Thank you for attending. Our webinar will begin shortly.
How to secure SCADA/ICS systems: strategies that work

Josh Drake  
Indiana University Center for Applied Cybersecurity Research

Dr. Stefan Lüders  
CERN

Phil Salkie  
Jenariah Industrial Automation/ TallyEngine, LLC
Housekeeping

- All participants are on mute.
- Ask your questions via the Q&A feature.
- We will record this webinar and provide a link.
- Slides will also be made available.
- Tech troubles? Sign out and back in.
Today’s presenters

Josh Drake
Sr Security Analyst, Indiana University
Center for Applied Cybersecurity Research
History of ICS Cybersecurity Incidents

McLaughlin et al.: The Cybersecurity Landscape in Industrial Control Systems

- **2003**
  - Process control servers in petrochemical company infected by Nachi virus.
  - Impact: production shut down for about 5 hours.

- **2005**
  - DaimlerChrysler plant infected by Zotob worm.
  - Impact: production stopped for about 50 minutes.

- **2007**
  - The Aurora attack used a malicious program to rapidly open and close the circuit breakers of a diesel generator.
  - Impact: the diesel generator exploded.

- **2008**
  - Pipeline leak detection system in oil derricks hacked.
  - Impact: the coastline exposed to oil contamination.

- **2009**
  - Industrial sites in Iran including a uranium-enrichment plant was infected with the Stuxnet worm.
  - Impact: the centrifuges self-destructed.

- **2010**
  - Hackers hacked the infotainment system of vehicle. Potential attacks to robots in automated manufacturing environment.
  - Impact: remotely controlled the critical electronic control units of the vehicle.

- **2014**
  - Control system of steel plant attacked by accessing the network using spear-phishing.
  - Impact: inappropriately shut down a blast furnace.

- **2015**
  - Control system of Baku-Tbilisi-Ceyhan pipeline attacked using vulnerabilities of in camera software.
  - Impact: 30,000 barrels of oil spilled above water aquifer. Cost: BP and partners $5 million a day in tariffs.
Changing Landscape of ICS Cybersecurity

Frequency of malware targeting ICS is increasing year over year, along with the number of attacks.

- More internet connected ICS devices
- ICS devices use of common microprocessor architecture increasing
- Increasing complexity of distributed networks

Cybersecurity Challenges in ICS

- Integrity and Availability over Confidentiality

- Systems are designed for much longer life spans with much higher replacement costs

- Security Controls we’re familiar with may not be available in OT

Information Technology and Operational Technology have different priorities and challenges. Many of our ICS systems were designed before operational security was a primary consideration and may not be due for replacement for years or decades.
Today’s presenters

Dr. Stefan Lüders
Computer Security Officer, CERN
Why (Control System) Cyber-Security sucks…
Department of Homeland Security: Cyber Security Procurement Language for Control Systems

September 2009
How to move from “annually” to “promptly”?

...and how to counter fantasy prices for security measures?

New kids on the block: How to patch IoTs (RasPI, Arduino, SoC...)?

Evolution vs. Security 💣💣💣💣💣
Dealing with USB ports is already problematic...

...but embedded WLAN & WAPs are becoming a pain!

And next comes LoRaWAN...
Do network cells still make sense?

How to control (inter-)dependencies?

How to best manage redundant firewall segregation?

What if we’re forced to use cloud services & external license servers (e.g. Github, Office365)?
A new axis of complexity: virtualization & containers, provisioning, monitoring, and IPMI/BMC…

Where/How to manage/split common Cloud/IT/OT services?
How to securely import (external) software libraries (e.g. PyPi, npm)?

How to make sure that blunder, bugs & vulnerabilities are detected early enough?
How to split development & initial testing, final testing & roll-out, and operations?
When do we get the defaults right?

How to integrate into SSO/AD/LDAP anyhow?

Where (What!) is an 2FA (open source) solution for Win, SSO/web & LX?
Lack of Education

Why do BSc/MSc students, computing engineers, control system engineers, come w/o security knowledge?
Why (Control System) Cyber-Security sucks...
Today’s presenters

Phil Salkie
Founder/Managing Member, Jenariah Industrial Automation/TallyEngine, LLC
Prerequisite 1: Inventory and Discovery

An overlooked part of ICS security, but it's critical to doing the job properly.

- Do a complete survey of the industrial controls infrastructure in whatever facility you're trying to protect, whether that's a single lab room or a university building.
- Document all PLC and OIT components, all communications devices like Ethernet switches, serial protocol converters, modems, gateways, etc.
- There's no single "silver bullet" box that you can install to fix the problem, so you have to know what it is you're trying to protect before you can act.
Prerequisite 2: Budgeting and Triage

You are likely to find that there's more to do than you have money or manpower.

• Life/Safety systems first
• Business mission critical systems
• Important but non-critical
• Decorative systems*

*Beware the back door
Prerequisite 3: Documentation and Backup

Knowing an ICS system is connected is not equal to knowing everything about it.
Need to know what it's supposed to do, how it does it, and precisely how it talks to all the things it communicates with.
Get copies of all the software and data - what’s stored in the vault may not be what’s in the controller.
Get software and hardware you’ll need to make backups.
Strategy: Ignore a given system (for now)

Decide what comes first and what waits

Not working on a system at this time isn't the same as choosing not to do anything at all anywhere - it’s a valuable tool for using your scarce resources to best effect.
Strategy: Monitor / Protect, but don't Interfere

Install an interposing Ethernet switch and monitor the SPAN port so you can build alerts and understand the traffic sufficiently to configure the rules for a later firewall installation.

ICS traffic tends to be limited in quantity, scope, and range

Generally only going to a few well-defined locations

Set alerts on traffic that's larger than usual, an unusual protocol, or is going outside those known hosts
Strategy: Isolate a system - lose functionality, keep core systems running

Some existing communications channels may be too risky to leave open!

You may find DSL modems, WiFi bridges, Vendor maintenance access tunnels, even FTP or Telnet servers sitting on the wide-open Internet.

The wise decision may be to close those doors and come up with a temporary way to transfer that data or gather that information while you come up with a better answer.
Strategy: Protocol - Aware Firewalling

Some devices are deeply aware of the more common ICS protocols, and can firewall on the specific details of a given communication attempt. Modbus firewalls are a good example.

Requires complete knowledge of what will be transferred, or at least how to trigger every possible data exchange.

Protocol converters can be used in a firewall-like way for protocols which don't have specific firewalls available.
Strategy: Hardware / Firmware Updates (rarely happens, often with good reason)

Updating the firmware or user software in a given ICS system is usually frowned upon.
Validation issues - can be very expensive and time consuming.
Discovering an unknown regression in the firmware.
Convincing the customer that the reward of security is worth the risk to operations.
Vendors often don’t fix known vulnerabilities.
Hardware replacement may be required.
Strategy: Upgrade the Controllers

Leave most of a control panel in place and just change out the PLC and HMI devices. Selecting the new controls wisely can make the needed wiring changes easier. Adding protocol conversion can allow a newer controller to communicate with older equipment while providing a layer of firewalling. Requires full understanding of the system's operation and all the communications pathways. Requires down time or temp replacement system and complete re-check of system operation.
Strategy: Replace the system

Replacing systems is usually the last resort, but is often a less expensive answer. Only makes sense if you specify secure design in the replacement systems. Unless you specify robust security, you will receive a new system with absolutely NO security, because designers will choose what’s easiest to implement.
For More Information

NSF Summit Course Information

Connect with ResearchSOC

Visit the ResearchSOC website: https://researchsoc.iu.edu/

Subscribe to the ResearchSOC announcements list: https://researchsoc.iu.edu/contact/index.html

Read the ResearchSOC Blog: https://blogs.iu.edu/researchsoc/

Join our Community of Practice: https://ask.cyberinfrastructure.org/c/rsoc

Follow ResearchSOC on Twitter @IUResearchSOC
Upcoming ResearchSOC Events

**Webinars:**
How to select and use operational cybersecurity metrics to make cybersecurity operations more effective
March 19, 2020 3pm Eastern

[https://researchsoc.iu.edu/webinars](https://researchsoc.iu.edu/webinars)

**Conferences:**
Internet2
March 29-April 1

Educause SPC
April 21-23

PEARC
July 26-30
Thank you!

researchsoc.iu.edu

We thank the National Science Foundation (grant 1840034) for supporting our work.

The views and conclusions herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.
Thank you for attending.