DoD Software Assurance Initiative

Mitchell Komaroff, OASD (NII)/DCIO
Kristen Baldwin, OUSD(AT&L)/DS

Agenda

- Background
- Software Assurance Definition
- Guiding Principles for SwA
- DoD SwA Strategy Elements
  - Engineering in Depth
  - Science and Technology
  - Industry Outreach
- Conference Expectations

Background

- In October 2002, the President's Critical Infrastructure Protection Board (PCIPB) created the National Security Agency (NSA) -led IT Security Study Group (ITSSG) to review existing IT acquisition processes.
- In July 2003, the Assistant Secretary of Defense for Networks and Information Integration [ASD(NII)] established the Software Assurance Initiative to examine software assurance issues
- On 23 Dec 04, Undersecretary of Defense for Acquisitions, Technology and Logistics [USD(AT&L)] and ASD(NII) established a Software Assurance (SwA) Tiger Team to:
  - Develop a holistic strategy to reduce SwA risks within 90 days
  - Provide a comprehensive briefing of findings, strategy and plan
- Tiger Team presented its strategy to USD(AT&L) and ASD(NII) on March 28, and on May 2 was tasked to proceed with 180 day Implementation Phase

Related Studies

- Multiple avenues of concern regarding potential IT/Software Assurance uncertainties
  - In May 2004, GAO reviewed how DoD mitigates risks from foreign suppliers of software, recommending that DoD make changes to its acquisition processes to better manage this risk http://www.gao.gov/new.items/d04678.pdf
  - In November 2004, GAO began study of Software Development Off-shoring to address risks of off-shoring to critical infrastructure, and steps being taking by federal government
  - Jan 2005 President's Information Technology Advisory Committee Subcommittee on Cyber Security Update

Software Assurance

- ***Scope***: Software is fundamental to the GIG and critical to all weapons, business and support systems
- ***Threat agents***: Nation-state, terrorist, criminal, rogue developer who:
  - Gain control of IT/NSS through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities***: All IT/NSS (incl. systems, networks, applications)
  - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Consequences***: The enemy may steal or alter mission critical data; corrupt or deny the function of mission critical platforms

Software assurance (SwA) relates to 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.

Guiding Principles for SwA

- Understand problem from a systems perspective
- Response should be commensurate with risk
- Sensitive to potential negative impacts
  - Degradation of our ability to use commercial software
  - Decreased responsiveness/ increased time to deploy technology
  - Loss of industry incentive to do business with the Department
  - Minimize burden on acquisition programs
- Exploit and extend relationships with:
  - National, international, and industry partners
  - DoD initiatives, e.g., trusted integrated circuits and Information Assurance

Strategy Elements

- Partner with Industry to focus science and technology on research and development of technologies
  - Improve assured software development tools and techniques
  - Strengthen standards for software partitioning and modularity
  - Enhance vulnerability discovery
- Employ repeatable Systems Engineering (SE) and test processes to identify, assess, and isolate critical components, and mitigate software vulnerabilities
- Leverage and coordinate with industry, academia and national and international partners to address shared elements of the problem

Engineering-in-Depth
Status/Critical Enablers

Status:

- Developed strategy to implement SwA into the engineering process:
  - Requirements, sensitivity analysis, scenarios, T&E, M&S, risk management, configuration management, technical reviews, red teams, standards, education & training
  - Document SwA planning in Systems Engineering Plans (SEP) and Test and Evaluation Master Plans (TEMP)
- Initiated standards work with Industry
- Working with Service, Industry SE community to define process impacts

Critical Enablers:

- Develop SwA “handbook” to provide detailed guidance on implementing SwA into the engineering process
- Develop industry standards and metrics
- Insert enhancements into DoD acquisition policies and guidance

Science & Technology
Status/Critical Enablers

Status:

- Drafted DoD Directive for an Executive Agent for Software Vulnerability Mitigation and Discovery
- Developed concept for Center for Assured Software
  - Identified key partners across the Government and Industry

Critical Enablers:

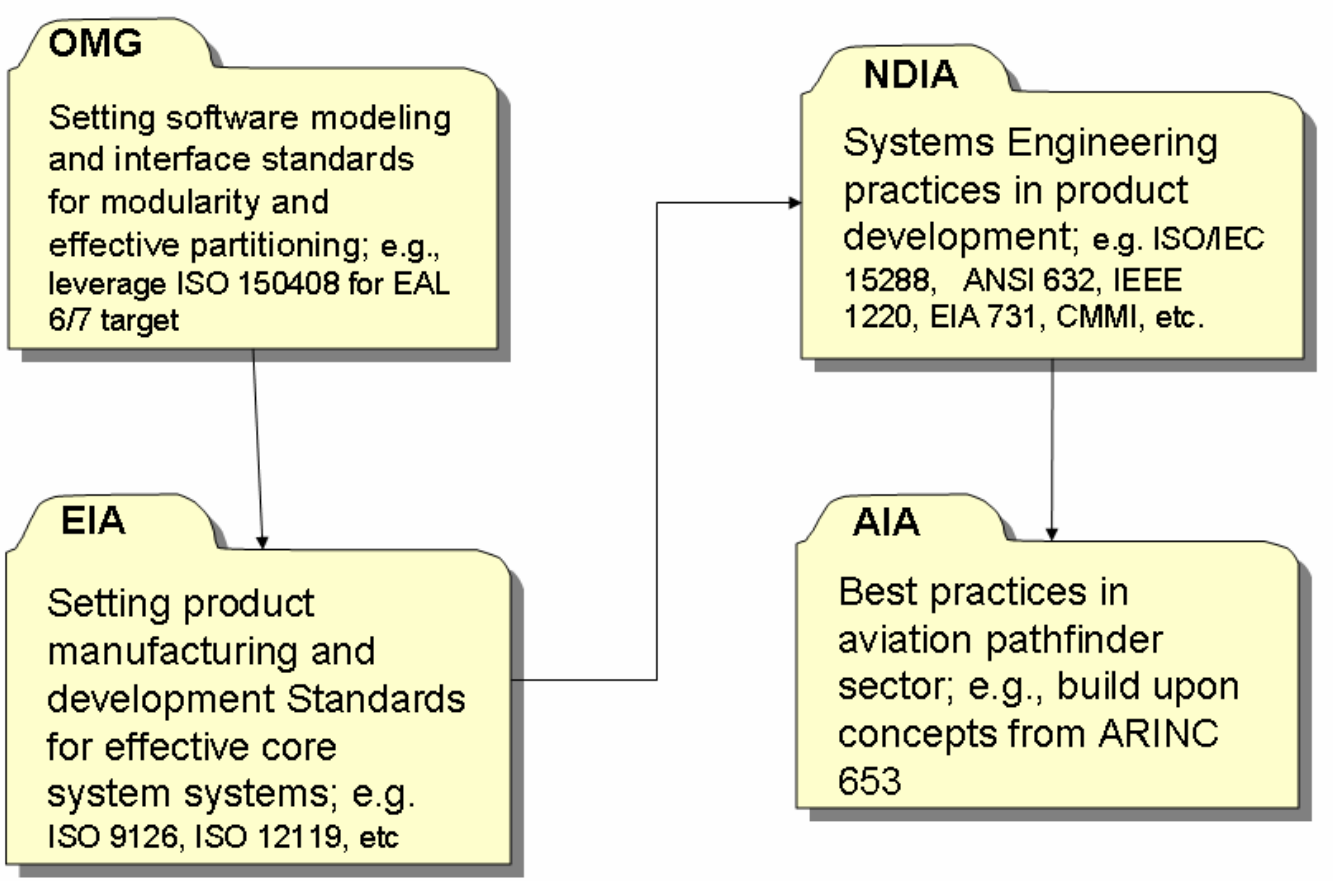
- Resources for the Center for Assured Software
- Promulgate DoD Directive, and Executive Agent (NSA)
- Technology to advance vulnerability detection and mitigation

Industry Outreach

Goal: Partner with industry to create a competitive market that is building demonstrably vulnerability-free software

- USD(AT&L)/ASD(NII) memo to Industry
  - Requested participation in an Executive Roundtable
- Tiger Team held initial meetings with directors:
  - National Defense Industrial Association (NDIA)
  - Government Electronics & Information Technology Association (GEIA)
  - Aerospace Industries Association (AIA)
  - Object Management Group (OMG)
- Identified areas of interest for SwA white papers
  - OMG will leverage ongoing standards activities
  - NDIA hosting SwA Summit; will consider SE, C4ISR, IT implications
  - GEIA will share lessons and collaborate to develop new processes
  - AIA will help integrate SwA processes into mainstream integration activities

Industry Leadership Interactions



Build the standards…

Build the boxes to the standards…

Engineer the boxes into systems…

Integrate the systems into platforms…

SwA Executive Round Table

- **Goals:**
  - Industry leadership gains understanding of DoD perspectives/desires
  - DoD gains understanding of industry issues, approaches, & enablers
  - Identify ways to work together to achieve improved SwA
    - Short-term: Study products, white papers, workshops
    - Longer-term: Research, tools & standards development, certification processes
- **Participants**:
  - Industry Associations
  - DoD Stakeholders, Guest federal agencies (DHS)
- **Agenda topics:**
  - DoD Open Dialogue on its issues/needs
  - Industry presentations on perspectives/best practices
  - Discussion of collaborative opportunities and way ahead

Conference Expectations

Determine how the DoD and Industry can work together to achieve assured systems

- Elicit industry insights and ongoing assurance efforts
  - How has industry defined the problem
  - What are industry strategies, best practices
  - What lessons have been learned
- Engage industry in the DoD strategy elements
  - Vet each element (e.g. barriers, issues, experiences)
  - Flesh out the detailed strategy plans and products
  - Identify industry enablers (e.g. IR&D, methodologies, processes)
- Identify recommended actions for continued collaboration