NSA Center for Assured Software

Information Security And Privacy Board

March 21, 2006

Software Assurance Definition

DoD Software Assurance Initiative

DoD Software Assurance Tiger Team

- The level of confidence that software is free of exploitable vulnerabilities, either intentionally designed into the software or accidentally inserted

- And that the software functions in a manner as expected.

Problem Statement (1)

"The ubiquity of software and its development and usage without consistent engineering, has resulted in ad hoc management and mitigation efforts in a race to protect systems against breaches"

NII Sponsored

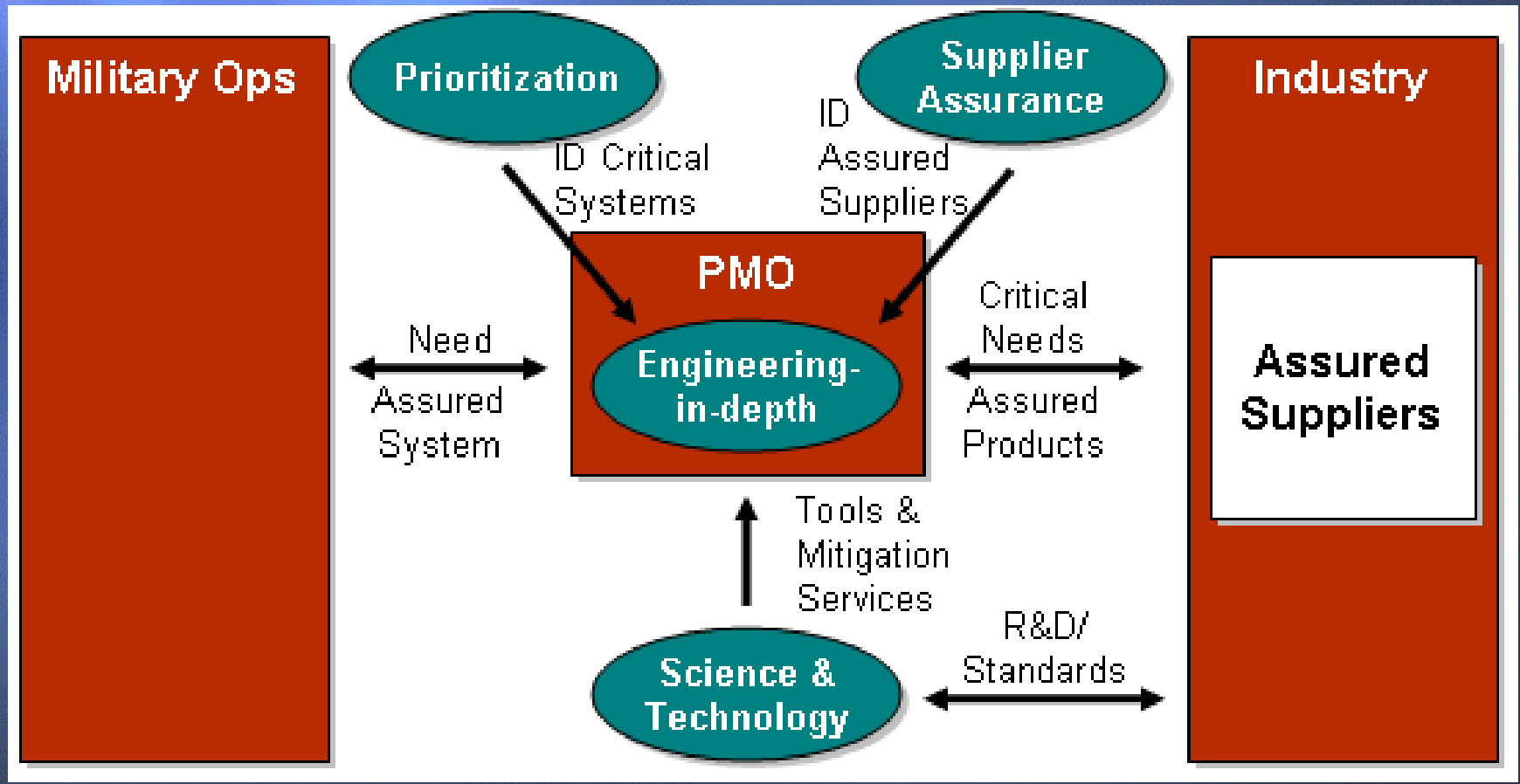
Software Assurance Tiger Team

Problem Statement (2)

There's too much software

There's too little assurance

DoD SwA CONOPS: Interacting Processes



Science & Technology

- Provide software evaluation services
- Use tools to detect vulnerabilities
- Coordinate DoD R&D for vulnerability detection and mitigation
- Work with industry to develop standards/solutions
- Recommended a DoD Executive Agent for Software Vulnerability Mitigation and Discovery
  - Establish a DoD Center for Assured Software

NSA Center for Assured Software (CAS)

- Stood up in November, 2005
- A Focal Point for Software Assurance (SwA) Issues with the following objectives:
  - Partner with our customers, government, the private sector and academia to identify SwA Issues and resolutions
  - Develop and utilize tools and methods to analyze the trustworthiness of software

NSA Center for Assured Software (CAS) (cont)

- Objectives (cont)
  - Evaluate mission critical components
  - Establish/Identify software standards and practices to increase the availability of assured software products

CAS "domain of operation"

Binary analysis tools/techniques

Role of Formal Methods

Source Code analysis tools/techniques

Developmental Processes

Static/Dynamic analysis

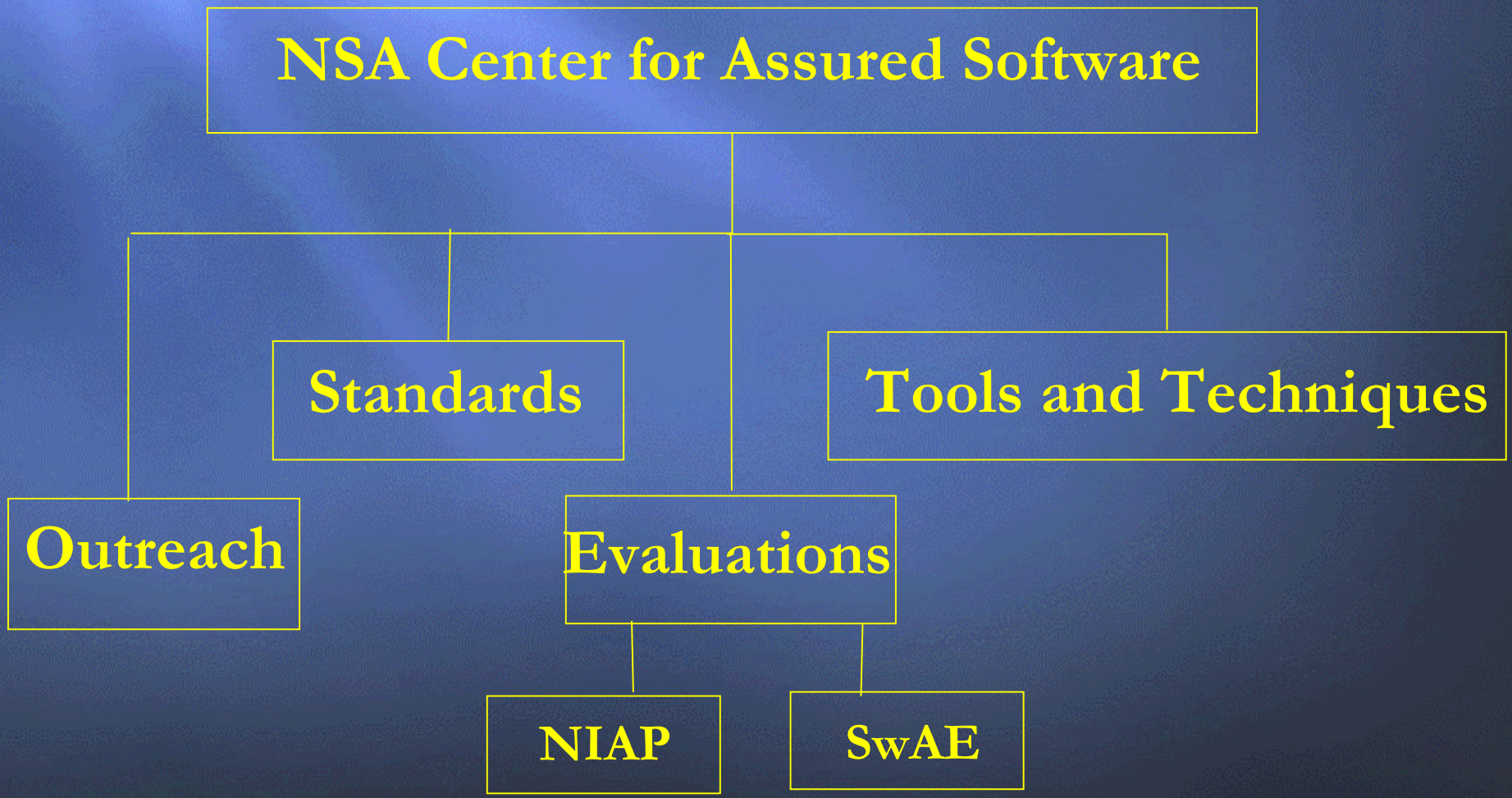
Product Evaluation

Requirements	Design	Implementation	Testing	Deploy	Maintenance

Safe Language Standards

Development Tools/techniques

What we look like today…



Where we are working today …

- NIAP
  - Fully operational
  - Beginning to address recommendations from the GAO and IDA NIAP review reports

- Software Assurance Evaluations
  - Are evaluating some specific software of interest to NSA in the context of a pilot
    - First report due in 30 days

Where we are working today (cont) …

- A repeatable SwAE methodology based upon available tools
  - Involves a tools survey as wells as incorporating lessons learned from our pilot

- Strategies for :
  - Public Software Assurance Standards participation
  - Internal NSA Software Assurance Standards and compliance
  - Outreach
  - High Assurance

Using Tools for to gain Confidence in Software

Measuring Software Assurance

- Looking for properties of software that are indicators of the assurance level
  - Degree of confidence that software will securely and appropriately perform its intended functions
  - Degree of confidence that software will not perform any unauthorized functions
  - Degree of confidence that software does not contain implementation flaws that could be exploited.

Measuring Software Assurance

Process Phases:

- Acceptance
- Extraction/Inspection
- Analysis
- Meta-Analysis
- Reporting

Acceptance

- Are there existing tools and techniques that address the software to be evaluated?
  - Platform/Machine Language
    - x86, Sparc, ARM, etc.
  - Source Language
    - C/C++, Java, Microcode, etc.
  - File Format
    - PE, ELF, ROM Image, etc.
  - Environment
    - Windows, Real-time O/S, Linux

Measuring Software Assurance

CAS: Identify and fill capability gaps

Phase Report Card:

C+

- Acceptance
- Extraction/Inspection
- Analysis
- Meta-Analysis
- Reporting

Extraction/Inspection

- Apply tools and techniques that extract relevant metadata from the software
  - Control Flow Graphs
  - Complexity Metrics
  - Module Dependencies
  - Disassembly/Decompilation
  - Functional Extraction
  - Instruction Effects Analysis
  - Identification of Code vs. Data

Extraction/Inspection

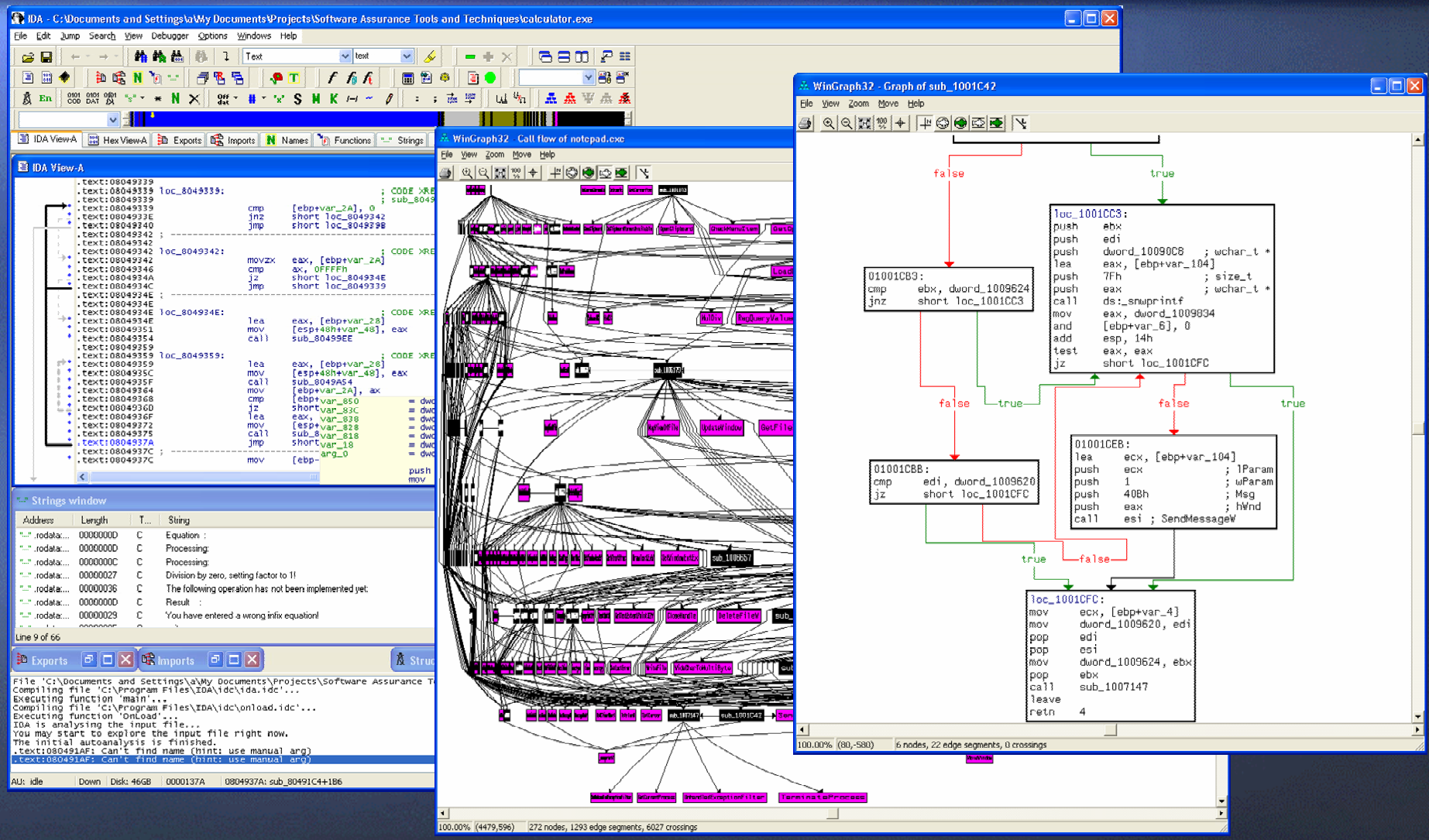
- Extraction/Inspection tools are the most sophisticated tools available today
  - Most academic and commercial research and development is in this area
  - Much of the research is driven by the need to port legacy applications to newer platforms and binary formats

Extraction/Inspection

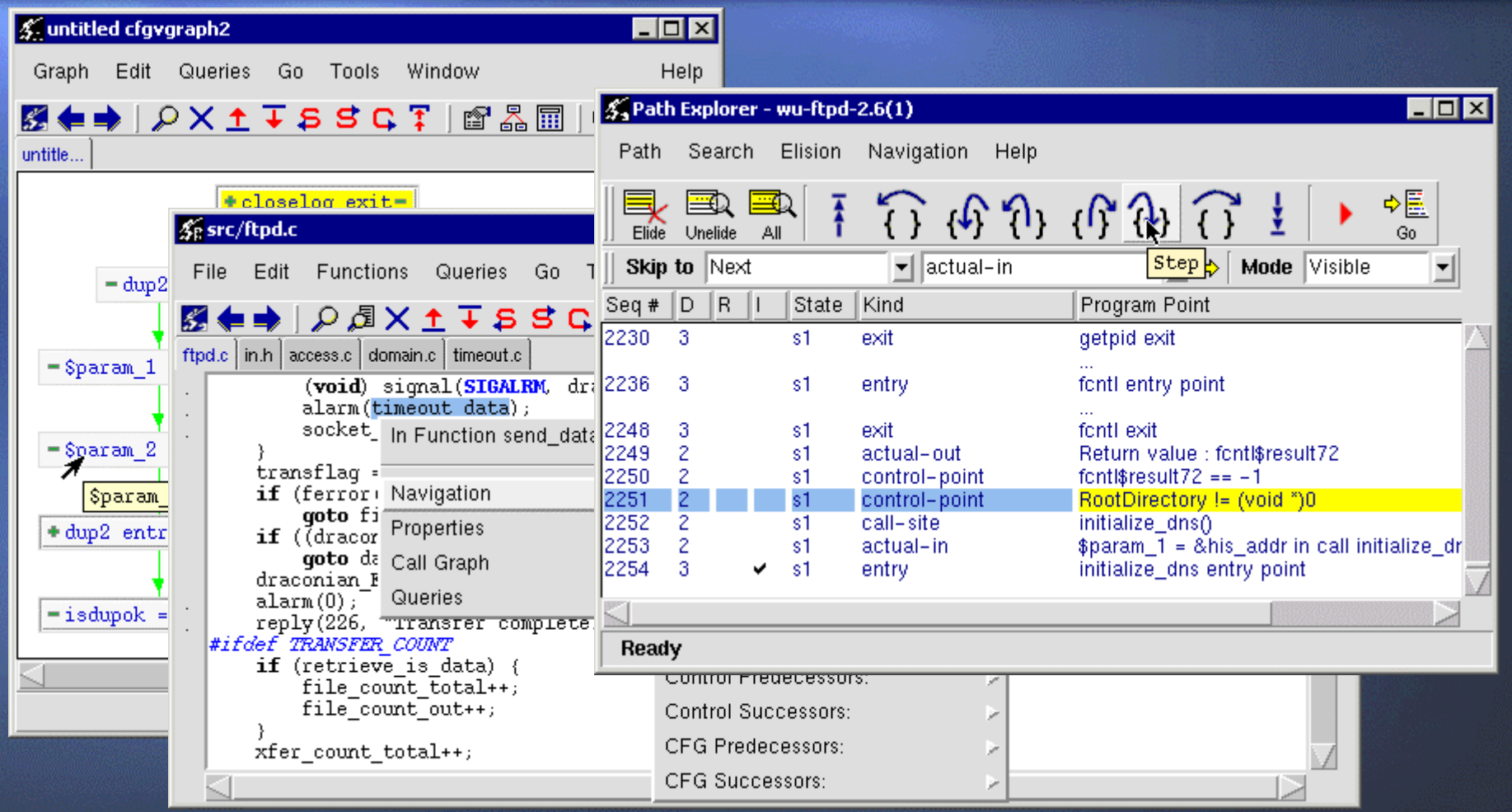
- Extraction/Inspection tools have complex output
  - Use requires a high level of training
- Tool results create the environment for analysis, but in most cases only indirectly indicate assurance
- Integration of extraction/inspection tools with analysis tools is poor
  - Metadata formats are typically proprietary with specialized programming interfaces

Sample tool output …

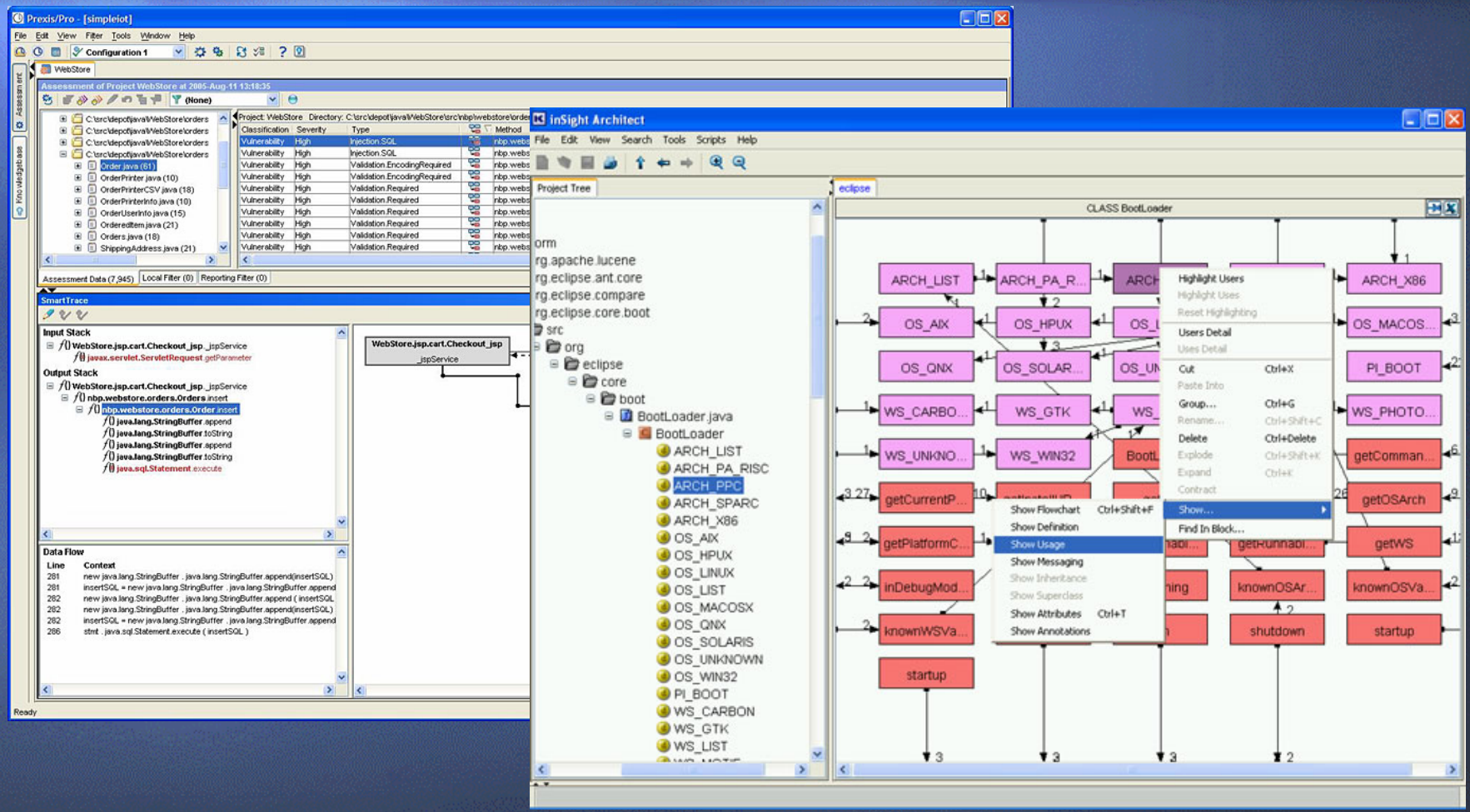
Extraction/Inspection



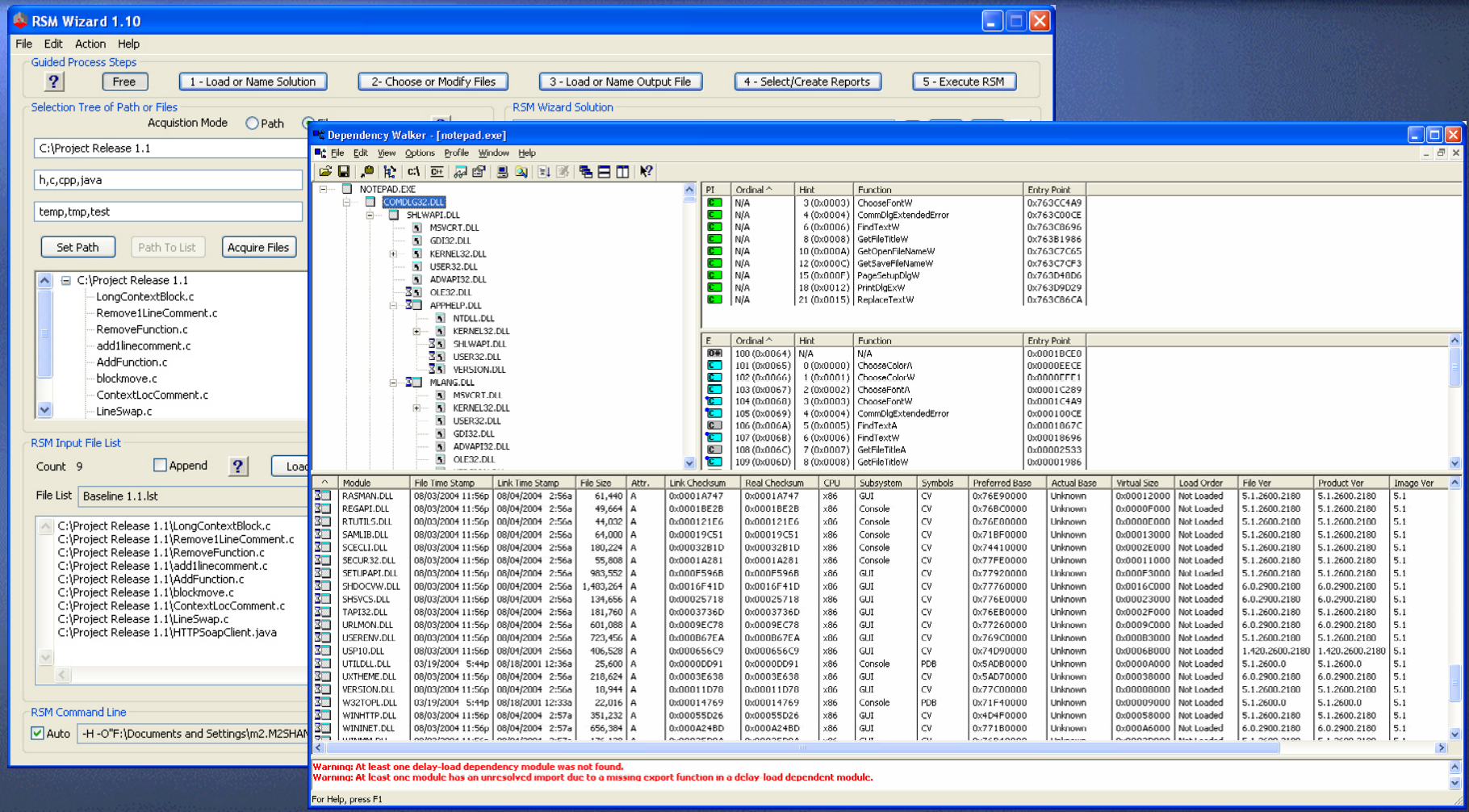
Extraction/Inspection



Extraction/Inspection



Extraction/Inspection



Measuring Software Assurance

Phase Report Card:

- C+ • Acceptance
- B+ • Extraction/Inspection
- • Analysis
- • Meta-Analysis
- • Reporting

CAS: Identify and fill capability gaps

CAS: Foster integration and promote further research

Analysis

- Apply tools and techniques that query the metadata for properties or indicators of assurance
  - Existence of Buffer Overflows
  - Improper Memory Management/Object Reuse
  - Insecure Storage of Cryptographic Keys
  - Lack of Authentication
  - Race conditions
  - Covert Channels
  - Unexpected Functionality

Analysis

- Existing analytical tools:
  - Relatively primitive
  - Typically tailored to a specific sets of bugs
    - Not easily modified to address new questions
  - Typically highly coupled to a particular extraction/inspection tool
    - Simple analytic capability carries with it the cost of sophisticated tool
  - Lots and lots of false positives

Analysis

- Analysts typically create small programs on the fly to answer specific questions
  - Custom tools generally aren't refined to cover all relevant cases
  - Limited distribution and support of tool
  - Tools themselves are not well-engineered or extensible
  - No integration into an overall evaluation methodology

Measuring Software Assurance

Phase Report Card:

- C+ • Acceptance
- B+ • Extraction/Inspection
- C- • Analysis
- • Meta-Analysis
- • Reporting

CAS: Identify and fill capability gaps

CAS: Foster integration and promote further research

CAS: Generate quality tools, reduce false positives

Meta-Analysis

- Integrate output from multiple analytical tools and techniques to discern higher-order assurance indicators
  - Some tools may increase the confidence in the results from another tool
  - Use one tool to focus the analysis of a following tool or filter the results of a preceding tool
  - Independent indicators help rank results
  - Perform analytical tests not within the capability of any one tool

Meta-Analysis

- No technological methodology currently exists that:
  - Leverages the strengths of multiple tools
  - Contains the technological "glue" to connect tools from different vendors
  - Models software assurance through a diverse set of direct and indirect indicators
  - Is repeatable, scalable, and well-documented

Measuring Software Assurance

Phase Report Card:

- C+ • Acceptance
- B+ • Extraction/Inspection
- C- • Analysis
- I • Meta-Analysis
- • Reporting

CAS: Identify and fill capability gaps

CAS: Foster integration and promote further research

CAS: Generate quality tools, reduce false positives

CAS: Weave tools into a scalable methodology

Reporting

- Transform analytical results into comprehensible reports
  - Ranked "raw" data for follow-on deep analysis
  - Comparative results for systems design decisions
  - Summary results linked to standardized evaluation criteria for use as part of a larger evaluation process
  - Formal evaluation report for technology-only evaluations
- Report formats are not currently defined

Measuring Software Assurance

Phase Report Card:

- C+ • Acceptance
- B+ • Extraction/Inspection
- C- • Analysis
- I • Meta-Analysis
- I • Reporting

CAS: Identify and fill capability gaps

CAS: Foster integration and promote further research

CAS: Generate quality tools, reduce false positives

CAS: Weave tools into a scalable methodology

CAS: Define customer-focused report formats

Center for Assured Software

Kris Britton

TD, NSA Center for Assured Software

rkbritt@missi.ncsc.mil

410-854-4543