International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 2 Issue 11 ǁ November. 2014 ǁ PP.88-94

Encryption Security in SCADA Networks

Rahul Kumar[1], Rishabh Shukla[2], Ajit Pratap Singh[3], Sachin Kumar
[1,2,3,4]*M.Tech,Sam Hagginbottom Institute of Agriculture Technology & Sciences ,*

Abstract: *Supervisory control and data acquisition (SCADA) are applications that collect data from a system in order to automate the monitoring and controlling of its activities. Several industrial fields such as, electric utilities, water supplies and buildings' facilities have already adopted SCADA systems to increase the efficiency and reduce cost. However, the IT community is concerned about the level of security that any applied SCADA system provides. This paper concentrates on the major security threats encountered in SCADA systems. In addition, it discusses a new proposed methodology in order to increase the system security with minimal impact on efficiency. The proposed scheme provides several security services which are mutual authentication, confidentiality, data integrity and accountability.*
Keywords: *SCADA · Smart grid · Security · Mutual authentication.*

I. Introduction

Supervisory control and data acquisition (SCADA) systems have been one of the active topics for researchers in the last five years, and due to the IT technology evolution it has become more complicated and advanced. 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.

In November 2011, the US department of Homeland Security and the FBI probed a cyber attack on the water system. The attackers accessed the network of the water utility in state capital Springfield using stolen credentials from a company that supplies software to control industrial systems. Cyber security experts commented on the incident by highlighting the risk that attackers can break into what is known as SCADA systems [1].

In July 2010, Belarus-based Security Company discovered a worm called Stuxnet into a computer belonging to Iranian client. Since then the Stuxnet has been studied by security researchers. At the start they thought it has been written to steal industrial information. However, after months from private security forensics, some of the researchers said that the worm has a kind of fingerprint that tells it has been designed to destroy something large that it looks for a very specific Programmable Logic Controller (PLC) that runs in a SCADA system, such as the Iranian's nuclear reactors [2].

Targeted cyber attacks that caused multiple-city blackout have been reported to the CIA, January 2008 [3]. Although there are no physical damage reports, somehow lives could be depending on the availability of electricity in hospitals, airports, or train networks. There-fore, the information pushed between the components of the smart grid network should be secure. From the previous incidents, we conclude that a secure SCADA network is crucial to any critical infrastructure facilities. Therefore, searching for the SCADA security require-ments that address majority of the threats is a must in order to provide a suitable security methodology.

Section 2 provides an explanation of SCADA security and some proposed schemes in this field. Section 3 discusses our proposed scheme for smart grid systems. The analysis and evolution of our scheme are given in Sect. 4. Finally, Sect. 5 concludes the paper and suggests some future work in this field.

II. SCADA Security And Related Work

Sommestad et al. in [4] have 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. Figure 2 shows some statistics about the threats on SCADA systems. Also, the study found out that the most common threat that occurred in SCADA systems was malicious code, and then comes the threat on data communication that comes from authentication, integrity and confidentiality issues such as, spoofing, replay attack, Man-In-The-Middle (MITM), interception, and data integrity. In the third place, the availability attacks such as Denial of Service attacks (DoS) and Distributed DoS (DDoS)The percentage of this attack is marginally equal the percentage of overall attacks targeting the authentication, confidentiality and integrity. This makes the DoS solution more required in securing SCADA, however, it is not an easy field to address. The other remaining threats were addressed for information gathering, threats from employees, social engineering, and other threats such as password stealing, web-attacks, non-repudiation attack, etc.

The definition of some of these threats can be explained as the following:

Malicious Code or 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 horsēs, spyware and other malicious programs[5].

- 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.

Most control systems transmitting their measures and control commands via SCADA

network to the substations or owners. The attacker can find a way to exploit the existing vulnerabilities in this network and impact on the physical appliances. Therefore, several solutions have been proposed to secure SCADA systems. In [6], Hong et al. developed two computational algorithms to detect malicious attempts in a power system environment. They gave cyber security scenarios for their algorithms and evaluated it on University College Dublin (UCD) testbed. In addition, they apply an Inter-Control Center Communications Protocol (ICCP) to link between two testbeds in UCD and Iowa State University. In [7], Davis et al. 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".

They also used tools for their demonstrations; these tools are PowerWorld [8] for simulation and RINSE [9] for realistic emulation of a large network. In [10], Chim et al. proposed a privacy-preserving authentication protocol for smart grid system so-called PASS.

Their scheme is meant to be for providing authenticated messages between the substations smart meters and the control center. They suggest supporting the smart appliances with sort of tamper-resistant

devices in order to secure the data from cracking. The major feature of their protocol is providing the privacy of the electricity usage for each consumer while the control center can appropriately generate enough amount of electricity. From the previous work [5– 12], we can conclude that the most threats that affect the SCADA system security are the ones linked to authentication, confidentiality, and integrity. Therefore, we propose a novel solution that provides several security requirements as mutual authentication, confidentiality, data integrity and accountability by combining both hardware and software security tools into one scheme to prevent these types of attacks in SCADA systems

III. Our Proposed Scheme

In this section, we first explain the preliminaries of the proposed scheme, and then we discuss in details how it works.

3.1 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:

$MAC = H(K, m)$

Where the *HMAC* is generated using the following technique:

$HMAC = HMAC(K, m) = H((K \oplus opad)\_ H((K \oplus i\,pad)\_m))$

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*) [13] 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.

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.

3.2 The Proposed Scheme

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 [15]. 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.

Step 1. The smart meter is turned on. It generates a nonce N1 and combines it with SN using SAlgo function to generate KS. Then, the SM uses the Ki to produce *HMAC* of the [KS_N1]. The

result is sent to ContC as the following:

KS : SAlgo*(*N1, SN*)*

SM → ContC : *SMid_ N*1*_ H M AC(Ki , M)*

Where*M* = [KS_N1]

Step 2. When the consumer wants to communicate with its smart meter, he/she has to login into the smart grid network by a username and password. The consumer types them into the downloaded software from the electricity company which has an embedded virtual token that generates SecureIDs. Then, his/her smart device generates KC from the hashed password and encrypts the nonce N3 and SecureID, then it sends them along with the username, as the following

C → ContC : Cid_{N3_SecureID}KC

Step 3. The control center receives the Cid and gets its password's hash value from the secure database. The control center generates KC , in order to decrypt the nonce and SecureID. If the decryption process succeeds, then the first factor authentication is verified. The con-trol center generates a SecureID based on the Cid's software, and then matches it with the received one. If they match, the second factor authentication is also

verified. The control center generates a session key KC,SM between the consumer and its smart meter. In addition, it will generate a ticket for the consumer to forward it to the smart meter. As shown in the syntax below, the ticket has a freshness parameter *(*N4*)*.

ContC → C : {N3_KC,SM_VPT}KC_{T}KS

WhereT = [Cid_N3_N4_KC,SM_VPT]

Then, the consumer decrypts the first part of the message using the K^{C}, and by checking the response nonce N^{3}, a mutual authentication is achieved between the consumer and control center. Of course the consumer cannot decrypt the second part of the message because he/she does not have the key KS.

Step 4. The consumer prepares request to monitor the collected data by the smart meter and sends the request along with the ticket received from the control center.

C → SM : Cid_{N3_Req}KC,SM_{T}KS

Step 5. The smart meter decrypts the ticket and ensures the freshness by checking N^{4}, then, it uses the $K^{C,SM}$ to decrypt the consumer's request. By successful decryption and matching the N^{3} from both parts of the message, the smart meter authenticates the source Cid. It sends the result encrypted using $K^{C,SM}$ along the N^{3} and a new nonce N^{5} to prove freshness. The following syntax shows the last required message in our scheme:
SM → C : SMid_{Res_N3_N5}KC,SM

Step 6. The smart meter is responsible for reporting all the consumer actions from mon-itoring to sending commands and his behavior in using the electricity to SCADA central. These reports should be secured in order to be used later on for consumer accountability. The following syntax shows the content of secure reports along with freshness parameter *(*N6*)*.

SM → ContC : SMid_{Report_Cid_N6}KS

IV. Security Analysis

In this section, we analyze 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.

4.1 Smart Meter and Control Center Security Analysis

From *Step 1* and *Step 2*, 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.

1) *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.

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

3) *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.

4.2 Consumer, Control Center and Smart Meter Security Analysis

From *Steps* (3–7), 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 tokencode 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.

1) *Mutual Authentication:* the proposed scheme is based on change and response technique using nonce and two-factor authentication to provide mutual authentication between the consumer and the control center. The change and response technique is also provided between the consumer and the smart meter along with encrypted ticket which the intended smart meter only is able to decrypt. The consumer could have more than one place to monitor. The control center is able to provide the authenticated consumer with an authentication icket for each smart meter, and then the consumer has the option to choose the smart meter to connect. The login stage of the consumer does not require the password to be sent in the network. The only things which are sent are the consumer ID and an encrypted secureID by the hash value of the consumer's password. The secureID is a tokencode changing regularly, which makes it impossible to the attacker to login into the system even if he/she successfully guesses the password with a dictionary or brute-force attack. Although, the attacker could somehow find the password and find out the nonce N3 (freshness element), in order to change the request of the consumer by replacing {N3_Req}KC,SM by his/her request, he/she should have the KS to change the content of the ticket. As mentioned previously KS is a variable secret key between the control center and smart meter. Therefore, impersonating the consumer in this scheme is very difficult, unless the attacker has the user name and password along with the device that has the licensed application.

2) *Confidentiality:* Our proposed scheme guarantees that all the communication for the consumer is secured using cryptography schemes such as AES. Once the consumer login, his/her password will be hashed to generate a secret key in order to encrypt the generated nonce for the login process. In addition the response from the control center is encrypted using the same key except the ticket which is encrypted using the smart meter secret key. Our scheme prevents any eavesdropping or any attempts to disclose the information.

3) *Integrity:* Even though there is no one-way hash function in the consumer communication with the control center and smart meter, the transmitted data cannot be changed as long as they are encrypted. In addition, each message between the participants in our scheme consists of at least two parts; where one part ensures the authenticity of the other.

4) *Accountability*: Each consumer should pass through a trusted third party (control cen-ter) in order to communicate with his/her smart meter. The control center recodes the consumer ID and his session key with the smart meter in secure database. Any action taken from the consumer side on the smart meter will be reported to the control center. For example, if the consumer decides to perform a real-life monitoring, the smart meter reports this request to the control center, the same for switching off the light in a room. The smart meter's reports have evidence that the consumer took the action.

V. Conclusion And Future Work

This paper first introduces SCADA's elements in the smart grid systems and how they are connected to each other. Then, it highlights some of the recent security incidents on existing SCADA systems and how much risks will be incurred if users ignore its security threats. The paper also discusses some of the related work in the field of securing SCADA systems . and offers a survey on the most recent attacks performed on them. Then, it proposes a novel scheme which aims to provide enhanced security for remote monitoring and control over building electricity consumption. The proposed scheme provides mutual authentication, confidentiality, data integrity and non repudiation between the participants of smart grid SCADA system against cyberattacks. In this paper, a block diagram for the proposed scheme was provided with details for its secure communication. In addition, 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. As future work, a security analysis and verification based on a formal model could be pro-vided. The verification process for our proposed scheme can be implemented using ProVerif tool [16]. This process can clearly expose and evaluate the security mechanism of the scheme and detect any security defects and develop model for information security criteria for smart grid system as in [17]. Finally, as some of the related work, a demonstration using the freeware "Power World" or a simulation using RINSE would be provided in order to collect results about the stability of our scheme.

BIBLIOGRAPHY

[1.] Hussam M. N. Al Hamadi, Chan Yeob Yeun, Mohamed Jamal Zemerly .A Novel Security Scheme for the Smart Grid and SCADA Networks Wireless Personal Communications December 2013, Volume 73, Issue 4, pp 1547-1559.

[2.] Prolexic. (2012). Prolexic Quarterly Global DDoS Attack Report. Prolexic.com Retrieved from http://www.prolexic.com/kcresources/attack-report/prolexic-quarterly-global-ddos-attack-report-q412-1713/ProlexicQuarterlyGloba_DDoS_Attack_Report_Q412_011413.pdf

[3.] G. Preetha, B.S. Kiruthika Devi, and S. Mercy Shalinie. Combat model based ddos detection and defence using experimental testbed: a quantitative approach. International Journal of Intelligent Engineering Informatics, pages 261-279, 2011.

[4.] T. Thapngam, S. Yu, W. Zhou, and G. Beliakov, "Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns," in Proceedings of the 30th Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2011), Shanghai, China, 2011, pp. 969 - 974.

[5.] Danny McPherson and Dave Oran. Architectural considerations of IP anycast. Draft -iab-anycast-arch-implications, February 2010.

[6.] http://thehackernews.com/2013/03/world-biggestddosattackthat-lmost.html

[7.] Behrouz A. Forouzan. Cryptography and network security, Fifth Edition ,Tata McGraw Hill Publication, 2010.

[8.] Arbor-Networks, "Worldwide Infrastructure Security Report: 2010 Report," Arbor Networks, 2011.

[9.] Shubha Kher Jinran Chen and Arun Somani. Mitigating denial of service attack using proof of work and token bucket algorithm. Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, pages 65{72, 2011}

[10.] G. Preetha, B.S. Kiruthika Devi, and S. Mercy Shalinie. Combat model based ddos detection and defence using experimental testbed: a quantitative approach. International Journal of Intelligent Engineering Informatics, pages 261{279, 2011}

[11.] Chin-Ling Chen, Chih-Yu Chang," A Two-Tier Coordinated Defense Scheme against DDoS Attacks", IEEE, 2011

[12.] Huey-Ing Liu, Kuo-Chao Chang" Defending Systems against Tilt DDoS Attacks"The 6th International Conference on Telecommunication Systems, Services, and Applications, IEEE 2011.

[13.] Chengxu Ye, Kesong Zheng, Chuyu She," Application layer DDoS detection using clustering analysis",2nd International Conference on Computer Science and Network Technology, IEEE, 2012.

[14.] S. Renuka Devi, P. Yogesh," An Effective Approach to Counter Application Layer DDoS Attacks", IEEE, ICCCNT'12.