Lost in Translation: When Industrial Protocol Translation Goes Wrong

This research paper delves into the vital role of protocol translation in industrial facilities by looking at the protocol gateway. It is a small device that translates the different protocols used by machinery, sensors, actuators, and computers that operate smart factories, dams, power plants, and other industrial facilities.

If protocol gateways fail, then the communication between the control systems and machinery would stop. Operators would lose visibility over the system, making them unable to tell if machines or generators are running properly. Translation failure can also prevent the operator from issuing commands to troubleshoot problems.

Key Discoveries

We have found various security issues and vulnerabilities in protocol gateways that could impact a facility's operations in different ways:

- Specific scenarios wherein an attacker could exploit vulnerabilities in the translation function to issue stealth commands that can sabotage the operational process
- Authentication vulnerabilities that allow unauthorized access
- Weak encryption that could allow decryption of configuration databases
- Weak implementation of authentication mechanisms that could expose sensitive information
- Conditions for denial of service (DoS)

These vulnerabilities could affect a facility's processes and output. Threat actors could leverage these flaws to prevent engineers from controlling or monitoring industrial systems, which could, in turn, cause failure to deliver essential output such as power and water or compromise the quality of manufactured products.

Scope and Impact

We designed this research for a broad technical audience so it is not limited to individuals who have a background in operational technology (OT) engineering. Those with an information technology (IT) perspective and trying to learn more about OT should be able to understand the paper's contents as we give an introduction on protocol gateways before tackling our findings.

Auditors and consultants can also learn about the business implications of the related vulnerabilities and attack scenarios in a dedicated section that focuses on impact. We used the MITRE ATT&CK framework for Industrial Control Systems to map out possible attack techniques, as well as the corresponding implications.

Recommendations

Lastly, we provide detailed recommendations and a security checklist to ensure that concerned parties can address or mitigate all the security issues and vulnerabilities raised in our research paper. Here are some of our recommendations.

- Consider the design aspects of protocol gateways, such as differences in filtering capabilities when procuring these devices.
- Configure and secure the gateway properly. Protocol gateways can be an overlooked aspect of an industrial facility's overall security.
- Treat protocol gateways as critical OT devices, to better frame a security plan for its function and prevent it from being overlooked in terms of defenses.

Read the full paper at **https://bit.ly/ProtocolGateways** for more on protocol translation device vulnerabilities and threat scenarios.

TREND MICRO™ | research