the security of SCADA systems as it has already brought to IT systems. Technical audits of SCADA devices and networks are critical to security. Today, there are many commercial and open source security tools that allow audits to be conducted on systems and networks to identify activities, patch levels, and common vulnerabilities. The problem that arises in this regard is in the components of SCADA systems that are of different ages and sophistication, which is why for many of them there is no capability of logging [12]. The costs of eliminating such disadvantages must be weighed against the potential benefits. In addition to the above problems, the question of the proprietary protocol also arises. Some SCADA systems use unique proprietary protocols for communications between field devices and servers. Often the security of SCADA systems is based on the security of these protocols, but these protocols provide very little security. Most SCADA systems currently in use have no security features at all. Modems, wireless, as well as wired networks used for communication and maintenance, are a significant vulnerability for SCADA networks and remote sites. In general, any location connected to the SCADA network is a target, especially unmanned or unguarded sites. To ensure the security of SCADA networks, the following steps need to be taken:

- Identify all connections to the SCADA network, through conducting a risk analysis to assess the risk and necessity for the existence of each of the connections.
- A good understanding of how all connections work and how those connections are protected.
- Disconnect all unnecessary connections.
- Isolate the SCADA network from other networks as much as possible.
- Evaluate the security of all remaining connections to the SCADA network by conducting penetration testing or vulnerability analysis.
- Use this information, along with the risk management process, to develop a protection strategy to strengthen the remaining connections [13].
- Strengthen SCADA networks by removing or disabling unnecessary services.
- Because SCADA control servers, built on commercial or open source operating systems, can be vulnerable to attacks through default network services, unused services and network daemons should be removed or disabled to greatest degree possible. This is especially important when SCADA networks are interconnected with other networks.
- Do not rely on proprietary protocols.
- Implement security features provided by device and system vendors and in that sense insist that system vendor provides features through product patches or upgrades.
- Establish strong control over any medium that is used as a backdoor into SCADA network.
- Apply strong authentication where there are backdoors or vendor connections in SCADA systems.
- Implement internal and external intrusion detection systems and strategy and establish 24-hour-a-day monitoring that includes alerting network administrators of malicious activity.
- Perform technical audits of SCADA devices and networks and any other connected networks.
- Conduct a physical security survey and inventory access points at each facility that has a connection to SCADA system and assess all remote sites connected to the SCADA network to evaluate their security.
- Establish SCADA “Red Teams” to identify and evaluate attack scenarios as well as potential system vulnerabilities. It is necessary to gain insight into the weaknesses of the overall network, SCADA systems, physical systems and security controls [14].

5. CONCLUSION

Information technology has led to more and more connected and complex infrastructures with increased centralization of control. Risks related to the level of critical infrastructure security are high, and the consequences of compromising the security and integrity of critical infrastructure can be dramatic. Security issue should concern us all. Of great interest in governments is the assessment of the security of critical infrastructure and industrial control systems managed by private companies.

Control systems within critical infrastructure are particularly vulnerable to cyber-attacks. SCADA systems are growing in their complexity and integration tests are necessary in the deployment phase. By adopting best practices, such as Virtual Private Networks (VPNs) for remote access, or removing, disabling, or renaming any default system account, prevention can be provided.

Global collaboration and sharing of information regarding possible cyber threats and vulnerabilities of every device that is qualified on the market, will bring overall security [15]. The security component is of the utmost importance and the overall security of critical infrastructures must be audited throughout the lifecycle of its components.

REFERENCES

[1] A. Reha and A. O. Said, “Tri-band fractal antennas for RFID applications,” Wireless Engineering and Technology, vol. 4, pp. 171-176, Oct. 2013.

[2] P. Salatin and H. Fallah, “Impact of information and communication technology (ICT) on governance quality,”

European Online Journal of Natural and Social Sciences, vol. 3, pp. 250-256, Mar. 2014.

[3] J. Joshi, A. Ghafoor, W. G. Aref and E. H. Spafford, “Digital government security infrastructure design challenges”, Computer, vol. 34, pp. 66-72, Feb. 2001.

[4] H. Shorr and S. J. Stolfo, “A digital government for the 21st century”, Communications of the ACM, vol. 41, pp. 15-19, Nov. 1998.

[5] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies”, IEEE Control Systems Magazine, vol. 21, pp. 11-25, Dec. 2001.

[6] D. Kilman and J. Stamp, “Framework for SCADA Security Policy,” Sandia National Laboratories report SAND2005-1002C, Oct. 2005.

[7] E. J. Byres, M. Franz and D. Miller, “The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems,” IEEE Conf. International Infrastructure Survivability Workshop (IISW ’04), Dec. 2004.

[8] J. Gao, J. Liu, B. Rajan, R. Nori, B. Fu, Y. Xiao, W. Liang and C. L. P. Chen, “SCADA communication and security issues,” Security Comm. Networks, vol. 7, pp. 175-194, Jan. 2014.

[9] A. Daneels and W. Salter, “What is SCADA,“ presented at the 8th Int. Conf. on Accelerator and Large Experimental Physics Control Systems, pp. 339-343, Oct. 1999.

[10] D.J. Gaushell and W. R. Block, **“**SCADA communication techniques and standards,“ IEEE Computer Applications in Power, vol. 6, pp. 45-50, Jul. 1993.

[11] A. A. Creery and E. J. Byres, “Industrial cybersecurity for a power system and SCADA networks - Be secure, ” vol. 13, pp. 49-55, Jul. 2007.

[12] R. L. Krutz, “Securing SCADA Systems,” Wiley Publishing, Inc., 2005.

[13] M. Berg and J. Stamp, “A Reference Model for Control and Automation Systems in Electric Power,” Sandia National Laboratories report SAND2005-1000C, Oct. 2005.

[14] V. M. Igure, S. A. Laughter and R. D. Williams, “Security issues in SCADA networks, “Computers & Security, vol. 25, pp. 498-506, Oct. 2006.

[15] Office of Cybersecurity, Energy Security, and Emergency Response, “21 Steps to Improve Cyber Security of SCADA Networks,” Jun. 2011.