Discussion of Standards, Metrics and Models for SwA
Breakout report Out

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) ODCIO
mitchell.komaroff@osd.mil
703-602-0980 x146

Participants

Name	Affiliation	email	Phone
Alvarez, Raquel	BAH (CTR-DIA)	raquel.alvarez@dia.mil	202.231.8899
Doohan, Brad	DCMA HQ	bradley.doohan@dcma.mil	
Goertzel, Karen	BAH	goertzel_karen@bah.com	
Liu, June	SAIC	liujh@saic.com	
Markeloff, Rich	Sparta	rmarkeloff@sparta.com	
Miller, Kent	Anti-Tamper	kent.miller@pentagon.af.mil	703.588.1467
Keeler, Kristi	SEI	kkeeler@sei.cmu.edu	
Morgan, Kevin	NGC	kevin.b.morgan@ngc.com	
Steffey, Raymond	NGC	ray.steffey@ngc.com	
Komaroff, Mitchell	OASD(NII)	mitchell.komaroff@osd.mil	
Frisina, Joseph	BAE Systems	joseph.frisina@baesystems.com	
Bourquin, Rene	GDC4S	rene.bourquin@gdc4s.com	
Redwine, Sam	JMU	redwinst@jmu.edu	
Jarzombek, Joe	DHS NCSD	joe.jarzombek@dhs.gov	
Rose, Dan	SAIC	rosedj@saic.com	
Johnson, Chuck	OUSD(AT&L) DS/SE AS	chuck.johnson.ctr@osd.mil	
Hong Fong, Ken	OUSD(AT&L) DS/SE ED	ekenneth.hongfong@osd.mil	703.602.0851 X123

Industry insights and ongoing assurance efforts

- How has industry defined the problem?
  - Application security
  - Network security
  - Defense-in-depth
  - Specific industry techniques, e.g., Securities Industry (stock markets)
  - Software Quality Assurance
  - Voluntary use of best practices
  - Gradual improvement
  - Fix vulnerabilities as discovered/uncovered
    - Effectiveness of patch management
    - Seek and destroy vulnerabilities
  - Unless contract has a contract specification for security, will not address (lacking ROI)
  - Quality Metric: “world class” considered 1 defect /1KLOC; therefore, defect count ≈ code size
  - Industry averse to construct of levels of goodness
    - Common Criteria-like construct leaves bad taste
    - Does not like to be judged on qualitative basis
    - Assurance measures vary in time and product

Bottom Line: No consensus on definition or magnitude of problem and inadequate incentives

Industry insights and ongoing assurance efforts

- What are Industry strategies and best practices?
  - CLASP Methodology – Secure Software Co.
  - MS Security Development Lifecycle (SDL)
  - UML Sec
  - TSP Secure
  - Smart Card
  - Model Driven Architecture (MDA)
  - Aspect Oriented Software Development (AOSD)
  - CMMI
  - Product Evlauation
  - Peer review
  - Threat Modeling
  - Source Code Scanning
  - Automated Security Testing (Commercial & Open Source Tools)
    - Penetration testing
    - Fuzz testing
  - ISO/IEC 15026 re-write
    - Plan assurance activities
    - Establish and maintain assurance arguments
    - Monitor and measure performance at system level

Bottom Line: Many techniques and tools & common practices, but no consensus on one set of best practices on this topic

Industry insights and ongoing assurance efforts

- ❑ What are lessons learned?
  - » Market driven by customers
  - » Customers don’t always agree
  - » Customer may not understand up front all of the security implications
  - » Out-side in vice inside out solutions
  - » Inappropriate to apply/rely on a network security model to software
  - » Can get better

Bottom Line: Organizational change is hard. When we can get behavior changed product improvement results

Industry Thoughts Regarding DoD Strategy Elements

- ❑ Vet each strategy element, e.g., identify barriers
- ❑ Flesh out the detailed strategy plans and products
- ❑ Identify Industry Enablers, e.g., IR&D, Methodologies, Processes

Recommended actions for continued collaboration

- ❑ Deserves more time and effort
- ❑ Need an acquisition model to incentives needed behavior
- ❑ Need to identify a named group that meets regularly (frequently) to engage. Already have two that may be relevsant
  - » DoD/DHS WG“Practices and Processes” DoD/DHS WG
  - » DoD/DHS WG “Product Evaluation Tools and Technology” Need