Industrial Control Systems, Networks, and Cybersecurity
2015 NSF Cybersecurity Summit
for Large Facilities and Cyberinfrastructure

8 AM, Monday, 17 August, 2015
Weston Arlington Gateway, Arlington, VA

Phil Salkie, Jenariah Industral Automation
phil@jenariah.com
+1-732-620-1900

Introduction

Thank you for attending! (Who is this guy?)

What are we going to talk about?

Industrial Automation Equipment

PLCs
OITs
DCS
SCADA
Sensors
Telemetry
Custom Hardware (often PLC Derived)

DHS's ICS Security Class

What it is
How to attend
How to prepare
What to bring
What to expect

Securing Controls System Networks

History of PLC Security
History of penetration software and crackers/attackers
Where we stand today
What do we do to respond?

Part One: Intro to Industrial Controls

Why should we care?

- Pervasiveness of this equipment
  - It's used in all areas of manufacturing
  - It's used in all large buildings
  - It's increasingly networked
  - It's uniformly vulnerable
  - Programmers rarely know or care
  - Vulnerabilities are rarely fixed
  - Software and Firmare are rarely updated
- Usefulness of this equipment
  - Save development time
  - Stop reinventing the wheel
  - Extreme reliability
  - Extreme servicability
  - Future-proofing
- Increasing capability footprint
  - More and more things can be done with PLCs
  - More and more things will be done with PLCs
  - If we don't start paying attention, more vulnerabilites will enter our areas of control.
- Increasing potential for damage from intrusion
  - The more these devices are used and networked, the more the chance that an intrusion will result in serious physical damage.

What's so special about this equipment?

- Reliability
- Maintainability
- Designer Efficiency
  - Bridge to Custom Hardware
- Familiarity
- Transferrability

Hardware Introduction - Show and Tell:

- PLC
    - Brick
    - Rack
    - Rackless
    - Integrated
- OIT
    - Membrane Keys
    - Touch Screen
- Tell:
- DCS
- SCADA
- Sensors
- Telemetry
- Custom Hardware (often PLC Derived)

Common themes in the hardware

- Direct connection of devices
- Optical Isolation, even when there are Mechanical Relays
- Full-Voltage Analog Devices
- RTD, Thermocouple, and Millivolt Analog
- Communications to Displays, 3rd Party Devices

What's so special?

- Slow, reliable processors
- Ruggedized Hardware
- Background OS layer Creates A Virtual Machine
- Harvard Architecture
- Specialized Programming Languages
- Hot Swappable Components
- Deterministic Networking

This is Boring! You Mentioned Touchscreens?

- Controllers have little or no user interface capability
    - Pushbuttons and Lamps
    - Dedicated Interface Terminals (OIT)
    - PC-Based Interfaces
    - SCADA
- Operator Interface Terminals - What's special about _them_?
    - Ruggedized Hardware
        - Water/Dust sealed
        - Passive Cooling
        - Class 1,Div II Explosion Proof Ratings
        - Multiple Interface Ports
        - No Rotating Storage
    - Specialized Software
        - Drivers for multiple devices
        - Configuration software for making displays easily
        - Scaling and Ranging
        - Password Levels
        - Event Logging
        - Alarm Handling and Logging
        - Data Passthrough between Devices
        - Data Passthrough between Displays
        - Programming of PLCs through other Display ports
- Downsides:
    - Lessened life expectancy
    - Shorter time in market
    - Shorter time for repairs after EOL

The actual hardware under control

- Operator Interface Devices
  - Pushbuttons
  - Selector Switches
  - Lights
  - Numeric Displays
  - Buzzers and Horns
  - Voice Annunciators
- Sensors
  - Limit Switches
  - Metal Sensors
  - Optical Sensors
  - Thermocouples and RTDs
  - Strain Gauges
  - Float Switches
  - Level Sensors
  - Water Detectors / Oil Detectors
- Actuators
  - Pneumatic Cylinders / Hydraulic Cylinders
  - Relays
  - Contactors / Motor Starters
  - Inverters
  - Servomotors & Drives
  - Solenoids
  - Motorized Valves

How are these things programmed?

- PLCs
  - Dedicated IDE application under Windows (some Mac/Linux)
    - Ladder Language
    - Instruction Logic
    - IEC Block Programming
    - Structured Text Language
    - Flow Chart / Logic Gate (more common on DCS systems)
  - Monitoring and Debugging built into the IDE
  - Simulation often part of IDE
- OITs
  - Dedicated IDE app under Windows, some systems now Browser-based
  - WYSIWYG visual editor for graphic layouts
  - Some have simulation capabilities
- PC Based SCADA
  - Combination of Graphic IDE and spreadsheet-like back end

Part Two - DHS ICS Cybersecurity Class, Idaho Falls, ID

What it is

> "Hands-on training in discovering who and what is on the network, identifying vulnerabilities, learning how those vulnerabilities may be exploited, and learning defensive and mitigation strategies for control system networks."

How to attend

```
https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT#workshop
https://ics-cert.us-cert.gov/Calendar
```

How to prepare

Reading list
Metasploit/Armitage practice
Firewall Rules
Snort Rules

What to bring

Burner laptop which boots from DVD
Personal laptop which is fully patched
Favorite net-related software / apps

What to expect

Attendees will have a wide variety of experience levels
Demonstration of exploits
Basic training on networking and how exploits work internally
Intro to tools like metasploit and armitage
Chance to attack a test network
Planning and co-ordinating attack or response (red/blue team)
10 hours of non-stop cyberattack
Five good lunches
Lunchtime presentations
CSET (Cyber-Security Evaluation Tool)
https://ics-cert.us-cert.gov/Assessments

ICS-CERT (Industrial Control System CyberEmergency Response Team)
https://ics-cert.us-cert.gov/

and AAL (Advanced Analytic Lab)
https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

Part Three - Securing ICS Networks

History of PLC Security

Stand-alone boxes

System programs in EPROM
Programs on EPROM, Battery RAM.
Programming - specialized hardware
Security - obscurity, physical access control, specialized hardware
Attack surface - basically not a consideration
No password protection

Stand-alone boxes with serial ports

System programs in EPROM
Programs on EEPROM, Battery RAM.
Programming - specialized hardware, then PCs
Security - obscurity, physical access control, specialized hardware, specialized software, proprietary protocols
Attack surface - disgruntled employees, war diallers
Minimal password protection
Advent of HMI devices, modems

Boxes with vendor-proprietary local networking

System programs in EPROM
Networking requires special hardware, protocols unpublished or only partially published with proprietary functions.
Programming - PCs via serial, then network
Remote HMI devices, SCADA systems
Security - obscurity, physical access control, specialized software, proprietary protocols
Attack surface - disgruntled employees, corporate espionage
Password protection available, rarely used, backdoors exist or passwords are sent in clear text from PLC, tend to be limited length and limited character set (numeric or hex or capital alphanumeric)
(PLC passwords are generally considered a defense against illegal copying of Intellectual Property, rather than against intrusion by third-party actors. Manufacturers of PLCs want the ability to override the passwords in case of a system failure which requires the program be read back from the PLC, and honestly, so do most end-users.)

Boxes with third-party defined open local networking

System programs in battery RAM or Flash
Programming - PCs via serial, proprietary network (rarely over open)
Security - obscurity, physical access control, specialized software,
unpublished extensions to networking, passwords
Attack surface - disgruntled employees, corporate espionage, state actors
Password protection available, rarely used, backdoors exist or passwords are sent
in clear text from PLC, tend to be limited length and limited character set
(numeric or hex or capital alphanumeric)
Third party networks rarely well supported or completly supported
Bridges to third-party SCADA systems

Boxes with ethernet connectivity

System programs in battery RAM or Flash
Programming - PCs via serial, proprietary net, ethernet
Security - obscurity, specialized software, unpublished extentions to
proprietary networks, passwords, external firewalls
Attack surface - significant fraction of the population
Password protection available, rarely used, backdoors exist or passwords are sent
in clear text from PLC, tend to be limited length and limited character set
(numeric or hex or capital alphanumeric) - with net connection, brute forceable
(PLCs allow repeated guessing attempts with no limits on tries, no time delays
between tries. AutoHotKey can be used to type passwords into GUIs, word lists
can be used on network attacks.)
Ethernet support, like third party support, is incomplete, insecure,
and allows dangerous access in the name of ease of use.
Remote access via Ethernet for all monitoring and programming.

History of penetration software and Crackers/Attackers

Stand-alone boxes, basically nobody.

Once serial ports and modems arrive, war-diallers show up, but obscure hardware and comms protocols keep them at bay.

PLC networking brings some corporate espionage possibilities, but that still requires some kind of physical access. Modem access now more dangerous since corporate money can buy the specialized software required to access the control systems.

Third party networks result in PLC modules which poorly implement various protocols, leaving opportunity to pull out data or possibly take down a control process - but rarely allow access to PLC program or System Program Flash memory.

Ethernet connectivity brings all the problems of poorly implemented third party networks with the ability to put a PLC system directly on the net, or on the net behind a failed or DMZ'ed firewall, or on a corporate net where Crackers have already gained entry.

Penetration software is now easier to use than Gmail.

Published vulnerabilities show up as plug-in modules in automatic updates multiple times per day.

No manufactured device can be considered "Obscure" at this point - it will be automatically detected, and any known vulnerability will be available as a click-button exploit.

Many corporations' IT departments consider their internal corporate networks to be compromised 100% of the time - they have conceded the battle, and direct their users to assume that anything sent unencrypted over the internal network will be visible to competing firms and foreign governments. This is of course true for any PLC-related traffic that hits the corporate network.

Trade-offs - Security, reliability <-> Ease of implementation, speed, expandability, functionality

(Note that "reliability" gets _worse_ with > ease, speed, expandability)

Systems which go together very easily tend to fail very easily, whereas systems which take some fussing at to get working tend to stay working for long periods of time. (Ethernet switch failures, switch configuration, inferior cabling quality, cheap connectors...)

So how do we combat this?

At The Implementation Level

Pick the low-hanging fruit. Many PLCs have "Run\Remote/Program" switches, don't leave them in "Remote" - that stops remote attackers from reprogramming the PLC without your knowledge.

Don't leave tools around - If you must have a general purpose PC around, there is rarely justification for having PLC programming software on an operator's workstation.

Supply a separate general-purpose workstation to keep operators from using controls system PCs "just to check my email real quick."

Use passwords - feel free to write them inside the panels so that in future, the system can be maintained in an emergency, but if nothing else it may slow down an intruder or cause their traffic to be detected.

Don't leave the digital keys in the lock - make sure that passwords aren't left sitting in a text file, or listed in the software. Don't leave the commented software sitting on the workstation. It's better to put everything (drawings, software, tools) on a USB stick that's duct-taped to the inside of the cabinet (threat vector becomes the few people with physical access) than to leave a password in a file on a workstation.

Keep PLC-PLC comms off corporate networks whenever possible. Corporate traffic can cause delays in PLC-PLC comms and standard maintenance on corporate IT hardware can cause PLC comms to malfunction with no apparent reason, and can make it difficult to get systems back up and running when something in a faraway closet has been shut off.

Talk to the site's IT department - have them assign an IP range you will use, ask them to set up their intrusion detection to alert on any traffic within that range. (Protects against someone adding a cable between PLC network and Corporate network.)

Label all communications cables, and make a map of what ports are in use on ethernet switches in your panels. (Make it easy to later identify if any cables have been added to the system.)

Determine minimum functionality needed for any data exchange.

Serial lines are more secure than proprietary networks
Proprietary networks are more secure than ethernet connectivity
Air-gapped ethernet is more secure than ethernet to the corporate net
Nothing can be sent back up a transmit-only serial pair

Use firewalls for third-party protocols.

Beware of default settings - most often, the default settings for a card are the most open and accessible, leave the most ports open and the most protocols available,

Lock down transmissions when that function is available (i.e. if a Modbus card has an "all access" mode and a "just these pre-defined points" mode, use the pre-defined points setting. (Can help with deflecting problems caused by leftover master communications configurations on Modbus networks as well.)

Beware of "multiple function" devices - ethernet ports which serve Modbus, but also can be used as programming ports, etc. - also watch out for cards which ignore port assignments (makes them harder to firewall.)

Use dedicated devices for user interface rather than general purpose computers. Operator Interface Terminals have become much more capable, but don't have the general reprogrammability and succeptibility to viruses that PCs have.

Check vulnerability databases for controls hardware (you'll be frightened)

PLC interface cards have come down in price enough that it pays to add a separate one specifically for external device access, and funnel all interface traffic through that single PLC - it may make sense to make a separate "comms interface" PLC on a larger network, which does nothing but compile data from the other PLCs and format it for external pickup.

For systems which require occasional connection to the net (for remote service, updates, etc.) consider adding a rail-mount ethernet switch which is powered by a PLC output. That output is only triggered by a password-protected button on the operator interface, and powers up the switch for a preset amount of time (say, 2 hours.) This cuts down the temporal attack surface from 24/7/365 to a couple of hours every few months - just tremendously worth it.

At The Specification Level

Insist that you receive commented source code and the development tools for all PLC systems that you purchase.

Insist that you have receive detailed documentation about all network communications implemented between devices.

Insist that the networking system used is the absolute minimum needed to accomplish the required tasks.
(Federal Reserve Bank - No Ethernet allowed between PLC panels.)

Ask for copies of the vulnerability assesments for all networking hardware supplied.

Ask vendors to supply detailed security plans for the systems they will supply.

Ask vendors to discuss their security plans for their own internal systems.

(We repaired the Y2K issue because everybody got in everybody else's face about it, and everyone fixed things because they had to in order to get contracts, not just because it was a good idea. If you have a choice between vendors, maybe you want the one who has spent some time making sure that your new system isn't arriving pre-hacked.)

Security Enhancement for Existing Systems

Discovery

- Find out what's in your building
- Find out what it's connected to, and if it's supposed to be connected
- Check with suppliers and hardware vendors for updates.

Budgeting

- How much time and money can you commit to these upgrades?

After those two disappointments – Planning

- Assess attack surface
- Estimate threat level and repercussions
- Determine mitigation pathway
    - Firewalls
    - Monitoring
    - Software verification
    - Limiting connections
    - One-way communications

Implementation

- One change at a time, check full functionality after changes.
- Penetration Testing
- Continued Monitoring

Thank you for your time and attention!

Phil Salkie
Jenariah Industrial Automation
446 Ridge Road, Suite 10
Greenbelt, MD 20770
phil@jenariah.com
+1-732-620-1900

Appendix A

DHS ICS CyberSecurity Class – Syllabus

`https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT#workshop`

Monday: 8-5

Morning	DHS Overview, ICS 301
	ICS Threats and Risks, Exploit Demonstration
Lunch	CSET Presentation
Afternoon	Other Attack Scenarios, Hands-on Network Discovery, Basic Networking Topics
	Passive Discovery, Host Discovery, Active Discovery, Nmap
Optional 5-6	Network Tools Refresher

Tuesday: 8-5

Morning	Active Discovery, Vulnerability Scanner, Discovery Review
	Metasploit, Terminology - Vulnerability and Exploits
	Basic Exploitation Process, Remote Exploits
Lunch	ICS-CERT Presentation
Afternoon	Metasploit Continued, Client Side Exploits, Payloads, Meterpreter Shell
	Separate into Red and Blue Teams, Initial Briefings
	Red Team/Blue Team Strategy Meetings
Optional 5-6:	Red Team/Blue Team Strategy Meetings

Wednesday: 8-5

Morning	Network Exploitation, Basic Web Hacking , Man-in-the-Middle, Passwords and Hashes, Network Defense
Lunch	AAL Presentation
Afternoon	Logging and Log Analysis, Network Architecture, Network Flow Data
	Red Team/Blue Team Strategy Meetings
Optional 5-6:	Red Team/Blue Team Strategy Meetings

Thursday: 7-5

Morning	Red Team/Blue Team Exercise
Lunch	Blue Team All Hands Meeting
Afternoon	Red Team/Blue Team Exercise

Friday: 8-1

Morning	Exercise Debrief
Lunch	Site Tour - open access to Blue Team, White Team, Red Team areas

APPENDIX B
Industrial Control System Cybersecurity (301) Workshop
Reading Materials

Recommended Reading *

Prior to attending the Process Control Security Training, and to increase your subject-specific knowledge, it is recommended that some or all of the following references are reviewed and studied.

Online training provided by DHS ICS-CERT

- http://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Basic Linux (the hands-on exercises are done in a Linux environment):

- http://www.linux-tutorial.info/
- http://www.ee.surrey.ac.uk/Teaching/Unix/

Metasploit users' guide: https://community.rapid7.com/docs/DOC-1751

- Mastering the Framework: http://www.offensive-security.com/metasploit-unleashed/
- Additional information http://framework.metasploit.com/about/

An introduction/overview of common SCADA communications, e.g.:

- http://www.dcbnet.com/notes/0108worldofwaterpaper.html
- http://www.dnp.org/pages/aboutdefault.aspx
- http://www.isa.org/journals/intech/TP04ISA048.pdf

Intrusion Detection:

- http://www.securityfocus.com/infocus/1577
- http://www.securityfocus.com/infocus/1852
- http://www.oracle.com/technetwork/systems/articles/snort-base-jsp-138895.html
- http://www.oracle.com/technetwork/systems/articles/intrusion-detection-jsp-140939.html

An explanation of SQL injection methods, e.g.:

- http://www.unixwiz.net/techtips/sql-injection.html
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html

HACKING: Art of Exploitation by Jon Erickson

- http://www.amazon.com/Hacking-Art-Exploitation-Jon-Erickson/dp/1593270070

Secure Coding in C and C++ by Robert Seacord

- http://www.informit.com/store/product.aspx?isbn=0321335724

DHS *Catalog of Control System Security: Recommendations for Standards Developers:*

- https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf

NIST Special Publication SP 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*

- http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

SANS ICS Security Summit interview (video)

- http://www.controleng.com/index.php?id=7229

For those with little or no ICS experience, these Wikipedia articles provide a brief introduction to the concepts and history of control systems that will be helpful to know for class.

- http://en.wikipedia.org/wiki/ICS
- http://en.wikipedia.org/wiki/SCADA
- http://en.wikipedia.org/wiki/Smart_grid
- http://nostarch.com/xboxfree - While this has nothing to do with control systems, it provides a great introduction to the concepts and techniques taught in this class to pen test embedded electronic hardware in ICS field/floor devices.
- http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf - Chapter 7 of the NIST Interagency Report 7628, titled Bottom-up Security Analysis of the Smart Grid, provides an overview of the challenges faced in Smart Grid and energy sector systems.

The OWASP Cheat Sheet Series

- https://www.owasp.org/index.php/Cheat_Sheets

Center for Internet Security

- http://www.cisecurity.org/

SANS

- http://www.sans.org
- “Twenty Critical Controls for Effective Cyber Defense” http://www.sans.org/critical-security-controls/cag4-1.pdf
- “Top Cyber Security Risks” http://sans.org/top-cyber-security-risks/

Australian Defense Signals Directorate (http://www.asd.gov.au/)

- “Top 35 Mitigation Strategies” http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- Mandatory Top 4 Strategies to Mitigate Targeted Cyber Intrusions http://www.dsd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

For more information on Snorby, Snort, and other Network System Monitoring (NSM) tools, see “The Practice of Network Security Monitoring: Understanding Incident Detection and Response, Understanding Incident Detection and Response” by Richard Bejtlich July 2013, 376 pp. ISBN: 978-1-59327-509-9

* The links provided here are for your convenience; in no way does this list imply endorsement by the DHS of the companies or websites listed.