Overview of Engineering in Depth Processes for Software Assurance

NDIA Summit on Software Assurance
September 7-8, 2005
Arlington, VA

Ken Hong Fong
Chuck Johnson
OUSD(AT&L), Defense Systems
Systems Engineering/Enterprise Development
ekenneth.hongfong@osd.mil; (703) 695-0472
chuck.johnson.ctr@osd.mil; (703) 602-0851 X123

Mitch Komaroff
OASD(NII) Commercial Policy & Oversight
mitchell.komaroff@osd.mil
703-602-0980 x146

Wednesday, September 7th
0800 - 1700

- Opening remarks - NDIA
- DoD Software Assurance Efforts – OSD Tiger Team
- DHS Software Assurance Efforts – DHS Dir, Software Assurance
- **Overview: Engineering-in-Depth – OSD DS/Systems Engineering**
- Overview: Science and Technology
- **Afternoon: Structured Breakout Sessions**
  - Science and Technology for SwA
  - Industry Best Practices for SwA

Thursday, September 8, 0800-1500

- Industry Perspective – TBD
- Report out from Wednesday Breakout
- Structured Breakout Sessions
  - Engineering processes for SwA
  - Standards, metrics, models for SwA
- **Afternoon: Breakout Sessions Report Out**
- General Discussion and Way Ahead

Software Assurance (SwA) Definition

Software assurance (SwA) is the level of confidence that software is free of exploitable vulnerabilities, either intentionally or unintentionally designed as part of the software or inadvertently created.

SwA Systems Goals and Objectives

- Free of exploitable vulnerabilities
- Function reliably as intended
- Free of malicious functionality
- Cannot be used as conduits for attack
- Secure from IA exploitation
- Leverage commercial technologies for cost, schedule, performance
- Logistically supportable, economically maintainable and technically up-gradable
- Efficiently hardened against malicious intent
- Can operate in increasingly hostile environments

Notional Workshop Goals

- Engineering In Depth Strategy Review
  - EID Model
    - How do we make it more effective?
  - Who we’ve engaged and results to date
    - OMG Problem Statement
  - Desires and Expectations for NDIA engagement
    - Whitepapers
    - Who would provide them?
    - By when?
    - What are the mechanisms for continued engagement?
- Standards, Metrics & Models
  - Concepts for review
  - Formulation of way-ahead

EID Core Members

- OSD
  - Ken Hong Fong, OUSD(AT&L) DS/SE AS
  - Chuck Johnson, CTR, OUSD(AT&L) DS/SE AS (Decisive Analytics)
  - David Wheeler, CTR, OASD(NII) (IDA)
- Department of the Army
  - Jim Linnehan, ASA(ALT)
- Department of the Navy
  - Brenda Zetterval, ASN(RDA) CHENG
  - Jim Dietz, CTR, ASN(RDA) Cheng (MITRE)
- Department of the Air Force
  - Ernesto Gonzalez, SAF AQR
- NSA
  - Janet Oren
  - Steve Lafontain
- MDA
  - Abe Bushra
  - Michael Smith
  - Margaret Powell

Engineering in Depth

- Top level definition:
  - An analytical approach of focusing SE to the issues of SwA
  - Like defense-in-depth seeks to implement multiple layers of strength, by building SwA into the product instead of adding it on
- Top level approach:
  - Work with industry to define SE enhancements
- Derive reasonable and cost effective enhancements
  - Insert agreed enhancements into DoD acquisition policies & guidance

SE Processes (Defense Acquisition Guidebook)

Technical Mgt Processes	Technical Processes
Decision Analysis 5 3	Requirements Development 1
Technical Planning	Logical Analysis
Technical Assessment 8	Design Solution 2
Requirements Mgt	Implementation
Risk Mgt 7	Integration
Configuration Mgt 9	Verification 4
Technical Data Mgt	Validation 6
Interface Mgt	Transition
	(Overarching:) 10 11 12

What Key SE processes can we enhance to achieve the best effects?

# = potential EID SE process intersects

Engineering-in-Depth Mechanisms Defined

1. **Develop a common core set of tailorable SwA requirements & metrics**
2. **Develop an approach for performing operational SwA sensitivity analysis**
3. **Develop an approach for identifying SwA driven scenarios for use in Analyses of Alternatives (AOA) and hazard analyses**
4. **Develop candidate SwA test metrics for inputs to Test and Evaluation Master Plan (TEMP) SwA Annexes, to include applicable:**
5. **Define an approach for SwA applicable Modeling and Simulation (M&S)**
6. **Define a mechanism for selective technical "red-team" reviews of key software**
7. **Develop a common core set of SwA threats and vulnerabilities with probability and consequence metrics**
8. **Develop top-level Software and SwA Entry/Exit Criteria for SE Technical review(s)**
9. **Develop an enhanced SwA informed CM process to ensure full life cycle protection**
10. **Examine strategies for providing enhanced DoD SwA Standards leadership and management**
11. **Develop and implement education, training and certification avenues for acquisition participants**
12. **Define a continuous process improvement approach based upon evolving threat assessments through an engineering community sensitized to SwA**

Workshop Task: NDIA Problem Statement

- This workshop
  - Leverage NDIA strengths
  - Provide “Industry” input for how best to achieve EID elements
  - Honest look at 12 proposed EID elements to discuss whether to:
    - Add
    - Subtract
    - Amend
    - Replace
  - Call for white-papers in topics of interest
    - Government purpose rights required

Standards Metrics & Models for SwA Discussion

The SwA knowledge environment

- Standards – many IA/IT security focused standards but none directly focused on all of SwA
  - SwA per se, is new ground
- Guidance – much IA/IT assurance related guidance
  - FIPS pubs, IATF, Academic and industry literature
- Processes – many processes in DoD that support key SwA elements, but none directly address all of SwA
  - DITSCAP for system security C&A
  - NIAP/Common Criteria evaluation to search for unintentional vulnerabilities in COTS components
  - DoD IA to address IS security controls to protect and defend information confidentiality, integrity, availability, authentication and non-repudiation

SwA Way Ahead Ground Rules

- Should not duplicate or contradict, but leverage other policies, processes, practices, tools and metrics:
    - Supporting Standards
    - NIAP/ISO 15408 (Common Criteria);
    - DITSCAP C&A process;
    - DoD Information Assurance (IA);
    - CMM/CMMI/SSE-CMM;
    - Information System Security Engineering (ISSE); and
    - Information Assurance Technical Framework (IATF)
    - Trusted Software Development Methodology (TSDM)
    - Others…
- Barriers:
    - No agreement on what constitutes SwA
    - Other processes on fringe

Much past work around idea of Software Assurance, but what do we really know?