A Strategy for Improved System Assurance

June 20, 2007

Kristen Baldwin
Deputy Director,
Software Engineering and System Assurance
Office of the Under Secretary of Defense
Acquisition, Technology and Logistics
• We continue to be concerned with assurance of our critical DoD assets:
  • Critical information
  • Critical technologies
  • Critical systems
• Observations:
  – Increasing numbers of network attacks (internal and external to DoD)
  – Broader attack space
• Trends that exacerbate our concerns:
  – Globalization of our contracts, expanding the number of international participants in our system developments
  – Complex contracting arrangements that further decrease transparency below prime, and visibility into individual components

These trends increase the opportunity for access to our critical assets, and for tampering
Top Software Issues*

1. The impact of requirements upon software is not consistently quantified and managed in development or sustainment.

2. Fundamental system engineering decisions are made without full participation of software engineering.

3. Software life-cycle planning and management by acquirers and suppliers is ineffective.

4. The quantity and quality of software engineering expertise is insufficient to meet the demands of government and the defense industry.

5. Traditional software verification techniques are costly and ineffective for dealing with the scale and complexity of modern systems.

6. There is a failure to assure correct, predictable, safe, secure execution of complex software in distributed environments.

7. Inadequate attention is given to total lifecycle issues for COTS/NDI impacts on lifecycle cost and risk.

*NDIA Top Software Issues Workshop August 2006
System Assurance – Working Definition

*Level of confidence* that a system functions as intended, is free of exploitable vulnerabilities, and protects critical program information.
Consequences of Fragmented Systems Assurance Initiatives

• Lack of Coherent Direction for PMs, and others acquiring systems
  – Numerous, uncoordinated initiatives
  – Multiple constraints for PMs, sometimes conflicting
  – Loss of time and money and lack of focus on applying the most appropriate engineering for systems assurance for each system

• Synergy of Policy – Multiple ownership
  – Failure to capitalize on common methods, instruction among initiatives

• DoD Risk Exposure
  – Lack of total life cycle view
  – Lack of a focal point to endorse system assurance, resolve issues, advocate PM attention
  – Lack of system-of-systems, architecture perspective on system assurance
  – Potential for gaps in systems assurance protection
Path Forward

- Create a ‘framework’ to integrate multiple security disciplines and policies
  - Leverage 5200.39: expand CPI definition to include system assurance and total life cycle
- Use the Program Protection Plan (PPP) to identify CPI and address assurance for the program
  - Link plans (e.g., Anti-Tamper, Software Protection, System Engineering, Assurance Case)
- Modify Acquisition and System Engineering guidance to integrate system assurance across the lifecycle
  - Milestone Decision Authority visibility
  - Guidebook on Engineering for Assurance for program managers/engineers

<table>
<thead>
<tr>
<th>Raise the bar:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
</tr>
<tr>
<td>- Knowledge of the supply chain</td>
</tr>
<tr>
<td>- Who has access to our critical assets</td>
</tr>
<tr>
<td>Protection</td>
</tr>
<tr>
<td>- Protect critical assets through security practices</td>
</tr>
<tr>
<td>- Engineer our systems for assurance</td>
</tr>
</tbody>
</table>
Policy Roadmap for System Assurance
Current Systems Security Policies

Component Protection Sought

Defense-In-Depth

Intelligence

Supply Chain

Engineering

Certification

Documented Plan

Critical Functionality
- Non-Security
- Security

Critical Information
- Classified
- Un-Classified

Critical Technology
- Software
- Hardware/Firmware

Policy Ownership
- DoD - CIO/DSS
- DoD - CIO/DISA
- CC/NSA
- DoD - AT&L
- DoD – AT&L/S&T
- DoD - USD(I)
- NIST

5200.39
Proposed Framework for Security Policies

Defense-In-Depth

Intelligence

Supply Chain

Engineering

Certification

Documented Plan

Component Protection Sought

Critical Functionality

Critical Information

Critical Technology

Non-Security

Security

Classified

Un-Classified

Software

Hardware/Firmware

5000.1/2/Systems Engineering

Proposed Framework with 5200.39

TF

FIPS

CC/NIAP

ISP

NISP

IA

CC/NIAP

FIPS

DIA Cap

OPSEC

DIA Cap

SPI

Anti-Tamper

Policy Ownership

DoD - CIO/DSS

DoD - CIO/DISA

CC/NSA

DoD - AT&L

DoD - AT&L/S&T

DoD - USD(I)

NIST
New Definition - Draft DoDI 5200.39:

- **E3.6.** Critical Program Information (CPI). Elements or components of an RDA program that if compromised, could cause significant degradation in mission effectiveness, shorten the expected combat-effective life of the system, reduce technological overmatch, significantly alter program direction, or enable an adversary to counter, copy, or reverse engineer the technology or capability.

- **E3.6.1. Technologies** become eligible for CPI selection when a DoD Agency or military component invests resources to demonstrate an application for the technology in an operational setting, or in support of a transition agreement with a Program Manager.

- **E3.6.2.** Includes **information** about applications, capabilities, processes, and end-items.

- **E3.6.3.** Includes **elements or components** critical to a military system or network mission effectiveness.
**Notional Assurance Implementation**

<table>
<thead>
<tr>
<th><strong>Notional Assurance Implementation</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Phase</strong></th>
<th><strong>Activities</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Concept Refinement</td>
</tr>
<tr>
<td>B</td>
<td>Technology Development</td>
</tr>
<tr>
<td>C</td>
<td>System Development &amp; Demonstration</td>
</tr>
<tr>
<td>IOC</td>
<td>Production &amp; Deployment</td>
</tr>
<tr>
<td>FOC</td>
<td>Operations &amp; Support</td>
</tr>
</tbody>
</table>

### Phase A - Concept Refinement
- Concept Decision
- Identify CPI in PPP
- Identify threats
- Develop Plans (AT, SEP, TES)

### Phase B - Technology Development
- (Program Initiation)

### Phase C - System Development & Demonstration
- CDR
- Approved SEP with details on Assurance
- Milestone Decision approves plans, sets SDD criteria
- Identified Threats
- Technology Readiness Assessment
- Technology Readiness Assessment
- Sensitivity Analysis
- CPI enter Horizontal Protection Database

### Phase IOC - Production & Deployment
- LRIP/IOT&E
- Source selection consideration of supplier FOCI and security practices
- Final AT Plan
- Technology Readiness Assessment
- Sensitivity Analysis
- CPI enter Horizontal Protection Database

### Phase FOC - Operations & Support
- Maintenance providers meet security practice
- Upgraded HW/SW configuration managed, validated and verified
- Final AT Plan
- Designs meet assurance plans
- Initial verification and validation of critical components

### Total Lifecycle Approach to Assured Systems
Guidebook on Engineering for System Assurance
• **Intent:**
  – Provide *practical guidance* on augmenting systems engineering practice for system assurance
  – Synthesize existing knowledge from organizations, standards and best practices
  – Recap concepts from standards

• **Implementation:**
  – Iterative releases with updates as new knowledge is gained and applied
  – Multiple Views for information dissemination
    • Technical Project Manager
    • System Engineer
    • Subject Matter Expert Detail
• Augments SE from documentation through engineering processes and technical reviews
  – Introduced as early as possible - Where there is the greatest impact
  – Continue through the life cycle
• Consistent with international standard and current best practices
  – E.g., Guidebook approach, presentation of process / procedure consistent with ISO/IEC 15288 standard for System Engineering
  – Integrates consideration and leverages numerous existing program protection or security disciplines (e.g., IA, AT, SwA, SPI, PPP)
  – Existing information security / assurance material is summarized, and leveraged by reference, not repeated
    • Test & Evaluation; Center for Assured Software (CAS)
    • Enhanced vulnerability detection techniques
    • SwA Body of Knowledge
• Intent is to yield assured program / system with demonstrable evidence of assurance
Guidebook Strategy

- Standards
- Instructions
- Directives
- Best Practice
- NIST, NSA Guidance
- Etc.

Systems Assurance Guidebook

- Systems Engineering View
- ISSE/IA View
- Program Management View
- Others as needed…

Future: Link to Acquisition Guidance, Evolve/Implement into training, education
SA Guidebook

Why this is hard...
Contributors

- NDIA
- INCOSE
- MITRE
- IDA
- SEI
- OSD, Joint Staff, Services
- Contractor community
- Academe
Milestones & Plan

• **Complete the Guidebook**
  – Increment versions through Summer, 2007
  – Focus: “Get the content right”…worry format and organization later

• **Stakeholder Review**
  – From the larger community, different perspectives

• **Pilots**
  – Systems Assurance innovators and areas where comprehensive expertise in one or more relevant domains exists
  – Starting Summer, 2007

• **Write SE, PM, ISSE/IA Views**
  – Focus: Derived from the Guidebook, “get the right content” (by audience)

• **Release version 0.9 by 30 September**

*Contact us to participate in stakeholder review*
Community Site

http://www.ndia.org/Content/ContentGroups/Divisions1/Systems_Engineering/Systems_Assurance_Committee.htm

http://tinyurl.com/222hvq
System Assurance: What does success look like?

- The requirement for assurance is allocated among the right systems and their critical components
- DoD understands its supply chain risks
- DoD systems are designed and sustained at a known level of assurance
- Commercial sector shares ownership and builds assured products
- Technology investment transforms the ability to detect and mitigate system vulnerabilities
Backups
Fragmented Systems Security Policies

Each policy:
- Affects different parts of the life cycle
  - R&D, acquisition, foreign ownership
- Applies to a different subset of DoD systems
  - NSS, IT, MDA, ACAT 1C, etc.
- Assures different ‘type’ of components
  - information, leading technology, functionality
- Mandates a different set of defense tactics
  - intelligence, engineering, documented plan, certification & accreditation

- CC – Common Criteria
- DIACAP – DoD Certification & Accreditation
- FIPS – Federal Information Processing Standards
- ITAR – International Traffic in Arms Regulation
- IA – Information Assurance
- ISP – Information Security Program
- NIAP - National Information Assurance Partnership
- NISP – National Industrial Security Program
- OPSEC – Operational Security
- 5200.39 – DODD 5200.39 Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection
- SA – System Assurance
- SPI – Software Protection Initiative
- TF - Trusted Foundry

Current approach does not have systems-of-systems perspective