CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Securing Industrial Control Systems

Key Message: Securing systems that control physical switches, valves, pumps, meters, and manufacturing lines as these systems connect to the internet is critical for service continuity.

Executive Summary

Industrial control systems are computer devices that are used in the delivery, transmission, and distribution of electricity, telecommunications, water, oil, and gas. They are also used to control complex manufacturing processes. Increasingly, these types of systems are moving away from standalone, physically isolated networks and custom protocols to more general purpose computers and networks, including the internet. While this migration results in significant gains in productivity, efficiency, and lower costs, it comes with increased exposure to networked-based attacks resulting from the exploitation of operating system and application software vulnerabilities.

In this podcast, Art Manion, a member of CERT’s Cyber Threat and Vulnerability Analysis Team, discusses the growing security risks for industrial control systems, many of which support national critical infrastructures. Art will also describe ways to mitigate these risks.

PART 1: EVOLUTION OF CONTROL SYSTEMS AND SECURITY RISKS

Defining Control Systems

Control systems, often referred to as industrial control systems, are computer devices that control a physical process such as a switch or an elevator.

They include

- Supervisory Control and Data Acquisition systems (SCADA): Such systems read data, gather data from the field, and monitor devices and output.
- Distributed Control Systems (DCS): Such systems make changes including turning a valve or a switch on or off.
- Programmable Logical Controllers (PLC): Such systems tend to be used where very regular, high-speed binary controls are required, such as controlling a high-speed printing press.
- Intelligent Electronic Devices (IED): Such devices are used in the electric power industry. They include microprocessor-based controllers of power system equipment, such as circuit breakers, transformers, and capacitor banks.
- Remote Terminal/Telemetry Units (RTU): A SCADA system uses RTUs to send supervisory data from the field to a control center.

Smart meters, being deployed as part of the Smart Grid, are some of the smallest, newest modern control devices.

How Control Systems Have Evolved

Historically, control systems were physically separated from the internet and other network connections. They used serial line connections and, in some cases, dry copper wire. They communicated using control-system-specific protocols.

Even a long-distance telecommunications network had private and leased lines. Custom-built hardware and software have been used to run pumps and other types of control systems.

With the advent of commodity platforms and common internet protocols, control systems can now be built at a much lower cost and can use generally available internet protocols. This results in increased efficiency and significant cost savings.

Why CERT Cares About Control Systems

The convergence of closed control systems with open internet-based networks, commodity operating systems, and commodity internet protocols has resulted in increased security risk.

CERT's Vulnerability Analysis Team is now involved in assessing and responding to these types of risks. Today, a vulnerability in a Linux kernel can directly affect a control system.

Those who own and operate control systems are generally aware of the cost and efficiency advantages of connecting to the internet but are often unaware of their increased security risks and exposures.

The same issues that have arisen in the internet community with respect to vulnerability disclosure, for example, are now coming up in the control systems community.

Risks and Vulnerabilities Unique to Control Systems

Clearly, internet-connected control systems are going to have the same security issues as more general-purpose systems, but there are some control-system specific vulnerabilities. For example, now that the control systems Modbus is layered on top of IP (internet protocol), someone with access to your IP network could send unauthorized Modbus packets to your device or control system.

Another example of a control-system-specific vulnerability is the use of a scanner to generate and send malformed packets that can cause devices to crash because the protocol parser doesn't know how to process them.

PART 2: ACTIONS TO MITIGATE RISKS; VULNERABILITY ASSESSMENT

Take Advantage of Known, Good Practice

Owners and operators of industrial control systems have a rich set of existing practices to draw from to secure general-purpose computers and networked systems, including those that are connected to the internet.

Building upon current IT security practices, those responsible for securing control systems should

- Follow guidance on how to secure enterprise IT networks.
- Collect an inventory of critical assets and assess their value. Determine the greatest risks, exposures, impacts, and costs if high-value assets are compromised.
- Scan and test your networks to identify what devices are connected to them.
- Determine the scope of and conduct vulnerability assessments.
- Make sure control systems engineers talk regularly with IT security staff. Those on the control systems side tend to resist making changes to working systems. IT security staff want to keep systems patched and up-to-date.
- Identify and document your network architecture. Identify security weaknesses in this architecture and address them.

Conduct Vulnerability Assessments

Take the following steps when conducting a vulnerability assessment:

- Identify the devices and other assets that need to be assessed. Determine their physical location, the responsible vendor and integrator, software versions on the device, and how they connect to the network.
- Assess device and asset exposure. Determine if they are accessible via open wireless or cellular mobile

networks.
- Organize assets into groups or classes so you can more easily determine the threats and trends they are subject to, and apply similar countermeasures to the group.

For determining the most meaningful scope for a vulnerability assessment, consider using processes that you already have in place for assessing your IT assets or business risk.

To Patch or Not To Patch

Control systems are involved in managing power, water flow, and manufacturing production lines. It can be very dangerous to bring these systems down at unplanned times or to patch them on the normal IT patch cycle (usually weekly, monthly, or quarterly).

When a production system is functioning properly, any change is high risk. Good change control is essential.

For critical systems that cannot be patched on a regular basis, consider isolating them in some manner from the general network. Methods include using firewalls, physical gaps, and air gaps. You can use your network architecture to help determine how best to separate a critical control system from the internet and your business networks to the greatest extent possible.

Additional Practices to Consider

IT security practices are generally applicable for securing control systems including

- encrypting network traffic
- enforcing acceptable use on user accounts and passwords (but manage passwords carefully as you don't want a forgotten password to impact accessing a control system in an emergency)
- using intrusion detection systems and firewalls
- securing remote access via virtual private networks and monitoring all means of remote access

Resources

U.S. Department of Homeland Security (DHS) Control Systems Security Program (CSSP)

DHS CSSP Industrial Control Systems ICS-CERT

CERT Vulnerability Analysis website

Vulnerability Notes database that contains examples of how control systems vulnerabilities were resolved

CERT podcast: Managing Risks to Critical Infrastructures

CERT podcast: Managing Security Vulnerabilities Based on What Matters Most