International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 2 [ISSN : 2250-3757]
Publication Date : 30 October, 2015

Security Analysis and Comparison of SCADA System Using Advance Cryptography Approaches

AAmir Shahzad, Malrey Lee, Kim Geon, Muhammad Irfan

***Abstract*— The SCADA (Supervisory control and data acquisition) system cyber in-security has been increasing day-by-day, due to larger interconnectivity with other open networks (and protocols). Like traditional networks, SCADA system has been also facing several security challenges, which warming the communication, and become disaster for the industrial processing. Therefore, strong security solution is required that has potential to secure the communication of SCADA system, against cyber attacks and vulnerabilities. After conducting the detail review, cryptography based security approaches are chosen as best solutions against SCADA in-security. This study analyzed, measured and made comparison between cryptography approaches, while deployments in various communications, followed by SCADA system acquirements. The security via cryptography has been implemented, and comparison is observed during SCADA abnormal transmission, with the specifications of SCADA system communication, in mind.**

Keywords— SCADA System, DNP3 Stack, Cryptography Approaches, Security Attacks, Attacks and Tools.

I. Introduction

SCADA system is one of the important, real time industrial processing system among other systems including DCSs (distributed control systems), and PLCs (Programmable logical controllers). SCADA system has been employed several advance protocols including DNP3, Modbus, Fieldbus, and Profibus, and also connected with modern networks for sharing information, over internet [1], [2]. Like traditional communication networks, SCADA system utilizing several components, that are helpful during communication such as SCADA main station, SCADA remote stations, sensors/actuators, other networks instruments [3], [4].

The active changed in computer networks, SCADA system also gained the advance technology, to connect its nodes with other open networks/protocols, over internet.

AAmir Shahzad, Malrey Lee
1,2561-756,Center for Advanced Image and Information Technology, School of Electronics & Information Engineering, Chon Buk National University, 664-14, 1Ga, Deokjin-Dong, Jeonju, ChonBuk, Korea

Kim Geon
Department of Records Management, Chon Buk National University, 664-14, 1Ga, Deokjin-Dong, Jeonju, ChonBuk, Korea

Muhammad Irfan
Infrastructure University Kuala Lumpur (IUKL), Malaysia

- In this study, the performance results are taken from our previous research

This vigorous changed, also creates several cyber security issues, during interconnectivity with proprietary networks/protocols. The security is an important concerned that has been counted during SCADA communication. Therefore, reliable and independent security solutions are required that have potentials to resist, against cyber attacks [2], [4].

II. Problem Statement

The SCADA system connectivity with modern networks and using of internet facilities, SCADA platform is vulnerable from several attacks that create major security issues during communication [8], [9]. Many end-to-end security approaches have been deployed for securing information, across internet and to overcome the attacks that are occurring in SCADA communication [1], [4]. These security solutions have various limitations including TCP/IP protocol dependency during message delivery, and utilization of cryptography algorithms for security purposes [10], [11].

After conducting the detail reviewed on SCADA security issues and vulnerabilities, cryptography based security solutions have been implemented within distributed network protocol (DNP3) as a part of SCADA system, rather than end-to.end implementations [5], [6], [13]. The end-to-end performance results are measured, for comparison purposes. The proposed solutions significantly enhanced the security, and reduced the potential attacks and vulnerabilities of SCADA communication.

III. Testbed Setup

In proposed SCADA/DNP3 testbed setup, seven remote nodes are connected with master node, with the bandwidth of 5 Mbps. The information has been transmitted number of times between master node and remote nodes or/and vice versa, and the performance results are measured, in-case of attack (or abnormal) and without attack (or normal) scenario [14], [15]. Basically, the latency is measured and compared during SCADA normal communication [5], [6].

IV. Performance Measurement And Discussion

In SCADA/DNP3 communication acquirements including unicasting, multicasting and broadcasting, the security solutions including Measurement[1] , Measurement[2], and Measurement[3], have been implemented and performance results are measured that are based on successful testing experiments. The detail related with

security solutions or Measurements is following:

- In Measurement[1] , the AES, RSA and SHA-2 hashing, cryptography algorithms are used to secure the SCADA uni-casting communication [5], [12], while same algorithms are used in Measurement2, but with technique of key encryption, rather than message [6], [12].
- SCADA multicasting and broadcasting scenarios have been employed Measurement3; mean that, the AES and SHA-2 hashing cryptography algorithms are used for security enhancements, basis on SCADA communication acquirements, in mind [7], [12].

The testbed measurement and discussion phase has been divided into three main sections such as section A, and section B. In section A, the security has been implemented and tested within SCADA/DNP3 protocol, while end-to-end performance results are measured in section B.

A. *Performance Measurement And Discussion Using Stack*

The testbed experiments have been tested 736 times by implementing Measurement[1] during SCADA/DNP3 unicasting communication. These experiments are distributed among four security objectives such as authentication, integrity, confidentiality and non-repudiation for performance evaluation. In table1, 736 times attacks have been launched to intercept the normal communication, which validated the security implementation and evaluated the measurements. The authentication attacks including guessing shared key, brute force, system/user login, and password guessing using attacking tools such as "cracking tools, sniffer, dsniff, winsniffer and password dictionary" have been launched 184 times and attacks detection percentage is measured. This abnormal process has been repeated 184 times for integrity attacks including "frame injection, data replay and data deletion " using attacking tools such as "airpwn, file2air, libradiate, wnet dinject/reinject, capture and injection tools, jamming and injection tools". During abnormal transmission, traffic has been analyzed and attacks detection percentage is measured. The attack detection percentage is calculated that based on total number of attacks detected during abnormal communication [5], [6].

TABLE 1. Performance using Measurement[1] and Measurement[2]

Security Tests	No. of Attacks Successful	
	Measurement[1]	Measurement[2]
Attack Detection	3%	8%
Attack Impact	1%	3%
Security	99%	97%

The confidentiality attacks including "eavesdropping, key cracking and man-in-the-middle" using attacking tools such as "ethereal, ettercap, kismet, commercial analyzers, aircrack, airsnort, dwepcrack, wepattack, wepdecrypt, weplab, dsniff, and ettercap" have been launched 184 times and attack detection percentage is measured. This abnormal process is also repeated 184 times for as non-repudiation attacks. The total attack detection percentage has been observed that based on 736 testbed experiments and subsequently, attack impact percentage is calculated that based on attack detection percentage. During abnormal communication, several times attacks have been detected but they have zero impact on system. In other words, the security implementation has potential resistance that successfully secured the SCADA/DNP3 system during abnormal communication. The overall performance such as computed attacks detection percentage, attack impact percentage and corresponding security percentage successfully evaluated the system performance and validated the security implementation that built a strong security wall against attacks [5], [6].

In table 1, testbed experiments have been also tested 736 times by implementing of Measurement[2] during SCADA/DNP3 unicasting communication. During transmission, the security objectives such as authentication, integrity, confidentiality and non-repudiation have been tested and corresponding performance results such as attacks detection percentage, attack impact percentage and security percentage are measured and compared with Measurement[1] performance results.

Using Measurement[2], the total attack detection percentage is 8%, which decreased to 3% by employing Measurement[1]. Other performance results such as impact percentage and corresponding security percentage are comparatively low during Measurement[2], while comparing with Measurement[1] performance results [5], [6].
Using Measurement[1], the security is measured as 99%, which is high by comparing with Measurement[2] security as 97%. The Measurement[2] implementation is twofold; security solution has been deployed to enhance the SCADA /DNP3 security and this implementation taken less latency, while comparing with Measurement[1] implementation [5], [6].

In table 2, the testbed experiments have been tested 300 times by implementing Measurement[3] during SCADA/DNP3 broadcasting communication. These experiments are distributed among three security objectives such as authentication, integrity, and confidentiality. The authentication attacks including guessing shared key, brute force, system/user login, and password guessing using attacking tools such as cracking tools, sniffer, dsniff, winsniffer and password dictionary have been launched 99 times, while one experiment is used for configuration test. This abnormal process is repeated same number of times for integrity attacks including frame injection, data replay and data deletion using attacking tools such as airpwn, file2air, libradiate, wnet dinject/reinject, capture and injection tools, jamming and injection tools and for confidentiality attacks including eavesdropping, key cracking and man-in-the-middle using attacking tools such as ethereal, ettercap, kismet, commercial analyzers, aircrack, airsnort, chopchop, dwepcrack, wepattack, wepdecrypt, weplab, dsniff, and ettercap. The abnormal traffic has been analyzed and performance results such as attacks detection percentage, attack impact percentage and corresponding security percentage are measured [7].

In SCADA/DNP3 testbed, 282 times experiments have been tested by implementing Measurement[3] during

SCADA/DNP3 multicasting communication. These experiments are also distributed among three security objectives same as Measurement[3] security objectives. In table 2, 94 times attacks such as authentication, integrity and confidentiality, have been launched to intercept the normal communication and performance results such as attacks detection percentage, attack impact percentage and corresponding security percentage are measured. The total of 18 experiments are used for special purposes such that 1 to 12 experiments are used during acknowledgment acquired from RTUs, 2 experiments are used during handling of transmission errors and checking communication flow and remaining 4 experiments are used during acknowledgment acquired from MTU.

TABLE 2. Performance Analysis using Measurement[3]

Security Tests	No. of Attacks Successful Using Measurement[3]	
	Broadcasting	Multicasting
Attack Detection	14%	11%
Attack Impact	8%	5%
Security	92%	95%

In above security implementations, cryptography dynamic buffer (CDB) has been employed for overall information storage related with security designed and implementation. The performance results evaluated that the CDB storage space is sufficient during whole SCADA/DNP3 protocol security development [12].

B. *End-To-End Performance Results and Discussion*

The security implementations such as Measurement[1], Measurement[2], and Measurement[3], have been implemented at each end of SCADA/DNP3 testbed communication. The testbed setup and number of experiments are same as in section 4.1, but security is deployed and tested at each end of SCADA/DNP3 testbed in both normal and abnormal communication. The performance results such as attack detection percentage, attack impact percentage, and security percentage have been measured to evaluate the security objectives such as authentication, integrity, confidentiality and non repudiation during abnormal communication and latency is measured and further comparison is created between security implementations results during normal communication.

TABLE 3. End-to-End Performance Analysis

Security Tests (End-to-End)	No. of Attacks Successful	
	Measurement[1]	Measurement[2]
Attack Detection	25%	28%
Attack Impact	20%	22%
Security	80%	78%

In table 3, the security has been implemented at each end of SCADA/DNP3 testbed communication and performance results such as attack detection percentage, attack impact percentage and security percentage are measured. These measurements show that the computed security percentage is comparatively low, while comparing with section 4.1 results or the security implementations within SCADA/DNP3 stack.

Using Measurement[1], total attack detection and attack impact have been computed 25% and 20%, while this percentage is low as 3% and 1% during security development within DNP3 protocol. At other side, the security observed is 80%, while this percentage is significantly high as 99%, during security development within DNP3 protocol.

Similar situation has been raised during employment of Measurement[2]. The attack detection and attack impact have been computed 28% and 22%, while this percentage is low as 8% and 3%, during security development within DNP3 protocol.

Overall, security percentage including 99%, and 97%, has been measured by implementing security solutions such as Measurement[1], Measurement[2], while the percentage including 80% and 78%, is comparatively low during same security implementations are tested at end of SCADA/DNP3 testbed communication. These security results conclude that the high security percentage has been computed in table 1, while comparing with table 3 results. The performance results in these tables including table 1, table 2 and table 3 also concluded that the security development within DNP3 stack has significantly high and better performance results, while comparing with end-to-end security development.

V. Performance Comparison

The performance figure 1 shows the average measurements included attack detection percentage, attack impact percentage and security percentage during SCADA/DNP3 communication by implementation of Measurements or security solutions such as Measurement[1], Measurement[2], Measurement[3], Measurement[4] or end-to-end implementation using Measurement[1] and without any security solution. The green color represents the security percentage, blue color represents the attack impact percentage and red color represents the attack detection percentage. The security percentage is very high as 99% using Measurement[1] and this percentage gradually decreased as 97%, 95%, 92%, 80% and 78% using Measurement[2], Measurement[3], and Measurement[4] in section 4.1 and section 4.2, while suddenly decreased to 5%, without security solution.

At other side, attack detection percentages using Measurement[4] are 25 % and 28%, and these percentages decreased to 14%, 11%, 8% and 3% using Measurement[3], Measurement[2] and Measurement[1] with attack impact percentages such as 20%, 22%, 8%, 5%, 3% and 1%, while attack detection and impact percentages are 95% and 90% during without security deployment.

In figure 1, the overall performance results concluded that the proposed security implementations within DNP3 protocol significantly enhanced the SCADA system security, while comparing with end-to-end security implementations. These security implementations have potential resistance to protect SCADA/DNP3 system, and significantly reduced the security risk and issues that are present in SCADA communication.

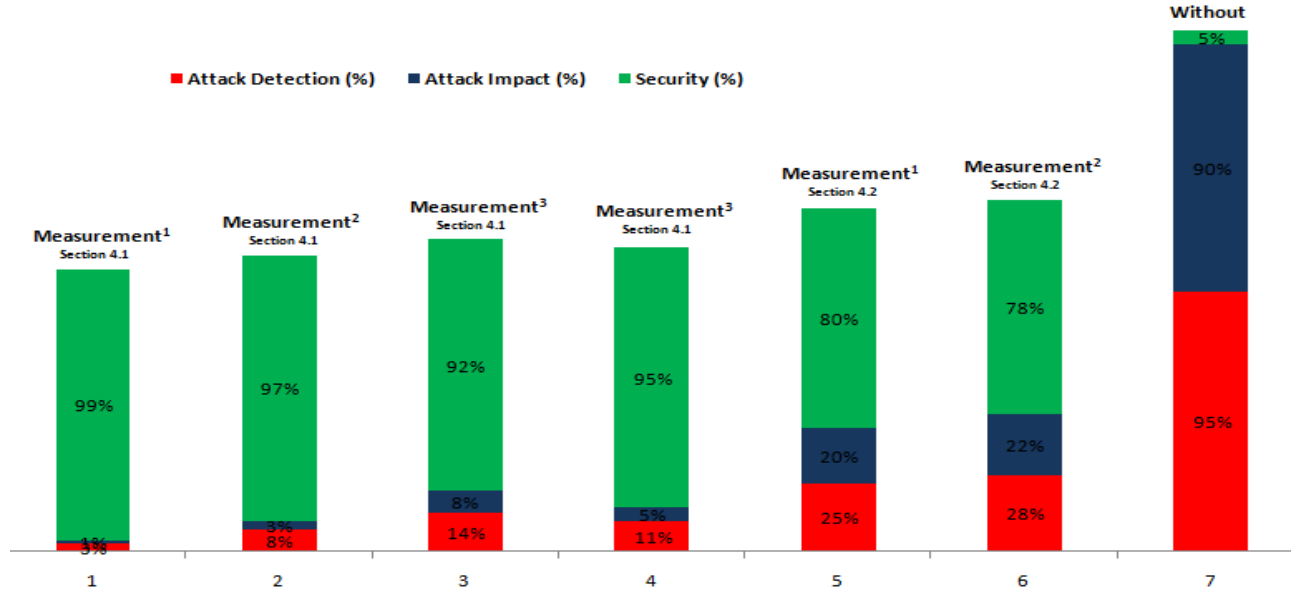

Figure 1. Performance Comparison

VI. Conclusion And Future Work

The security is a big challenge for SCADA communication, like other networks. The daily increasing of in-security within SCADA system, counted as a serious problem for industrial processing and automation. This study reviewed and select cryptography based security solutions as best approaches, against SCADA in-security. The security solutions are implemented and tested, according to the SCADA communication acquirements. The performance results are measured that significantly enhanced the SCADA system security during abnormal (attacks) scenario.

The new security placements within SCADA/DNP3 protocol, and overall performance results measured, open new research directions for further SCADA security enhancements.

VII. Acknowledgments

We would like to thank to our parents and our friend Mr.Irfan, boosted us morally and provided us great information resources.

VIII. References

[1] S. Musa, A. Shahzad, A.Aborujilah, "Secure security model implementation for security services and related attacks base on end- To-end, application layer and data link layer security", Proceeding ICUIMC '2013 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013, DOI: 10.1145/2448556.2448588

[2] K. Stouffer , J. Falco, K. Kent, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security", Recommendations of the National Institute of Standards and Technology, pp.2–13, 2006, http://www.cyber.st.dhs.gov/docs/NIST. pdf

[3] Communication Technologies, Inc, "Supervisory Control and Data Acquisition (SCADA) Systems", National Communications System, Technical Information Bulletin, pp.8–12, 2004, http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[4] S. Musa, A. Shahzad, A.Aborujilah, "Simulation base implementation for placement of security services in real time environment", Proceeding ICUIMC '2013 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013, DOI: 10.1145/2448556.2448587

[5] Shahzad, S., M. Irfan, "N-Secure Cryptography Solution for SCADA Security Enhancement", Trends in Applied Sciences Research, 2014, DOI: 10.3923/tasr.2014.381.395

[6] Shahzad, S., M. Irfan, "Key Encryption Method for SCADA Security Enhancement", Journal of Applied Sciences ,2014, DOI: 10.3923/jas.2014.2498.2506

[7] AAmir, S., M. Irfan, "The Protocol Design and New Approach for SCADA Security Enhancement during Broadcasting Communication", International Journal of Information Security and Privacy (IJISP), 2014, In-Press.

[8] Wang Chunlei Fang Lan, Dai Yiqi, "A Simulation Environment for SCADA Security Analysis and Assessment", Measuring Technology and Mechatronics Automation (ICMTMA), International Conference, Volume: 1 , 2010, DOI: 10.1109/ICMTMA.2010.603

[9] I. N. Fovino, A. Coletta, and M. Masera, "Taxonomy of Security Solutions for the SCADA Sector ,Security of Critical Networked Infrastructures (SCNI) Action", JRC-Joint Research Centre of the European

Commission, Version 1.1, 2010, http://www.cen.eu/cen/Sectors/Sectors/ISSS/Focus /D22.pdf

[10] AAmir, S., A. Aborujilah, M. Irfan, "The SCADA Review: System Components, Architecture, Protocols and Future Security Trends", American Journal of Applied Sciences, 2014, DOI: 10.3844/ajassp.2014.1418.1424

[11] Shahzad, S., A. Aborujilah, M. Irfan, "The Security Survey and Anaylsis on SCADA Communication", Journal of Computer Science, 2014, DOI: 10.3844/jcssp.2014.2006.2019

[12] Shahzad, S., M. Irfan, "Deployment of New Dynamic Cryptography Buffer for SCADA Security Enhancement", Journal of Applied Sciences ,2014, DOI: 10.3923/jas.2014.2487.2497

[13] O. Gervas, "Encryption Scheme for Secured Communication of Web Based Control Systems", Journal of Security Engineering ,2010, http://www.sersc.org/journals/JSE/vol/5.pdf

[14] Shahzad, S., A. Aborujilah, M. Irfan , "A New Cloud Based Supervisory Control and Data Acquisition Implementation To Enhance The Level 0f Security Using Testbed", Journal of Computer

Science, 2014, DOI: 10.3844/jcssp.2014.652.659

[15] Shahzad, S., A. Aborujilah, M. Irfan, "A Performance Approach: SCADA System Implementation within Cloud Computing Environment", ACSAT 2013, IEEE, DOI: 10.1109/ACSAT.2013.61