

The Globalization Challenge for Trusted Systems, and DoD Response



Larry Wagoner
NSA

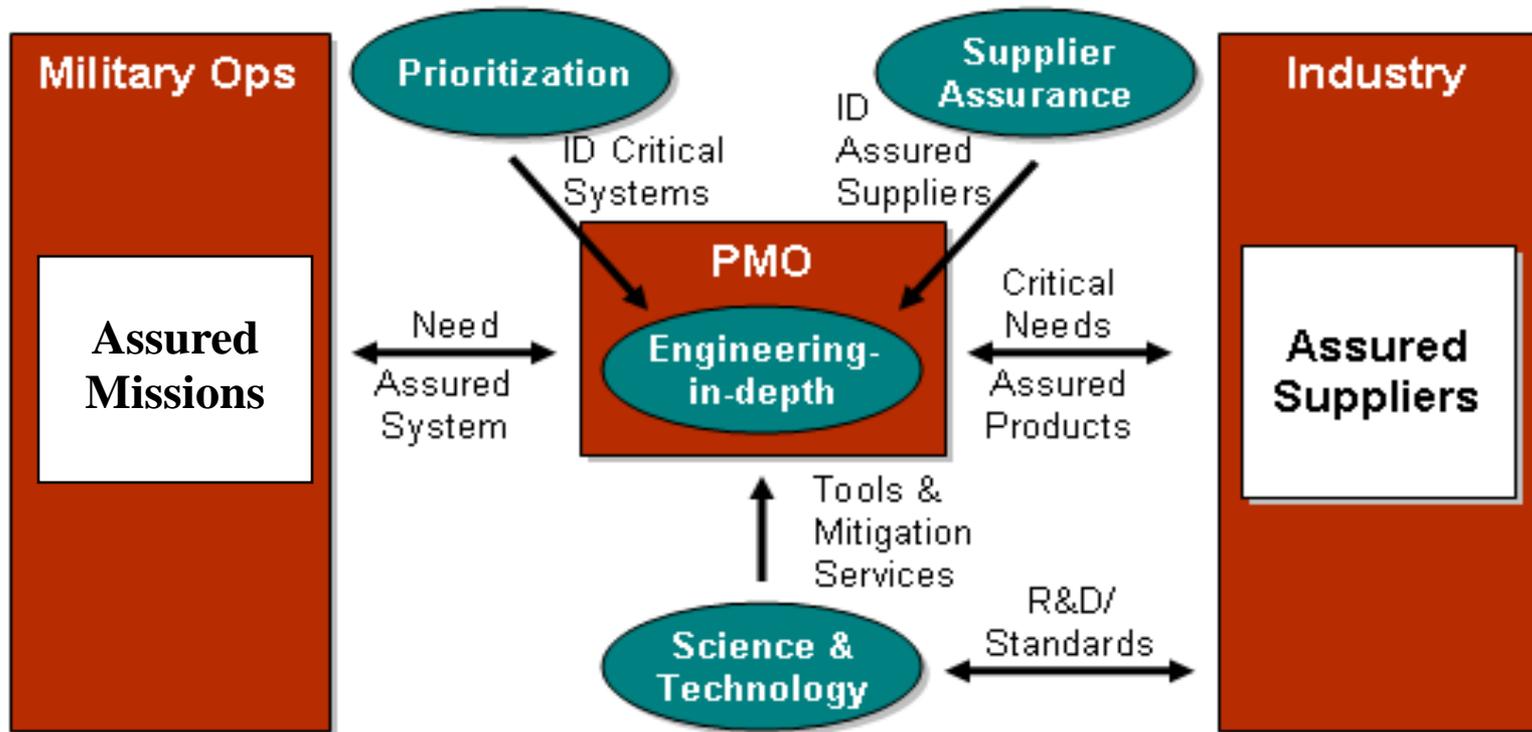


Agenda

- CONOPS
- Strategy
- Supply Chain Risk Management
- Evaluation Methodology
- Automation (Fundamental weaknesses)
- Standards
- Open Source Repository
- DoD Partnerships



DoD Systems/Software Assurance CONOPS



The strategy components interact with operations, acquisition, and industry to produce assured systems

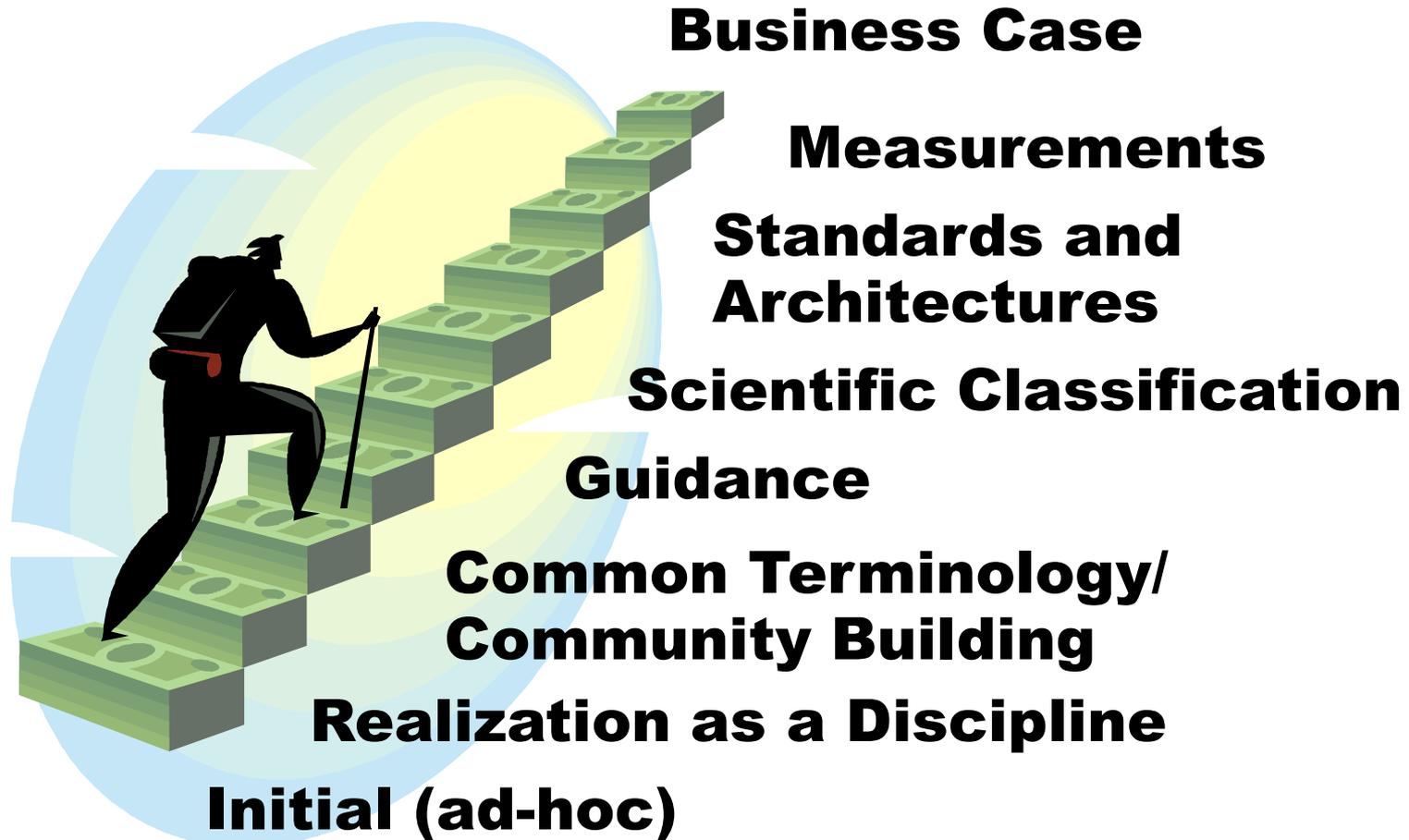


System Assurance Strategy

- CONOPS has been a key structure for establishing the DoD program for system assurance
- Taking stock of accomplishments
- Examining where gaps remain
- Interested in any gaps that you know exist
- Once finalized and vetted within DoD, will be shared



Assurance is Maturing





Supply Chain Risk Management (SCRM) /Engineering Guidance Update

- ❑ Engineering for System Assurance Guidebook
 - Developed by AT&L and NII through NDIA Systems Assurance Committee
 - Within the context of system and software lifecycles
 - Assurance of security and management of risk
 - Provide practical guidance within structure of ISO 15288 systems engineering technical process
 - Available for download at:
<http://www.acq.osd.mil/sse/docs/SA-Guidebook-v1-Oct2008.pdf>
- ❑ Developing Supply Chain Risk Management guidance
 - Focus is on engineering in depth elements of NDIA System Assurance Guidebook
 - Managing risk throughout the lifecycle
- DSD has signed out the Directive Type Memorandum (DTM) establishing a piloting program
- Will do real world vetting of the NDIA guidance practices



Center for Assured Software (CAS) Update

- ❑ Updated Static Analysis Test Suite and Tool Evaluations methodology for C/C++/Java
 - Methodology will target approximately 150 CWEs
- ❑ Performed a pilot evaluation of 4M SLOC using a Software Assurance Evaluation Methodology for C/C++ Source Code
- ❑ Continuing to improve and refine their methodology
- ❑ Performing an analysis of binary executable analysis tools and techniques

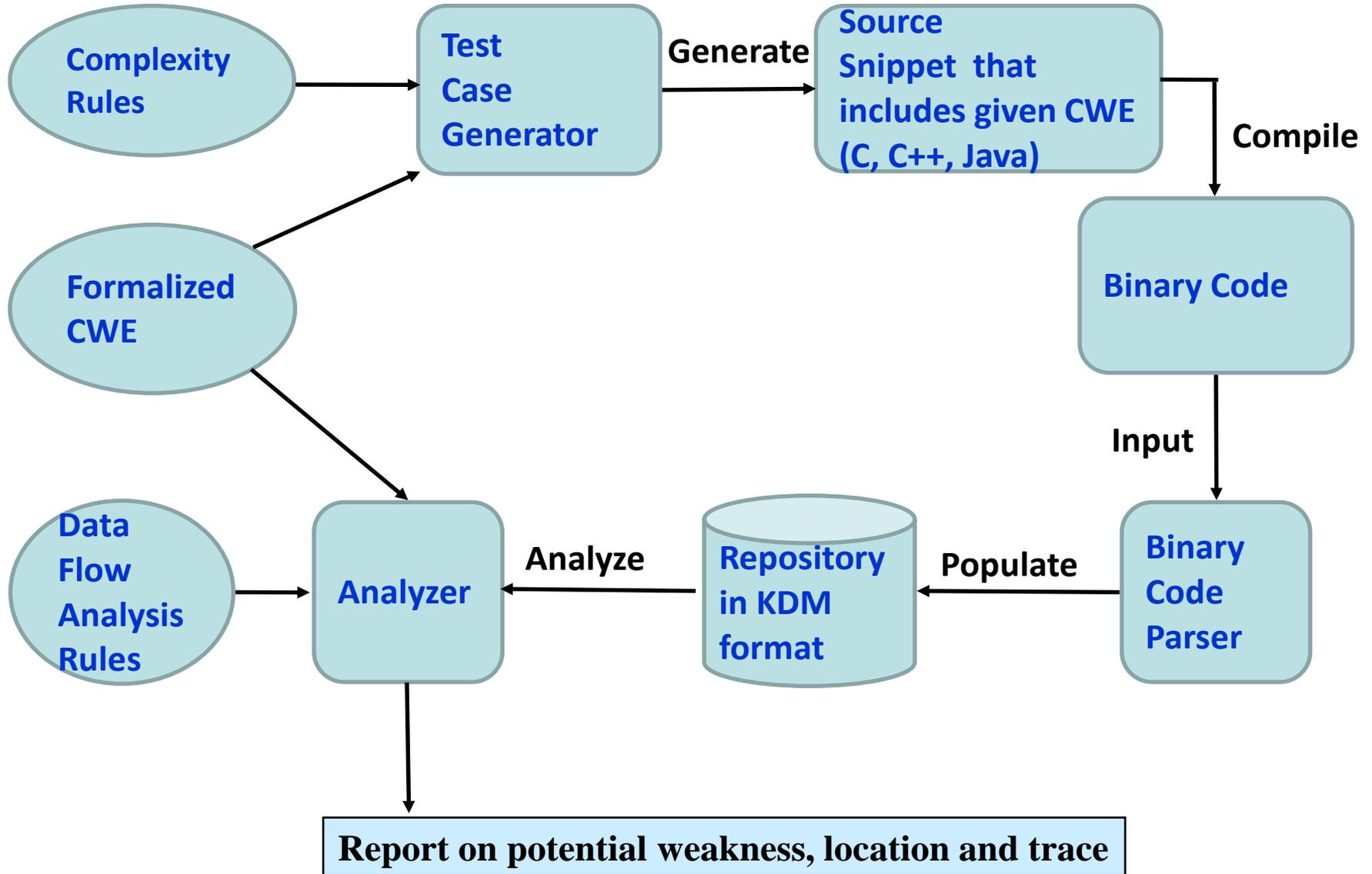


CWE Formalization and Analysis Proof of Concept

- Investment by DOD and NSA to demonstrate the value of formalization of some Common Weakness Enumeration (CWE) elements
- Leveraging
 - OMG standards for formalization
 - Knowledge Discovery Metamodel (KDM)
 - Semantics of Business Vocabulary and Business Rules (SBVR)
 - NIST/DHS Test Case Generator
 - COTS analysis tools
- OMG's KDM being evaluated by ISO/IEC
 - Going through "Fast Track" process
- Working to identify and formalize the core fundamental weaknesses
 - Estimated to number about 30-40



Proof of Concept Architecture





ISO/IEC JTC 1/SC22 WG23 Programming Language Vulnerabilities

- ❑ Previously called the “Other Working Group on Vulnerabilities (OWGV)”
- ❑ Producing Technical Report entitled “Guidelines to Avoiding Vulnerabilities in Language Selection and Use”
- ❑ Provides guidance to programming language users and suggestions on how programming languages could be made inherently safer and more secure
- ❑ Based on both an empirical approach and analytical approaches
- ❑ Annexes will describe the vulnerabilities relative to specific languages
- ❑ Preliminary Draft Technical Report (PDTR) was voted on and passed
- ❑ Website: <http://aitc.aitcnet.org/isai/>



High Assurance Components

- ❑ Systems Assurance CONOPS needs components that are provably secure and correct by construction
- ❑ Open Source Software becoming common
 - run the program for any purpose
 - study and modify the program, and
 - redistribute copies of either the original or modified program (without royalties, etc.)
- ❑ Foster a Community of Interest to identify and develop high assurance components that are needed
- ❑ Desire to encourage development of “Open Proofs”
 - Where Implementation and Proofs and Tools are OSS
 - Enables researchers, developers, etc. to collaborate
 - <http://www.openproofs.org>
- ❑ More tomorrow...



Expanding DoD Industry Partnership

- ❑ Acquisition Cyber Security is a long term interest for DoD
 - Fully anticipating Cyber Security will be an ongoing priority for the new administration
 - Other governments and industry expressing greater interest in acquiring “trustworthy” hardware and software for government and critical infrastructure

- ❑ Understand and impact global supply chain risk in COTS arena to compliment secure system engineering successes in DoD and DIB
 - Understand where risk is introduced in the COTS supply chain
 - Helps inform DoD processes (Must DoD accept risk?)
 - Identify points of vulnerability in engineering, procurement, security
 - Identify the state of the art in global sourcing risk management – policy, processes, tools
 - Work with JTC1 organizations (SC27 and SC7 TAGs initially) to drive a commercially reasonable standard



Questions?



CAS Achievements

- Software Assurance Evaluation Methodology for C/C++ Source Code
- Successful pilot evaluation of 4M SLOC
- Static Source Code Analysis Tools Evaluation Framework
- Completed proof of concept evaluation of five leading commercial tools
- Works in Progress (FY08-FY09)
- Updated Static Analysis Test Suite and Tool Evaluations for C/C++/Java
- Development of binary executable analysis tools and techniques
- Acquisition Security Risk Assessment Tool
- Software Assurance Evaluation Survey and Best Practices Report



Benefits of Approach

Clear separation of components

- Security Properties
- Software Engineering Constructs
 - Code constructs (CC)
 - Data-driven semantic analysis (e.g. DFA)

Use of Standards

- Interchangeable parts
- Each component could come from different supplier
- Each component can be addressed by experts in that domain
- Components can be used for multiple disciplines

End result of investment

- Test Code Generator that automatically generates a very large set of code samples for use in testing and evaluating analysis tools
- Demonstration that code (source or binary) can be analyzed against formalized CWEs



CAS Program Objectives

Provide expert guidance on tools, techniques, and processes for software assurance measurement

- Bridge the gap between research and evaluation capabilities

- Form and lead a DoD assurance evaluation community to share best practices

Provide expert guidance on assured software implementation standards and practices

- Identify and mitigate “root causes” of vulnerabilities

- Drive the definition of “Quality” in DoD acquisitions and influence COTS development

Enable informed risk management in DoD acquisitions and software engineering by enhancing measurement capabilities, and also on secure coding principles and practices to make software worth measuring.



DODI 5200.39 “Critical Program Information Protection Within the DoD”

It is DoD Policy to provide uncompromised and secure military systems to the warfighter by

- performing comprehensive protection of Critical Program Information (CPI)
- through the integrated and synchronized application of CI, Intelligence, Security, systems engineering, and other defensive countermeasures to mitigate risk

To minimize the chance that the Department’s warfighting capability will be impaired due to the compromise of elements or components being integrated into DoD systems by foreign intelligence, foreign terrorist, or other hostile elements *through the supply chain or system design*.

DoD is moving forward

DSD has signed out the Directive-Type Memorandum (DTM) establishing a piloting program