Cybersecurity of Buildings Workshop – OT and IT Convergence – A New Paradigm

Marriott Wardman Park
January 6, 2014
Agenda

Overview of Building Control Systems and Cybersecurity Efforts

Cybersecurity Initiatives and Tools

- Building Insecurity: the Industrial Control System Cyber Emergency Response Team (ICS-CERT) Cybersecurity Evaluation Tool (CSET)
- Cybersecuring U.S. Department of Defense (DoD) Industrial Control Systems
- Kali Linux
- SamuraiFTSU

Attacking and Defending the Building Control Systems and Networks

- Network Reconnaissance, Universal Serial Bus (USB) Attack, Human Machine Interface (HMI) Spoofing
- Accessing the Network through a Misconfigured Device, Password Cracking, Pivoting through the Network with Pass the Hash
- Water Plant Exploitation, Using Metasploit to Attack the Programmable Logic Controller (PLC)
Overview of Building Control Systems Cybersecurity Efforts

Michael Chipley, PhD PMP LEED AP
President

January 6, 2014

mchipley@pmcgroup.biz
Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs range from Building Automation Systems (BAS), Building Management Systems (BMS), Energy Management Systems (EMS), Emergency Management Information Systems (EMIS), and Electronic Security Systems (ESS).

*Within the controls systems industry, ICS systems are often referred to as Operational Technology (OT) systems.*

*Emerging Terms: Cyber-Physical Systems (CPS), Resilient Interdependent Infrastructure Processes and Systems (RIPS)*
# Operational Technology (OT)

<table>
<thead>
<tr>
<th></th>
<th>Information Technology</th>
<th>Operational Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Process transactions, provide information</td>
<td>Control or monitor physical processes and equipment</td>
</tr>
<tr>
<td><strong>Architecture</strong></td>
<td>Enterprise wide infrastructure and applications (generic)</td>
<td>Event-driven, real-time, embedded hardware and software (custom)</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td>GUI, Web browser, terminal and keyboard</td>
<td>Electromechanical, sensors, actuators, coded displays, hand-held devices</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>CIO, IT</td>
<td>Engineers, technicians, operators and managers</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td>Corporate network, IP-based</td>
<td>Control networks, hard wired twisted pair and IP-based</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>Supports people</td>
<td>Controls machines</td>
</tr>
</tbody>
</table>
OT Control System Components

Looks like IT, but configured, operates, and uses different ports and services; HMI, AMI, Modbus, BACnet, DNP 3, LonWorks, Fox, Proxibus, etc
The Cyber Threat Against ICS

Stuxnet - the ballistic missile of ICS warfare
Duqu - malware looks for information that could be useful in attacking industrial control systems
Flame - malware looks for engineering drawings, specifications, and other technical details about the systems and records audio, screenshots, keyboard activity and network traffic
Shamoon - destroyed over 30,000 Saudi Armco work stations

The Shamoon malware has the ability to overwrite the master boot record of a computer. Image credit: Securelist

*Bits and bytes can now be used to physically destroy, spoof, or disrupt every sector of CI*
Exploits written specifically for SCADA
Building Automation Systems

Washington Post - Tridium’s Niagara Framework: Marvel of connectivity illustrates new cyber risks

Researchers Hack Building Control System at Google Australia Office

Google Australia uses a building management system that’s built on the Tridium Niagara AX platform. Although Tridium has released a patch for the system, Google’s control system was not patched.
ICS Vulnerabilities, Patching, Scanning

ICS must typically always remain in the “On” position
• Electric grid cannot deenergize
• Water mains cannot depressurize
• Cascading failures
• Must patch IT OS and Vendor OT
• Unintended consequences; printer auto searches for IP addresses
• Scanning overwhelms devices (8 bits); DOS

*Patches, continuous monitoring and scanning can break OT*
## Security of IT Versus OT

<table>
<thead>
<tr>
<th>SECURITY TOPIC</th>
<th>IT</th>
<th>OT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus &amp; Mobile Code Countermeasures</td>
<td>Common; Widely Used</td>
<td>Uncommon; Difficult to Deploy</td>
</tr>
<tr>
<td>Support Technology Lifetime</td>
<td>3-5 Years</td>
<td>Up to 20 Years (or Longer)</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>Common; Widely Used</td>
<td>Rarely Used</td>
</tr>
<tr>
<td>Application of Patches</td>
<td>Regular/Scheduled</td>
<td>Slow (Vendor Specific)</td>
</tr>
<tr>
<td>Equipment Refresh</td>
<td>Regular/Scheduled</td>
<td>Legacy Based; Unsuitable for Modern Security</td>
</tr>
<tr>
<td>Time Critical Content</td>
<td>Delays are Generally Accepted</td>
<td>Critical Due to Safety</td>
</tr>
<tr>
<td>Availability</td>
<td>Delays are Generally Accepted</td>
<td>24x7x365 (Continuous)</td>
</tr>
<tr>
<td>Security Awareness</td>
<td>Good in Both Private and Public Sectors</td>
<td>Generally Poor Regarding Cyber Security</td>
</tr>
<tr>
<td>Security Testing/Audit</td>
<td>Scheduled and Mandated</td>
<td>Occasional Testing for Outages</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Secure</td>
<td>Very Good, But Often Remote and Unmanned</td>
</tr>
</tbody>
</table>

*There will be new workforce training and education required, new contract and procurement language, new assessment and management roles*
Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework").

The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.
Cybersecurity Framework

Summary:
Recognizing that the national and economic security of the United States is dependent on the reliable functioning of critical infrastructure, the President under Section 412 of the Homeland Security Act of 2002, "Improving Critical Infrastructure Cybersecurity" has directed the Department of Homeland Security and other federal agencies to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. The Framework will consist of standards, guidelines, best practices, and other cybersecurity measures to promote the protection of critical infrastructure. The Framework will include cybersecurity-related risk while protecting business confidentiality, customer privacy and civil liberties.

RFI - Framework for Reducing Cyber Risks to Critical Infrastructure

http://www.nist.gov/itl/cyberframework.cfm
Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.
Conceptual Information Sharing

Classified and Unclassified Reports and Data

- USCYBERCOM
- MAJCOM SOC/BOC/ROC
- Installation SOC/BOC/ROC
- DHS National Cybersecurity & Communication Integration Center
- Community Emergency Ops Center
- Commercial ICS Ops Center
- Building Ops Center (Owned or Lease Space)

For IT Systems, ICS In Progress

- Exists
- Probably Exists
- Yet to Exist
Standards - NIST 800-53 Rev 4

800-53 Rev 4 was released April 30, 2013

Defines the Risk Management Framework
800+ security controls
This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors.

This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

- 800-82 Rev 1 was released May 2013 - has 800-53 Rev 3 Appendix I controls
- 800-82 Rev 2 is scheduled for release spring 2014 - will have 800-53 Rev 4 controls
# NIST SP 800-82 ICS Key Security Controls

## Inventory
- CM-8 Information System Component Inventory
- PM-5 Information System Inventory
- PL-7 Security Concept of Operations
- PL-8 Information Security Architecture
- SC-41 Port and I/O Device Access
- PM-5 Information System Inventory

## Central Monitoring
- AU-6 Audit Review, Analysis, and Reporting
- CA-7 Continuous Monitoring
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- PE-6 Monitoring Physical Access
- PM-14 Testing, Training and Monitoring
- RA-5 Vulnerability Scanning
- SC-7 Boundary Protection
- SI-4 Information System Monitoring
- SI-5 Security Alerts, Advisories, and Directives

## Test and Development Environment
- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

## Critical Infrastructure
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-17 Alternate Work Site
- PM-8 Critical Infrastructure Plan

## Acquisition and Contracts
- AU-6 Audit Review, Analysis, and Reporting
- CA-7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

---

**Inbound Protection, Outbound Detection**
Campus / Installation Enclaves

- DHS NCCIC
  - US-CERT & ICS-CERT

- NOC
  - Internet
  - Test and Development Environment

- IT Operations Center
  - Test and Development Environment

- ICS Operations Center
  - Test and Development Environment

- Security Operations Center
  - Test and Development Environment

- Medical Operations Center
  - Test and Development Environment

- Logistics Operations Center
  - Test and Development Environment

- IT Enclave
  - Accounting
    - Business
      - E-mail

- ICS Enclave
  - Utilities
    - Buildings
      - Pipelines

- Security Enclave
  - CCTV
  - LMR
  - PACS

- Medical Enclave
  - Hospital
    - Laboratory
      - Devices

- Logistics Enclave
  - Storage
    - Ammunition
      - Manufacturing
Numerous ICS Sub-Enclaves

ICS Enclave

- Airfield Lighting
- Buildings
- Electrical
- Natural Gas
- Pier
- POL
- Rail
- Steam
- Traffic Management System
- Water
- Waste Water
Hybrid ICS & Security Sub-Enclaves

ICS Operations Center

Security Operations Center

Installation Enclave
ICS Building Sub-Enclave

Security Building Sub-Enclave
Cybersecurity

By Michael Chepey PhD, PMP, LEED AP, The PMC Group LLC
Last updated: 10/15/2013

INTRODUCTION

Industrial Control Systems (ICS) are physical equipment operated by control technologies and systems that deal with the actual running of plants and equipment. Include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently machine software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICS range from building environmental controls (HVAC, lighting), to systems such as the electrical power grid. With the increasing interconnectivity of ICS to the internet, the ICS can be an entry point into the organization’s other IT systems.

Within the controls systems industry, ICS systems are often referred to as Operational Technology (OT) systems. Historically, the majority of OT systems were proprietary, analog, vendor supported, and were not internet protocol (IP) enabled. Systems key components, such as Remote Terminal Units (RTU’s), Programmable Logic Controllers (PLC), Physical Access Control Systems (PACS), Intrusion Detection Systems (IDS), closed circuit television (CCTV), fire alarm systems, and utility meters have become digital and IP enabled. OT systems use Human Machine Interfaces (HMI’s) to monitor the processes, versus Graphical User Interfaces for IT systems. Most current ICS systems and subsystems are now a combination of Operational Technologies (OT) and Information Technologies (IT).

The Stuxnet, Duqu, Flame and Shamoon malware were specifically designed to target ICS and cause physical damage to the processes or equipment. Stuxnet “snooped” the integrity of the uranium centrifuges and caused the centrifuges to overspin and self-destruct, while the operators console showed the system was operating within normal parameters. The Duqu malware looks for information that could be useful in attacking industrial control systems. Its purpose is not to be destructive, the known components are trying to gather information. The Flame malware looks for engineering drawings, specifications, and other technical details about the systems and records audio, screenshots, keyboard activity, and network traffic. The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices. The most recent malware attack, Shamoon, destroyed over 30,000 Saudi Aramco workstations. Shamoon is capable of spreading to either

http://www.wbdg.org/resources/cybersecurity.php
CIO provides routers, switches and firewalls, OT connects in distribution closet
DHS Interagency Security Committee

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand Up Development and Test Environments</td>
<td>Establish development and testing environments so PACS developers and testers can conduct build activities in an environment that does not impact the agency’s production systems.</td>
<td>4 – 6 weeks</td>
</tr>
<tr>
<td>Build/Configure Servers</td>
<td>Build and/or configure servers to properly operate the PACS solution, as needed based upon the chosen implementation path.</td>
<td>1 – 2 weeks</td>
</tr>
<tr>
<td>Install Supporting Software</td>
<td>Install supporting software (i.e., Commercial Off-The-Shelf [COTS] Identity Access Management [IAM] Suite) on PACS servers, as needed based upon the chosen implementation path.</td>
<td>1 – 2 weeks</td>
</tr>
<tr>
<td>Configure Supporting Software</td>
<td>Configure PACS software to specifically meet the agency’s unique needs and/or perform certain functions, as needed based upon the chosen implementation path.</td>
<td>1 – 2 weeks</td>
</tr>
<tr>
<td>Implement and Assess Security Controls</td>
<td>Conduct Steps 3 and 4 of the Risk Management Framework (RMF) by applying the controls identified in the requirements and design phase and by assessing the adequacy and effectiveness of the security controls and documenting the findings in an assessment report.</td>
<td>12 – 20 weeks</td>
</tr>
<tr>
<td>Conduct Testing on Initial Build</td>
<td>Perform testing on the PACS solution in a development and/or test environment to ensure that system errors are found and corrected before the solution is deployed on the agency’s network.</td>
<td>2 – 4 weeks</td>
</tr>
<tr>
<td>Conduct Pilot Implementation Deployment</td>
<td>Conduct a pilot implementation to expose a small subset of the agency’s user base to the PACS solution for the purpose of evaluating the solution’s operations against real-world requirements.</td>
<td>Varies on size of deployment (number of facilities and</td>
</tr>
</tbody>
</table>

NIBS is convening a Workshop January 28-29, 2014
Planning and Design
- 90% design complete initial CSET evaluation
- Apply hardening criteria (e.g. DoD STIGS)
- Conduct initial Penetration Testing Construction (e.g. SamuraiFTSU)
- 50-75% construction complete conduct Factory Acceptance Testing (FAT) of major components
- 100% construction complete conduct Site Acceptance Testing (SAT)
- Conduct Penetration Testing
- Create System Security Plan (SSP)
- Create Plan of Action and Milestones (POAM)
1.0 SYSTEM HARDENING

System hardening refers to making changes to the default configuration of a network device and its operating system (OS), software applications, and required third-party software to reduce system security vulnerabilities.

1.1 FAT Measures

The Vendor shall verify that the Purchaser requires the results of cyber security scans (as a minimum a vulnerability and active port scan, with the most current signature files) run on the control system as a primary activity of the FAT. This assessment is then compared with an inventory of the required services, patching status, and documentation, to validate this requirement.

1.2 SAT Measures

The Vendor shall compare the results of cyber security scans run on the system, as a primary activity of the SAT, with an inventory of the required services, patching status, and required documentation. At the conclusion of the SAT and before cutover or commissioning, the above cyber security scans (with the most current signature files) must be run again.

1.3 Maintenance Guidance

Document the system operating system and software patches as the system software evolves to allow traceability and to verify no extra services are reinstalled. Anytime the system is upgraded, it is recommended that system Vendors rerun appropriate subsets of the FAT on the baseline system before delivery to the purchaser.
DHS NCCIC and ICS-CERT

National Cybersecurity and Communications Integration Center
http://www.us-cert.gov/nccic/

NIST 800-30
NIST 800-53 Rev 3
NIST 800-53 Rev 4
NIST 800-82 Rev 1
NIST 1108
NISTR 7628
CNSSI 1253 ICS Overlay
NERC CIP
DHS CSET 5.1
DHS CSET 6.0 (Jan 2014 release)
DHS ICS-CERT Training

Training Available Through ICS-CERT

Scheduled training is on the ICS-CERT Calendar.

Web-Based Training
OPSEC for Control Systems

Instructor Led Format—Introductory Level
Introduction to Control Systems Cybersecurity (101)—1 day or 8 hrs

Instructor Led Format—Intermediate Level
Intermediate Cybersecurity for Industrial Control Systems (201), lecture only—1 day or 8 hrs

Hands-On Format—Intermediate Level
Intermediate Cybersecurity for Industrial Control Systems (202), with lab/exercises—1 day or 8 hrs

Hands-On Format—Technical Level
ICS Cybersecurity (301)—5 days

The Control Systems Security Program provides training courses and workshops at various industry association events. These courses are packed with up-to-date information on cyber threats and mitigations for vulnerabilities. If your organization would like to learn more about training opportunities, please contact cssp_training@hq.dhs.gov.

https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT
SANS ICS 410 – ICS Security Essentials

• The SANS Industrial Control Systems Team is working to develop a curriculum of focused ICS courseware to equip both security professionals and control system engineers with the knowledge and skills they need to safeguard our critical infrastructures. The entry level course in the SANS ICS Curriculum is ICS 410 – ICS Security Essentials

• This course provides students with the essentials for conducting security work in Industrial Control System (ICS) environments. Students will learn the language, the underlying theory and the basic tools for ICS security in industrial settings across a diverse set of industry sectors and applications. This course will introduce students to ICS and provide the necessary information and learning to secure control systems while keeping the operational environment safe, reliable, and resilient.
SANS GISCP

- SANS GIAC is developing a vendor neutral, practitioner focused Industrial Control System certification. The Global Industrial Cyber Security Professional Certification (GICSP) will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.
- This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that an IT, Engineer, and Security professional should know if they are in a role that could impact the cyber security of an ICS environment.
NIST Cyber-Physical Systems Workshop

http://events.energetics.com/NIST-CPSWorkshop/index.html
Future - Industrial Internet Revolution

NY Times June 19, 2013

- General Electric Adds to Its ‘Industrial Internet
- Cisco Systems is in the middle of an “Internet of Everything” strategy that involves selling software and services for a world rich in sensors
- Phillips is also offering data-gathering connectivity in both its health care and lighting products
Summary

• Maintain Situational Awareness of the Cybersecurity Framework
• Prepare CIO and IT staff for new role scanning and protecting ICS systems
• Prepare Engineering, Transportation and other ICS functions staff for new cybersecurity requirements
• Prepare the Acquisition and Contracting staff for new contract and procurement language
• Conduct pilot self-assessments of ICS using the CSET Tool, understand baseline, potential vulnerabilities, risks and mitigation measures
• Consider developing ICS Overlays for your organization (similar to the CNSSI 1253)
• Coordinate with DHS NCCIC, evaluate options for information sharing
• New skills to learn, new methods, but based on Risk