Benchmarking Software Assurance Implementation

Michele Moss
SSTC Conference
May 18, 2011
**Benchmarking Software Assurance Implementation**

**1. REPORT DATE**  
18 MAY 2011

**2. REPORT TYPE**

**3. DATES COVERED**  
00-00-2011 to 00-00-2011

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA, 22102

**13. SUPPLEMENTARY NOTES**

Presented at the 23rd Systems and Software Technology Conference (SSTC), 16-19 May 2011, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License

**16. SECURITY CLASSIFICATION OF:**

- a. REPORT: unclassified
- b. ABSTRACT: unclassified
- c. THIS PAGE: unclassified

**17. LIMITATION OF ABSTRACT**  
Same as Report (SAR)

**18. NUMBER OF PAGES**  
20

**19a. NAME OF RESPONSIBLE PERSON**

Approved for public release; distribution unlimited
100 Apps Written By 100 Developers At 100 Companies

What CIOs Get

- 83 apps have serious vulnerabilities
- 72 apps have cross site scripting
- 40 apps have SQL Injection
- 100 apps contain code of unknown origin
- 90 apps use un-patched libraries with known flaws
- 5 apps have had a scan or pentest
- 1 app has had a manual security code review
- 0 apps provide any visibility into security

Why

- 1 company has a responsible appsec program
- 1 developer has any security training

Adapted from: The Open Web Application Security Project, Jeff Williams, Aspect Security, SWA Forum Sept 2010
### Process Improvement Best Practices Are Key To Addressing Cyber Challenges

<table>
<thead>
<tr>
<th>Who</th>
<th>Why</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specialists (i.e. SwA SMEs)</td>
<td>Customer pressure</td>
</tr>
<tr>
<td>Practitioners (Developers)</td>
<td>Reaction to an incident</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What</th>
<th>Why Not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure progress</td>
<td>Software security is not an explicit requirement in development contracts or acquisition processes</td>
</tr>
<tr>
<td>Internal policy</td>
<td>Secure software training is not given to developers and architects</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>During product development process</td>
<td>Executive leadership commitment</td>
</tr>
<tr>
<td>During Leadership discussions</td>
<td>Translate ROI to project manager vocabulary (cost, schedule, quality)</td>
</tr>
<tr>
<td>As part of development and acquisition reviews</td>
<td>Start small and build</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Where</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Development Organizations</td>
<td>Use standards (i.e. coding standards)</td>
</tr>
<tr>
<td>IT Acquisition Organizations</td>
<td>Avoid creating a new language</td>
</tr>
<tr>
<td>IT Integrator Organizations</td>
<td>Leverage what is already known</td>
</tr>
<tr>
<td></td>
<td>Increase automation of menial tasks</td>
</tr>
</tbody>
</table>

Courtesy of September 2010 SwA Panel SwA Practices – Getting to Effectiveness in Implementation
SwA requires multi-disciplinary collaboration

Without a common language we cannot communicate across disciplines

Communication Challenges

- Vocabulary
- Reserved Words
- Priorities
- Perspective
- Experience
- Objectives
- Drivers
- Risks

Source: https://buildsecurityin.us-cert.gov/swa/progresrc.html
Until recently, SwA communication tools focused on developer-centric audiences
Different types of benchmarks exist – process and product

- The chicken…. (a.k.a. Process Focused Assessment)
  - Capability Maturity Models (CMMI, Assurance PRM, RMM, Assurance for CMMI)
  - Lifecycle Processes (ISO/IEEE 15288, ISO/IEEE 12207)
  - COBIT, ITIL, MS SDL, OSAMM, BSIMM

- The egg … (a.k.a Product Focused Assessments)
  - SCAP - NIST-SCAP
  - ISO/OMG W3C – KDM, BPMN, RIF, XMI, RDF
  - OWASP Top 10
  - SANS TOP 25
  - Secure Code Check Lists
  - Static Code Analysis
  - Pen Test Results
To effectively produce better code, SwA needs to translate to organizational and mission/business-focused stakeholders.


- Applicable in diverse contexts – e.g., Defense, National Security, Finance, Healthcare, Aviations, Telecommunications
- Become a source of market differentiator rather than a source of liability or misunderstanding in acquisition decisions
Executives want to understand the benefits to their organization

Executive Vocabulary
- Contributions to the bottom line
- Alignment with business strategy/plan
- Financial return for investing
- Payback Period
- Net Present Value
- Benefit/Cost Ration
- Return on Investment

Application Security Gaps
- Explicitly connect with business strategy and mission
- Address accomplishments
- Connect the dots at the enterprise level
- It is a long term management process that may take time to demonstrate measurable results
Resiliency Management Model provides a framework for presenting our problem in executive terms.

- **Define Business Goals**
  - Development
  - Organization

- **Sustained environment to achieve business goals through technology**
  - Enterprise Assurance Support

- **Enable Resilient Technology**
  - Development Project
  - Development Engineering

- **Prioritize funds and manage risks**
  - CFO

Adapted from: Source: November 2009 SwA Forum-Evolution in SwA Processes Panel – David White, SEI
Assurance PRM provides a “vertical slice” that addresses assurance from executive to developer.

Define Business Goals

Prioritize funds and manage risks

Development Organization
DO 1 Establish the assurance resources to achieve key business objectives
DO 2 Establish the environment to sustain the assurance program within the organization

Development Project
DP 1 Identify and manage risks due to vulnerabilities throughout the product and system lifecycle
DP 2 Establish and maintain assurance support from the project
DP 3 Protect project and organizational assets

Enterprise Assurance Support
ES 1 Establish and maintain organizational culture where assurance is an integral part of achieving the mission
ES 2 Establish and maintain the ability to support continued delivery of assurance capabilities
ES 3 Monitor and improve enterprise support to IT assets

Development Engineering
DE 1 Establish assurance requirements
DE 2 Create IT solutions with integrated business objectives and assurance
DE 3 Verify and Validate an implementation for assurance

Enable Resilient Technology

Sustained environment to achieve business goals through technology

Acquisition and Supplier Management
AM 1 Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities.

https://buildsecurityin.us-cert.gov/swa/proself_assm.html
Assurance PRM holistically connects executive-focused RMM and more detailed CMMI frameworks.

https://buildsecurityin.us-cert.gov/swa/proself_assm.html
The MS SDL Provides Ready To Use Resources For Application Security

https://buildsecurityin.us-cert.gov/swa/proself_assm.html

www.microsoft.com/sdl
Multiple tools exist for measuring the implementation of SwA practices

<table>
<thead>
<tr>
<th>Assessment Tool</th>
<th>Overview</th>
<th>Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability Maturity Model Integration (CMMI)</td>
<td>Defines the “What” for systems and software development, services, and acquisition</td>
<td>Development, services, acquisition, and associated organizational elements</td>
</tr>
<tr>
<td>Resiliency Management Model (RMM)</td>
<td>Defines the “What” for converging security, business continuity, and IT operations in support of operational risk management</td>
<td>Enterprise Operations</td>
</tr>
<tr>
<td>Assurance Process Reference Model (PRM)</td>
<td>Defines the “What”-level practices for addressing assurance in the context of software/system, development, operations, and enterprise</td>
<td>Development and associated organizational and enterprise elements</td>
</tr>
<tr>
<td>Assurance for CMMI</td>
<td>Defines the “What”-level practices for addressing assurance in the context of software/system, development,</td>
<td>Development/integration in the context of CMMI</td>
</tr>
<tr>
<td>Microsoft Secure Development Lifecycle (SDL)</td>
<td>Detailed example of “How” for implementation of engineering efforts</td>
<td>Development</td>
</tr>
<tr>
<td>Open Software Assurance Maturity Model (SAMM)</td>
<td>Example of “How” from the context of software assurance with many examples portable to security architecture</td>
<td>Development, operations, and enterprise</td>
</tr>
<tr>
<td>Build Security In Maturity Model (BSIMM)</td>
<td>Example of “How” from the context of real world examples primarily from large product vendors and financial services organizations</td>
<td>Development, operations, and enterprise</td>
</tr>
</tbody>
</table>
Software Assurance Maturity Models identify pre-defined paths for implementing SwA
Understanding investment *impact* across the organization requires analysis and interpretation of diverse measures.
To be effective, benchmarks should address all stakeholders and all relevant considerations

- Process and Organization
  - Process-based gap analysis or “SCAMPI-like” assessment
  - Capability maturity benchmarks
  - Expectations for repeatable results

- Specific Practices
  - Industry defined SwA program implementations
  - Specific implementation paths
  - Explicit milestones for tracking progress

- Resiliency Management Model (RMM)
- Assurance Process Reference Model (PRM)
- Assurance for CMMI
- Capability Maturity Model Integration (CMMI)

- Open Software Assurance Maturity Model (SAMM)
- Microsoft Secure Development Lifecycle (SDL) Optimization Model
- Build Security In Maturity Model (BSIMM)
We need to use a toolbox to be successful

- Very little of this is rocket science, however, it may be tedious and not exciting at times

- Both Process and Product assessments are valuable within specific contexts – we need to explicitly decide on our objectives to use them right

- There are LOTS of ways to communicate – no single way speaks to all audiences NOR it is effective by itself

- We are ALL trying to say the same things – we just use different words

- There is plenty of resources out there on how to develop better code

- There are also resources out there on how to demonstrate value

**Benchmarking is possible today by using the wealth of the available content and applying it to the problem!!!**
Back-up
The DHS SwA Processes and Practices Working Group has synthesized the contributions of leading government and industry experts into a set of high-level goals and supporting practices (an evolution of the SwA community’s Assurance Process Reference Model)

The goals and practices are mapped to specific industry resources providing additional detail and real world implementation and supporting practices

- Assurance Focus for CMMI
- Building Security In Maturity Model
- Open Software Assurance Maturity Model
- CERT® Resilience Management Model
- CMMI for Acquisition
- CMMI for Development
- CMMI for Services
- SwA Community’s Assurance Process Reference Model – Initial Mappings
- SwA Community’s Assurance Process Reference Model - Self Assessment
- SwA Community’s Assurance Process Reference Model – Mapping to Assurance Models

Other valuable resources that are in the process of being mapped include

- NDIA System Assurance Guidebook
- Microsoft Security Development Lifecycle
- SAFECODE