Daftar Pustaka

[1] D. K. Nilsson, L. Sun, and T. Nakajima, “A framework for self-verification of firmwareupdates over the air in vehicle ecus,” *2008 IEEE Globecom Work. GLOBECOM 2008*, pp. 1–5, 2008.

[2] K. Doddapaneni, R. Lakkundi, S. Rao, S. G. Kulkarni, and B. Bhat, “Secure FoTA Object for IoT,” *Proc. - 2017 IEEE 42nd Conf. Local Comput. Networks Work. LCN Work. 2017*, pp. 154–159, 2017.

[3] H. Chandra, E. Anggadjaja, P. S. Wijaya, and E. Gunawan, “Internet of Things: Over-the-Air (OTA) firmware update in Lightweight mesh network protocol for smart urban development,” *Proc. - Asia-Pacific Conf. Commun. APCC 2016*, pp. 115–118, 2016.

[4] K. Fan, Y. Ren, and Z. Yan, “Secure Firmware Updates for IoT: A Survey,” *2018 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, pp. 1349–1354, 2018.

[5] N. Cheng, Y. Wang, X. Zhao, and N. Li, “The digital fingerprint of XML Electronic Medical Records based on HMAC-SHA256 Algorithm,” *2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, ICCSN 2011*, vol. 9, no. 1, pp. 338–340, 2011.

[6] A. Bhawiyuga, M. Data, and A. Warda, “Architectural design of token based authentication of MQTT protocol in constrained IoT device,” *Proceeding 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2017*, vol. 2018-Janua, pp. 1–4, 2018.

[7] J. P. Kaps, “Cryptography for ultra-low power devices,” *Analysis*, 2006.

[8] K. Daimi, M. Saed, S. Bone, and M. Rizwan, “Securing Vehicle ECUs Update Over The Air,” *Twelfth Adv. Int. Conf. Telecommun. Secur.*, no. c, pp. 45–50, 2016.

[9] A. Schweizer, “Secure over-the-air updates for ESP32,” 2017. [Online]. Available: https://blog.classycode.com/secure-over-the-air-updates-for-esp32-ec25ae00db43.

[10] B. C. Choi, S. H. Lee, J. C. Na, and J. H. Lee, “Secure firmware validation and update for consumer devices in home networking,” *IEEE Trans. Consum. Electron.*, vol. 62, no. 1, pp. 39–44, 2016.

[11] S. Falas, C. Konstantinou, and M. K. Michael, “A Hardware-based Framework for Secure Firmware Updates on Embedded Systems,” *IEEE/IFIP Int. Conf. VLSI Syst. VLSI-SoC*, vol. 2019-Octob, pp. 198–203, 2019.

[12] D. M. Shila, P. Geng, and T. Lovett, “I can detect you: Using intrusion checkers to resist malicious firmware attacks,” *2016 IEEE Symp. Technol. Homel. Secur. HST 2016*, pp. 1–6, 2016.

[13] J. Selin, “Evaluation of Threat Modeling Methodologies A Case Study,” *Sch. Technol. Inf. Commun. Technol.*, vol. Master, no. May, 2019.

[14] OWASP, “Owasp Top 10(En),” 2017. [Online]. Available: https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication.