DoD Software Assurance (SwA) Overview

Thomas Hurt
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

17th Annual NDIA Systems Engineering Conference
Springfield, VA | October 29, 2014
Overview

• Plan — Where are we going?
• Progress — Where are we now?
• Challenges — What do we need?
• Industry input — How can DoD and industry optimize the relationship?

Software Assurance. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

NDAA 2013 Section 933

Our objective is to establish software assurance as a mature SE discipline across DoD
Motivation: Current Assurance Outlook

- **Threat:** Nation-state, terrorist, criminal, or rogue developer who:
  - Exploits vulnerabilities remotely
  - Gains control of systems through supply chain opportunities
- **Vulnerabilities**
  - All systems, networks, and applications (Hardware & Software)
  - Intentionally implanted (e.g., malicious code insertion)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile software)
- **Traditional Consequences:** Loss of critical data and technology
- **Emerging Consequences:** Software vulnerabilities that are targeted or surface in sustainment, and exploitation of development and manufacturing supply chain
  - Either can damage National Security or critical warfighting capability

Today’s acquisition environment drives the increased emphasis:

<table>
<thead>
<tr>
<th>Then</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand-alone systems</td>
<td>Networked systems</td>
</tr>
<tr>
<td>Some software functions</td>
<td>Software-intensive and critical functions in software</td>
</tr>
<tr>
<td>Known supply base</td>
<td>Prime Integrator, multiple opaque tiers of suppliers</td>
</tr>
<tr>
<td>CPI (technologies)</td>
<td>CPI and critical components</td>
</tr>
</tbody>
</table>
Trusted Defense Systems and Networks Strategy

Drivers/Enablers

- National Cybersecurity Strategies
- Globalization Challenges
- Increasing System Complexity
- Pervasive networks & SW-intensive systems
- SW-based critical functions
- Intellectual Property Protection

Delivering Trusted Systems

Prioritize by Mission Dependence

Comprehensive Program Protection Planning

Enhance R&D for Vulnerability Detection and Response

Partner with Industry

Program Protection Plan

USD(AT&L)
http://www.acq.osd.mil/se/pg/guidance.html

Report on Trusted Defense Systems

USD(AT&L)
ASD(NII)/DoD CIO
Executive Summary:
http://www.acq.osd.mil/se/pg/spec-studies.html
Public Law Driving SwA Evolution

  – Required section 932 Report delivered to the Committees

• Public Law 112-239-January 2, 2013, NDAA for Fiscal Year 2013, Section 933, Improvements in Assurance of Computer Software Procured by the Department of Defense:
  – A research and development strategy to advance capabilities in software assurance and vulnerability detection
  – The state-of-the-art of software assurance analysis and test
  – How the Department might hold contractors liable for software defects or vulnerabilities

• Public Law 113-66, NDAA for Fiscal Year 2014, Section 937, Joint Federated Centers for Trusted Defense Systems for the Department of Defense
  – JFAC Charter in signature process with DEPSECDEF
  – Section 937 Report to the Committees due for final draft 15 Oct 2014
  – Activities to initiate JFAC operation in-process
DoD SwA Community of Practice (COP)

DoD SwA CoP Objectives

- Create a DoD community of Software Assurance practice
- Develop a system for recovering and spreading emerging best practices across the DoD
- Establish communication and coordination within DoD SwA community
- Mature software assurance practice within the PPP

Key Activities

- Engage Programs
- Conduct Workshops
- Provide tutorials
- Manage CoP Portal

NDAA 2013 Section 933

- SwA across life cycle
- Use automated tools

Plan of Action & Milestones

SwA CoP

- Contract Language WG
- SwA Metrics WG
- Enterprise Coord. & Sharing WG
- Software Test & Eval WG
- Workforce WG

SwA Core Team

(DoD AT&L, DoD CIO, NSA CAS)

Responsible for bringing together community of practice

Technical Advisors

(MITRE, DIA, CMU/SIE, ...)

 Draws on

informs

DoD SwA Community of Practice (COP)
Software Assurance: As Integrated into the DoD System Lifecycle

SwA in each part of the lifecycle
- Chain of custody of knowledge, risks and products
- Engineering level traceability from MDD through disposal

Identify & mitigate sources of software vulnerabilities
- COTS known vulnerabilities
- Secure coding practices & automated code analysis tools
- Secure development environment and toolset

SwA blends into Engineering Process
- Processes, Tools, Techniques
- Requirements & Metrics
- System Architecture, SW Design, Coding Practice
- Test and Evaluation
- Prevent, Detect, Respond

Focus Scope of Protection
Tailorable RFP Language is Available

Emphasizing Use of Affordable, Risk-based Countermeasures
### Software Assurance as a Systems Engineering Discipline: Countermeasure Selection

**Development Process**

Apply assurance activities to the procedures and structure imposed on software development.

**Operational System**

Incorporate countermeasures in the requirements, architecture, design, and acquisition of end-item software products and their interfaces.

**Development Environment**

Apply assurance activities to the environment and tools for developing, testing, and integrating software code and interfaces.

### Trends

- **Increased use of automated tools for detection, analysis, and remediation**
- **Requirement to use SwA tools and methodology across DoD system life cycle**
- **Monitor and assess application of software assurance countermeasures**

### Table 5.3-5: Application of Software Assurance Countermeasures (sample)

<table>
<thead>
<tr>
<th>Software (CPI, critical function components, other software)</th>
<th>Developmental CPI SW</th>
<th>Developmental Critical Function SW</th>
<th>Other Developmental SW</th>
<th>COTS CPI and Critical Function SW</th>
<th>COTS (other than CPI and Critical Function) and NDI SW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Analysis p/a</td>
<td>100/80%</td>
<td>100/80%</td>
<td>none</td>
<td>Vendor SwA</td>
<td>No</td>
</tr>
<tr>
<td>Design Inspect</td>
<td>Two Levels</td>
<td>Two Levels</td>
<td>One level</td>
<td>Vendor SwA</td>
<td>No</td>
</tr>
<tr>
<td>Code Inspect p/a</td>
<td>100/60</td>
<td>100/60</td>
<td>100/65</td>
<td>Vendor SwA</td>
<td>No</td>
</tr>
<tr>
<td>CVE p/a</td>
<td>100/60</td>
<td>100/60</td>
<td>100/60</td>
<td>Vendor SwA</td>
<td>No</td>
</tr>
<tr>
<td>CAPEC p/a</td>
<td>100/60</td>
<td>100/60</td>
<td>100/60</td>
<td>Vendor SwA</td>
<td>No</td>
</tr>
<tr>
<td>CWE p/a</td>
<td>100/60</td>
<td>100/60</td>
<td>100/60</td>
<td>Vendor SwA</td>
<td>No</td>
</tr>
<tr>
<td>Pen Test</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Test Coverage p/a</td>
<td>75/60%</td>
<td>75/60%</td>
<td>50/25%</td>
<td>UNK</td>
<td>UNK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover</td>
</tr>
<tr>
<td>Supplier Redundancy</td>
</tr>
<tr>
<td>Fault Isolation</td>
</tr>
<tr>
<td>Least Privilege</td>
</tr>
<tr>
<td>System Element</td>
</tr>
<tr>
<td>Isolation</td>
</tr>
<tr>
<td>Input checking / validation</td>
</tr>
<tr>
<td>SW load key</td>
</tr>
<tr>
<td>30%</td>
</tr>
<tr>
<td>Partial</td>
</tr>
<tr>
<td>Partial</td>
</tr>
<tr>
<td>Partial</td>
</tr>
<tr>
<td>Partial</td>
</tr>
</tbody>
</table>

State-of-the-Art Resources for SwA

• Technical Approach
  – SwA objectives (e.g., countering weaknesses) were organized and consolidated into categories that the DoD acquisition community can use
  – State-of-the-art of SW analysis and test tools and techniques were organized into families
  – SwA objectives were mapped to tools and techniques, providing a sound basis for a tool selection and use methodology by DoD programs

• Assessment Results
  – There is utility in grouping SwA tools and techniques into families
  – Some tools are costly, and use of any tool or technique incurs program cost
  – Policy, guidance and resources must evolve at pace with constantly changing threats
  – No “silver bullet”, tool or technique exists

Available at http://www.acq.osd.mil/se/initiatives/init_pp-sse.html
SwA Analysis and Test SOAR: Key Findings

• There is utility in grouping SwA tools and techniques into families
  – Aids DoD SwA community in understanding available tools or techniques to use for each identified software weakness
  – Enables comparison of potential suppliers within a family

• No “silver bullet” tool or technique exists
  – No single tool meets all weaknesses; multiple tool or technique types must be combined
  – In most cases, a tool or technique does not completely address a weakness (doesn’t find all vulnerabilities associated with a SW weakness)
  – There are a few cases for which no tool was found effective

• Some tools are costly, and use of any tool or technique incurs program cost
  – Select tools in general use require significant expertise to use in SW defect and vulnerability remediation
  – Licensing and training are additional cost-drivers

• Policy and guidance must evolve at pace with constantly changing threats
  – SwA is best integrated in engineering and test activities across the system and product development lifecycle
  – While SwA-related policy needs to be broad, guidance and implementation for SwA tools and techniques must be agile
SwA Analysis and Test SOAR: Representative Tool Matrix

Tool and technique selection methodology:
1. Select technical objectives based on context (e.g., criticality).
2. Select tool/technique families to address those technical objectives.
3. Select tools/techniques within family based on effectiveness, cost, etc.
4. Summarize selection and rationale in SwA part of PPP
5. Apply, assess, report, remediate, iterate

<table>
<thead>
<tr>
<th>Technical Objective</th>
<th>Tool/Technique Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Counter known...</td>
<td>✓</td>
</tr>
<tr>
<td>...</td>
<td>✓</td>
</tr>
<tr>
<td>Authentication &amp;</td>
<td>✓</td>
</tr>
<tr>
<td>Access Control</td>
<td>✓</td>
</tr>
</tbody>
</table>

Legend
- Completely addresses this objective. This indicator is, unfortunately, rarely used
- Can be highly cost-effective measure to address this objective; investigate further
- Can be cost-effective for partial coverage of this objective
- Not identified as being typically applied for this objective
Summary and Plans

• **Continue DoD SwA implementation actions**
  – Evolve policy and guidance; continue program engagement
  – Promulgate SwA Analysis and Test SOAR, update the framework over time
  – Continue coordination and development activities using the DoD SwA Community of Practice
  – Work toward implementation of federated SwA (and HwA) capability

• **Align Department software assurance activities as part of the Joint Federated Assurance Center (JFAC)**
For Additional Information

Thomas Hurt
Deputy Director, Software Assurance, DASD(SE)
571-372-6129 | thomas.d.hurt.civ@mail.mil
Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se