CyberDanube:
Industrial Protocol Testing

In-Depth Technical Security Assessments of Industrial Network Protocols.

Industrial protocols play a crucial role in Operational Technology (OT) infrastructure. They allow communication and data exchange between Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), and other operational devices. The data transmitted is often used for remote control and monitoring in industries such as manufacturing, energy and transportation.

Many industrial protocols were not designed with security in mind, making them often vulnerable to cyberattacks. Due to the criticality of the data, these attacks can lead to severe consequences such as production downtime, equipment damage, or even safety hazards.

Technical Assessment

- Authentication & Encryption Weaknesses
- Replay and Injection Attack Testing
- Testing for Memory Corruption Vulnerabilities
- Fuzz Testing of Protocol Implementations
- Protocol Reverse Engineering for proprietary solutions

A comprehensive security assessment of industrial protocols involves testing the entire stack, from network communication layers to application-specific message parsing. This includes testing for replay and injection attacks, authentication & encryption weaknesses, memory corruption vulnerabilities and reverse engineering of proprietary implementations.

With the help of CyberDanube's digital twin framework >MEDUSA< we have the major advantage of identifiying flaws independant of hardware, making it a possible to implement fuzz testing on a scale.

Typical Challenges

- Risk of Service Disruption – Testing on productive systems can halt industrial processes.
- Limited Documentation – Many proprietary protocls lack publicly available specs.
- Hardware Limitations – Industrial Devices are often not build for heavy load.

To overcome these challenges, a controlled test environment or digital twin (firmware emulation with MEDUSA) is often used to conduct the security assessment. This makes sure that live production is not affected and enables advanced reverse engineering and debugging approaches which would not be possible on the physical device.

Typical Findings

- Buffer Overflows
- Type Confusion
- Integer Over/Under-flows
- Denial-of-Service vulnerabilities

CyberDanube has found multiple critical flaws in the past ranging from Fieldbus & Serial Protocols like Modbus, PROFINET and DeviceNet to Network-Based Protocols like OPC-UA, MQTT, EtherNet/IP. Our specialists leveraged cutting-edge fuzzing frameworks, network analysis tools, and firmware reverse engineering techniques to uncover these issues.

Testing Process

The assessment starts with a scope definition during a kick-off appointment. During preparation, conditions like available documentation, devices and possible client/server software are communicated. On project start the protocol gets analysed and reverse engineered in order to find vulnerable attack paths as well as fuzzing targets. Here, the documentation as well as network monitoring tools and binary analysis is used to gain insight into the industrial protocol. Afterwards, the security of these critical paths is assessed with the help of automate & manual testing. In the end a vulnerability report and proof-of-concept exploits is delivered and explained in an final mitigation meeting.

Experts Contact

Sebastian Dietz
Industrial Security Expert

About CyberDanube

CyberDanube is a specialized cyber security company, offering OT, (I)IoT & Embedded Security testing services. CyberDanube provides a unique security toolset & technical consulting, e.g. penetration testing capability with a dedicated hardware lab for in-depth product analysis. With a proven track record in pentesting, research and published advisories including zero-day vulnerabilities, CyberDanube is a trusted authority (CNA) which operates independently from manufactures & investors as trustworthy partner in the security industry.

If you need a Pentest of a OT Infrastructure or an (I)IoT/Embedded Device,

Contact us via : office@cyberdanube.com

This Whitepaper has been inspired by real word projects.