MIDI 2025 Conference

Cybersecurity Analysis of Programmable Logic Controllers Under Distributed Denial-of-Service Attacks

Abstract

The increasing integration of industrial control systems with global networks exposes critical components such as Programmable Logic Controllers (PLCs) to severe cyber-attacks.

This paper explores the impact of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks on PLC performance, focusing on control cycle time and the availability of the embedded web server service. A test environment featuring a Siemens S7-1215 PLC, TIA Portal, and PLCSIM Advanced was subjected to simulated assaults. Custom Python scripts with Scapy and Requests were implemented to execute high-rate SYN Flood and HTTP Flood attacks, with network traffic analysed using Wireshark. The results indicate that both attack vectors successfully blocked the web server and introduced a severe extension of the control cycle time, forcing the PLC into a fault state. The application-layer HTTP Flood attack proved to be the most impactful.

These findings confirm the dire threat such attacks pose to PLC stability and real-time operation, highlighting the compelling necessity for robust, multi-layered cybersecurity in modern industrial control systems.