



SwA Practices - Getting to Effectiveness in Implementation

Facilitator: Michele Moss, Booz Allen Hamilton
Co-Chair Processes and Practices Working Group

September 29, 2010



Homeland
Security



- Why do developers reuse untested code without determining if it is “fit-for-purpose”?
- Why is software continuously exploited?
- Why are there Top 10/25 CWEs found in newly developed code?
- Why?
- Why?
- Why?

... We Must Understand How To Communicate With Them



- **Dan Reddy, EMC:**
 - 5+ year journey at EMC
 - Dan Reddy is a Consulting Product Manager in the Product Security Office at EMC, a group that is charged with the continued driving of security improvements into EMC products. His primary focus is to work with EMC engineering groups to follow best practices to assure the integrity of EMC products as they are developed within the software supply chain.
- **Keith Turpin, Boeing:**
 - Boeing's secure coding practices and checklist
 - Keith leads the Boeing Company's enterprise application security assessment team, serves as a U.S. delegate to the International Standards Organization's sub committee on cyber security, and is the project leader for the OWASP Secure Coding Practices Quick Reference Guide.
- **John Steven, Cigital:**
 - Research results on scaling static analysis and making the overall process more effective
 - John Steven is a Senior Director at Cigital. His experience includes research in static code analysis and hands-on architecture and implementation of high-performance, scalable Java EE systems.
- **Steve Lavenhar, Booz Allen:**
 - Lessons learned in reaching developers and gaining leadership support
 - Steven Lavenhar is a Lead Associate with Booz Allen Hamilton. He manages a software assurance group which performs secure code reviews, architectural risks assessments, threat analysis and application penetration tests. He has over 30 years of software consulting experience in the commercial, civilian federal and defense sectors.