Firmware Attacks: The Silent Threat to Your IoT Connected Devices

I. Dwaraka Srihith[1]
[1]Alliance University, Bangalore
A. David Donald[2], T. Aditya Sai Srinivas[2]
[2]Ashoka Women's Engineering College, Kurnool
D. Anjali[3], A. Chandana[3]
[3]G. Pulla Reddy Engineering College, Kurnool

Abstract: *Firmware attacks on IoT devices have become a growing concern in recent years. These attacks exploit vulnerabilities in the firmware, which is the low-level software that controls the hardware of the device, to gain access to sensitive data or control the device remotely. Firmware attacks are particularly dangerous because they can be difficult to detect and can allow attackers to maintain access to a device for an extended period of time. In this paper, we explore the silent threat of firmware attacks on connected devices and the potential consequences of a successful attack. We discuss the methods that attackers use to exploit firmware vulnerabilities and the impact these attacks can have on the security and privacy of users. We also provide recommendations for protecting against firmware attacks, including keeping firmware up to date, using strong passwords, and monitoring for suspicious activity on the network. By understanding the risks and taking proactive steps to protect against firmware attacks, users can help to ensure the security and integrity of their connected devices*.

Keywords: Internet of Things (IoT), Firmware attacks.

REFERENCES

[1]. Alrawais, A., Alhothaily, A., Hu, X., Cheng, X., & Li, F. (2018). Security in the internet of things: A review. Journal of Network and Computer Applications, 107, 10-28.

[2]. Goyal, M., & Goyal, V. K. (2018). A review on security threats in Internet of Things. Journal of Computer Networks and Communications, 2018.

[3]. Garcia, F. D., & Jacobsen, H. A. (2018). Security and privacy challenges in the Internet of Things: Current status and future perspectives. Journal of Reliable Intelligent Environments, 4(1), 1-14.

[4]. Zhang, X., Chen, Q., & Wang, X. (2020). Security and privacy in the Internet of Things: A comprehensive review. Journal of Network and Computer Applications, 150, 102510.

[5]. Kumar, S., Gill, S. S., & Singh, S. (2019). Internet of Things (IoT): Security challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 10(6), 2179-2202.

[6]. Singh, D. K., Tripathi, A., Kumar, P., & Kumar, N. (2018). A comprehensive study of security of Internet of Things. Journal of Information Security and Applications, 41, 38-50.

[7]. Shen, Y., Mao, X., & Li, L. (2019). A review on firmware vulnerabilities and attacks in embedded systems. Journal of Cybersecurity, 5(1), tyz002.

[8]. Palmieri, P., &Riccobene, S. (2019). Firmware hacking: The threat to IoT security. Future Internet, 11(10), 215.

[9]. Sears, R. J., Butler, K. R., & Hunker, J. (2018). Firmware attacks and defenses: A taxonomy and research directions. Journal of Cybersecurity, 4(1), tyy001.

[10]. Dorri, A., Kanhere, S. S., &Jurdak, R. (2019). A survey on security threats and countermeasures for the Internet of Things. IEEE Communications Surveys & Tutorials, 21(3), 2702-2731.

[11]. Dinh, T. N., Thai, M. T., & Kim, D. (2019). A comprehensive review of security issues in the Internet of Things: A survey. Journal of Network and Computer Applications, 126, 22-43.

[12]. Carrión, M. Á., Triviño, G. N., & Ceballos, J. M. (2020). Firmware security in embedded systems. Journal of Systems Architecture, 104, 101703.

[13]. Sfar, H., Elleuch, H., &Bouallegue, R. (2018). IoT security: Review, blockchain solutions, and open challenges. Journal of Ambient Intelligence and Humanized Computing, 9(4), 1015-1033.

[14]. Srinivas, T. "Aditya Sai et MANIVANNAN, SS Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm." Computer Communications (2020).

[15]. Zarpelão, B. B., Miani, R. S., &Kawakani, C. T. (2017). Internet of Things (IoT) security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[16]. Fernandes, J., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. IEEE Symposium on Security and Privacy, 2016, 636-654.

[17]. Kolias, C., Stavrou, A., Voas, J., Bojanova, I., & Kuhn, R. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

[18]. Liu, L., Gong, X., & Chen, C. (2020). The evolution of IoT malware and related defense techniques. Journal of Network and Computer Applications, 152, 102508.

[19]. Ammar, M., Russello, G., &Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Security and Communication Networks, 2018, 1-18.

[20]. Srinivas, T. "Aditya Sai, B." In Ravindra Babu, Miskir Solomon Tsige, R. Rajagopal, S. Devi, and Subrata Chowdhury." Effective implementation of the Prototype of a digital stethoscope using a Smartphone." In 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), pp. 1-8.

[21]. Liu, Y., &Abouzied, A. (2019). Firmware security analysis and attack surface measurement: A case study of a smart bulb. IEEE Internet of Things Journal, 6(1), 1069-1081.

[22]. Trabelsi, S., Yahyaoui, T., &Bouallegue, R. (2021). Survey of firmware security vulnerabilities and countermeasures in the Internet of Things. Journal of Ambient Intelligence and Humanized Computing, 12(9), 10349-10368.

[23]. "Firmware Security" by HovavShacham and Stefan Savage. IEEE Symposium on Security and Privacy, 2008.

[24]. "The State of Firmware Security" by John Loucaides. Black Hat Asia, 2019.

[25]. "Internet of Things Security: A Review" by Ali Abbasi and Mohammad Rezaeirad. Journal of Information Security and Applications, 2019.

[26]. Mahalaxmi, G., R. Varaprasad, and T. Aditya Sai Srinivas. "Blockchain Solutions for IoT Devices Against DDoS Attacks: A Review." IUP Journal of Information Technology 18, no. 4 (2022): 25-46.

[27]. "A Survey of Firmware Vulnerabilities and Defenses in Embedded Systems" by Yeongjin Jang and Kangbin Yim. IEEE Communications Surveys and Tutorials, 2018.

[28]. "Firmware Security Challenges in Embedded Systems" by Hatem Hammami and ChirazTrabelsi. International Conference on Advanced Technologies for Signal and Image Processing, 2020.

[29]. Srihith, I. Venkata Dwaraka, I. Venkata Siva Kumar, R. Varaprasad, Y. Rama Mohan, T. Aditya Sai Srinivas, and Y. Sravanthi. "Future of Smart Cities: The Role of Machine Learning and Artificial Intelligence." South Asian Res J Eng Tech 4, no. 5 (2022): 110-119.

[30]. "Internet of Things: A Review of Current Security and Privacy Issues" by Raja Naeem Akram, Muhammad Khurram Khan, and Syed Ali Hassan. IEEE Communications Surveys and Tutorials, 2019.

[31]. "Security in the Internet of Things: A Review" by Marko Jäntti and Timo Hämäläinen. International Journal of Communication Systems, 2017.

[32]. "Firmware Security: Best Practices for Firmware Security" by Tim Lewis. Synopsys, 2019.

[33]. "Securing IoT with Lightweight Cryptography: A Review" by Shib Sankar Sana and Sanjay Kumar Biswas. Journal of Ambient Intelligence and Humanized Computing, 2018.

[34]. "IoT Security: Review, Blockchain Solutions, and Open Challenges" by Andrea Saracino and Tommaso Cucinotta. Sensors, 2021.