NIST and US Government Activities in area of System Assurance

Michael Kass
Computer Scientist
NIST Information Technology Laboratory

michael.kass@nist.gov
• NIST Information Technology Laboratory (ITL)

  – *Who we are*
    • ITL Mission
    • Core Competencies

  – *How ITL Contributes to Security Assurance*
To promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics.
Core Competencies

Technology Development

- IT Measurement and Testing
- Mathematical and Statistical Analyses for Measurement Science
- Modeling and Simulation for Measurement Science
- IT Standards Development and Deployment

Customers
- Government
- Industry
- Academia
- Standards Orgs.
ITL’s Role in Security Assurance

- NIST publications, standards and testing support U.S. regulatory/policy decisions in the areas of federal system security and information assurance
ITL Security Assurance Efforts

- Supply Chain Risk Management (SCRM) Pilot
- Guidance Publications in support of Federal Information Security Management Act (FISMA)
- The Security Content Automation Protocol (SCAP)
- National Vulnerability Database (NVD)
- Software Assurance Metrics and Tool Evaluation (SAMATE)
- Security Management and Assurance through Cryptography
- National Voluntary Lab Accreditation Program (NVLAP)
- Voting System Assurance
- Metrics, Measurement and Assurance

Background

• **Comprehensive National Cybersecurity Initiative #11**: “Develop Multi-Pronged Approach for Global Supply Chain Risk Management (SCRM)”

• Provide US Government with robust toolset of supply chain methods and techniques

• Multi-tiered Approach:
  – Cost effective procurement related strategies
  – Industry input into supply chain practices and development of international standards
  – Ability to share supply chain incident information
NIST Supply Chain Risk Management Guidance

  - To be Published: April, 2010
- Future NIST Special Publication
  - First Public Draft: Winter, 2011
SCRM Requirements Process
Step 1 - Determine Supply Chain Risk Threshold

- NIST Special Publication 800-53 Rev. 3 Security Control: SA-12 Supply Chain Protection - “The organization protects against supply chain threats ... as part of a comprehensive, defense-in-breadth information security strategy.”
Step 2 - Identify Potential Suppliers

- Conduct a market analysis
- Post a “sources sought” notification
- Gather information from open-sources
Step 3 - Perform Source Analysis

- Review all data gathered during the presolicitation
- Obtain any additional information
- Document findings
- Consider a procurement strategy
- *Include applicable practices as requirements in the RFP...*
Applicable SCRM Practices Include

- Harden supply chain delivery mechanisms
- Manage requirements creep
- Identify critical components
- Manual Code Review
- Static Analysis
- Protect the Supply Chain Environment
  - Physical defenses
  - Logical defenses
  - Test the defenses
- 26 Other Pilot Practices
Federal Information Security Management Act (FISMA), 2002

• *Title III of E-government Act:* Requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems
ITL FISMA Support

- **NIST ITL Role:** promote the development of key security standards and guidelines to support the implementation of and compliance with FISMA including:
  - Standards for categorizing information and information systems by mission impact (FIPS 199)
  - Standards for minimum security requirements for information and information systems (FIPS 200)
  - Guidance for selecting appropriate security controls for information systems (SP 800-53)
  - Guidance for assessing security controls in information systems and determining security control effectiveness (SP 800-53A)
<table>
<thead>
<tr>
<th><strong>Security Content Automation Protocol</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>MITRE</strong></th>
<th><strong>Naming</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>MITRE</strong></th>
<th><strong>Expressing</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>MITRE</strong></th>
<th><strong>Assessing</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>FIRST</strong></th>
<th><strong>Scoring</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>CVE</strong></th>
<th>Common Vulnerabilities and Exposures</th>
<th>Standard nomenclature and dictionary of security related software flaws</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CCE</strong></td>
<td>Common Configuration Enumeration</td>
<td>Standard nomenclature and dictionary of software misconfigurations</td>
</tr>
<tr>
<td><strong>CPE</strong></td>
<td>Common Platform Enumeration</td>
<td>Standard nomenclature and dictionary for product naming</td>
</tr>
<tr>
<td><strong>XCCDF</strong></td>
<td>eXtensible Configuration Checklist Description Format</td>
<td>Standard XML for specifying checklists and for reporting results of checklist evaluation</td>
</tr>
<tr>
<td><strong>OVAL</strong></td>
<td>Open Vulnerability and Assessment Language</td>
<td>Standard XML for test procedures</td>
</tr>
<tr>
<td><strong>CVSS</strong></td>
<td>Common Vulnerability Scoring System</td>
<td>Standard for measuring the impact of vulnerabilities</td>
</tr>
</tbody>
</table>

Cisco, Qualys, Symantec, Carnegie Mellon University
What is SCAP?

**Languages**
- Means of providing instructions
  - Community developed
  - Machine readable XML
  - Reporting
  - Representing security checklists
  - Detecting machine state

**Metrics**
- Risk scoring framework
  - Community developed
  - Transparent
  - Metrics
    - Base
    - Temporal
    - Environmental

**Enumerations**
- Convention for identifying and naming
  - Community developed
  - Product names
  - Vulnerabilities
  - Configuration settings

---

XCCDF | OVAL | CVSS
--- | --- | ---
CVE | CCE | CPE

---

National Institute of Standards and Technology
What are we trying to achieve with SCAP?

**Minimize Effort**
- Reduce the time and effort of manual assessment and remediation
- Provide a more comprehensive assessment of system state

**Increase Interoperability**
- Enable fast and accurate correlation within the enterprise and across organizations/agencies
- Shorten decision cycles by rapidly communicating:
  - Requirements (What/How to check)
  - Results (What was found)
- Allow diverse tool suites and repositories to share data
- Foster shared situational awareness by enabling and facilitating data sharing, analysis, and aggregation
Current SCAP Use Cases

- **Vulnerability Management** – detect, prioritize, and remediate vulnerabilities (software flaws) on a system
- **Configuration Verification** – determine whether system configuration settings comply with organizational policies
- **Patch Compliance** – determine whether appropriate patches have been applied on a system
- **System Inventory** – identify products installed on the system (e.g., hardware, operating system, and applications)
- **Malware Detection** – detect presence of malware on a system
  - Zero day signature building for consumption by SCAP validated products
SCAP Validation Program

As of 2 March 2010,

- 9 NVLAP Accredited labs

**Validated Products**

- 24 vendors
- 32 products
- 96 capabilities-based validations
- 15 standards-based validations
• NVD is the U.S. government repository of public vulnerability management information.
• XML data feeds for SCAP reference data
• Used by government, industry and academia
• 40,837 CVE entries with the NVD Analysis Team evaluating over 6,000 vulnerabilities a year
• Product dictionary containing 18,000 unique product names
• CCE to 800-53 control mapping data feed
• Spanish and Japanese language translations
Software Assurance Metrics and Tool Evaluation

- NIST SAMATE co-sponsored with DHS to:
  - Measure of the effectiveness of today’s software assurance tools
  - Identify gaps in technology
  - Recommend areas of research to DHS NCSD
  - Define metrics for the measurement of SwA tool effectiveness
Software Assurance Metrics and Tool Evaluation

• SAMATE Reference Dataset (SRD) of tool tests
  – An online repository of thousands of discrete tool tests (C, C++, and Java source code to date). Tests currently based upon white box definitions of CWEs.
  – Contributed from NIST, academia, tool developers
  – New test contributions coming from multiple sources

• The Static Analysis Tool Exposition (SATE)
  – “Real-world” source code used to represent the more complex problems facing today’s SwA tools
  – Tool developers participate in analysis of “real world” applications
Security Management and Assurance through Cryptography

• Testing-focused activities include:
  – The validation of cryptographic modules and cryptographic algorithm implementations,
  – Accreditation of independent testing laboratories,
  – Development of test suites,
  – Providing technical support to industry forums
  – Conducting education, training, and outreach programs.
  – **Cryptographic Algorithm Validation Program (CAVP)**
    – Provides testing requirements and tools against FIPS and NIST recommended cryptographic algorithms
    – A prerequisite to the Cryptographic Module Validation Program (CMVP)
  – **Cryptographic Module Validation Program (CMVP)**
    – Validates cryptographic modules to Federal Information Processing Standards (FIPS)140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards
SHA-3 Cryptographic Hash Competition

- Develop a new cryptographic hash algorithm via a public worldwide competition
- Motivated by collision attacks on commonly used hash algorithms, particularly MD5 & SHA-1, that can impact the Internet and e-Commerce
- Held 2 hash workshops in 2005 & 2006
- Proposed criteria for new hash algorithm in Jan 2007

*Many comments received*
SHA-3 Cryptographic Hash Competition

• “SHA-3” Competition announced on Nov. 2, 2007
• Received 64 submissions for candidate hash algorithms (10/08)
• Held First SHA-3 Candidate Conference, announced 51 first-round candidates (2/09)
• Announced 14 second-round candidates (7/09)
• Future Work
  • Hold Second SHA-3 Candidate Conference at UCSB (8/10)
  • Announce finalists (Fall/10)
  • Select winner and publish report on selection (est. 8/12)
  • Send proposed standard to Sec. of Commerce for signature (est. 2/13)
National Voluntary Laboratory Accreditation Program (NVLAP)

- Provides third-party accreditation to testing and calibration laboratories
- Lab accreditation programs are established in response to:
  - Congressional mandates
  - Administrative actions by the Federal Government
  - Requests by private-sector organizations
NVLAP Laboratories

- Common Criteria Evaluation Labs
- Cryptography and Security Testing Labs
  - CAVP
  - CMVP
- Voting System Testing Labs
Voting

• The 2002 Help America Vote Act (HAVA) gave NIST a key role in helping to realize nationwide improvements in voting systems to improve:
  – Security
  – Privacy
  – Use-ability
  – Correctness

• A set of specifications and requirements against which voting systems can be tested
• In addition, the guidelines establish evaluation criteria for the national certification of voting systems
• NIST test suites address human factors, security and core functionality requirements for voting systems to:
  – Promote consistent results and transparency of testing process
  – Assist manufacturers in the development of conforming products by providing precise test specifications.
  – Also, they can help reduce the cost of testing (common tests)
  – Improve confidence in voting systems
Metrics, Measurement and Assurance (MMA)

- Developing a case study in building an assurance case model for voting systems
- Focusing upon open-ended vulnerability testing portion of VVSG
- Looking to work with NIST SP 800-53 writers to expand upon system assurance guidelines
  - Assurance case guidance
NIST ITL Future Direction

• Currently focus is on checklists and controls
• Future, more pro-active, assurance based guidance