A Review of SCADA IoT Device Vulnerabilities in the Power Grid (A Case Study of Smart Meter)

Ahmed MWENDA[1], Daniel NGODYA[2]
[1] Research, Tanzania Electric Supply Company, Dodoma, Tanzania
Ahmed.mwenda@tanesco.co.tz
[2] Department of Computer Science and Engineering, The University of Dodoma, Dodoma, Tanzania
dngondya@gmail.com

Abstract

This article summarizes and organizes recent research findings in information and communication technology security developments integrated with smart grids. A vital component of a smart grid is a smart meter. It is relevant because it can collect, process, and transport customer's data over the Internet. Whereas developments in smart grid and smart meter technologies have given new productivity gains, they have also presented new security concerns. Security is essential in defending both the smart grid and smart meter from cyber-attack. Guaranteeing safety is one of the most challenging aspects of designing and deploying a smart metering infrastructure. This study presents a thorough investigation of the integrity of smart metering technologies from multiple different viewpoints. It focuses on threats, countermeasures, and estimations. This article makes four contributions: First, all potential vulnerabilities in smart metering components are described and examined. Second, it assesses the impact of attacks that use these weaknesses to boost the performance of each part and the whole smart meter structure. Thirdly, potential countermeasures to defend smart meters are discussed. lastly, it discusses the unresolved issues surrounding smart meter security and future research areas. This evaluation is distinctive due to its exhaustive treatment of security weaknesses and attacks on smart meter components. In conclusion, the future vision is described.

Index terms: IoT, SCADA, Smart Grid, Smart Meter, vulnerabilities

References

[1]. S. Ant´on, D. Fraunholz, C. Lipps, F. Pohl, Marc. Zimmermann and H, Schotten, "Two Decades of SCADA Exploitation:Brief History," IEEE, pp. 1-2, 2017.

[2]. V. Poosapati, V. Katneni and V. Manda, "Super SCADA Systems: A Prototype for Next Gen SCADA System," IAETSD JOURNAL FOR ADVANCED RESEARCH IN APPLIED SCIENCES, vol. 5, pp. 110-114, 2018.

[3]. G. Yadav & K. Paul, "Assessment of SCADA System Vulnerabilities," IEEE, pp. 1-2, 2019.

[4]. T. Simon, "Critical Infrastructure and the Internet of Things," Centre for International Governance Innovation, 2017.

[5]. F. Aloul, A. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions," International Journal of Smart Grid and Clean Energy, p. 3, 2012.

[6]. Busom, N., Petrlic, R., Sebé, F., Sorge, C., & Valls, M., "Efficient SMing based on homomorphic encryption," Computer Communications, pp. 82, 95-101., 2016.

[7]. Beigi-Mohammadi, N., Mišić, J., Khazaei, H., and Mišić, V. B., "An intrusion detection system for smart grid neighborhood area network," In 2014 IEEE International Conference on Communications (ICC), pp. pp. 4125-4130). IEEE., 2014, June.

[8]. K. Gupta, S. Sahoo, B. Ketan, F. Blaabjerg and P. Popovski, "On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids," MDPI, pp. 14(16), 4941., 2021.

[9]. S. Naz Islam, Z. Baig, and S. Zeadally, "Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures," IEEE, 2020.

[10]. B. K. Nitin, "Cybersecurity of SMs," International Journal of Innovative Science and Research Technology, 2022.

[11]. E. Erdemir, D. Gunduz and P. Dragotti, "Privacy in Dynamical Systems," in SM Privacy, Pringer, 2019, pp. 6-7.

[12]. C. Sun, J. Sebastioan, A. Hahn, and C. Liu, "Intrusion detection for cybersecurity of SMs.," IEEE Transactions on Smart Grid, p. 3, 2020.

[13]. K, Sgouras, A. Birda and D. Labridis, "Cyber attack impact on critical smart grid infrastructures.," IEEE, pp. 3-5, February 2014.

[14]. F. Tabrizi and K. Pattabiraman, "A Model-Based Intrusion Detection System for SMs," IEEE 15th International Symposium on High-Assurance Systems Engineering, p. 23, 2014.

[15]. K. Y, "A survey on SMing and smart grid communication," Elsevier, pp. 314 - 315, 2016.

[16]. S. Islam, Z. Baig and S. Zeadally, "Physical Layer Security for the Smart Grid: Vulnerabilities, Threats and Countermeasures," IEEE, pp. 4 - 5, 2018.

[17]. T. Alladi, V. Chamola, B. Sikdar and Kim, Raymond, "Consumer IoT: Security Vulnerability Case Studies and Solutions," IEEE Consumer Electronics Magazine, pp. 7 - 8, 2019.

[18]. X. Liu, P. Zhu, Y. Zhang and K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure," IEEE TRANSACTIONS ON SMART GRID, vol. 6, pp. 5-6, 2015.

[19]. L. Kiarie, P. Langat and C. Muriithi, "Application of Spritz Encryption in SMs to Protect Consumer Data," Hindawi: Journal of Computer Networks and Communications, pp. 2 - 5, 2019.

[20]. W. Xu, J. Sun, R. Cardell-Oliver, A. Mian and J. Hong, "A Privacy-Preserving Framework Using Homomorphic Encryption for SMing Systems," MDPI, pp. 8 - 19, 2023.

[21]. P. Kumar, A. Gurtov, M. Sain, A. Martin and P. Ha, "Lightweight Authentication and Key Agreement for SMing in Smart Energy Networks.," IEEE Transactions on Smart Grid, pp. 2 - 5.

[22]. Harishma et al, "Safe is the new Smart: PUF-based Authentication for Load Modification-Resistant SMs," IEEE: Transactions on Dependable and Secure Computing, pp. 4, 8, 10 -14.

[23]. S. Qaddoori and Q. Ali, "An embedded intrusion detection and prevention system for home area networks in advanced metering infrastructure.," John Wiley & Sons Ltd, 2022, pp. 314 - 325.

[24]. T. Andrysiak, A. Saganowski and P. Kiedrowski, "Anomaly Detection in SMing Infrastructure with the Use of Time Series Analysis," Hindawi, pp. 5-7, 2017.