Enhancing Industrial Device Onboarding Using Remote Attestation

Volodymyr Trykoz[1], Björn Leander[2], Saad Mubeen[1], and Mohammad Ashjaei[1]

[1] Mälardalen University, Västerås, Sweden
[2] ABB Process Automation, Process Control Platform, Västerås, Sweden
firstname.lastname@mdu.se[1]; firstname.lastname@se.abb.com[2]

Volodymyr Trykoz is the presenting author

Abstract. As industry moves toward modern and flexible solutions such as modular automation and increased vendor diversity, the security of automation systems becomes increasingly critical. The attack surface expands as more network interfaces are introduced and devices become exposed to the internet and cloud environments. At the same time, these advances encourage the rapid introduction and replacement of devices, making it challenging to track vulnerabilities and ensure that no malicious components are introduced into the system. Therefore, establishing trust in a device prior to onboarding is essential for maintaining the overall security and safety of the system. In this work, we propose enhancing the onboarding process with a remote attestation mechanism aligned with the Remote ATtestation ProcedureS (RATS) architecture. To demonstrate the feasibility of the approach, we present a reference implementation that integrates remote attestation into Open Platform Communications Unified Architecture (OPC UA). Furthermore, we provide a security analysis of the proposed solution using a STRIDE-based threat model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege).