Security Controls for Industrial Control Systems

EEI/AGA Security Committee Fall Meetings

September 13, 2006
Boston, MA

Stuart Katzke and Keith Stouffer, National Institute of Standards & Technology, Gaithersburg, MD
Marshall Abrams, The MITRE Corporation, McLean, VA
David Norton, Entergy, Inc. New Orleans, LA
Joe Weiss, KEMA, Inc., Cupertino, CA
Presentation Contents

• NIST Responsibilities for Industrial Control Systems (ICS) Security
• NIST Information Security Program
• NIST ICS Security Project
  – ICSs and Information Systems
  – Applying Security Controls to ICS
  – Invitational ICS Workshop
  – Research Findings
  – NIST Plans
  – Contact Information
NIST Responsibilities for Industrial Control Systems (ICS) Security

• In general
  – NIST promotes the U.S. economy and public welfare
  – NIST develops mandatory standards and guidelines for use by federal agencies (except national security systems)
  – Standards and guidelines may also be voluntarily used by nongovernmental organizations

• Specifically concerning ICS
  – Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems requires that federal agencies implement minimum security controls for their organizational information systems
    • ICS have many unique characteristics differentiating them from traditional information systems
NIST ICS Security Project

Objectives

• Work cooperatively with federal stakeholders and industry to interpret SP 800-53 security controls* for ICSs

• Publish SP 800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security initial public draft - September 2006

• Improve the security of public and private sector ICSs
  – Work with the many on-going industry standards activities
    • Standards for the ICS industry, if widely implemented, will raise the level of control systems security
    • Foster convergence
  – Use open public process in developing candidate set of security requirements

*Control has two different uses: (1) An adjective of "system" (e.g., control system, industrial control system) (2) A noun (e.g., security control)
NIST Publications

Security Standards and Guidelines

- Federal Information Processing Standards (FIPS)
  - Developed by NIST in accordance with FISMA.
  - Approved by the Secretary of Commerce.
  - Compulsory and binding for federal agencies; not waiverable.

- NIST Guidance (Special Publication 800-Series)

- Other security-related publications
  - NIST Interagency and Internal Reports and Information Technology Laboratory Bulletins provide technical information about NIST's activities.
  - Mandatory only when so specified by OMB.
Key Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)

Many other FIPS and NIST Special Publications provide security standards and guidance supporting the FISMA legislation…
Information Security Program

Links in the Security Chain: Management, Operational, and Technical Controls

- Risk assessment
- Security planning
- Security policies and procedures
- Contingency planning
- Incident response planning
- Security awareness and training
- Physical security
- Personnel security
- Certification, accreditation, and security assessments
- Access control mechanisms
- Identification & authentication mechanisms (Biometrics, tokens, passwords)
- Audit mechanisms
- Encryption mechanisms
- Firewalls and network security mechanisms
- Intrusion detection systems
- Security configuration settings
- Anti-viral software
- Smart cards

Adversaries attack the weakest link…where is yours?

National Institute of Standards and Technology
The NIST Risk Framework

Starting Point
FIPS 199 / SP 800-60

Security Categorization
Define criticality / sensitivity of information system according to potential impact of loss

Security Control Selection
Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

FIPS 200 / SP 800-53

Security Control Refinement
Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

FIPS 200 / SP 800-53 / SP 800-30

Security Control Implementation
Implement security controls; apply security configuration settings

SP 800-70

Security Control Documentation
Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-18

FIPS 200

Security Control Selection
Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

FIPS 200 / SP 800-53

System Authorization
Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-37

Security Control Monitoring
Continuously track changes to the information system that may affect security controls and reassess control effectiveness

SP 800-37 / SP 8800-53A

Security Control Assessment
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-53A

SP 800-37

SP 800-60

FIPS 199

FIPS 200

SP 800-18

SP 800-70

SP 800-30

FIPS 200 / SP 800-53 / SP 800-30

National Institute of Standards and Technology
ICSs and Information Systems

• ICSs are information systems
  – Historically, little resemblance to typical information systems
    • Originally, isolated systems running proprietary control protocols
    • More stringent safety, performance and reliability requirements
    • Used special purpose operating systems and applications
  – Today, ICSs resemble corporate information systems
    • Connected to corporate information systems
    • Increased connectivity, remote access capabilities, Internet protocols
• ICS cyber security implications
  – Significantly less isolation
  – More vulnerable to compromise or takeover
  – Greater need to secure these systems
Applying Security Controls to ICS

• ICSs have many special characteristics compared to typical information systems
  – Reliability and availability are key drivers
  – Different risks and priorities
  – Significant risk to the health and safety of human lives
  – Serious damage to the environment
  – Serious financial risks such as production losses
  – Negative impact to a nation’s economy

• Goals of safety and security sometimes conflict with the operational requirements of ICSs

• ICS failures can result in serious disruptions to critical national infrastructures
Applying SP 800-53 to ICS

• SP 800-53 provides a rich set of security controls
  – Consistent & complement other security standards
  – Compliance can demonstrate due diligence

• Research/study
  – Bi-directional mappings & analysis of SP 800-53 ⇔ NERC CIPs
    • Generally, meeting SP 800-53 meets NERC CIPs
    • Meeting NERC CIPS does not automatically meet SP 800-53
  – U.S. Government (USG) stake holder working group
    • Get USG stake holder's inputs/experience
    • Evolve SP 800-53 in cooperation with USG stake holders
Invitational USG ICS Workshop

- Workshop April 19-20, 2006 at NIST to discuss the development of security requirements and baseline security controls for federally owned/operated industrial/process control systems based on NIST SP 800-53
- Attended by Federal agency stakeholders
- Results
  - Some incorporated SP 800-53, Rev 1
  - Continuing work to be reflected in future revisions to SP 800-53
ICS Workshop Activities

• Develop draft material for an Appendix and/or Supplemental Guidance material that addresses the application of SP 800-53 to ICS

• Review the SP 800-53 controls to
  – Determine which controls are causing challenges when applied to ICS
  – Discuss why a specific control is causing a challenge
  – Develop guidance on the application (or non application) of that control to ICS
  – Determine if there are any compensating controls that could be applied to address the specific control that can’t technically be met
Workshop Result
SP 800-53 Appendix I

• Industrial Control Systems: Interim Guidance on the Application of Security Controls
• Provides initial recommendations for organizations that own and operate industrial control systems:
  – Use Section 3.3 of SP 800-53, Tailoring the Initial Baseline, to modify or adjust the recommended security control baselines when certain conditions exist that require that flexibility.
  – Develop appropriate rationale and justification as described in the compensating control section of SP 800-53 to meet the intent of a control that can’t technically be met.

Comparing control sets from different organizations/ frameworks is difficult and subject to interpretation

NERC CIP standards generally correspond to controls in one or more of the SP 800-53 control families

- Most NERC CIP requirements* correspond to controls in SP 800-53.

* Requirements, measures, and compliance are reserved words defined in the NERC CIP
Mapping Table Extract

<table>
<thead>
<tr>
<th>Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 NERC req ≈ SP 800-53 controls</td>
</tr>
<tr>
<td>9 NERC more specific than SP 800-53 control</td>
</tr>
<tr>
<td>13 NERC ⊂ SP 800-53 control</td>
</tr>
<tr>
<td>17 NERC less specific than SP 800-53 control</td>
</tr>
</tbody>
</table>

### NERC CIP FINAL

<table>
<thead>
<tr>
<th>SP 800-53 Rev. 1 Controls</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td></td>
</tr>
<tr>
<td>AC-1 Access Control P &amp; P</td>
<td>4</td>
</tr>
<tr>
<td>AC-2 Account Management</td>
<td>8</td>
</tr>
<tr>
<td>AC-3 Access Enforcement</td>
<td>8</td>
</tr>
<tr>
<td>AC-4 Information Flow Enforcement</td>
<td>12</td>
</tr>
<tr>
<td>AC-5 Separation of Duties</td>
<td></td>
</tr>
<tr>
<td>AC-6 Least Privilege</td>
<td>17</td>
</tr>
<tr>
<td>AC-7 Unsuccessful Logon Attempts</td>
<td>8</td>
</tr>
<tr>
<td>AC-8 System Use Notification</td>
<td></td>
</tr>
<tr>
<td>AC-9 Previous Logon Notification</td>
<td>13</td>
</tr>
<tr>
<td>AC-10 Concurrent Session Control</td>
<td>13</td>
</tr>
<tr>
<td>AC-11 Session Lock</td>
<td>17</td>
</tr>
<tr>
<td>AC-12 Session Termination</td>
<td></td>
</tr>
<tr>
<td>AC-13 Supervision and Review—A C</td>
<td>12</td>
</tr>
<tr>
<td>AC-14 Permitted Actions without I or A</td>
<td>9</td>
</tr>
<tr>
<td>AC-15 Automated Marking</td>
<td>8</td>
</tr>
<tr>
<td>AC-16 Automated Labeling</td>
<td></td>
</tr>
<tr>
<td>AC-17 Remote Access</td>
<td>7</td>
</tr>
<tr>
<td>AC-18 Wireless Access Restrictions</td>
<td>17</td>
</tr>
<tr>
<td>AC-19 Access Control for Portable and Mobile Systems</td>
<td>17</td>
</tr>
<tr>
<td>AC-20 Personally Owned Information Systems</td>
<td>17</td>
</tr>
</tbody>
</table>

### Codes
- **8 NERC req ≈ SP 800-53 controls**
- **9 NERC more specific than SP 800-53 control**
- **13 NERC ⊂ SP 800-53 control**
- **17 NERC less specific than SP 800-53 control**
Research Findings (1 of 2)

- Conforming to moderate baseline in SP 800-53 generally complies with the management, operational and technical security requirements of the NERC CIPs; the converse is not true.
- NERC contains requirements that fall into the category of business risk reduction
  - High level business-oriented requirements
  - Demonstrate that enterprise is practicing due diligence
  - SP 800-53 does not contain analogues to these types of requirements as SP 800-53 focuses on information security controls (i.e., management, operational, and technical) at the information system level.
Research Findings (2 of 2)

- NERC approach is to define critical assets first and their cyber components second
  - No criteria for criticality
  - Non-critical assets barely mentioned
- FIPS 199 specifies procedure, applied to all information and information systems for identifying the security categories based on potential impact
  - Confidentiality, availability, and integrity evaluated separately
  - Possible outcomes are low, moderate, and high
  - Highest outcome applies to system
- Documentation requirements differ; more study required
NIST Plans

• Anticipated FY07 Products
  – White paper on ICS cyber security in the FISMA paradigm
  – Annotated SP 800-53 addressing conformance to NERC CIP
  – Annotated NERC CIP showing correspondence to FISMA paradigm
  – Input to revision 2 of SP 800-53

• Continue working with the federal ICS stakeholders
  – Including FERC, Department of Homeland Security (DHS), Department of Energy (DOE), the national laboratories, and federal agencies that own, operate, and maintain ICSs
  – To develop an interpretation of SP 800-53 for ICSs that permits real/practical improvements to the security of ICSs and, to the extent possible, ensures compliance with the management, operational, and technical requirements in the NERC CIP standards
NIST SP 800-82

- **Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security**

- **Purpose**
  - Provide guidance for establishing secure SCADA and ICS, including the security of legacy systems

- **Content**
  - Overview of ICS
  - ICS Vulnerabilities and Threats
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS in the Federal Information Security Management Act (FISMA) Paradigm
  - ICS Security Controls

- **Initial public draft - September 2006**

SP 800-82 Audience

- Control engineers, integrators and architects when designing and implementing secure SCADA and/or ICS
- System administrators, engineers and other IT professionals when administering, patching, securing SCADA and/or ICS
- Security consultants when performing security assessments of SCADA and/or ICS
- Managers responsible for SCADA and/or ICS
- Researchers and analysts who are trying to understand the unique security needs of SCADA and/or ICS
- Vendors developing products that will be deployed in SCADA and/or ICS
NIST ICS Security Project
Summary

• Issue ICS security guidance
  – Evolve SP 800-53 *Recommended Security Controls for Federal Information Systems* security controls to better address ICSs
  – Publish SP 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security* initial public draft - September 2006

• Improve the security of public and private sector ICSs
  – Raise the level of control system security
    • R&D and testing
  – Work with on-going industry standards activities
    • Assist in standards and guideline development
    • Foster convergence
NIST ICS Security Project
Contact Information

100 Bureau Drive  Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leaders

Keith Stouffer  Dr. Stu Katzke
(301) 975-3877  (301) 975-4768
keith.stouffer@nist.gov  skatzke@nist.gov

sec-ics@nist.gov

Web Pages

Federal Information Security Management Act (FISMA) Implementation Project

http://csrc.nist.gov/sec-cert

NIST ICS Security Project

http://csrc.nist.gov/sec-cert/ics