EVALUASI DAMPAK SERANGAN *MAN-IN-THE-MIDDLE* TERHADAP PERFORMA KOMUNIKASI ICS BERBASIS PLC S7-1500

Nurrizky Ajihan
21/474838/TK/52402

Diajukan kepada Departemen Teknik Nuklir dan Teknik Fisika Fakultas Teknik
Universitas Gadjah Mada pada tanggal 15 Maret 2025
untuk memenuhi sebagian persyaratan untuk memperoleh derajat
Sarjana Program Studi Teknik Fisika

INTISARI

Industrial Control System (ICS) memiliki peran penting dalam mengelola proses industri, namun adanya integrasi antara Teknologi Informasi dan Teknologi Operasional meningkatkan potensi kerentanan, terutama pada komunikasi data PLC Siemens S7-1500 yang menggunakan protokol S7CommPlus tanpa enkripsi. Penelitian ini bertujuan untuk menganalisis kerentanan tersebut terhadap serangan *Man-in-the-Middle* serta mengevaluasi dampaknya terhadap performa komunikasi ICS.

Penelitian ini menggunakan ICS *Testbed* yang terdiri dari PLC Siemens S7-1500, *Engineering Workstation*, dan Raspberry Pi yang menjalankan Kali Linux. Dua skenario serangan MitM diimplementasikan, yaitu modifikasi *byte trailer* dan injeksi data palsu ke memori PLC. Performa komunikasi dianalisis dengan mengukur metrik *Round-Trip Time* dan *Throughput* menggunakan Wireshark, dengan membandingkan data pada kondisi normal, saat serangan aktif, dan setelah serangan dihentikan.

Hasil penelitian menunjukkan bahwa pada skenario modifikasi *byte trailer*, terjadi peningkatan RTT sebesar 52,2% dari 100 ms menjadi 152,268 ms dan *Throughput* menurun 28,9% dari rata-rata 1,678 KBps menjadi 1,194 KBps pada saat serangan aktif, diikuti dengan pemutusan sesi. Pada skenario injeksi data palsu menunjukkan perubahan kecil pada RTT namun terdapat penurunan *Throughput* sebesar 13,18% dari 1,768 KBps menjadi 1,535 KBps. Penelitian ini menekankan pentingnya penerapan enkripsi dan sistem deteksi intrusi untuk meningkatkan keamanan serta menjaga performa komunikasi pada ICS.

Kata kunci: *Man-in-the-Middle*, PLC S7-1500, *Round-Trip Time*, *Throughput*

Pembimbing Utama : Dr.-Ing. Ir. Awang Noor Indra Wardana, S.T., M.T., M.Sc., IPM.
Pembimbing Pendamping : Dr. Eng. Ir. Dwi Joko Suroso, S.T., M.Eng., IPP.

EVALUATION OF IMPACT MAN-IN-THE-MIDDLE ATTACK ON COMMUNICATION PERFORMANCE OF ICS BASED PLC S7-1500

Nurrizky Ajihan
21/474838/TK/52402

Submitted to the Departement of Nuclear Engineering and Engineering Physics
Faculty of Engineering Universitas Gadjah Mada on March 15, 2025
in partial fulfillment of the requirement for the Degree of
Bachelor of Engineering in Engineering Physics

ABSTRACT

Industrial Control Systems (ICS) are crucial in managing industrial processes. However, integrating Information Technology and Operational Technology increases potential vulnerabilities, especially in the data communication of Siemens S7-1500 PLCs that use the S7CommPlus protocol without encryption. This study aims to analyze these vulnerabilities against Man-in-the-Middle attacks and evaluate their impact on communication performance of ICS.

This research utilizes an ICS Testbed comprising a Siemens S7-1500 PLC, an Engineering Workstation, and a Raspberry Pi running Kali Linux. Two MitM attack scenarios are implemented, one involving modification of the byte trailer and another involving injection of false data into the PLC's memory. Communication performance is analyzed by measuring Round-Trip Time and Throughput using Wireshark, with data compared across normal conditions, during active attacks, and after the attacks are halted.

The results showed that in the byte trailer modification scenario, the RTT increased by 52.2% from 100 ms to 152.268 ms, and Throughput decreased by 28.9% from an average of 1.678 KBps to 1.194 KBps during the active attack, followed by session termination. In the false data injection scenario, RTT showed minimal changes, but Throughput decreased by 13.18% from 1.768 KBps to 1.535 KBps. These findings underscore the importance of implementing encryption and intrusion detection systems to enhance security and maintain reliable communication performance within ICS.

Keywords: Man-in-the-Middle, PLC S7-1500, Round-Trip Time, Throughput

Supervisor : Dr.-Ing. Ir. Awang Noor Indra Wardana, S.T., M.T., M.Sc., IPM.
Co-supervisor : Dr. Eng. Ir. Dwi Joko Suroso, S.T., M.Eng., IPP.