International Journal of Advanced Research in Engineering Technology & Science

ISSN: 2349-2819

Email: editor@ijarets.org Volume-8, Issue-1 January - 2021 www.ijarets.org

DETERMINE THE SCADA SYSTEM'S COMPONENTS AND CONSTRUCTION OF A COMPREHENSIVE CYBER SECURITY MODEL

Geetanjali Kumari

M.Phil, Roll No: 140437

Session: 2014-15

University Department of Computer Science

B.R.A Bihar University, Muzzaffarpur

Abstract

The Supervisory Control and Data Acquisition (SCADA) system is a basic framework that requires a complete cyber security model to defend against digital threats. In this paper, we distinguish the parts of a SCADA system, including equipment, software, and correspondence organizations, and the related weaknesses that can be taken advantage of by digital assailants. We likewise examine the improvement of a far reaching cyber security model for SCADA systems that comprises of different layers of protection, including access control, interruption recognition and counteraction, encryption, and occurrence reaction.

Keywords: SCADA (Supervisory Control and Data Acquisition) system, Cyber security, Threat modeling, Risk assessment, Security architecture, Security protocols

Introduction

Supervisory Control and Data Acquisition (SCADA) systems are basic for the proficient and safe activity of many modern cycles. With the rising dependence on technology and network, SCADA systems are progressively being designated by vindictive entertainers trying to upset or acquire unapproved admittance to modern cycles. Thusly, it is urgent to carry out extensive cyber security measures to shield SCADA systems from potential digital threats.

The improvement of a far-reaching digital protection model for SCADA systems includes the ID and examination of the different parts of the system, for example, the equipment, software, correspondence organizations, and human variables. These parts cooperate with one another in complex ways, and each presents a novel arrangement of weaknesses that can be taken advantage of by digital aggressors.

The objective of a far-reaching digital protection model is to recognize these weaknesses, survey the expected effect of digital threats on the system, and execute suitable security controls to relieve the risks. This includes the utilization of many security advancements and works on, including firewalls, interruption discovery and avoidance systems, encryption, access control, and occurrence reaction arranging.

Also, SCADA systems are often incorporated with different systems, including undertaking asset arranging and client relationship the board systems, which increment the intricacy of the network protection model. In this way, it is important to guarantee that these systems are likewise enough safeguarded and that the security controls are composed and coordinated across every one of the systems.

Introduction to SCADA Systems and Cyber security

Supervisory Control and Data Acquisition (SCADA) systems are a basic piece of current modern cycles, used to screen and control huge scope modern systems like power networks, oil and gas pipelines, and water treatment plants. Because of the significance of these systems, they have turned into an ideal objective for digital assaults, and their cyber security has turned into an inexorably significant concern. To shield SCADA systems from digital threats, a far-reaching cyber security model is essential. This model ought to incorporate different parts, for example, threat modeling, risk assessment, access control, network security, actual security, occurrence reaction, and cyber security preparing and mindfulness. This paper will examine the different parts of a complete SCADA cyber security model, and investigate the turn of events and execution of such a model to improve the security of SCADA systems.

Components of a Comprehensive SCADA Cyber security Model

A comprehensive SCADA cyber security model should include the following components:

1. Threat Modeling and Risk Assessment: This part includes distinguishing possible threats and weaknesses to the SCADA system, and surveying their probability and expected influence. A risk assessment assists with focusing on cyber security gauges and designate assets really.
2. Authentication and Access Control: This part includes laying out secure client confirmation techniques and executing access controls to forestall unapproved admittance to the SCADA system.
3. Network Security: This part incorporates measures to safeguard the SCADA network from digital assaults, like firewalls, interruption discovery systems, and organization division.
4. Physical Security: This part includes actual measures to shield SCADA equipment and offices from unapproved access or harm, like reconnaissance cameras, biometric access controls, and got fenced in areas.
5. Incident Response and Recovery Planning: This part includes fostering an arrangement for answering and recuperating from cyber security occurrences, including episode detailing methods, data reinforcement and recuperation, and system rebuilding.
6. Cyber security Training and Awareness: This part includes giving preparation and mindfulness projects to SCADA system administrators, directors, and other staff to build their insight and understanding of cyber security risks and best practices.
7. Compliance and Auditing: This part includes guaranteeing that the SCADA system is agreeable with applicable cyber security guidelines and standards, and directing occasional reviews to survey consistence and recognize regions for development.

Development of a SCADA Cyber security Model

The development of a SCADA cyber security model involves several key steps:

1. Identify the scope of the SCADA system: This step includes recognizing the particular resources and cycles that are remembered for the SCADA system, as well as any outer points of interaction or conditions.
2. Conduct a risk assessment: This step includes recognizing potential cyber security threats and weaknesses, surveying their probability and possible effect, and focusing on cyber security estimates in view of their risk level.

3. Develop a cyber security policy: This step includes fostering a proper strategy for safeguarding the SCADA system, which incorporates methods for access control, episode reaction, data reinforcement and recuperation, and consistence with pertinent cyber security guidelines and standards.

4. Implement cyber security controls: This step includes carrying out specialized and authoritative controls to safeguard the SCADA system, for example, access controls, firewalls, interruption discovery systems, and occurrence reaction plans.

5. Monitor and assess cyber security effectiveness: This step includes monitoring the adequacy of the cyber security controls over the long run, directing occasional reviews, and making changes depending on the situation to further develop the system's security pose.

6. Provide training and awareness: This step includes giving preparation and mindfulness projects to SCADA system administrators, supervisors, and other staff to expand their insight and understanding of cyber security risks and best practices.

7. Continuously improve the cyber security model: This step includes constantly evaluating and further developing the cyber security model to address new threats, weaknesses, and administrative prerequisites.

Threat Modeling and Risk Assessment for SCADA Systems

Threat modeling and risk assessment are fundamental parts of any exhaustive security procedure, particularly for SCADA (Supervisory Control and Data Acquisition) systems. SCADA systems are utilized in many basic foundation areas, including energy, water, and transportation. In that capacity, any weaknesses in these systems could have critical results, including disturbance of administrations or even actual mischief to individuals.

Here are some key steps for conducting threat modeling and risk assessment for SCADA systems:

1. Identify the assets: The most vital phase in threat modeling and risk assessment is to distinguish the resources that should be secured. On account of SCADA systems, this incorporates equipment and software parts, as well as any data put away or communicated by the system.

2. Identify the threats: Then, recognize the potential threats that could affect the SCADA system. These could incorporate digital assaults, cataclysmic events, actual assaults, or even human mistake.

3. Assess the vulnerabilities: When the threats have been recognized, evaluating the weaknesses of the SCADA system is significant. This includes investigating the system's architecture, protocols, and design to distinguish any shortcomings that could be taken advantage of by aggressors.

4. Determine the likelihood and impact of each threat: Subsequent to evaluating the weaknesses, deciding the probability and effect of every threat is significant. This includes considering elements, for example, the recurrence of the threat, the potential harm it could cause, and the probability of it finding success.

5. Prioritize risks: When the probability and effect of every threat not entirely set in stone, focusing on the risks is significant. This implies recognizing the risks that represent the best threat to the SCADA system and focusing on them for moderation.

6. Mitigate risks: At long last, it is essential to carry out measures to relieve the risks recognized during the risk assessment process. This could include carrying out specialized controls like firewalls, interruption recognition systems, or encryption, as well as non-specialized controls, for example, approaches and techniques for access control and occurrence reaction.

Conclusion

In Conclusion, an extensive digital protection model for SCADA (Supervisory Control and Data Acquisition) systems should be created to guarantee the security and versatility of these basic framework systems. This model should distinguish the parts of the SCADA system, including equipment, software, and data, and survey the likely threats and weaknesses that could affect the system. The improvement of the network protection model for SCADA systems should focus on risk relief and imply the execution of specialized and non-specialized controls, for example, firewalls, interruption location systems, access control arrangements, and occurrence reaction methodology. Given the rising recurrence and complexity of digital assaults on SCADA systems, associations liable for these basic framework systems should put resources into vigorous network safety measures to safeguard against expected threats. By taking on an exhaustive network safety model, associations can guarantee the proceeded with activity and dependability of their SCADA systems, defend basic foundation, and safeguard public safety.

Reference

1. Wei Ye and John Heidemann. Enabling interoperability and extensibility of future ’scada’ systems. In Proceedings of the National Workshop on Beyond ’SCADA’: Networked Embedded Control for Cyber Physical Systems, Pittsburgh, PA, USA, November 2006.
2. Cristina Alcaraz, Isaac Agudo, David Nuñez, and Javier Lopez. Managing incidents in smart grids à. Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011, pages 527–531, 2011.
3. Philip Church, Harald Mueller, Caspar Ryan, Spyridon V. Gogouvitis, Andrzej Goscinski, and Zahir Tari. Migration of a scada system to iaas clouds - a case study. Journal of Cloud Computing, 6(1):11, 2017.

4. P. Shakarian, D. Paulo, M. Albanese, and S. Jajodia. Keeping intruders at large: A graph-theoretic approach to reducing the probability of successful network intrusions. In 2014 11th International Conference on Security and Cryptography (SECRYPT), pages 1–12, Aug 2014.
5. V. Lakshmi priya and C. Bala Subramanian. A proposed architecture for scada network security. In 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), pages 142–145, March 2011.
6. Aditya Ashok, Adam Hahn, and Manimaran Govindarasu. A cyber-physical security testbed for smart grid: System architecture and studies. In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, page 20. ACM, 2011.
7. Hossein Ghassempour Aghamolki, Zhixin Miao, and Lingling Fan. A hardware-in-the-loop scada testbed. 2015 North American Power Symposium, NAPS 2015, pages 1–6, 2015.
8. Junho Hong, Shinn Shyan Wu, Alexandru Stefanov, Ahmed Fshosha, Chen Ching Liu, Pavel Gladyshev, and Manimaran Govindarasu. An intrusion and defense testbed in a cyber-power system environment. IEEE Power and Energy Society General Meeting, (July), 2011.
9. Adnan A. Farooqui, Syed Sajjad Haider Zaidi, Attaullah Y. Memon, and Sameer Qazi. Cyber security backdrop: A scada testbed. Proceedings - 2014 IEEE Computers, Communications and IT Applications Conference, ComComAp 2014, pages 98–103, 2014.
10. Nora Cuppens-Boulahia, Jorge E.López Cuppens, Frédéric and De Vergara, Enrique Vázquez, Javier Guerra, and Hervé Debar. An ontology-based approach to react to network attacks. Proceedings 2008 3rd International Conference on Risks and Security of Internet and Systems, CRiSIS 2008, pages 27–35, 2008.
11. Daniel Krauß and Christoph Thomalla. Ontology-based detection of cyber-attacks to scada-systems in critical infrastructures. 2016 6th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2016, pages 70–73, 2016.
12. John Bigham, David Gamez, and Ning Lu. Safeguarding SCADA Systems with Anomaly Detection, pages 171–182. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.
13. Hassan Lahza, Kenneth Radke, and Ernest Foo. Applying domain-specific knowledge to construct features for detecting distributed denial-of-service attacks on the goose and mms protocols. International Journal of Critical Infrastructure Protection, 20:48 – 67, 2018.
14. Béla Genge, Flavius Graur, and Piroska Haller. Experimental assessment of network design approaches for protecting industrial control systems. International Journal of Critical Infrastructure Protection, 11:24 – 38, 2015.

15. Chao-Rong Chen, Chi-Juin Chang, and Cheng-Hung Lee. A time-driven and event-driven approach for substation feeder incident analysis. International Journal of Electrical Power & Energy Systems, 74:9 – 15, 2016.
16. Robert M Lee, Michael J Assante, and Tim Conway. German steel mill cyber-attack. Industrial Control Systems, pages 1–15, 2014.
17. Robert Czechowski, Pawel Wicher, and Bernard Wiecha. Cyber security in communication of scada systems using iec 61850. 2015 Modern Electric Power Systems (MEPS), pages 1–7, 2015.
18. Krushna Chandra Mahapatra and S Magesh. Analysis of vulnerabilities in the protocols used in scada systems. International Journal of Advanced Research in Computer Engineering & Technology, 4(3), 2015.
19. Udara Perera. Comparisons of scada communication protocols for power systems, 2015.
20. Neel H Pathak. Modern scada systems. International Journal of Engineering Development and Research, 2(2):1693–1699, 2014.