IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 1, January 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201068 |

Issues and Challenges of Security in SCADA Networks

Vandna Kumari

Dept. of Computer Science Engineering, Dr. Shakuntala Misra National Rehabilitation University, Mohaan Road, Lucknow, U.P, India

ABSTRACT: The collected information and requests would be sent to the electricity supplier systems (control center) via a SCADA system. However, within the past few years, some of the existing SCADA systems had suffered from cyber attacks due to their existing vulnerabilities. Modern SCADA systems have a number of added features which increase the system complexities and are thus difficult to maintain. Some of the added features include control logic, communication protocols, user interfaces, and security. Moreover, the communications are vulnerable to various threats. In the past few years, the number of cyber attacks in general, is rising and has been affecting power station, water, gas, and nuclear control systems. The pattern of cyber-attacks has also evolved beyond the simple attacks such as Denial of Service or Man-in-the-Middle. The hackers gained access to the core command and control system by using a cellular modem. Thus, the schemes are categorized into detection of attacks on SCADA networks, and prevention of the attacks. It further explores and compares all the protocols that fall under each main category. It also addresses the security concerns and requirements that a SCADA security scheme needs to approach in future.

KEYWORDS: SCADA, complexities, communication, protocols, cyber and attacks.

I.INTRODUCTION

Nowadays, one of the indispensable critical infrastructures, such as water treatment facilities, chemicals plants and nuclear reactors to gas pipelines, dams and switches on train lines. The electric power systems are also adopting SCADA systems and producing intelligent networks called smart grid networks. In electric networks, controlling the electricity consumption in the house can be remotely enabled for the consumer, in order to fulfill their demands and avoid excess electricity gen-eration. This feature is made possible in the smart grid system by having smart meters and controllers, substations, power operator, and communication networks for monitoring, control and operation. Figure 1 shows a general architecture of a smart grid network. Each substation is monitored and controlled by a smart meter. All the smart appliances in the substation will be connected to a smart meter by internal wireless technology such as WiFi. The smart meter will communicate the collected information with its substation owner and the control center via the available communication network. The substation owner device (using a smart phone application) collects real-time usage information from the smart meter and can reduce the usage of the electricity by sending a request. The collected information and requests would be sent to the electricity supplier systems (control center) via a SCADA system. However, within the past few years, some of the existing SCADA systems had suffered from cyber attacks due to their existing vulnerabilities. Modern SCADA systems have a number of added features which increase the system complexities and are thus difficult to maintain. Some of the added features include control logic, communication protocols, user interfaces, and security.

Moreover, the communications are vulnerable to various threats. In the past few years, the number of cyber attacks,in general, is rising and has been affecting power station, water, gas, and nuclear control systems. The pattern of cyber-attacks has also evolved beyond the simple attacks such as Denial of Service or Man-in-the-Middle. The hackers gained access to the core command and control system by using a cellular modem. SCADA networks also comprise of resource-constrained devices such as Remote Terminal Units and Programming Logic Units, and these devices require lightweight ciphers. Traditional intrusion detection systems (IDSs) are now unable to protect from new threats . Robust security schemes involving machine learning to detect intrusions and encryption algorithms are essential to ensure a secure encrypted communication between nodes in SCADA networks. These threats and attacks have motivated researchers and organizations to develop new robust and secure techniques for SCADA networks.

Malware is software designed to steal sensitive information or gain unauthorized access into a critical infrastructure. It comes in different shape of code or script that are called viruses, worms, Trojan horses, spyware and

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201068 |

other malicious programs. Eavesdropping attack is the attempt of sniffing the network bandwidth and reading the data content for valuable information such as, passwords, keys, results, or any kind of secret information. DoS and DDoS attacks are one of the most common attacks that can affect SCADA systems. They mostly deprive the consumer from the service such as electricity blackout, or forbid the control center from monitoring or communicating with its substations. These attacks come with a lot of concerns due to their impact of suddenly losing a service.• Spoofing and MITM attacks are related to authentication attacks that threaten the SCADA systems by either claiming to be the control center or smart meter, and then they send false information and corrupt the system. Data Integrity attacks impact the SCADA system by manipulating the information and forcing the control center to make decisions based on wrong information.

II. REVIEW OF LITERATURE

Hussam M. N et al. (2013) Analyzed the SCADA security using a comprehensive search on a large number of documents produced by governmental agencies and standardization bodies. This search was to come up with standards and recommendations that are related to SCADA security. Based on their statistics, they identified how much attention is given to the countermeasures and threats in SCADA systems. For countermeasures, authentications with cryptographic techniques have taken the most interest percentage in order to secure SCADA. However, on the other side of the scale, a few interests were found in developing a secure organization, supporting system management tools; creating a system resilience or hardening of computers and services.

S. Renuka Devi, P. Yogesh (2011) presented an experiment by using the client network to act as a control station in a power system. Their experiment demonstrated the vulnerability of the control station to a DDoS attack and the possibility for reducing the effects of the attacks. They define an attack by "a way to prevent data from reaching its destination across the network".

G. Preetha, et al.(2011) proposed a privacy-preserving authentication protocol for smart grid system so-called PASS.

Sajid *et al.* (2016) The security and challenges of the SCADA systems. However, the paper does not provide a comparison of all the security protocols and standards for SCADA systems.

III.METHODOLOGY

The method used in this paper is descriptive-evaluative method. The study is mainly review based. It is purely supported by secondary source of data, i.e. books, journals, papers and articles and internet.

IV.RESULTS AND DISCUSSIONS

SCADA COMMUNICATION ARCHITECTURE

SCADA systems consist of several entities organized in a hierarchical structure . They are used in monitoring variouskinds of infrastructure and industries. They comprise the integration of data acquisition systems, data transmission systems and Human-Machine Interface (HMI) . The HMI is a user interface that connects a person to a device. It is mainly used to visualize data, and monitor production time, machine inputs and outputs.

- Master Station Unit or Master Terminal Unit (MSU/MTU) is the control center of a SCADA network.
- Sub-MSU or Sub-MTU acts as a sub-control center.However, it is not needed in some cases. The MSU canconnect to the remote station units directly.
- Remote Station Units are Remote Terminal Unit (RTU),Intelligent End Device (IED) and Programmable LogicController (PLC). They are used to monitor sensors and actuators to collect data values.

A communication link is shared between the MSU and Remote Station Units. Various types of communication links may be used, such as wired ethernet, WiFi or satellite link. SCADA system architectures have four typical architectural styles .Thus, as the size of the SCADA architecture and added features increase, the complexity of the SCADA architecture also increases. This makes managing large amount of data more dif_cult leading to loss of data availability. Furthermore, it makes the SCADA architecture susceptible to cyber-threats .

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201068 |

SECURITY THREATS FACED BY SCADA NETWORKS

Like any other system or network, a SCADA network faces the following threats :

- Loss of availability can cause power outages and can have a negative impact on the efficiency of power supply. This condition may have a cascading effect in the physical domain. Thus, achieving availability as a security goal should be one of the primary objectives of a SCADA network.
- Loss of integrity is a scenario when the attacker modifies the data, and thus, the receiver receives the changed data. This type of scenario is achievable by launching a Man-in-the-Middle attack, which can further result in malware injection and IP spoofing.
- Loss of confi0dentiality can be achieved by eavesdropping on a channel. It leads to the loss of privacy and stealing of data as private data is exposed.
- Repudiation is where the sender denies they have sent the data at that time.
- Slowloris, GoldenEye for operating system Kali Linux.
- And, another tool named Low Orbit Ion Cannon (LOIC) .
- Lack of authentication in the Distributed Network Protocol 3.0 (DNP 3) used in SCADA systems which can lead to an impersonation attack .

ATTACKS ON SCADA NETWORKS:

The usage of Internet connectivity, cloud computing, wireless communications, and social engineering on SCADA networks have made its architecture vulnerable . One of the main reasons for the vulnerabilities in SCADA is the lack of strong encryption and real-time monitoring. Attacks can occur at all layers from the supervisory level to the field instrumentation level . The most common attacks are outlined in Table 1A and 1B . They can also be categorized based on attacks on hardware, software, and network connection 3.

- *Attack on hardware:* This is a scenario where the hacker gets unauthenticated access to the units and tampers with them or their functions. The primary challenge in securing hardware is access control. For example, the doorknob-rattling attack.
- *Attack on software:* The SCADA system utilizes a varietyof software to enhance its efficiency by full flling the functional demands. However, due to poor implementation, it is vulnerable to SQL injection, trojan horse and buffer overflow. These are a few examples of attack on software.
- *Attack on network connection:* The attack on communication stack can be on the network layer, transport layer, and the application layer.

Preliminaries *Symmetric key encryption* is a shared key algorithm where both parties should agree on one key K . This key should be secret and no untrusted entity knows it. Ciphertext C is the result of encryption performed on plaintext m using the symmetric-key K and the encrypt algorithm E. $C = EK\{m\}$ The ciphertext C is sent to the second party which has to decrypt the ciphertext C. The second party has a decryption algorithm D and the symmetric-key K in order to decrypt the ciphertext C and obtains the plaintext m. $DK\{C\} = DK\{EK\{m\}\} = m$ *Hash-based Message Authentication Code*(***HMAC***)has the same technique from the original message authentication code (*MAC*). It uses a cryptographic hash function with a secret key sharing between both parties. However in *HMAC*, the secret key is used to produce other two keys; using outer pad (opad) and inner pad (ipad). This technique is used to provide an evidence for data integrity between the communicated parties. In the MAC technique: $M\ AC = H\ (K\ ,\ m)$ Where the *HMAC* is generated using the following technique: $H\ M\ AC = H\ M\ AC(K\ ,\ m) = H\ ((K \oplus opad)\_\ H\ ((K \oplus i\ pad)\_m))$ The reason of choosing *HMAC* over *MAC* is that the *HMAC* is more resistant to integrity attacks than *MAC*. Also, the reason why we choose *HMAC* over digital signature is because it requires less computation time for providing integrity check. *Nonce* (*N*) is usually a random number used for authentication process in order that the message cannot be reused and its freshness is guaranteed, thus avoiding the replay attack. In our scheme, in addition to providing freshness and authentication, the nonce is also used to generate symmetric keys to encrypt the information between the smart meters and control center. *Security Integrated Circuit* (*SIC*) is a physical temper resistant IC that has an internal security algorithm to generate unclonable symmetric keys using nonce and another attribute called secret number (SN) which is stored in the SIC. This IC is embedded into each produced smart meter from the power generators. Malicious entities could impersonate authorized smart meter and send false information to the control center. Therefore, the SIC provides active logical process for the smart meter to protect the shared information against various kinds of physical and logical tampering attacks. *Two-factor Authentication* (*T-FA*) is an authentication approach when the system requires two or more evidences to verify the identity of the user. Nowadays, several critical institutes and companies are using two factor authentication techniques to identify their customers such as tokens with a display, USB tokens or smartcards. On account of the smart grid critical system, two factor authentications are required from the consumer.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201068 |

Since we are relaying on a mobile device usage, therefore, a software token [14] could be adopted in the electricity company's application The application should produce a tokencode from 6 or 8 digits (secureID) each 30–60 seconds for real-time communication. *Secret Key Generation Algorithm* is a security algorithm implemented in the SIC. There could be more than one algorithm inside the SIC and they are independent from the hardware manufacturers in their operation. They can be used to generate keys, challenges, encrypted data or hash values.

Based on the smart grid SCADA system, the system consists of number of smart meters, set of servers which formation the control center, the consumer who wants to monitor and adjust his electricity usage from a mobile device. The smart meters in our proposed solution are produced from the power generators with each of which has a unique ID. This ID refers to the consumer in the control center's secure database. Also, each smart meter has a SIC that store a secret key *(*Ki*)* and a secret number (SN). These secret information also store in the secure database. Each consumer in our SCADA system should have a username and password along with his/her unique ID. The consumer could have smart meters for his/her house, company, and farm, therefore, more than one unique ID could be linked to his/her username.

In brief, the control center might be located inside the electricity main station, where it works continuously. The smart meter is installed by the electricity technicians inside a house, company or any institute supplied by the electricity company. In addition, the smart meter should be linked to all the available smart electricity sockets and smart appliances inside the premises. The consumer or substation owner should install software to monitor and control the smart meter in his/her mobile devices such as smart phones, tablets or laptops. The software has an embedded token generator linked to the user account for two-factor authentication. When the smart meter is installed and turned on, it directly communicates with the control center by a wired or wireless medium. Then, the control center verifies the smart meter and starts monitoring its electricity usage. In the consumer side of view, the owner of the smart meter enters his/her username and password in the application to authenticate his/her identity to the control center. The control center verifies the consumer and provides him/her with current secret key of the smart meter along with a ticket for verification. Finally, the consumer can securely monitor the collected data from his/her smart meter about the active electricity smart sockets and he/she can initiate action remotely to disable or enable these sockets. Any actions done from the consumer will be recorded from the smart meter and transmitted to the control center.

Security Analysis:

The security properties of our proposed scheme. The analysis will focus on how this scheme can address the security requirements. Our scheme givesthe monitoring and controlling process for the smart grid network a secure environment that verifies the participant devices and end-users (consumers or control center operators) in a mutual authentication process. It also provides a data integrity proof in order to verify the integrity of requests and responses in the network. Our scheme supports a robustness key exchange methodology based on a secret shared numbers, algorithms, and keys that stored in a secure integrated circuit and databases. Therefore, data privacy using symmetric cryptographic keys is granted. The security analysis will be divided into two parts; one that covers the security requirements available between the smart meter and control center; and another covers the security requirement available for consumer's processes in the system

Smart Meter and Control Center Security Analysis: The smart meter in this proposed scheme has physically a SIC that is sensitive from any tampering attempts in order to secure the integrity of the internal secret number, SAlgo, and internal key. This SIC provides the smart grid systems with a better security level by providing mutual authentication, integrity and confidentiality for the communication process.

Mutual Authentication*:* Smart meter has basically two sides of communication; the first one is with the smart electric sockets in the building, and the second one is with the control center server. Each electric socket is connected in a way that communicates the information with a smart meter via IPv4 level of trust. The smart meter can remotely activate or deactivate electronic socket based on its owner (consumer) or control center commands. On the other side, the smart meter authenticates the control center using a change and response technique. It sends a nonce which ensures the freshness as a plaintext along with the hash value for the nonce and the generated secret key to the control center. Then, when the smart meter receives a hash value for the same nonce combined with a new nonce and a new generated secret key, it verifies the control center. Via a simple comparison for the HMAC value, the control center authenticates the identity of the smart meters; and vice versa.

Confidentiality: Generating a new secret key between the smart meter and the control center is a must to complete the mutual authentication process between them. This secret key is either randomly generated every time the smart meter is restarted or automatically in regular basis case. The generated key from the nonce and the secret number should be long

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201068 |

and does not have pattern with used nonce. The smart meter uses this key to communicate securely with the control centre.

Data Integrity*:* All the initial communications require a hash value which is generated using HMAC function. This process supports the data integrity service in the scheme in order to verify the identities and generated secret key authenticity. The usage of the hash value is to check if the message has been tampered with or not. In case something went wrong the control center or the smart meter obviously would reject the message and report the event.

Consumer, Control Center and Smart Meter Security Analysis : basically, each consumer should be confident that only his/her devices can access his/her own smart meter for monitoring or controlling purpose. Therefore, two-factor authentication is adopted in our proposed scheme. Each consumer has a username and password which is something only he/she knows and a licensed software application downloaded in his/her mobile device which produces token code for real time communication. Our proposed scheme provides the consumer with a mutual authentication service with the control center and the smart meter, in addition to integrity and confidentiality. Moreover, our scheme provides authorization level for multiple system users, in addition to accountability.

V.CONCLUSION

A security analysis of the scheme highlighted the benefit from combining several security techniques such as two-factor authentication, nonce, hash-based message authentication code (HMAC), and symmetric key cryptography. It discusses and classifies the frequent attacks on SCADA networks, and potential attack by a quantum computer. Furthermore, it lists all current standards used by organizations standards and provides the security threats of each standard. The two main security threats are lack of defense against Denial of Service attack and, using weak key exchange protocol. To address these two security requirements, researchers offered various novel security schemes. The paper classifies these schemes based on the addressed issue of the current standards. Thus, the schemes are categorized into detection of attacks on SCADA networks, and prevention of the attacks. It further explores and compares all the protocols that fall under each main category. It also addresses the security concerns and requirements that a SCADA security scheme needs to approach in future. Thus, the article gives a foundation to provide a course for further researches and assist an organization to decide on a suitable standard and scheme.

REFERENCES

1. Hussam M. N. Al Hamadi, Chan Yeob Yeun, Mohamed Jamal Zemerly(2013) A Novel Security Scheme for the Smart Grid and SCADA Networks Wireless Personal Communications , Volume 73, Issue 4, pp 1547-1559. 2013,
2. 2. G. Preetha, B.S. Kiruthika Devi, and S. Mercy Shalinie.(2011) Combat model based ddos detection and defence using experimental testbed: a quantitative approach. International Journal elligent Engineering Informatics, pages 261-279, 2011.
3. 3. S. Renuka Devi, P. Yogesh ,An Effective Approach to Counter Application Layer DDoS Attacks", IEEE, --ICCCNT'12. , 2011
4. 4.Sajid, H. Abbas, and K. Saleem, ``Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," IEEE Access, vol. 4, pp. 1375_1384, 2016.
5. 5.P. K. Amiri, ``Quantum computers," IEEE Potentials, vol. 21, no. 5,. 6-9, Dec. 2002.
6. 6.N. Kumar and D. Goswami, ``Quantum algorithm to solve a maze: Convertingthe maze problem into a search problem," pp.:1312.4116,2013,
7. 7.S. Mittra, ``Iolus: A framework for scalable secure multicasting," ACM SIGCOMM Comput. Commun. Rev., vol. 27, no. 4, pp. 277-288, 1997.
8. 8.B. Babu, T. Ijyas, M. P., and J. Varghese, ``Security issues in SCADA based industrial control systems," in Proc. 2nd Int. Conf. Anti-CyberCrimes (ICACC), , pp. 47-51, 2017.
9. 9.N. Challa and J. Pradhan, ``Performance analysis of public key cryptographic systems RSA and NTRU," Int. J. Comput. Sci. Netw. Secur., vol. 7, no. 8, pp. 87-96, 2007.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details