CONTROL SYSTEM SECURITY, ARE WE LIVING ON LUCK?

Chris Sistrunk
About Me

Chris Sistrunk, PE
@chrissistrunk
Electrical Engineer
Sr. Consultant, FireEye
- NSM and DFIR for ICS
- ICS Village (DEF CON & RSA Conference)

Entergy (11+ years)
- SCADA Engineer (10 years)
- Project Robus (ICS Protocol Fuzzing)
  - 30+ DNP3 implementation vulnerabilities
- Substation Security Team

BSidesJackson – Nov 12, 2016 our 5th year!
How far have we gotten?

SCADA and ICS for Security Experts: How to Avoid Cyberdouchery

James Arlen, CISA
SECTOR - Toronto - 2010

CYBER!
Industrial Control Systems -are everywhere-
So many control systems
Becoming digital
...to the Internet
Search for Modbus apps on Google Play.
What happens when you use nmap on an ICS?
Public ICS Vulnerabilities

Threats to ICS: Us & Them

Location: WeAreTheBlackX
Vendor Name: Emerson Network Power
Application Software: IS-IPBML_HID10_5.1E0.0_069921
Firmware: IS-IPBML_HID10_5.1E0.0_069921
Model Name: Liebert Challenger
Description: WeAreTheBlackX
Us
Us

Posting too many ICS details to
- Public web forums
- Job postings
- LinkedIn, Facebook, Twitter, etc
- Utility websites (Transmission OASIS, etc)
Us

- Upgrading?
- Patching?
Vendors

Vendor Excuses
@vendorexcuses

We've received your vulnerability report.

Vendor Excuses
@vendorexcuses

We've reviewed the PoC frame you submitted, but our development team wouldn't send that.

Vendor Excuses
@vendorexcuses

The bug wasn't ours, but we fund it useful, at 3:21 PM - 20 Jul 2015

To 650 ★ 3

Vendor Excuses
@vendorexcuses

A backdoor password was discovered in our firmware. We've changed it. Thank you.
12:01 PM - 31 Dec 2014

To 120 ★ 74
BWL: FBI helping investigate cyberattack

Customers can still pay bills online, receive service. Ongoing problem affects about 25,000 owned utility.

LANSING - A cyber Water and Light's unprecedented dilemma for the city-owned utility that requires help from the Federal Bureau of Investigation, BWL General Manager Dick Peffley told the Lansing State Journal early Tuesday afternoon.

City-owned utility received nearly $2 million in invoices and purchase agreements to address ransomware attack, records show.
Them: Hacktivists

Hacker says he broke into Texas water plant, others

Annoyed with the downplaying of the risk to critical infrastructure systems, a hacker targets a water plant in South Houston following news of an Illinois water plant intrusion.

By Elnor Mills / @elnormills / November 18, 2011 3:34 PM PST
Part of my workstation at the power plant!

@rabite @kenbone18 that's pretty neat. What kind of PLC/SCADA do they use in coal fired facilities?

@notdan @kenbone18 You see Ken? You've got weeV asking you questions about this. You've doomed us all.

@rabite @kenbone18 Nonsense, I'm just curious. I can't do that much with control of a coal facility anyways.

@notdan @kenbone18 Certainly can't shed load at gens and cause a cascading failure that takes down massive areas of populations.

@rabite @kenbone18 If they don't have power, they can't post videos about their miseries. Not my style.
Them: Physical attacks

**Shots in the Dark**
A look at the April 16 attack on PG&E's Metcalf Transmission Substation

1. 12:58 a.m., 1:07 a.m.: Attackers cut telephone cables
2. 1:31 a.m.: Attackers open fire on substation
3. 1:41 a.m.: First 911 call from power plant operator
4. 1:45 a.m.: Transformers all over the substation start crashing
5. 1:50 a.m.: Attack ends and gunmen leave
6. 1:51 a.m.: Police arrive but can’t enter the locked substation
7. 3:15 a.m.: Utility electrician arrives

Sources: PG&E, Santa Clara County Sheriff’s Dept., California Independent System Operator, California Public Utilities Commission, Google (image)
So the line was crossed...

- Dec. 23, 2015: Two Ukrainian regional distribution providers publicly claimed power outage due to cyber attack
- Sources say a third was also affected; six more “attacked” but no indication of outage
Ukraine Power Grid Attack

- Call center flooded with calls to prevent outage reporting
- Battery backups (UPSes) switched off
- Numerous non-ICS computers infected and wiped
But...

- ICS and power grids fail all the time
- Ukraine power back in 6 hours
- Evil Hackers 1 – Squirrels 100,000
So are we living on luck???

When someone asks:

How was your control system breached?
Visibility?
Visibility?
So how do we get in front?
ICS is Defensible!

- No encryption
- Very static
- ICS devices aren’t mobile
- Low bandwidth
Security Bingo Time

We’re gonna build a

We’re gonna pay for it!

SCADAGreatAgain
Protect

- Segment
- Control remote access (multifactor auth)
- Harden devices
  - Standard configurations
  - Patch!
  - Lab testing
  - Think like an attacker with your prints!
Network Security Monitoring

- Model for action, based on network-derived data
- Requires people and process, not just technology
- Focuses on the adversary, not the vulnerability
Collect
Detect - “Hunt for Evil”

- Analyst looks at detected anomalies or alerts then escalates to incident.
Detect
Analyze – “Find Evil”

FLYING SQUIRREL ATTACK!!!!!!
ICS Security needs People

WE WANT YOU
Some numbers

Industrial Control System Humans
MANY
Engineers, Technicians, Operators, Vendors, etc

Security Humans
~189,000

ICS Security Humans
<1000
0.5% of Security

“LinkedIn data identified over 189,000 professionals in active information security positions worldwide as of June 2015.”
- Cory Scott
Is 0.5% enough?
IT Security > ICS Security

- You’ve got the computer and networking skills
- You know how business technology work
- You probably already know:
  - Routers, switches, firewalls, domain controllers
  - Web, email, and business applications
  - Certifications like CCNA and CISSP
  - HIPAA or PCI DSS requirements

- But you don’t know the engineering and physics behind the process
Google all the Things

- YouTube & Vimeo
- “SCADA”
- “Control Systems”
- “PLC”
- Conference Talks
- “How It’s Made” Marathon!
Make an ICS network at home

- Raspberry Pi
  - opendnp3, modbus, BACnet
- Arduino
  - modbus
- $15 HMI from eBay (got lucky)
- ~$700 for a new Phoenix Contact PLC
You know security, but not ICS...

- ....YET
- What I am about to tell you is the single greatest secret to go from IT Security into ICS...
Donuts
Get your hardhat dirty

LITTLE BOBBY

WHAT ARE YOU DOING?

BREAKING IN MY PERSONAL PROTECTIVE EQUIPMENT.

WHY WOULD YOU RUIN BRAND NEW PPE?

THE FIRST RULE TO GOING ON-SITE IS TO WEAR PPE.

THE SECOND RULE IS NEVER LOOK LIKE YOU JUST STARTED.

by Robert M. Lee and Jeff Haas
Ask questions

- What is it?
- Why is it important?
- How can we secure it?

Example:
Ladder logic on a PLC

Understand the why...
...then try to secure/monitor it
Collaborate

Problem:
- ICS network is flat with the corporate network
- ICS network has no logging or visibility
- IT has security goals
- OT has safety and uptime goals
- Can you do some things that satisfy both?
ICS Security Resources

THIS IS SCADA
Connect!

- SCADAsec email list at Infracritical
- ICS Security Conferences
  - ICSJWG – FREE
  - DigitalBond’s S4
  - SANS ICS Summit
  - 4SICS
  - EnergySec
  - Oil & Gas Security Summit
  - ICS Cyber Security Conference “Weisscon”
Information Sharing

National Council of ISACs

- Downstream Natural Gas
  - www.dngisac.com

- Electricity
  - www.esisac.com

- Oil & Natural Gas
  - www.ongisac.org

- Water
  - www.waterisac.org

ISAOs coming, knowledge sharing, ICS-ISAC, “BEER-ISAC”
Books

- Robust Control System Networks, Ralph Langner
- Cybersecurity for Industrial Control Systems, Macaulay & Singer
- Countdown to Zero Day, Kim Zetter
- Hacking Exposed Industrial Control Systems, Bodungen, et al
- Handbook of SCADA/Control Systems, 2nd Ed., Radvanovsky & Brodsky
Standards

- NIST SP800-82 Rev 2
- IEC 62443
- NERC/CIP
- CFATS
- …to name a few
Training

- ICS-CERT
  - Free online training and resources
  - Free 5-day Red vs Blue ICS exercise
- ICS Vendor Training
- SANS ICS
  - ICS410 and ICS515
- Red Tiger Security
- Lofty Perch
- SCADAhacker
Certification

- There isn’t a Professional Engineering license for Security...
  ...but not everyone is an engineer.
- GICSP cert: teach IT folks the basics of ICS and ICS folks the basics of security.
Links

- https://ics-cert.us-cert.gov/Standards-and-References
- http://dx.doi.org/10.6028/NIST.SP.800-82r2
- http://scadaperspective.com/
- http://www.netresec.com/?page=PcapFiles
- https://www.shodan.io/explore/category/industrial-control-systems
Lucky?

It's better to be lucky than good.

— Lefty Gomez —
Let’s just be good

Le mieux est l'ennemi du bien.
(The perfect is the enemy of the good.)

~ Voltaire
Questions?

THANKS CHRIS

VERY USEFUL

memegenerator.net