International Journal of Information Processing, 8(1), 73-91, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

A Framework to Mitigate Attacks and Establish Secure Communications in SCADA Systems

Pramod T C[a], N R Sunitha[a]

[a]Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka India, Contact: tcpramodhere@gmail.com, nrsunithasit@gmail.com.

SCADA systems are being the part of many national infrastructures. As deliberate cyber attacks or misuse on these systems are increasing, it is essential to achieve secure communication between the devices of critical infrastructures. For this we are proposing a key establishment scheme that uses Elliptic curve Diffie Hellman (ECDH), Matrix based scheme and Polynomial based scheme. Novelty of the proposed scheme is the secret key is never transmitted over the network for any type of communications. Thus, the chances of exposure of secret keys are reduced. As and when real time data is transmitted, security breaches; which might include unauthorized access, flawed aggregation from field level to control level, packets drops, routing attacks etc. may occur. This results in compromise of availability, integrity, confidentiality and trust relationship between the devices of SCADA systems. By considering the constraints and efficiency requirements of automation and control networks, we propose an approach to identify malicious activities and mitigate the attacks using analysis of Log data. As the hierarchy of devices increase, the attributes maintained in Log also increases and thus the devices are able to detect more vulnerable activities, thereby supporting towards the growth of secure critical infrastructures.

Keywords : Attacks, Key Establishment, Log Management, SCADA.

1. INTRODUCTION

Industrial Control Systems (ICS) are computer controlled systems used to continuously monitor and control the critical industrial infrastructures worldwide. ICS encompasses several types of control systems used to automate industrial processes [1]. This includes Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and other smaller control system configurations such as Programmable Logic Controllers (PLCs) and Remote Terminal Unit (RTUs). Automation in industries is the use of these control systems integrated with information technologies without significant human intervention to carry out the task smartly and achieve performance superior to manual operation.

The use of SCADA creates a drastic change in optimizing the production processes in industries. It is very much essential for the industries to survive in today's globally competitive world. Providing accuracy, quality, safety and in time delivery of what stakeholders exactly wants is possible only with automation and it is the key for successful business. SCADA performs vital functions across many of our nation's critical infrastructures [2], including electric power generation, transmission and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing *etc.*.

The IACS (Industrial automation and control system) is usually portrayed in the form of pyramid [3] as shown in Figure 1. It consists of Enterprise, Supervisory control system, Control level and Field level for controlling, monitoring and commanding to achieve automation and control the IACS.

This pyramid gives an idea of the number of devices at different levels and the amount of

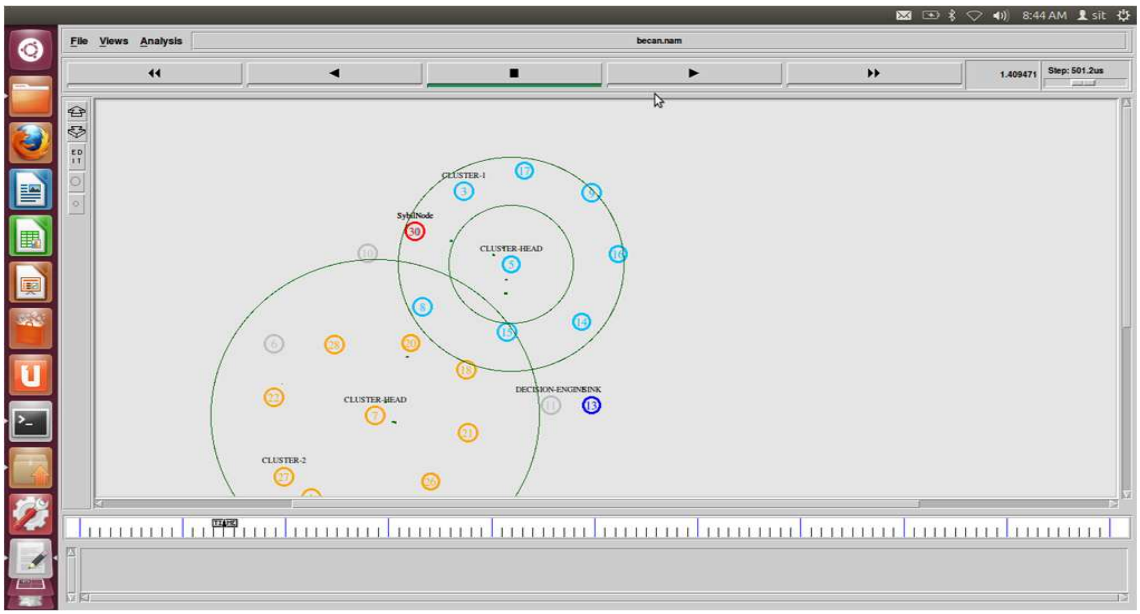

Figure 15. Sybil Attack

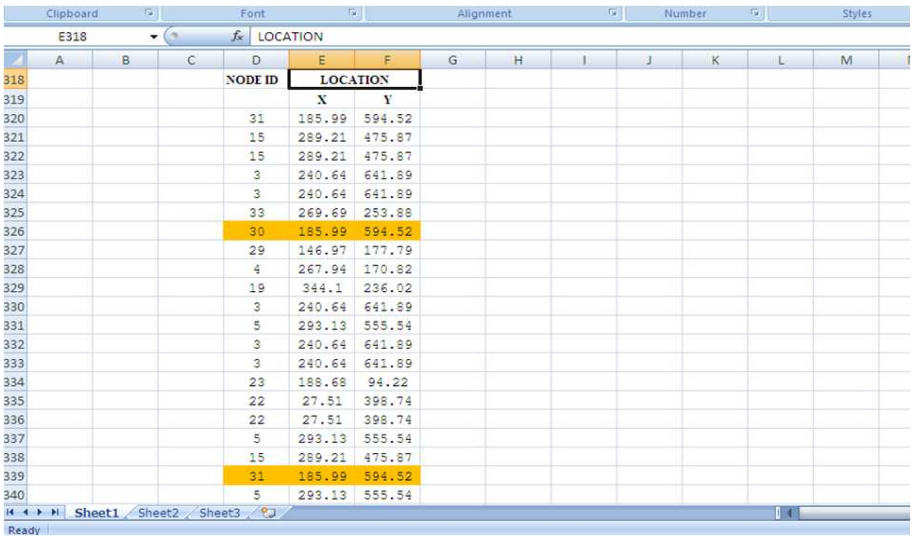

Figure 16. Node Creating Sybil Attack

REFERENCES

1. Keith Stouffer, Joe Falco, Karen Scarfone. NIST- Guide to Industrial Control Systems (ICS) Security, 2011.
2. http://en.wikipedia.org/wiki/SCADA
3. Infenion - Industrial Automation Products for Energy Efficient Applications, 2010.
4. Jayne Caswell. Survey of Industrial Control System Security, 2011.
5. D Robert, B Colin, D Ed and M G N Juan. SKMA a Key Management Architecture for SCADA Systems, *In Proceedings of 4th*

Australasian Information Security Workshop, pages 138–192, 2006.
6. Sungjin Lee, Donghyun Choi, Choonsik Park and Seungjoo Kim. An Efficient Key Management Scheme for Secure SCADA Communication, *World Academy of Science, Engineering and Technology*, 2008.
7. Alan Price, Kristie Kosaka and Samir Chatterjee. A Secure Key Management Scheme for Wireless Sensor Networks, *In Proceedings of the Tenth Americas Conference on Information Systems, New York*, 2004.
8. Chi Yuan Chen and Han Chieh Chao. A Survey of Key Distribution in Wireless Sensor Networks, *Published Online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.354*, 2011.
9. Seyita Camtepe and Bulent Yener. A Survey on Key Distribution Mechanisms for Wireless Sensor Network, 2007.
10. NikolasBardis and NikolasDoukas. A New Approach of Secret Key Management Lifecycle of Military Applications, *Wseas Transactions on Computers, ISSN: 1109-2750*, 2008.
11. Kishore Rajendiran, Radha Sankararajan and Ramasamy Palaniappan. A Secure Key Predistribution Scheme for WSN Using Elliptic Curve Cryptography, *ETRI Journal, 33* , October 2011.
12. Karen Kent and Murugiah Souppaya. Guide to Computer Security Log Management, *By National Institute of Standards and Technology(NIST)*, 2006.
13. Choudhury Aditya Narayan. Data-Logging and Supervisory Control in WSN, 2005.
14. Mary Mathews, Min Song, Sachin Shetty and Rick McKenzie. Detecting Compromised Nodes in Wireless Sensor Networks, *In proceedings of Eighth ACIS International Conference on Software Engineering, Artificial Intelligence,* 2007.
15. C I Ezeife and Maxwell-WIDS. A Sensor-Based Online Mining Wireless Intrusion Detection System, *In proceedings of 12th International Database Engineering and Applications Symposium (IDEAS 2008)*, Portugal, 2008.
16. Andriy Stetsko, Lukas Folkman and Vashek Matyas. Neighbor-based Intrusion Detection for Wireless Sensor Networks, *In proceedings of ICWMC 6th International Conference on Wireless and Mobile Communications,* Pages 420–425, 2010.
17. Bonnie Zhu and Anthony Joseph. A Taxonomy of Cyber Attacks on SCADA Systems, 2012.
18. Bonnie Zhu Shankar Sastry. SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy, 2011.
19. Blundo, A De Santis, A Herzberg, S Kutten, U Vaccaro and M Yung. (Perfectly-Secure Key Distribution for Dynamic Conferences), *In Advances in Cryptology CRYPTO 92, LNCS 740*, pages 471–486, 1993.
20. Suraj Kumar. Compuatational Analysis of Modified Blom Scheme, 2011.
21. Stallings W. Cryptography and Network Security Principles and Practices, 4th ed. USA:Prentice Hall, 2005.
22. Hani Alzaid, DongGook Park, Juan Gonzlez Nieto, Colin Boyd and Ernest Foo1. A Forward and Backward Secure Key Management in Wireless Sensor Networks for PCS/SCADA, *In Proceedings of the 1st International ICST Conference on Sensor Systems and Software, Pisa.*, 2009.

Pramod T C obtained his B.E from Visvesvaraya Technological University, India.He is presently pursuing research work at Siddaganga Institute of Technology, Tumkur, Karnataka, India. His research interest includes Information and Network Security.

N R Sunitha obtained her B.E from Gulbarga University, India, M.S. from Birla Institute of Technology, Pilani, India and Ph.D from Visvesvaraya Technological University, India. She is presently working as Professor in the Department of Computer Science, Siddaganga Institute of Technology, Tumkur, India.