DoD Software Assurance Initiative

Mitchell Komaroff, OASD (NII)/DCIO

Agenda

- Background
- Software Assurance Definition and Strategy
- Guiding Principles for SwA
- DoD SwA Strategy Elements
- Industry Outreach
- NDIA System Assurance Initiative
- Commercial Industry Strategic Goals

Background

- In July 2003, the Assistant Secretary of Defense for Networks and Information Integration [ASD(NII)] established a 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
- On 28 Mar 05, Tiger Team presented its strategy to USD(AT&L) and ASD(NII) and was subsequently tasked to proceed with 180 day Implementation Phase

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

DoD SwA 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

Industry Outreach

- 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 leveraging ongoing standards activities of ADM to apply meta-model concept to assurance problem
  - NDIA hosted SwA Summit and Standing up SwA Committee
  - GEIA will share lessons and collaborate to develop new processes
  - AIA will help integrate SwA processes into mainstream integration activities
- DoD/Industry Executive Roundtable held in December 2005
  - Planned Industry-DoD initiatives encouraged

NDIA System Assurance Committee Goals

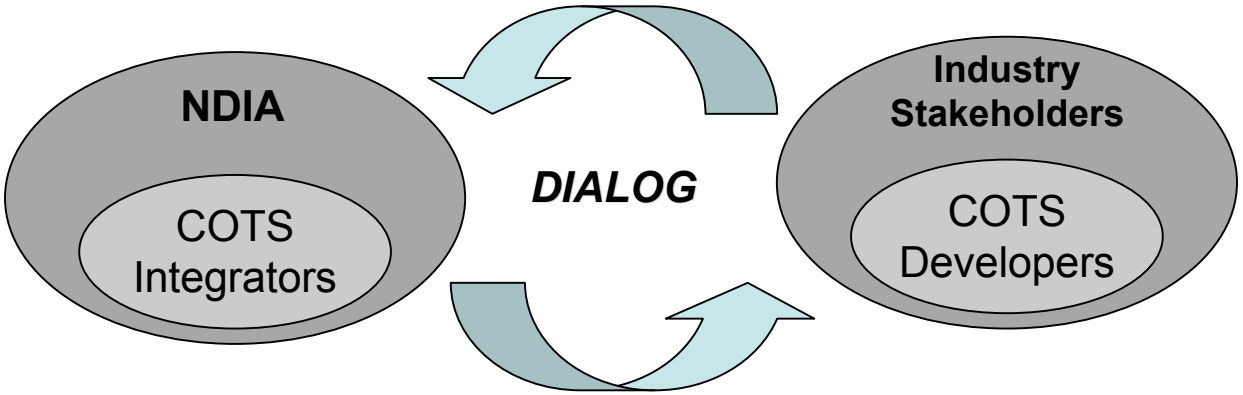
- Create a uniform perspective on system assurance problems and solutions
  - Start bridging the gap between:
    - the weapons systems and the enabling technologies communities
    - traditional DoD industrial base and commercial industry
    - DoD and critical infrastructure (e.g. telecom, finance, energy, medical)
- Goal – Extended community to engage in system assurance strategy

NDIA System Assurance Committee Charter

- Extend community to engage in system assurance strategy
- Vet and comment on recommendations coming out of DoD strategy
- Develop a System Assurance Handbook
- Leverage standards activities
- Chairs
  - Paul Croll, NDIA SED
  - Kristen Baldwin, OUSD AT&L
  - Mitchell Komaroff, OASD NII

Commercial Industry: Strategic Goals

- Create Commercial Industry Center of Mass to sort out assurance issues
  - Dialog with NDIA System Assurance Committee
  - Include broad commercial participation
- Develop Industry End-to-end reference models (RM), standards, requirements
  - Product level assurance properties ◊ Systems of Known Assurance
  - Express RM/Standards/Requirements in modeling language
- Identify methods for validating compliance with requirements/ standards, using industry-developed tools



- Commercial Developers develop products within reference model
  - Understood assurance properties meeting Business Model
  - Become stakeholders in models: *tools become key to standards compliance*
- Systems Integrators compose systems with system-level assurance properties based upon technically demonstrable product-level properties.

Questions?