THE PITFALLS OF LEGACY TECHNOLOGY

Exposing Critical Flaws in Programmable Industrial Machines

Industrial automation enables enterprises across sectors in the manufacturing industry — including automotive, avionics, military, food and beverage, and pharmaceuticals — to produce goods on a large scale. In our research paper "Rogue Automation: Vulnerable and Malicious Code in Industrial Programming," we reveal previously unknown design flaws that threat actors could exploit to hide malicious functionalities in robots and other programmable industrial machines.

The technology that drives programmable industrial machines was designed decades ago, but it remains to be the backbone of modern manufacturing. This is why the flaws we found are hard to fix at their root and can be mitigated only with specific secure network architectures.

Security-Sensitive Features in Industrial Automation

Our main discovery revolves around security-sensitive features that are present in the legacy programming languages of some of the most popular industrial robotic platforms. We demonstrate how these features could lead to vulnerabilities or be abused by malicious actors to create new strains of self-propagating malware that traditional endpoint scanners would not be able to detect.

Failure to address these issues could allow an advanced, state-level attacker to remain persistent within the digital equipment of a smart factory for surveillance and reconnaissance, and to perform a variety of malicious activities — from altering the quality of products and halting the manufacturing line to causing damage to robots and even exfiltrating intellectual property.

Actionable Advice for the Manufacturing Industry

We coordinated with Robot Operating System – Industrial (ROS-I), a consortium of leading original equipment manufacturers and research organizations, to establish practical security recommendations that can help users avoid common configuration and programming mistakes. Used with proper network security equipment, these guidelines can help reduce the exploitability of the vulnerabilities that we discovered. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the US Cybersecurity and Infrastructure Security Agency (CISA) also released an alert confirming the severity of our findings and acknowledging the suggested mitigation strategy. Our recommendations can be summarized thus:

- **Network segmentation:** Use proper network protection devices to isolate industrial robots that need to process data coming from other networks.
- **Secure programming:** Promote secure programming guidelines among control process engineers and programmers.
- **Automation code management:** Know and keep track of the automation code that is produced by a system integrator and runs in the factory.

For the details of our findings and security recommendations, read our research paper at http://bit.ly/rogueautomation.

TREND MICRO™

In partnership with

POLITECNICO MILANO 1863
DIPARTIMENTO DI ELETTRONICA INFORMAZIONE E BIOINGEGNERIA