SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

3 March, 2011

“Technology, Tools and Product Evaluation Working Group Outbrief”

Michael Kass, NIST and Larry Wagoner, NSA
Co-chair(s)
michael.kass@nist.gov

NIST
National Institute of Standards and Technology

Homeland Security

TT&PE Goals

- *Measurement through Standards*
  - – The Software Assurance Ecosystem
    - OMG System Assurance Taskforce
    - Implementations
- *Tool Evaluation*
  - – SAMATE
- *Making Security Measurable*
  - – Cyber Ecosystem – Bob Martin (MITRE)

Software Assurance Ecosystem

- SwA Ecosystem is a formal framework for analysis and exchange of information related to software security and trustworthiness
- Provides a technical environment where formalized claims, arguments and evidence can be brought together with formalized and abstracted software system representations to support high automation and high fidelity analysis.
- Based entirely on ISO/OMG Open Standards
  - Semantics of Business Vocabulary and Rules (SBVR)
  - Knowledge Discovery Metamodel (KDM)
  - Structured Metrics Metamodel (SMM)
  - Structured Assurance Case Metamodel (SACM) (Adopted June 2010)
    - Software Assurance Evidence Metamodel (SAEM)
    - Argumentation Metamodel (ARM)
- Architected with a focus on providing fundamental improvements in analysis

Plans to Expand SwA Ecosystem Standards

- Two key models in Extending the Assurance Case
  - – Assurance Traceability Model (ATM)
    - Connects evidence to high level policy
  - – Common Fact Model (CFM)
    - Connects system artifacts to evidence

SwA Ecosystem Implementations

- KDM Analytics Tool Output Integration Framework (TOIF)
  - An Small Business Innovation Research (SBIR) effort through DHS
  - One of the key challenges is that analysis solution consists of multiple tools, information sources and services that are currently fragmented lacking intuitive and efficient integration due to
    - *Inconsistency in the nomenclature* of reported vulnerabilities caused by ambiguity of vulnerability definitions (*inconsistency in interpretation of CWE instances)*
    - *Lack of agreement* on what are the parts of vulnerability to report – *what constitutes vulnerability report*
    - *Lack of interoperability* that is based on common definition of system artifacts

TOIF Technological Achievements

- Creating next-generation composite vulnerability analysis tool on top of existing off-the-shelf vulnerability detection tools
- Improving the breadth and accuracy of vulnerability analysis
- Improving the rigor of assessments by bringing vulnerability detection into architecture context
- Normalizing vulnerability reporting protocols
- Leveraging OMG Software Assurance Ecosystem standards and formalizations of CWE content

TOIF SBIR Deliverables

- A ready-to-use *open source composite vulnerability analyzer* integrating 5 existing open source vulnerability detection tools
- Integrating proprietary architecture analysis tool
- A protocol for exchanging vulnerability findings
- *Blueprints for adaptors* of the protocol
- Practical *usability and accuracy data* based on the case study

CWE Formal Definition

- Code generation based upon formal definitions of Common Weakness Enumerations
  - ~20 CWEs formally defined
  - Test Case generation tool produces thousands of test cases based on weakness variants and code complexities
  - ~50 CWE general “patterns” identified

Other SwA Ecosystem Implementations

- Hatha Systems (code, architecture, process analysis)
- Benchmark Consulting (Code Generation)
- European Firms

Tool Evaluation

- SAMATE
  - 60,000 C,”C++ and Java test Cases (177 unique CWEs) to be added to SAMATE
    - NIST is making those tests publicly available
    - Integrating those tests into the SAMATE Reference Dataset (SRD)
    - Richard Struse to introduce XML Schema for Tool Compatibility Claims against CWEs at SATE IV Planning Meeting tomorrow morning

Making Security Measurable

- Bob Martin, MITRE
  - Contributions to the Cyber Ecosystem
    - Enumerations
    - Metrics
    - Current activities