Protecting Critical Infrastructure is Critical

Robert M. Hinden

Check Point Fellow
American Blackout

Learn what it means to be powerless. NatGeo presents a world premiere movie event, Sunday October 27th at 9/8C.

Full Video at: http://www.youtube.com/watch?v=FYoXxVnTePA
Critical Infrastructure is at Risk!

• Critical Infrastructure is part of our world

• Many Vulnerabilities
  - Just like other IT systems, but

• The consequences of an attack are much greater
  - Power failures
  - Water pollution or floods
  - Disruption of transportation systems
  - Deaths of people on life support systems
Talk Overview

Why this issue is Critical
Real Attacks
SCADA Industrial Control Protocol
Security Issues with Control Systems Platforms
Recommendations and Actions
Industrial Control Systems are Everywhere
Critical Infrastructure is Targeted

- Manufacturing 65
- Energy 79
- Communications 14
- Commercial Facilities 7
- Chemical 4
- Unknown 6
- Water 14
- Transportation 12
- Nuclear 6
- Information Technology 5
- Healthcare 15
- Government Facilities 13
- Finance 3
- Food and Agriculture 2

Attacks are Happening
BlackEnergy Malware Compromised Industrial Control Systems

• Attack has been ongoing since 2011 via Operator console via Internet Connections

• Targets GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC

• Affects Microsoft Windows and Windows Server 2008 and 2012

• Various attacks point to shared command and control systems

https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B
Cyber Attack on German Steel Factory

- German Federal Office for Information Security reported
  - Hackers accessed production network, and tampered with Blast Furnace controls

- Hackers gained access via spear phishing and social engineering to get credentials to access office network

- Blast furnace could not be shut down, resulting in “massive damage to plant”

http://www.wired.com/2015/01/german-steel-mill-hack-destruction/
Malware in South Korean Nuclear Plant

• Malware found in computers connected to nuclear power facility

• Reactor controls of Korea Hydro and Nuclear Power (KHNP) were not connected to any external networks

• Malware likely introduced via USB drive

Multiple-Vector Attack on Industrial CS

• Attack used multiple attack vectors
  - Phishing emails
  - Redirects to compromised sites
  - Installed infected update installers on at least three ICS vendor sites

• Installers were infected with Havex Trojan malware

• Malware collected information on topology, nodes, control systems
  - Caused some systems to intermittently crash

https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
Observation

• Many of the recent attacks were collecting data about Critical Infrastructure deployments
  - Devices, topology, protocols, etc.

• What does this mean?

Attackers are collecting data to enable future attacks
Critical Infrastructure Constraints

- Critical Infrastructure use dedicated systems, on specialized networks, with unique protocols
- Deployments can’t be changed easily
- Solutions need to last for 10, 20, or 30 years

Attackers are moving very fast and don’t have these constraints
Supervisory Control and Data Acquisition Protocol (SCADA)
SCADA Overview

• Protocol to monitor and control remote equipment. Used for
  - Pipelines, civil defense systems, heating/cooling systems, etc.

• Main components
  - Remote terminal units (RTU) – Connect to sensors and convert to digital data
  - Programmable Logic Controllers (PLC) – Like RTU, but are programmable
  - Human-Machine Interface (HMI) – Presents data to human operator
  - Network – LAN, WAN, Cellular, satellite, etc.
Why Attacks Can Happen?

- SCADA devices and protocol were not designed for security
  - Security by obscurity?
- Assumed to be isolated from organizations network and Internet
- Assumed shared trust

None of these assumptions are true!
SCADA Devices are Vulnerable

- Programmable Logic Controllers (PLC) are purpose-built computers used for automation of electromechanical processes such as control of pumps, valves, pistons, motors, etc.

- PLCs are small computers. They have software applications, accounts and logins, communication protocols, etc.

- Analysis of PLCs from leading vendors shows variety of vulnerabilities:
  - Backdoors
  - Lack of authentication and encryption
  - Weak password storage
  - Bugs leading to buffer overruns
Typical SCADA Network Structure

MANAGEMENT FACILITY

PRODUCTION FACILITY
Typical SCADA Network Structure
IT and SCADA Networks are Interconnected

Survey of hundreds of Energy sector environments
Average of 11 direct connections and up to 250 in some cases
(US National Cybersecurity and Communications Integration Center, 2011)
This is a Real Problem

• F-Secure found SCADA Attack that targets European Industrial Control Systems
• STUXNET worm designed to attack SCADA Program Logic Controllers
• Banking Trojans Disguised As ICS/SCADA Software Infecting Plants
• Hackers gain “full control” of critical SCADA systems
• Hackers aggressively scanning ICS, SCADA default credentials

http://www.darkreading.com/as-stuxnet-anniversary-approaches-new-scada-attack-is-discovered/d/d-id/1278881
http://en.wikipedia.org/wiki/Stuxnet
# Examples of SCADA Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>SCADA Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unpatched Published Vulnerabilities</td>
<td>Most Likely Access Vector</td>
</tr>
<tr>
<td>Web Human-machine Interface (HMI) Vulnerabilities</td>
<td>Supervisory Control Access</td>
</tr>
<tr>
<td>Use of Vulnerable Remote Display Protocols</td>
<td>Supervisory Control Access</td>
</tr>
<tr>
<td>Improper Access Control (Authorization)</td>
<td>Access to SCADA Functionality</td>
</tr>
<tr>
<td>Improper Authentication</td>
<td>Access to SCADA Applications</td>
</tr>
<tr>
<td>Buffer Overflows in SCADA Services</td>
<td>SCADA Host Access</td>
</tr>
<tr>
<td>SCADA Data and Command Message Manipulation and Injection</td>
<td>Supervisory Control Access</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>Data Historian Access</td>
</tr>
<tr>
<td>Use of Standard IT Protocols with Clear-text Authentication</td>
<td>SCADA Credentials Gathering</td>
</tr>
<tr>
<td>Unprotected Transport of SCADA Application Credentials</td>
<td>SCADA Credentials Gathering</td>
</tr>
</tbody>
</table>

Source: Idaho National Lab, 2011
Examples of PLC Vulnerabilities

<table>
<thead>
<tr>
<th>Feature</th>
<th>A-B</th>
<th>Schneider Electric</th>
<th>GE</th>
<th>SEL</th>
<th>Koyo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
</tr>
<tr>
<td>Ladder Logic</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
</tr>
<tr>
<td>Backdoors</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
</tr>
<tr>
<td>Fuzzing</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
</tr>
<tr>
<td>Web</td>
<td>![]</td>
<td>![]</td>
<td>N/A</td>
<td>N/A</td>
<td>![]</td>
</tr>
<tr>
<td>Best Configuration</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
</tr>
<tr>
<td>Exhaustion</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
</tr>
<tr>
<td>Non-doc Features</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>![]</td>
</tr>
</tbody>
</table>

*Vulnerability is present in the system and is easily exploited*

*Vulnerability exists but exploit is not available*

*System lacks this vulnerability.*

Source: Digital Bond January 2012
Choice of Platform for Control Systems
Sometime I Wonder Why People

• <RANT>
  - Choose the platform with the most exploits?
  - Don’t upgrade to the latest version of the Operating System?
  - Don’t apply patches and updates?
  - Don’t run AV, Anti-Malware, etc.?
  - Run systems with no support?
• </RANT>

They must WANT to run Malware!
Industrial Control Computers are Not Immune from Enterprise Security Challenges

• General purpose computers bring with them Enterprise vulnerabilities
  - Very common to use enterprise OS as base for industrial controllers

• Recent Problems
  - Siemens Open SSL Vulnerabilities
  - Shellshock / Bash Shell Vulnerabilities affect Industrial Control Systems

https://ics-cert.us-cert.gov/advisories/ICSA-14-198-03G
Industrial Control Computers

• Using old platforms for Critical Infrastructure increases the risk of an Attack
  - The attackers’ don’t need to learn new techniques to compromise these systems
• This is a symptom that Critical Infrastructure operators are not taking Security seriously

Why make the attacker’s job easier?
Recommendations
How to Apply in Your Environment

- Deploy strong perimeter security
- Select platforms for their security characteristics
- Use SCADA prevention technologies
- Make Security a Priority
Deploy Strong Perimeter Security

• Conventional Security Tools
  - Firewall
  - Intrusion Prevention
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
  - Data Loss Prevention (DLP)

• Critical to keep tools and signatures current
  - Internet Connection needed
Platform Security

• Make security a priority when selecting and/or upgrading computing platforms

• Aggressively replace old platforms and operating systems
  - Only run Operating Systems that are actively supported
  - Don’t run Windows 95, 98, XP, Vista, 7

• Always apply latest patches and security fixes

• Always run current AV, Anti-Malware, etc.

• Control usage of USB ports
SCADA Prevention Approach

LOG ALL SCADA TRAFFIC

Define Normal Baseline
- Full visibility (Known / Unknown / Not Allowed)
- Does not depend on SCADA devices ability to log
- No risk of interference on production mirror port
- Have forensics in case of attack

Identify Deviations and Attacks

Alert and Prevent Attacks
ICS Network with SCADA Prevention

MANAGEMENT FACILITY

Central Operation

Corporate Network

LAN

DMZ

DC

INTERNET

VPN

REMOTE USER

PRODUCTION FACILITY

Operation Network

FW+VPN

Local operation

PLC

Process

Gateways learn and control SCADA traffic

Check Point
SOFTWARE TECHNOLOGIES LTD

36
Make Security a Priority

• Make Security part of the procurement process
  - Include Security in Service Level Agreements

• Invest in staff security training
  - This will be a cultural change, but critical

• Periodic Security Audits

• Actively track Industrial CERTs and Vendor Notifications
  - [https://ics-cert.us-cert.gov](https://ics-cert.us-cert.gov)

• Don’t be afraid to report attacks and compromises
Closing Thoughts

• This issue is Critical

• Attackers are getting better and are preparing for major attacks

What are you going to do?
Thank You

Bob Hinden
rhinden@checkpoint.com