SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

15 October 2008

# DHS-DoD-DoC Software Assurance Forum Technology, Tools and Product Evaluation Working Group Status Briefing

Co-chairs

Michael Kass (NIST)
Larry Wagoner (NSA)

October 15, 2008

# *TT&PE Working Group Goal*

- *To assist in bringing software assurance (SwA) 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.*
- Current state of SwA technology and tools is “stovepipe” in nature, making a tool-based argument for software assurance difficult:
  - Tools use different terminology and definitions for software weaknesses
  - Software assurance tools vary in their capabilities , tool users need a way to measure and compare them
  - Standards are needed to bring software assurance tools and technology into one “eco-system” to create a full solution that supports the assurance case

# *TT&PE Working Group Actions*

- Develop a Common Weakness Enumeration (CWE)
- Develop a Common Attack Pattern Enumeration and Classification (CAPEC)
- Measure and Evaluate SwA Tool Effectiveness (SAMATE)
- Support SwA Tool Interoperability, Testing and Integration with the Assurance Case through OMG/ISO Standards

# *Common Weakness Enumeration (CWE)*

- A DHS-sponsored, community-developed dictionary of software weakness types that provides a unified, measurable set of software weaknesses that will enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses
- Available online at http://cwe.mitre.org
- Contains ~700 descriptions and associated information for weaknesses introduced anywhere in the software development lifecycle

# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

## *CWE on the web at http://cwe.mitre.org*

# Common Weakness Enumeration

*A Community-Developed Dictionary of Software Weakness Types*

Search by ID: Go

**CWE List**
- Full Dictionary View
- Development View
- Research View
- Reports

**About**
- Sources
- Process
- Documents

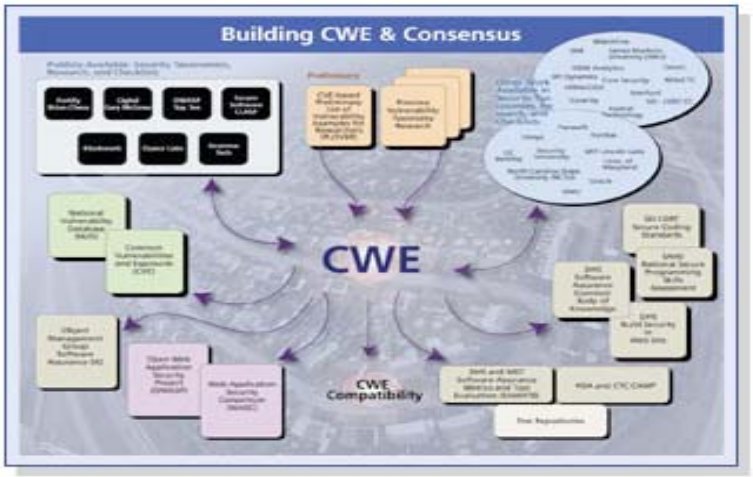
**Community**
- Related Activities
- Discussion List
- Research

**News**
- Calendar
- Free Newsletter

**Compatibility**
- Program
- Requirements
- Declarations
- Make a Declaration

**Contact Us**
- Search the Site

**International in scope and free for public use, CWE™ provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.**




**News**

- CWE Version 1.0 Now Available
- Cenzic, Inc. Makes Two CWE Compatibility Declarations
- CWE Compatibility Used as Feature to Compare Products in *Software Development Times*
- Making Security Measurable table booth at *Security Automation Conference 2008*

...more

**Upcoming Events**

- CWE briefing at *DHS/DoD SwA Forum*, October 14-16
- CWE/Making Security Measurable briefing at *MILCOM 2008*, Nov 17-19

...more

**Status Report**

Version 1.0 posted September 9, 2008. Updates include new major views, including "Research Concepts" and "Development Concepts"; more PDF graphs; several new white papers on CWE; an improved and stabilized schema; 39 new entries; and modifications to every CWE entry. Review the Major Changes and Difference Reports.

**More Information**

cwe@mitre.org

# *CWE Content*

**Identifying Information**

- CWE ID
- Name

**Describing Information**

- Description
- ***Extended Description***
- Alternate Terms
- Demonstrative Examples
- Observed Examples
- Context Notes
- Source Taxonomy
- References
- ***Whitebox Definition***
- ***Blackbox Definition***
- ***Formal Definition***

**Scoping & Delimiting Information**

- Type
- Functional Area
- Likelihood of Exploit
- Common Consequences
- Enabling Factors for Exploitation
- Common Methods of Exploitation
- Applicable Platforms
- Time of Introduction

**Prescribing Information**

- Potential Mitigations

*The Common Attack Pattern Enumeration and Classification (CAPEC)*

- **CAPEC** is sponsored by the Department of Homeland Security as part of the Software Assurance strategic initiative of the National Cyber Security Division. The objective of this effort is to provide a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy

# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

***CAPEC on the web at http://capec.mitre.org***

CAPEC

## Common Attack Pattern Enumeration and Classification

**A Community Knowledge Resource for Building Secure Software**

Home > CAPEC List | View the CAPEC List

**CAPEC List**
- Full CAPEC Dictionary
- Classification Tree
- Other Views

**About CAPEC**
- Documents
- Resources

**Community**
- Related Activities
- Collaboration List

**Contact Us**
- Search the Site

## CAPEC View by Classification (Release 1.1)

The Common Attack Pattern Enumeration and Classification (CAPEC), is a list of common attack patterns. Creating the list is a community initiative. Together, these organizations and any others that wish to join the effort, are creating specific and succinct definitions for each of the elements in the CAPEC List. By leveraging the widest possible group of interests and talents we hope to ensure that the CAPEC elements are adequately described and differentiated. The next steps are to adequately capture the specific effects, behaviors, exploit mechanisms, and implementation details in the CAPEC dictionary as well as to review and revise the presentation approaches that will best suit this information.

### CAPEC View by Classification (Release 1.1)

Expand All | Collapse All

Common Attack Pattern Enumeration and Classification
- ⊞ Abuse of Functionality
- ⊞ Spoofing
- ⊞ Probabilistic Techniques
- ⊞ Exploitation of Authentication
- ⊞ Resource Depletion
- ⊞ Exploitation of Privilege/Trust
- ⊞ Injection (Injecting Control Plane content through the Data Plane)
- ⊞ Data Structure Attacks
- ⊞ Data Leakage Attacks
- ⊞ Resource Manipulation
- ⊞ Time and State Attacks

Search by ID

**Section Contents**
- CAPEC List
  - Full CAPEC Dictionary
  - Classification Tree
- Download
  - Other Views

BACK TO TOP

# CAPEC Primary Attack Pattern Content

- Attack Pattern ID
- Attack Pattern Name
- Description *(newly extended)*
- Related Weaknesses
- Related Vulnerabilities
- Methods of Attack
- Examples-Instances
- References
- Solutions and Mitigations
- Typical Severity
- Typical Likelihood of Exploit
- Attack Prerequisites
- Attacker Skill or Knowledge Required
- Resources Required
- Attack Motivation-Consequences
- Context Description
- Purpose
- Confidentiality/Integrity/ Availability Impact
- Technical Context
- Keywords
- Pattern Abstraction Level
- Source

# CAPEC Status

- Web site contains the initial set of content and will continue to evolve with public participation and contributions
- All current authored patterns (101) as well as all potential patterns in the attack taxonomy have been tagged
- Attack Pattern multi-level abstraction tagging
  - Meta
  - Standard
  - Detailed

# *Software Assurance Metrics and Tool Evaluation*

- NIST SAMATE project co-sponsored with DHS to:
  - Measure of the effectiveness of today's software assurance tools
  - Identify gaps in technology and make recommendations to DHS for areas of research
  - Define metrics for the measurement of software assurance tool effectiveness

# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

***SAMATE on the web at http://samate.nist.gov/***

NIST National Institute of Standards and Technology

DHS National Cyber Security Division

article | discussion | edit | history

**NAVIGATION**

- Main Page
- Tools
- Resources
- Bibliography
- SRD
- Group Pages
- Help

**SEARCH**

Google™ Custom Search

Search

**TOOLBOX**

- What links here
- Related changes
- Special pages

# Main Page

## SAMATE - Software Assurance Metrics And Tool Evaluation [edit]

Welcome to the NIST SAMATE* project. This is sponsored by the U.S. Department of Homeland Security (DHS) National Cyber Security Division and NIST.

This project supports the DHS Software Assurance Tools and R&D Requirements Identification Program. The objective of part 3, Technology (Tools and Requirements) is the identification, enhancement and development of software assurance tools. NIST is leading in (A) testing software evaluation tools, (B) measuring the effectiveness of tools, and (C) identifying gaps in tools and methods.

For us, Software Assurance (SA) is

> ... the planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures
>
> from NASA Software Assurance Guidebook and Standard (see quality assurance (1) in IEEE 610.12)

to help achieve

- Trustworthiness - No exploitable vulnerabilities exist, either of malicious or unintentional origin
- Predictable Execution - Justifiable confidence that software, when executed, functions as intended

# *SAMATE Work to Date*

- **SAMATE products include:**
  - **SAMATE Reference Dataset (SRD) of tool tests**
    - An online repository of thousands of discrete tool tests (C, C++ and Java source code to date)
    - Tests based upon interpretation of current software weakness definitions
    - Contributed by NIST, academia, tool developers
  - **SwA Tool Functional Specifications** (NIST Special Publications 500-268,500-269) for source code analyzers and web application scanner tools respectively
  - **Papers**
    - Building a Test Suite for Web Application Scanners
    - Software Assurance with SAMATE Reference Dataset, Tool Standards, and Studies
    - Effect of Static Analysis Tools on Software Security: Preliminary Investigation

# SAMATE Work to Date (cont.)

- **SAMATE products (cont.)**
  - **Automated Source Code Analyzer Test Case Generation**, using formal CWE definitions to auto-generate source code tests and provide additional testing coverage
    - Based on formal white-box definitions of software weaknesses
    - Generated tests for 27 CWEs
    - Long term, automated test case generation will cover many CWEs
  - **The Static Analysis Tool Exposition (SATE)** – "Real-world" source code used to represent the more complex problems facing today's SwA tools
    - 9 tool developers participating
    - Results reported by developers at Static Analysis Workshop (June 2008)
    - SATE 2009 planning underway

# *TT&PE Standards Activity*

- **TT&PE supports the software assurance "ecosystem"** to provide an interoperability framework for automated tool technology in support of the assurance case
  - TT&PE members are involved in the development of OMG Standards that facilitate SwA tool interoperability through technical-level formalization:
    - ***The OMG Knowledge Discovery Metamodel (KDM)*** specification defines a meta-model for representing information related to existing software assets and their operational environments
      - This facilitates technical-level formalization of "white-box" definitions of CWEs that can be used to verify the presence or absence of those CWEs in an application
      - KDM 1.1 is now published

# TT&PE Standards Activity

- OMG KDM Specification is being implemented, evaluated and aligned with other standards through (respectively):
  - CWE formalization (sponsored by DHS and DoD)
  - Tool test case generation and validation(through SAMATE) and KDM-enabled tool interoperability demonstrations
  - Alignment with ISO/IEC 15026 “Systems and Software Assurance”

# TT&PE Standards Activity

- Software Assurance Metamodel (SAM) - Broken down in 2 parts
  - Argumentation Metamodel
    - related to representation of Claims and Arguments – Request for Comments on Submitted Spec will be published in March 2009
  - Evidence Metamodel
    - Joint Submission presented - completion date set for the end of 2009
    - It consists of 3 major parts: core framework, imported ontology and audit (signing authority) information

# SwA Landscape Resources

- Recent addition to Ecosystem is Software Metrics Metamodel (SMM)
  - Beside presenting measurement and metrics information group will focus on defining libraries of metrics that support decision making in area of modernization, quality and security assurance
- New work started in area of Governance of Assurance Cases (ACs) titled Management of Regulations and Compliance (MRC) focusing on
  - Decision making process for AC
  - Dependences and correlation of multiple ACs
  - Risk assessment process

# *Collaboration with SwA Metrics WG*

- Measurement, what it means for TTPE
  - Can be used for:
    - Tool/Technology Product Comparison
    - Service provider benchmarking
    - Analysis tool for improvement of tools and technology, analysis tool for SwA improvement
    - Communicate tool/technology goodness to users, communicate security of software through tool output
  - Follow-up:
    - Meet with Measurement WG to drill down into these areas

# *Next TTPE WG Meeting in December*

- Discuss progress on TTPE projects
- Continue discussion with Metrics W/G
- Present new work in TTPE