DAFTAR PUSTAKA

[1] H. Lan, X. Zhu, J. Sun, dan S. Li, "Traffic Data Classification to Detect Man-in-the-Middle Attacks in Industrial Control System," dalam *Proceedings - 2019 6th International Conference on Dependable Systems and Their Applications, DSA 2019*, 2020, hlm. 430–434. doi: 10.1109/DSA.2019.00067.

[2] D. Formby dan R. Beyah, "Temporal Execution Behavior for Host Anomaly Detection in Programmable Logic Controllers," *IEEE Transactions on Information Forensics and Security*, vol. 15, hlm. 1455–1469, 2020, doi: 10.1109/TIFS.2019.2940890.

[3] Ž. Jakovljević dan D. Nedeljković, "Cybersecurity Issues in Motion Control - An Overview of Challenges," dalam *Proceedings - 10th International Conference on Electrical, Electronic and Computing Engineering, IcETRAN 2023*, 2023. doi: 10.1109/IcETRAN59631.2023.10192157.

[4] H. Lan, X. Zhu, J. Sun, dan S. Li, "Traffic Data Classification to Detect Man-in-the-Middle Attacks in Industrial Control System," dalam *Proceedings - 2019 6th International Conference on Dependable Systems and Their Applications, DSA 2019*, 2020, hlm. 430–434. doi: 10.1109/DSA.2019.00067.

[5] D. Urbina, J. Giraldo, N. O. Tippenhauer, dan A. Cardenas, *Attacking fieldbus communications in ICS: Applications to the SWaT testbed*, vol. 14. 2016. doi: 10.3233/978-1-61499-617-0-75.

[6] N. LaLone, *On the growing importance of routine cybersecurity*. 2024. doi: 10.1016/B978-0-12-809526-3.00011-7.

[7] W. Alsabbagh dan P. Langendorfer, "You Are What You Attack: Breaking the Cryptographically Protected S7 Protocol," dalam *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS*, 2023. doi: 10.1109/WFCS57264.2023.10144251.

[8] H. Hui, K. McLaughlin, dan S. Sezer, "Vulnerability analysis of S7 PLCs: Manipulating the security mechanism," *International Journal of Critical Infrastructure Protection*, vol. 35, 2021, doi: 10.1016/j.ijcip.2021.100470.

[9] F. Zare, P. Mahmoudi-Nasr, dan R. Yousefpour, "A Real-Time Network based Anomaly Detection in Industrial Control Systems," *International Journal of Critical Infrastructure Protection*, vol. 45, Jul 2024, doi: 10.1016/j.ijcip.2024.100676.

[10] S. Banik, T. Banik, S. M. M. Hossain, dan S. K. Saha, "Implementing Man-in-the-Middle Attack to Investigate Network Vulnerabilities in Smart Grid Test-bed," dalam *2023 IEEE World AI IoT Congress (AIIoT)*, Institute of Electrical and Electronics Engineers Inc., Mei 2023. [Daring]. Tersedia pada: http://arxiv.org/abs/2306.00234

[11] A. Robles-Durazno, N. Moradpoor, J. McWhinnie, G. Russell, dan I. Maneru-Marin, "PLC memory attack detection and response in a clean water supply system," *International Journal of Critical Infrastructure Protection*, vol. 26, Sep 2019, doi: 10.1016/j.ijcip.2019.05.003.

[12] O. Eigner, P. Kreimel, dan P. Tavolato, "Detection of man-in-the-middle attacks on industrial control networks," dalam *Proceedings - 2016 International Conference on Software Security and Assurance, ICSSA 2016*, Institute of Electrical and Electronics Engineers Inc., Feb 2017, hlm. 64–69. doi: 10.1109/ICSSA.2016.19.

[13] E. E. Miciolino, G. Bernieri, F. Pascucci, dan R. Setola, "Communications network analysis in a SCADA system testbed under cyber-attacks," dalam *2015 23rd Telecommunications Forum Telfor (TELFOR)*, IEEE, Nov 2015, hlm. 341–344. doi: 10.1109/TELFOR.2015.7377479.

[14] A. Ocaka, D. Ó Briain, dan K. Barrett, "Evaluating the Impact of Cyberattacks on PLC Performance: A Systematic Implementation and Empirical Investigation," dalam *IFAC-PapersOnLine*, Elsevier B.V., Jun 2024, hlm. 387–392. doi: 10.1016/j.ifacol.2024.07.182.

[15] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, dan N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput Secur*, vol. 89, 2020, doi: 10.1016/j.cose.2019.101677.

[16] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, dan A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, Jun 2015. doi: 10.6028/NIST.SP.800-82r2.

[17] K. Stouffer *dkk.*, "Guide to Operational Technology (OT) security," Sep 2023. doi: 10.6028/NIST.SP.800-82r3.

[18] W. Alsabbagh dan P. Langendorfer, "You Are What You Attack: Breaking the Cryptographically Protected S7 Protocol," dalam *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/WFCS57264.2023.10144251.

[19] C. Lei, L. Donghong, dan M. Liang, "The spear to break the security wall of S7CommPlus," dalam *Black Hat Europe 2017*, Black Hat, Des 2017. Diakses: 2 Februari 2025. [Daring]. Tersedia pada:

https://www.blackhat.com/docs/eu-17/materials/eu-17-Lei-The-Spear-To-Break%20-The-Security-Wall-Of-S7CommPlus-wp.pdf

[20] E. Biham, S. Bitan, A. Carmel, A. Dankner, U. Malin, dan A. Wool, "Rogue7: Rogue Engineering-Station attacks on S7 Simatic PLCs," dalam *Black Hat USA 2019*, Black Hat, Agu 2019. Diakses: 2 Februari 2025. [Daring]. Tersedia pada: https://i.blackhat.com/USA-19/Thursday/us-19-Bitan-Rogue7-Rogue-Engineering-Station-Attacks-On-S7-Simatic-PLCs-wp.pdf

[21] R. Shimonski, "Assumption (Man in the Middle)," dalam *Penetration Testing For Dummies*, 2020, hlm. 69–78.

[22] B. Pingle, A. Mairaj, dan A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," dalam *2018 IEEE International Conference on Electro/Information Technology (EIT)*, IEEE, Mei 2018, hlm. 0192–0197. doi: 10.1109/EIT.2018.8500082.

[23] A. Sagynbay, A. Balapan, dan T. Alizadeh, "Design and Implementation of a Fault Inspection System for the Festo Modular Production System (MPS)," dalam *2023 23rd International Conference on Control, Automation and Systems (ICCAS)*, IEEE, Okt 2023, hlm. 706–711. doi: 10.23919/ICCAS59377.2023.10316847.

[24] M. Gao, D. Feng, dan J. Chu, "Analysis of delay attacks based on game theory in time synchronization protocols," dalam *WIT Transactions on Information and Communication Technologies*, 2014, hlm. 987–995. doi: 10.2495/ICCT131131.

[25] Q. S. Qassim, N. Jamil, M. Daud, N. Ja'affar, W. A. W. Kamarulzaman, dan M. N. Mahdi, *Compromising the Data Integrity of an Electrical Power Grid SCADA System*, vol. 1347. 2021. doi: 10.1007/978-981-33-6835-4_40.

[26] A. S. Tanenbaum dan D. J. Wetherall, *Computer Networks*, 5 ed. Boston: Prentice Hall, 2010.

[27] B. Cassottana, M. M. Roomi, D. Mashima, dan G. Sansavini, "Resilience analysis of cyber-physical systems: A review of models and methods," *Risk Analysis*, vol. 43, no. 11, hlm. 2359–2379, 2023, doi: 10.1111/risa.14089.

[28] F. Abut, "A distributed measurement architecture for inferring TCP round-trip times through passive measurements," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 27, no. 3, hlm. 2106–2120, 2019, doi: 10.3906/elk-1808-190.

[29] K. Johan. Aström dan R. M. . Murray, *Feedback Systems: an Introduction for Scientists and Engineers*. Princeton University Press, 2010.

[30] C. Gao, W. Ding, Y. Zhang, dan J. Gong, *Estimating average round-trip time from bidirectional flow records in NetFlow*, vol. 157 LNEE, no. VOL. 2. 2012. doi: 10.1007/978-3-642-28798-5_56.

[31] N. G. Goudru, R. P. Puneeth, dan K. P. N. Rao, *Enhancement of Performance of Round-Trip Time Using Kalman Filtering*, vol. 752 LNEE. 2021. doi: 10.1007/978-981-16-0443-0_8.

[32] Y. Won, M.-J. Choi, B. Park, dan J. W.-K. Hong, "An approach for failure recognition in IP-based industrial control networks and systems," *International Journal of Network Management*, vol. 22, no. 6, hlm. 477–493, 2012, doi: 10.1002/nem.1804.

[33] S. Ziya, "On the relationships among traffic load, capacity, and throughput for the M/M/1/m, M/G/1/m-PS, and M/G/c/c queues," *IEEE Trans Automat Contr*, vol. 53, no. 11, hlm. 2696–2701, 2008, doi: 10.1109/TAC.2008.2007173.

[34] A. B. Firdaus, "Perancangan Sistem Otomasi Proses Stasiun Kerja Modular Production System of Automation Processes (MPS AP) Festo," Fakultas Teknik, Universitas Gadjah Mada, Yogyakarta, Indonesia, 2023.