Cyber Security Threats

Identifying and preventing cyber attacks for Industrial Control Systems

BEDROCK
OPEN SECURE AUTOMATION

ICONICS

Table of Contents

What You Want in a "Secure" System

Like all software and hardware, HMI/SCADA and industrial control hardware are a potential target. Industrial Control Systems (ICS) are uniquely high-value targets as they are responsible for critical infrastructure. So how exactly do you distinguish one attack from another, and what countermeasures can you leverage to protect yourself from each type of cyber attack?

CONFIGURATION

No one else can change your configuration

AVAILABILITY

No one can deny you control of your system

DATA CONTROL

No one else is writing to data or changing it

DATA VISIBILITY

No one else is snooping or listening in

Malware

ATTACK OBJECTIVE

Introduce vulnerabilities into a system through code or directly attack the system integrity.

How? By using virus software that is either standalone or hidden within legitimate programs to get into the computer. Software may open ports, disable security, or directly attack specific applications or services.

COUNTER MEASURES

- Stay updated on OS patches
- Use trusted and reputable anti-virus software
- Limit the amount of excess software installed

EXAMPLES

WannaCry

2017

2017

THREAT

Denial of Service

ATTACK OBJECTIVE

Overload or bring down a service so that no one has access to it.

How? By using a large number of devices (willing or unwilling) to attack a site and overwhelm it with communications (DDoS – Distributed Denial of Service).

COUNTER MEASURES

- Air gap or isolate networks when appropriate
- Set limited IP ranges
- Load balance or scale web servers

EXAMPLES

BBC — 2015

IoT_reaper — 2017

THREAT

Phishing

ATTACK OBJECTIVE

Gain privileged access to the application through someone providing their user credentials.

How? By using "social engineering" (tricking people into giving their information or password to the wrong people). It can be as simple as a well-worded email.

COUNTER MEASURES

- Corporate security training
- Email rules to block .zip, .exe, .bat, and others
- Separate email and SCADA networks

EXAMPLES

RSA 2011

TARGET 2013

THREAT

Password Cracking

ATTACK OBJECTIVE

Gain privileged access to an application by logging in using a high-level user account.

How? Repeatedly trying to access the system either with brute force or by focusing on short obvious passwords such as "123456," "qwerty," "password," and "password123."

COUNTER MEASURES

- Encrypt password storage
- Implement maximum password attempt rules
- Implement minimum password complexity rules

EXAMPLES

LinkedIn — 2012

Ashley Madison® .com — 2015

THREAT

SQL Injection

ATTACK OBJECTIVE

Use otherwise normal data entry fields to "inject" code into the application running it.

How? By inserting database instructions that corrupt or access data. Ideally, data fields should throw out incorrectly formatted entries, but sometimes they get through.

COUNTER MEASURES

- Ensure quality product design to prevent vulnerabilities
- Stay updated on OS patches
- Enforce security credentials on all write access points

EXAMPLES

McAfee 2016

Schneider Electric 2017

THREAT

Man-in-the-middle

ATTACK OBJECTIVE

Listen in on communications between systems and possibly inject their own information.

How? By using applications specially designed to listen in on network communications. The message is captured, read, and passed along to the normal destination, possibly being modifed as it passes.

COUNTER MEASURES

- Enforce use of trusted certificates ensuring encryption and mutual authentication
- Utilize firewalls and network segmentation

EXAMPLES

Google 2014

Jeep 2015

THREAT

Want to Learn More?

ICONICS Resources

Highly Secure HMI SCADA and Automation Systems whitepaper
Visit the ICONICS website for industry and product specific information
Follow ICONICS on social media for news on product releases and show attendance

Bedrock Automation Resources

Securing Industrial Control Systems – Best practices
Free training videos on the Bedrock website
Bedrock Industry News – Stay up to date on recent attacks and see how Bedrock could prevent them

Founded in 1986, ICONICS is an award-winning independent software provider offering real-time visualization, HMI/SCADA, energy management, fault detection, manufacturing intelligence, IoT, and a suite of analytics solutions for building automation and operational excellence. ICONICS solutions are installed in 70% of Global 500 companies around the world, helping customers to be more profitable, agile, efficient, and sustainable. ICONICS promotes an international culture of innovation, creativity, and excellence in product design, development, technical support, training, sales, and consulting services for end users, system integrators, OEMs, and channel partners. ICONICS has over 350,000 applications installed in multiple industries worldwide.
To learn more, visit www.iconics.com.

BEDROCK
OPEN SECURE AUTOMATION

This eBook was developed in partnership with Bedrock Automation.
Bedrock Automation is the maker of the Bedrock Open Secure Automation (OSA®) control system, which protects against malware, denial of service, phishing, password cracking, SQL injection, man-in-the middle, and other cyber intrusion by embedding encryption and authorization capability into the system electronics at birth.
To learn more, visit www.bedrockautomation.com.