ABSTRACT

From Legacy to Resilience: Securing Industrial Protocols in a Connected Era

Alexander Gebhard

Marquette University, 2026

The convergence of Information Technology (IT) and Operational Technology (OT) in Industry 4.0 environments has greatly expanded the attack surface of critical infrastructure systems. Legacy industrial protocols that were originally intended to only be used in isolated networks are now exposed across interconnected systems. This interconnectivity enables adversaries to target power grids, manufacturing plants, and other critical systems with increasing sophistication. While vendors have retroactively introduced security extensions to industrial protocols such as EtherNet/IP (CIP) and OPC Unified Architecture (OPC UA), the adequacy and practical feasibility of these security measures remains understudied.

This dissertation advances the security of industrial protocols through three main contributions. First, we introduce an extendable attack-defense tree methodology for threat modeling industrial protocols. We show its practicality by applying it to both CIP and OPC UA. Our analysis reveals that the two protocols take fundamentally different security approaches. CIP leverages standardized technologies such as Transport Layer Security (TLS), while OPC UA employs custom protocol-specific solutions. This gives each protocol positives and negatives in terms or security. While both protocols mitigate common threats, both protocols share a common failure to mitigate multicast-based threats.

Second, we empirically evaluate the use of Ed25519 digital signatures to secure the Precision Time Protocol (PTP). We deployed a modified version of LinuxPTP to support Ed25519 across all four PTP clock types on Raspberry Pi 5 hardware to gauge the impact of Ed25519 on PTP. PTP is a challenging protocol multicast security due to its strict sub-microsecond timing requirements. Our measurements demonstrate that Ed25519 introduces no degradation to clock synchronization accuracy. Although, we saw modest increases in residence time, memory consumption, and CPU utilization. Third, we propose and evaluate two key management architectures for distributing Ed25519 keys in PTP networks: a centralized scheme aligned with ongoing IEEE 1588 working group standardization efforts, and a decentralized peer-to-peer scheme. Both architectures are validated through threat modeling and formal verification. Additionally, we implemented the decentralized approach and open-sourced as an extension to LinuxPTP. We further discuss how digital signatures can be applied to secure multicast in protocols such as CIP and OPC UA. Together, these contributions forward research efforts for securing industrial time-synchronization and control protocols in resource-constrained, real-time environments.