CONNECTIVITY SURPRISE FACTOR: WHAT’S IN YOUR ICS?

Presented by: Doug Wylie, CISSP

23 February 2016
HIDING IN PLAIN SIGHT

FIND ME?
What’s our “view” of our control system?

What are we seeing today?

What aren’t we seeing?

Why aren’t we looking?

Do we even know where to look?
IT & OT OPERATIONAL OBJECTIVES:
SIMILAR BUT DIFFERENT

Real Things Happen!

Data Happens!

INFORMATION

IT

OT

OPERATIONS
IT & OT COMMON CHALLENGES AND SHARED OBJECTIVES

Security Objective: Protect against all threats

Attacker Objective: Exploit just one weakness
INDUSTRIAL CONTROL SYSTEMS ARE NOT JUST BUILT, THEY ARE ENGINEERED

Everything happens for good reason...
Communications is at the heart of the operations of industrial control systems and...

Safety, Security and Operational Integrity challenges continue to be amplified and become more complex.
SEEING THE FOREST AND THE TREES...

...AND LISTENING TO WHAT’S IN-BETWEEN
WHAT YOU CAN’T SEE MIGHT BE DANGEROUS

Seeing clearly from a distance?

Now what?!!

Where to begin... ...where to end?

OMG!?!?

F P T O Z L P E D P E C F D E D F C Z P

Hiding in plain sight—Who, what & where?

Speculation & Interpretation?
Devices that want to talk... 
...must first make noise!

- Connect to the physical network
- Identify themselves on the network
- Often request or hold an IP Address
- Open communication ports
- Establish TCP sessions (1:1)
- Initiate UDP messages (1:1 & Many)
- Format Data per protocol standard

Then...
...Send data over and over and over...
Layer 3
- IPv4
- IPv6
- BGP
- IPSec
- ARP
- LLDP
- STP
- RARP
- VLAN

Layer 2
- Ethernet
- EtherCAT (Beckhoff)
- Profinet (B&R)
- Powerlink (B&R)
- SERCOS III (Bosch Rexroth)
- Some proprietary variants

Layer 1

Examples:
- BACnet/IP
- DNP3
- EtherCAT
- EtherNet/IP (Rockwell)
- Foundation Fieldbus HSE
- IEC 61850 (aka GOOSE)
- Modbus/TCP (Schneider)
- OPC
- PROFINET (Siemens)

Examples:
- CC-Link (Mitsubishi)
- EtherCAT (Beckhoff)
- Powerlink (B&R)
- SERCOS III (Bosch Rexroth)
- Some proprietary variants

More to come???
UKRAINIAN POWER GRID ATTACK

First fully-reported intentional cyber attacks directly responsible for power outages – December 23, 2015

- Planned
- Coordinated
- Used multiple attack vectors and specific tools
- Across multiple regional distribution power companies
Sophisticated malware and direct remote used to:

• Cause undesirable state changes to the electricity distribution infrastructure causing the outages
  – Kyivoblenergo reported 30 substations disconnected serving 80,000 customers (homes)
  – Other sources report +1.5 million people directly affected

• Blind system dispatchers and deny customer calls

• Restoration thwarted and forensics activities hampered by wiping SCADA servers

Could the attack have been seen heard, tracked ...and prevented?
RECOMMENDATIONS & MITIGATION

• “Organizations should isolate ICS networks from any untrusted networks, especially the Internet.”

• “…know who and what is on your network through hardware & software asset management automation”

• “Static nature of some systems...make these ideal candidates to run application whitelisting”

• “All unused ports should be locked down and all unused services turned off.”

Asset Discovery: Find What's Connected

Asset Discovery

Internet of Stuff & Things...

Details

- Devices?
- Address?
- Host Names?
- Ports?
- Protocols?
- Payloads?
- Routes?
- Role/Function?

Characteristics

- Data Rates?
- Frequency?
- Persistent?
- Transient?
- Function?
There is great appeal in the path of least resistance...

Our objective is to move data securely and efficiently...

...and to avoid complexity and risks everywhere possible
1. Scanner to Adapter process data
2. Scanner to Adapter configuration
3. Scanner to adapter across zones
4. SCADA and HMI to Adapter (PLC)
5. Scanner to Scanner
6. Engineering PC to Adapter, scanner, and HMI for configuration and diagnostics
7. Enterprise to Adapter (e.g., energy object)
8. Configuration tool to network infrastructure
9. Local Machine Remote Access
10. Enterprise remote access
WHAT’S UNDER THE SHEETS?
What this depicts

- Establishing a TCP Session
  - *SYN*
  - *SYN-ACK*
  - *ACK* (3-way handshake)
- Logic focuses on Endpoints
- Network often ignored
- Many potential points of failure
- Many potential points of latency
- Validates why simple is better
  - Configuration & Maintenance
  - Stability & Performance

NOTE: Omits many non-ICS services and ICS data once connection established (e.g. DNS, Active Directory, DNP, Modbus TCP, OPC, EtherNet/IP, etc.)
EXAMPLE: GERMAN STEEL MILL CYBER ATTACK

Information Source:
German Bundesamt für Sicherheit in der Informationstechnik (BSI)

Incident Details (December 2014)
• Spear phishing email gave access to corporate network then plant network.
• Adversary had ICS knowledge and caused multiple components to fail.
• Directly impacted critical process destabilizing the system which led to massive physical damage.

Could the attack have been seen heard, tracked ...and prevented?

NOISE MATTERS INSIDE

INDUSTRIAL CONTROL SYSTEMS
<table>
<thead>
<tr>
<th>Situation</th>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every device is assigned an IP address.</td>
<td>Why are some devices sending DHCP messages?</td>
</tr>
<tr>
<td>All ICS devices are active and operational.</td>
<td>Why is there ICMP traffic from a router to a client?</td>
</tr>
<tr>
<td>Firewall configured to block TCP/443.</td>
<td>Why is there SSL traffic on Port 80?</td>
</tr>
<tr>
<td>Telnet services disabled on all devices.</td>
<td>Why is there communication to TCP/23?</td>
</tr>
<tr>
<td>Configuration change to remove devices.</td>
<td>Why are there ARP requests to non-existent IPs?</td>
</tr>
<tr>
<td>Kerberos services not operating</td>
<td>Why is there HTTP traffic on TCP/88?</td>
</tr>
<tr>
<td>Only ICS devices are physically connected</td>
<td>Why is there a Print Server? What’s SIP protocol?</td>
</tr>
<tr>
<td>System is configured for IPv4 addresses.</td>
<td>Why is there IPv6 traffic? What’s 6in4 protocol?</td>
</tr>
<tr>
<td>OPC traffic expected between PLC and HMI.</td>
<td>Why is there OPC traffic between HMIs?</td>
</tr>
<tr>
<td>Device has been hardened to disable unnecessary services.</td>
<td>Why have new communication ports been opened on a device after a security patch was applied?</td>
</tr>
</tbody>
</table>

Everything happens for a reason—including the Good, Bad and Ugly.
EXTERNAL MONITOR

1. New external connection seen emanating from Firewall (Packet Detail + DPI)
2. New external connection tracked to unauthorized location (IP geolocation)
3. Data exchange encrypted as SSL over TCP/80 not 443 (Packet Detail + DPI)

INTERNAL MONITOR(S)

1. Unauthorized device seen connecting to ICS (ARP, ICMP)
2. Authorized device seen establishing RDP session to HMI (TCP/3389 + DPI)
3. HMI opens DCOM connections to other HMIs (TCP/135 + DPI)
4. Data exchange seen between HMIs (TCP/various + DPI)
5. Event notification through Firewall (TCP/80)
6. SSL traffic stream seen passing to Firewall (TCP/80 + DPI + Packet Details)
7. Events logged; Alert notifications issued; Data sent to SIEM/UTM
HOW DO WE GET IN FRONT OF THE RISK?
FIRST STEP: KNOW WHAT YOU HAVE

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configs for H/W, S/W on Mobile Devices, PCs and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configuration for Network Devices (Firewalls, Routers, Switches)
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises
“passive instead of active,” to collect information often “queried” (i.e. scanned) by automated vulnerability & penetration testing tools.

“allow collection of the necessary vulnerability information without the risk of causing a failure while testing.”
WHAT GOOD LOOKS LIKE

DETAILS
- Devices?
- Addresses?
- Hosts Names?
- Ports?
- Protocols?
- Payloads?
- Routes?
- Role/Function?
CONCLUSION

‘CONNECTIVITY SURPRISE-FACTOR’

What can be gained by...

- Passive industrial network anomaly detection
- Looking below the surface of traditional IT systems
- Performing real-time network asset-inventories
- Tracking & tracing device interactions and data flows
- Base-lining normal & expected communication patterns

**GOAL:** Better protect the safety, security and operational integrity of control systems throughout their lifecycle.
RISK MANAGEMENT TECHNIQUES
THANKS FOR YOUR PARTICIPATION