Panel Discussion - Understanding Technology Stakeholders: Their Progress and Challenges

Facilitator: Michael Kass, NIST

- Co-Chair DHS SwA Technology/Tools and Product Evaluation Working Group

Mini-Keynote: John Gilligan, The Gilligan Group

Software Assurance Forum

4 November, 2009

- Technology, Tools and Product Evaluation (TTPE) Working Group Goal:
  - To assist in bringing software assurance tools and technologies into the government's effort to improve the speed and accuracy of software assurance evaluation and certification of COTS, GOTS and open source software.

Some TTPE Objectives

- Specify dictionaries for low-level descriptions of software weakness (CWE), attack patterns and terminology (CAPEC)
- Measure the assurance tool functionality and capability of SwA tools through SAMATE (SATE)
- Support development of OMG Software Assurance Ecosystem Specifications
- The Software Assurance Findings Expression Schema (SAFES)
- Software Assurance Landscape Document

- Help answer questions
  - Where are we in software assurance?
  - Where are we going?
  - What challenges do we face?
  - What suggestions do we have for the SwA Forum?

- Mini-Keynote: John Gilligan, The Gilligan Group
- Panelists:
  - Bruce Weimer, U.S. Army CECOM LCMC, Software Engineering Ctr
  - Djenana Campara, KDM Analytics
  - Todd Landry, Klocwork
  - Sean Barnum, Cigital Federal

Understanding Technology Stakeholders: Their Progress and Challenges

John M. Gilligan

Software Assurance Forum

November 4, 2009

- Historical Perspectives
- Cyber Security Threats--A National Crisis
- Cyber Security Commission Recommendations
- Near Term Opportunities
- Longer-Term Game Changing Initiatives
- Closing Thoughts

- Internet, software industry, (personal) computers—rooted in creativity not engineering
- Security in the Cold War Era
  - Security “Gurus”—Keepers of the Kingdom
- The World Wide Web changes the security landscape-- forever
- Post Cold War: The Age of Information Sharing

Legacy of the past is now our “Achilles Heel”

- Our way of life depends on a reliable cyberspace
- Intellectual property is being downloaded at an alarming rate
- Cyberspace is now a warfare domain
- Attacks increasing at an exponential rate
- Fundamental network and system vulnerabilities cannot be fixed quickly
- Entire industries exist to "Band Aid" over engineering and operational

Cyber Security is a National Security Crisis!

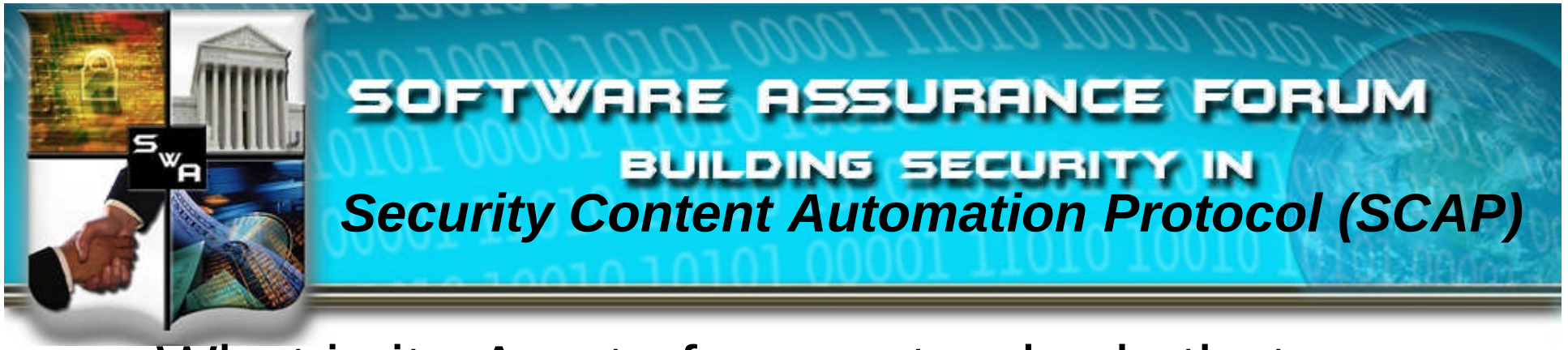
- Create a comprehensive national security strategy for cyberspace
- Lead from the White House
- Reinvent public-private partnerships
- Regulate cyberspace
- Modernize authorities
- Leverage government procurement (Supply Chain Risk Management)
- Build on recent progress with CNCI (comprehensive national cyber-security initiative)

- Cyber security needs to be reflected in our contractual requirements
- Many “locked down” configuration defined
- Use government-industry partnership to accelerate implementation of secure configurations
- Get started now, improve configuration guidelines over time and leverage SCAP!

Build on FDCC Successes and Lessons Learned

- Change the dialogue: Reliable, resilient IT is fundamental to future National Security and Economic Growth
- New business model for software industry
- Redesign the Internet
- Get the “man out of the loop”—use automated tools (e.g., SCAP)
- Develop professional cyberspace workforce
- Foster new IT services models

Need to Fundamentally “Change the Game” to Make Progress



- What is it: A set of open standards that allows for the monitoring, positive control, and reporting of security posture of every device in a network.
- How is it implemented: Commercial products implement SCAP protocols to exchange and enforce configuration, security policy, and vulnerability information.
- Where is it going: Extensions in development to address software design weaknesses, attack patterns, and malware attributes.

SCAP Enables Automated Tools To Implement And Enforce Secure Operations

- What is it: 20 key actions (called security "controls") that organizations must take if they hope to block or mitigate top known attacks.

- How is it implemented: (Mostly) automated means used to implement and continuously enforce/monitor controls.

Consensus Audit Guidelines permits organizations to prioritize security implementation and continuously enforce controls

- How do we make measurable progress in improving security?
- How do we assess the effectiveness of security tools?
- How do we change the software industry to produce reliable and secure products?

It is time to get off the treadmill and start making measurable progress in securing our systems!

- Government and Industry need to treat cyber security as an urgent priority
- Near-term actions important but need to fundamentally change the game to get ahead of threat
- IT community needs to reorient the dialogue on cyber security—the objective is reliable and resilient information
- Cyber Security in DoD is more mature—but still woefully inadequate

Cyber Security is Fundamentally a Leadership Issue!

Contact Information

John M. Gilligan

jgilligan@gilligangroupinc.com

www.gilligangroupinc.com

AMC IA COE

U.S. Army CECOM LCMC
Software Engineering Center (SEC)
Software Assurance Division

DRAFT

DoD-DHS-NIST Software Assurance Forum Presentation: Software Technology Vendors Need to Better Understand DoD Requirements

Presented By: Bruce Weimer
Team Lead - Software Quality Assurance Division
Bruce.Weimer@conus.army.mil
(732) 532-5020/ DSN 992

DRAFT

Who am I:

Team Lead – Independent Software Quality Assurance

My Perspective For This Panel

- My team provides Software Quality Assurance services to DoD and Federal Agencies
- We are a consumer of software quality assurance technology to support our services

- **Voice of Customer:** Software Assurance technology vendors need to have a better understand the DoD processes and requirements in order to support our mission.
  - Deliver safe, secure, and reliable systems to the Warfighter
  - Avoid spending tax-payer dollars for software defect costs

Improvement Ideas for Vendors

- Knowledge of Acquisition Process (contracts, deliverables, life-cycle phases, key performance parameters, terminology)
- Knowledge of DoD software requirements (DoDD, DoDI, STIGs, "service-specific" requirements, BBPs)
- Knowledge of DoD process for system/software assurance (certification and accreditation, networthiness)
- How does your technology support industry process that the DoD requires and uses (ISO 9000/9001, CMMI, LSS)?
- Contributions to communities that the DoD engages (SAFECode, Build Security In, Open Source Software, Academia)
- Sell into our listening!

DRAFT

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

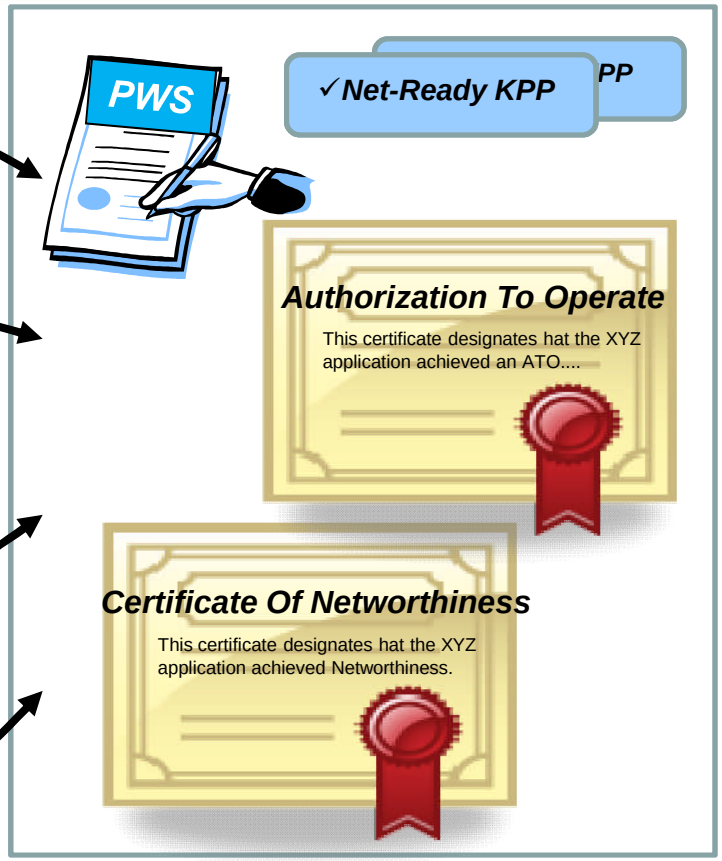
Understand What DoD Follows and Why!

Federal Acquisition Regulation (FAR) – "Appropriate techniques should be applied to manage and mitigate risks during the acquisition of information technology."

DoD Directive 5000.01, E1.1.25 – "Acquisition of software intensive systems shall use process improvement and performance measures. "

DIACAP Requirements - DoDI 8500.2, IA Control DCSQ-1 requires software compliance to DISA guidance

Army Networthiness Requirements - AR 25-1, Ensures application compliance with Federal, DoD and Army mandates, regulations, and guidelines.



DRAFT

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

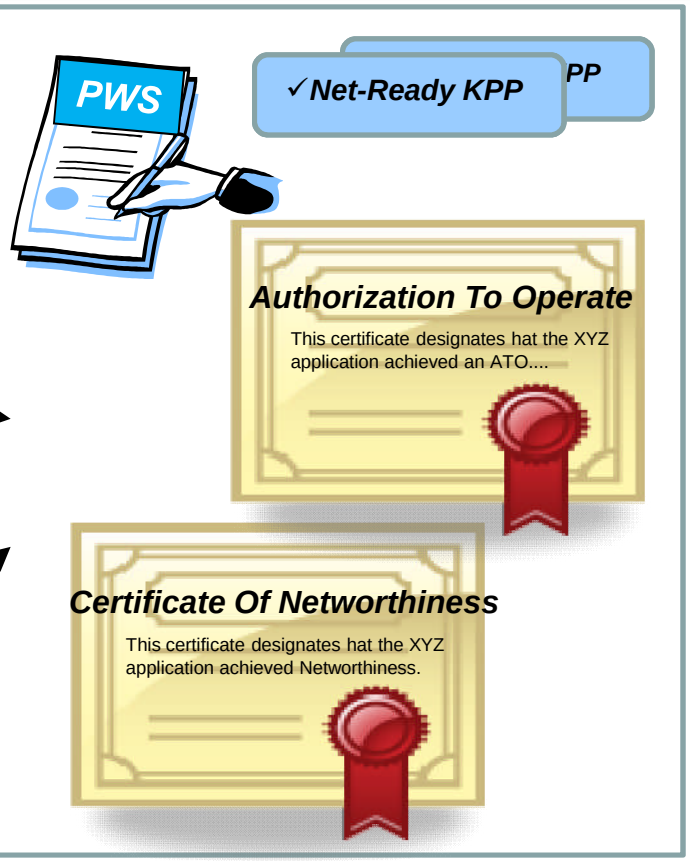
Understand What DoD Follows and Why!

Army Open Source Software - AR 25-2, Permitted when source code is available to examine for malicious content, configuration implementation guidance is implemented, protection profile exists, or risk and vulnerability assessment has been conducted.

Defense Acquisition Guidebook (DAG) - Chapter 4, Risk management includes the impact of software development and integration activities.

Net-ready Key Performance Parameter (CJCSI 3170.01G) - Addresses information needs, information timeliness, information assurance (IA), and net-readiness.

Build Security In, SAFECode, CMMI, LSS, ISO – Community best business practices.



DRAFT

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Example: DoD Tailored Technology

CODE INSPECTION RESULTS									
DISA Application Security and Development STIG		**Instances**	**CAT I**	**CAT II**	**Minor**	**Bad Style**	**No Defect**	**Informational**	**% Assessed**
INSPECTION ATTRIBUTES									
APP No.									
3050	**Defects:** Dead or Dormant Code	388	0	2					
3100	**Defects:** Apparent Unclosed Stream	10	0	2					
3120	**Exception Handling Attributes:** Error Handling	2353	0	25					
3120	**Exception Handling Attributes:** The program can potentially dereference a null pointer, thereby causing a segmentation fault.	2300	0	115					
3100	**Defects:** Unreleased Resource	230	0	0					
2060.4	**Defects:** Dangerous Functions	10	0	0					
3120	**Exception Handling Attributes:** Ignoring Return Value Of Symbol	4	0	0					
DATA SECURITY									
3150.2	**Cryptography:** Standard pseudo-random number generators cannot withstand cryptographic attacks	19	0						
3310	**Password Management:** Credential Management-Passwords Stored as Clear Text	6	2	0					100
INPUT VALIDATION									
3570	**Command Injection:** Executing commands that include un-validated user input can cause an application to act on behalf of an attacker.	5	0	1	0	0	4	0	100
3510	**General Input Validation:** No Usable Struts Validation	490	0	15	0	0	30	3	10
3540.1	**SQL Injection:** SQL Injection User Input	583	0	0	0	0	21	562	100
3580	**Cross Site Scripting:** CrossSiteScripting	110	0	0	0	0	0	109	99
3530	**General Input Validation:** Web Character Set	382	0	0	0	0	0	382	100
3520	**General Input Validation:** Trust Boundary Violation	125	0	0	0	0	0	3	2
3540.1	**SQL Injection:** SQL Injection User File	316	0	0	0	0	18	298	100
PORTABILTY AND SECURITY									
3600	**Code Hacking Attributes:** Canonical Representation Vulnerabilities	79	0	0	0	0	4	75	100
3630.3	**Code Hacking Attributes:** Deprecated Thread Functions	600	0	0	0	0	0	600	100
	SUMMARY OF ISSUES FOUND		2	160	0	0	1626	4775	
	KEY DEFECTS		162						
	ALL DEFECTS		162						

- Category of Finding
- STIG Requirement Number
- Validate "Real and Actionable"
- Actionable Results Feed Into developer's "Get Well Plan" for the system.

DRAFT

- **Voice of Customer:** Software Assurance technology vendors need to have a better understand the DoD processes and requirements in order support our mission.
  - Deliver safe, secure, and reliable systems to the Warfighter
  - Avoid spending tax-payer dollars for software defect costs

- **Impact to DoD from Vendor Improvements**
  - DoD is faster to adopt and more effective at using technology to support our mission
  - DoD benefits from Contractors who adopt the technology

KDM Analytics™

OBJECT MANAGEMENT GROUP

System Assurance Approach with Focus on Automation

Djenana Campara

CEO, KDM Analytics

Board Director, Object Management Group (OMG)

Co-Chair System Assurance and Architecture Driven Modernization, OMG

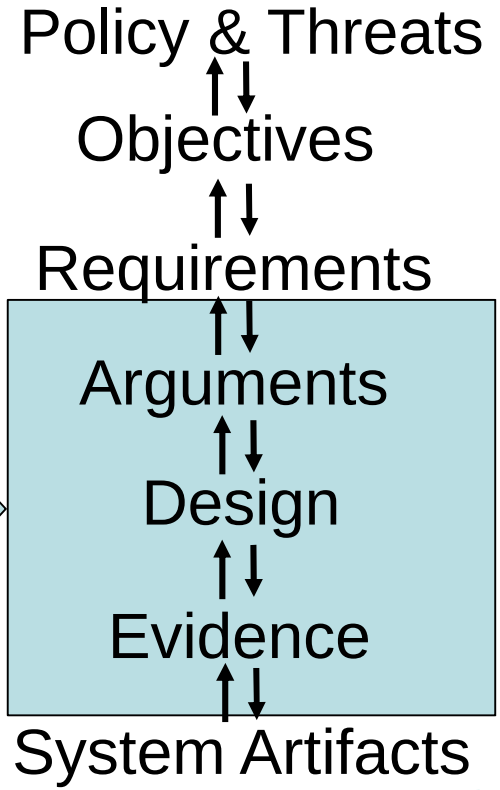
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Current Assessment Approaches - Limitations

- Lack of formalized methodology between high level policy, evidence and system artifacts means a laborious, unrepeatable (subjective), lengthy and costly certification process
- Current assessment approaches resist automation

Methodology Gap



Key Requirements –

1. Specified assurance compliance points through formal specification
2. Transparency of software process & systems
3. End-to-end Traceability: *from code to models to evidence to arguments to security requirements to policy*
4. Standards based Integrated tooling environment

Together, these requirements enable the management of system knowledge and knowledge about properties, providing a high degree of transparency, traceability and automation

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Software Assurance Ecosystem =

System Assurance Approach with Focus on Automation

Process Docs & Artifacts

Requirements/Design Docs & Artifacts

Reports
Risk Analysis, etc)

Process, People & Documentation Evaluation Environment

- Some point tools to assist evaluators but mainly manual work
- Claims in Formal SBVR vocabulary
- Evidence in Formal SBVR vocabulary
- Large scope requires large effort

Process, People documentation Evidence

Formalized Specifications

Assurance Case Repository

- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships

Supported by the following standards:
- ISO/IEC 15026
- ISO/TC 37 / OMG SBVR
- OMG ARM
- OMG SEAM

Software System / Architecture Eval

- Many integrated & highly automated tools to assist evaluators
- Combination of tools and ISO/OMG standards
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

Supported by ISO/IEC 19506

Software system Technical Evidence

Executable Specifications

Software System Artifacts

Hardware Environment

Data Structures

Protection Profiles

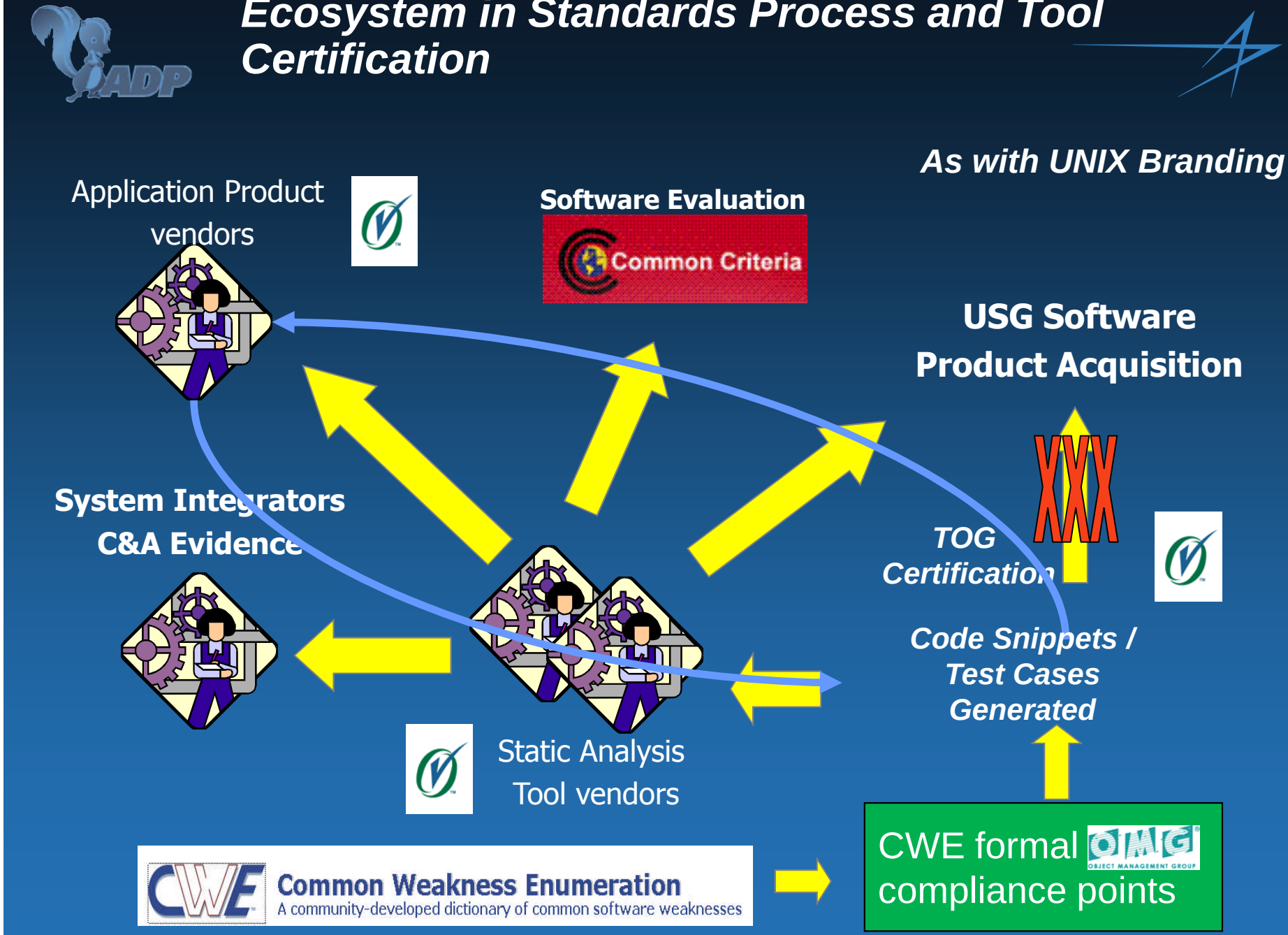
Security Controls

CWE

KDM Analytics ™

OMG OBJECT MANAGEMENT GROUP

Ecosystem in Standards Process and Tool Certification



Prepared by Dr. Ben Calloni, LM Aero

Understanding Technology Stakeholders: Their Progress and Challenges

Todd Landry

Senior Product Manager - Klocwork

- Klocwork provides a family of developer and team productivity tools built on our industry leading source code analysis capability

- Business and technology strengths:
  - More than 550 customers around the globe
  - Proven value and scalability on some of the largest code bases in the world
  - Strong technology pedigree with many industry firsts

- Value we provide:
  - Complete source code analysis solution that addresses multiple productivity bottlenecks in the development lifecycle
  - Single solution that can address a wide range of security, quality, architecture and maintainability issues in code

Our Goals

Productivity Result for Developers:
More bugs reports, more fire drills
Less time to write new code

Release
Huge costs associated with bugs shipped to customers
Difficult to predict stability with large code bases

Testing
Resources here should be focused on requirements
Extended testing time can delay release and increase costs

Integration Builds
Critical milestone in development process
Unstable integrations will slow down entire team

Peer Code Reviews
Time consuming activity involving senior resources
Should focus on critical code & design issues

Implement | Build | Unit Test | Check-in | Integration Build | System Test | Release

- Research time
  - Many different security issues to look for…time is limited

- Vulnerabilities vs. Weaknesses
  - Static technology aimed at weaknesses in code
  - Most effort is put into vulnerability catching
  - Vendors on their own

- DHS Forum has great potential...but it has a long way to go
  - Outbound delivery of message is strong
    - Awareness and education of tool users very good
  - Exercise of analyzing projects was not
    - Presentation of results was poor
      - No conclusions
      - Unable to interpret

Sean Barnum

Principal Consultant

Cigital Federal, Inc.

cigital

Homeland Security

- Evangelize software assurance & risk management
- Help organizations address software assurance holistically
- Push the state of the art in thought leadership and knowledge
- Push the state of the art in methodology & practice
- Push and leverage the state of the art in technology and automation

cigital

Sean Barnum
sbarnum@cigital.com

Homeland Security

- Trees & Forests
- A little knowledge is a dangerous thing
- E) All of the above
- Tower of Babel

Sean Barnum
sbarnum@cigital.com

cigital

Homeland Security

- Software Assurance Findings Expression Schema (SAFES)

- Sponsored by the NSA Center for Assured Software (CAS)
- Objectives:
  - Enable and encourage consistency in software assurance tool findings
  - Establish more structured and effectively useful software assurance tool results
  - Enable integration of results from multiple software assurance tools
  - Enable automated processing of software assurance tool results

cigital

Sean Barnum
sbarnum@cigital.com

Homeland Security

- Community collaboration
- Build from state of the practice
- Enhance with state of the art
- Define a comprehensive schema covering all aspects of software assurance analysis reporting
- Layer the schema into a framework for composable and focused use
- Strive for flexibility and extensibility

cigital

Sean Barnum
sbarnum@cigital.com

Homeland Security

- In-scope perspectives for initial effort:
  - Static source code analysis
  - Static binary code analysis
  - Web application penetration testing
  - Data security analysis
  - Fuzzing
  - Threat modeling
  - Architectural risk analysis
- Some vendors actively collaborating others were passively incorporated

cigital

Sean Barnum
sbarnum@cigital.com

Homeland Security

- Currently finishing Review Candidate 1 (RC1) draft for review by key stakeholders
  - Hopefully distribute next week
- Allow ~6 weeks for review of RC1
- Evaluate review input and make revisions
- Publish Version 1 release in January

cigital

Sean Barnum
sbarnum@cigital.com

Homeland Security