SCADA Cyber Security in the Age of Internet of Things

Presented at Remote Monitoring and Control 2016

Ed Nugent, COO PcVue Inc.

Agenda

Remote 2016 Conference

- IoT and Mobility Impacts to SCADA
- The Pillars of SCADA Cyber Security
- Identify – Recognizing Suspicious Behavior
- Protect - The Dissolving Perimeter
- Detect – Abnormal and Suspicious Behavior
- React – Minimize Damage, Ensure Recovery
- Summary

IoT and Mobility Impacts to SCADA

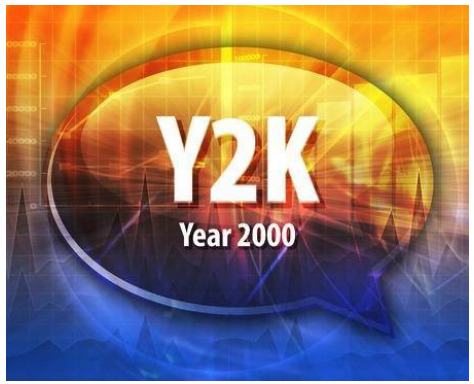
- Industrial Control Systems
  - Long history going back decades
  - Evolution from specialized to generalized
  - Evolution from closed to open systems
  - Evolution from isolated to connected

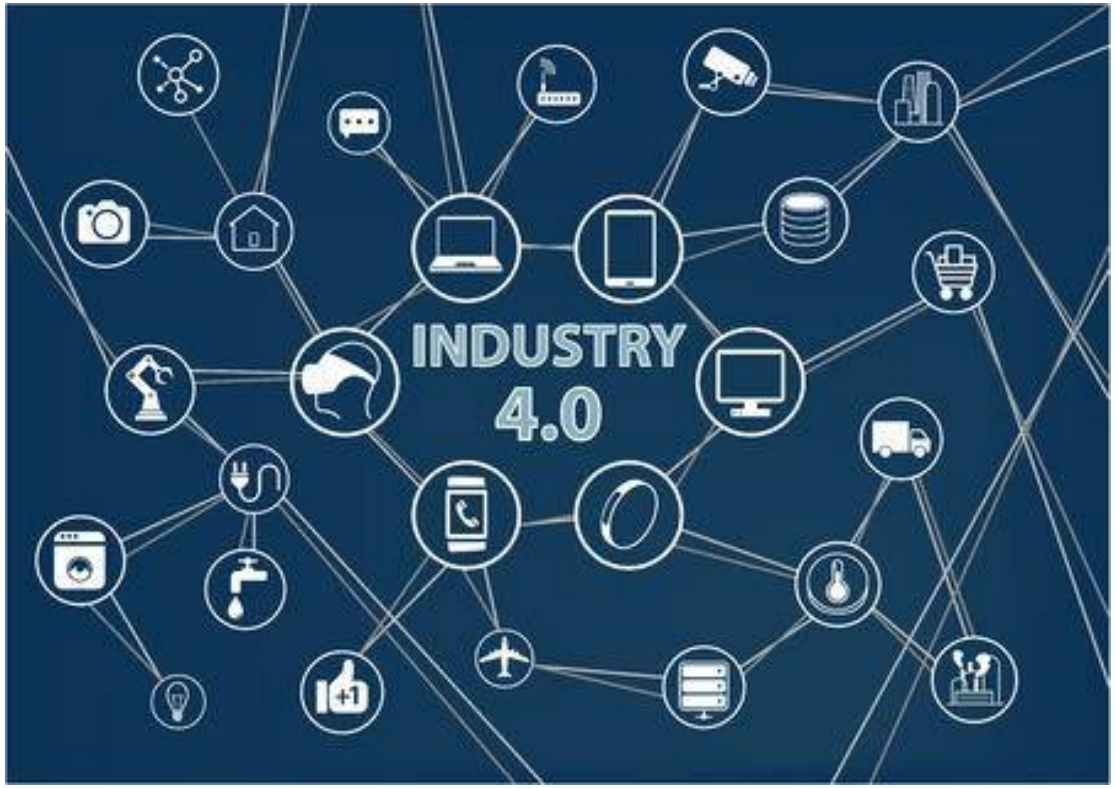
IoT and Mobility Impacts to SCADA

- Evolution from specialized to generalized
  - SCADA – RTU/Telemetry
  - SCADA – PLC based
  - DCS
  - Human Machine Interface
  - Manufacturing Execution Systems
  - Building Management Systems
- Evolution from closed to open systems
  - 1990's Microsoft NT Operating System
  - OPC Foundation

IoT and Mobility Impacts to SCADA

- Evolution from isolated to connected
  - Y2K concerns and IT oversight of ICS
  - Widespread ERP Adoption
  - Internet of Things
    - Industrial Internet of Things
    - Industry 4.0





IoT and Mobility Impacts to SCADA

- IIoT transformation
  - Disrupting work processes
  - Changing the role of the Control Room
- Emerging Contexual HMI component of IIoT
  - O&M productivity gains
  - Expands the perimeter of ICS
  - Impacts cyber threat management
    - Increases the perimeter

The Pillars of SCADA Cyber Security

- For ICS Vendors cyber security must be built into the quality process.
  - ISO 9001 Quality Process for development and production
  - Incorporate the Software Engineering Institute's Cyber Risk and Resilience Management.
- Objectives
  - Transparency on internally or externally reported vulnerabilities
  - Act quickly to minimize risk to customers.

CERT | Software Engineering Institute | Carnegie Mellon University

The Pillars of SCADA Cyber Security

- ICS vendors should also participate in standards organizations focused on cyber security
  - National Institute of Standards and Technology – NIST USA.
  - Institute of Electrical and Electronic Engineers – IEEE USA
  - International Electrotechnical Commission – IEC Europe
  - National Agency for the Security of Information Systems – ANSSI France

NIST National Institute of Standards and Technology U.S. Department of Commerce

IEEE Advancing Technology for Humanity

IEC

The Pillars of SCADA Cyber Security

- NIST has provided a framework
  - Systematically identify critical assets
  - Systematically identify threats
  - Secure critical assets
- Pillars of Cyber Security
  - Identify assets and normal behavior
  - Protect the perimeter
  - Detect intrusions
  - React and recover from attacks

NIST National Institute of Standards and Technology
U.S. Department of Commerce

Identify – Recognizing Suspicious Behavior

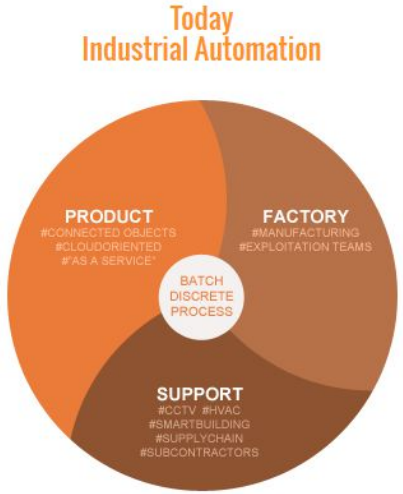
- What is normal?
  - Prior to Boston Marathon in 2016 Homeland Security surveyed “normal” radiation levels throughout the region.
  - Objective: recognize nuclear threats
- SCADA Systems have “normal behavior”
  - Expected data communication
  - Changes to programs are controlled
- Automated tools that map and monitor industrial networks help
  - Enterprise IT monitoring are not industrial aware
  - SNMP is a bridging technology between IT and industrial networks.

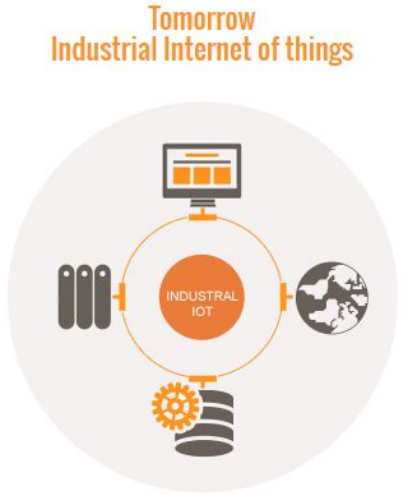
Identify – Recognizing Suspicious Behavior

- Build the ICS Baseline
- Extract metadata from the network flow
  - Passive sensors
- Inventory components & connections
  - Visual map
- Monitor and learn normal behavior
  - Statistical and behavioral descriptions
- Recommend preventative actions
- Trigger incident response
  - Upon evidence of compromise

Identify – Recognizing Suspicious Behavior

- ICS networks primarily use static IP so monitor for:
  - Changing IP addresses
  - Duplicate IP and MAC addresses
  - Device or cable movement
  - Unauthorized connections
- Mobility and IIoT complications
  - Sensors and mobility workers connecting through wireless access points have dynamically assigned IP





Protect - The Dissolving Perimeter

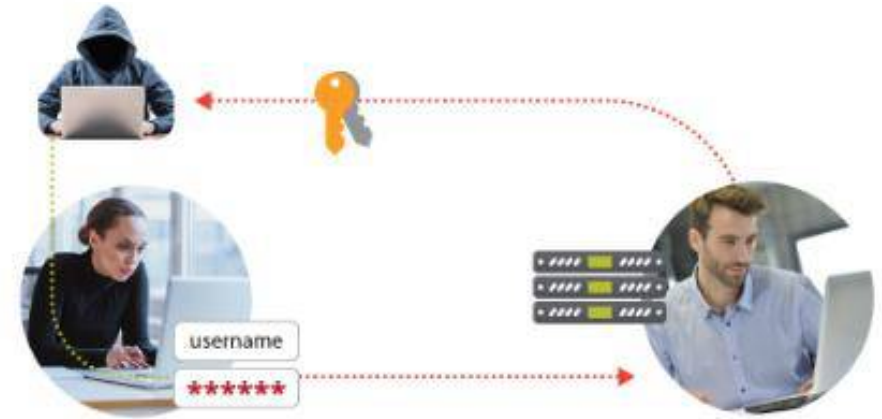
- Identity is the new perimeter
  - of breaches are compromised credentials
  - hackers target all; including privileged users
  - traditional perimeter security is insufficient
  - require context-based policies
- We see a dissolving perimeter of ICS
  - move to open and connected systems
  - culture of security is needed

Protect - The Dissolving Perimeter

- Control Engineers & Operators focus is safety
  - Protect processes and people against hardware failure or environmental casualties
- Cybersecurity is not part of ICS culture.
  - Fighting against malicious people is very different.
- An inter-organizational team approach is needed
  - New regulations demanding critical infrastructure operators to implement cybersecurity best practices
  - Chief Security Officer has the best practices

Protect - The Dissolving Perimeter

- Industrial networks provide the first level of defense.
  - Firewalls, VPNs, switches and routers
- ICS Vendors must do their part
  - Encrypt configuration files
  - Monitoring and alarm of connection attempts
  - Use secure protocols such as HTTPS
- Most importantly is strong identity management
  - Full integration with Microsoft Active Directory
    - Enables ICS single sign on
  - Dynamic context-based rights
    - Depending on physical location
    - Depending on role



Detect – Abnormal and Suspicious Behavior

- Real-time comparison to baseline
  - Asset inventory
  - Behavior templates
- Protect mobile devices
  - Mobile Device Management
  - Active monitoring
    - Rooting – Android devices
    - Jail-breaking – IOS devices

React – Minimize Damage, Ensure Recovery

- ICS Version control
  - Restore to a safe reference point
  - Keep on a separate secure server
  - Audit configuration changes to ICS
- Operations history protection
  - Redundancy helps reliability
    - Does not protect against corruption
  - What is the impact of loss?
    - Frequency of data backup and storage
- Use of Virtual Machines
  - Provides for rapid recovery
  - Allows for Disaster Recovery as a Service – (DRaaS)

Summary

- SCADA cyber security requires a holistic approach
- Development of culture of cyber security
- Secure computing infrastructure
- Strong identity management
- Implementation of the four pillars of cyber security
- Vendors committed to security quality and features

PcVue Solutions®

Your Independent Global **SCADA** Provider

Please visit us in booth 219!

SCADA Technology Summit