Being Explicit About Weaknesses

Robert A. Martin - MITRE
Sean Barnum - Cigital
Steve Christey - MITRE

1 March 2007
Software Security Assurance

Don't Let Your Applications Get You Down

Exploited software flaws cost the U.S. financial services industry more than $3 billion per year, according to the National Institute of Standards & Technology.

BY JOHN K. WATERS

Most enterprises have figured out the importance of software and information security, although essential to their respective bottom lines, no longer provide adequate protection. Hackers and other security threats are increasingly concentrating on exploiting vulnerabilities in applications.

These vulnerabilities are costing businesses a fortune. According to the National Institute of Standards & Technology, companies are spending $3 billion a year on software and information security.

Part of the problem is the changing nature of enterprises. Attackers now attack Internet-based services that are now connected to customers, partners, and suppliers. The Web.

Another part of the problem is the nature of development. As applications become more and more complex, security professionals are faced with the challenge of integrating security into the development process. The DoD Software Engineering News.

Secure Software Engineering

The DoD Software Engineering News.

Procurement is key to security, IT execs say

Procurement officers have the power to significantly improve the security of government IT systems by including software reliability and security requirements in the contracts they award to vendors—and strengthening the country's cyber-infrastructure in the process.

By PATIENCE WAIT | GCN STAFF

That key message was hammered home repeatedly at a two-day forum earlier this month hosted jointly by the Defense and Homeland Security departments.

“We have to shift the paradigm from patch management to software assurance,” said Andy Pardy, acting director of DHS National Cyber Security Division.

Vendors will not invest in improving the quality of their software if their own vulnerabilities, said Francella Gaitlin, deputy CIO and deputy assistant secretary of Defense for networks and information integration.

“We’ve got to use acquisition organizations to put together a software assurance policy. We have to make sure it’s part of the way we buy.”


SC MAGAZINE

Nominations are now open. Click here to go to SC Magazine Asia Pacific.

Latest News

Software quality, FISMA top federal CISO concerns

By Marco Savage

[Mon, Aug 29, 2005] Software quality and FISMA compliance topped a list of concerns expressed by federal CISOs in a recent survey.

Conducted by Intelligent Decisions, a Washington, D.C.-based systems integrator, the survey of 29 federal CISOs ranked increased software quality assurance as the top area that the private sector needs to focus on.

26 eWEEK | JUNE 27 / JULY 4, 2005
Software Assurance

**Background**
- In October 2002, the President’s Critical Infrastructure Protection Board (PCIPB) created the National Security Agency (NSA) led IT Security Study Group (ITSSG) to review existing IT acquisition processes.
- In July 2003, the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) established the Software Assurance initiative to examine software assurance issues.
- On 23 Dec 04, Undersecretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) and ASD(NII) established a Software Assurance (SwA) Tiger Team to:
  - Develop a holistic strategy to reduce SwA risks within 90 days
  - Provide a comprehensive briefing of findings, strategy and plan
- Tiger Team presented its strategy to USD(AT&L) and ASD(NII) on March 28, and on May 2 was tasked to proceed with 180 day Implementation Phase.

**Requirements**
- What functional statements in OSD Guidance for SwA requirements best enable optimal vendor solutions?
  - Require higher level written policy to specify need for SwA requirements
  - “Compelling arguments and evidence that...commensurate with risk”
- Written SwA Principles in policy
  - Looked at 8500, 5002.2.6, 6000, 5170, 6212, ...
  - In 8500.2 Annex language to potentially leverage for SwA:
    - “...use IA best practices,...”
    - “...software will be well-behaved...”
    - Point to language in contracts
  - Contract language to show equivalence to ISO 15026 practices
  - Burden on PMO to understand and have confidence in level of SwA
- Requirement in policy that whenever a new risk is ID’d or an old risk changes, contractor must be notified

**Basis for SwA Technology**
- Offensive side
  - Pedigree problem
  - Interconnectivity
  - Value of IT information
  - Many untrusted
- Defensive side
  - Fragmented efforts
  - Immature science
  - Lack of resources

**Driving Needs for Software Assurance**
- Software vulnerabilities jeopardize intellectual property, business operations and services, infrastructure operations, and compliance
- Growing awareness and concern over the ability of an adversary to subvert the software supply chain
  - Federal Government relies on COTS products and commercial devices foreign and non-operating domestic suppliers to meet majority of IT needs
  - Software development offers opportunities to insert malicious code at design and build software enabling exploitation
- Growing concern about inadequacies of supplier’s capabilities and deliver software with required levels of integrity
  - Current education & training provides too few practitioners with required competencies in secure software engineering
  - Concern about suppliers not exercising “minimum level of responsibility”
  - Growing need to improve both the state-of-the-practice and the state-of-software capabilities of the nation
- Processes and technologies are required to build trust into software acquired and used by Government and critical infrastructure

**Software Assurance (SwA) Definition**
Software assurance (SwA) is the level of confidence that software is free of exploitable vulnerabilities, either intentionally or unintentionally designed as part of the software or inadvertently created.
Motivation for Classes of Software Security Flaws & Vulnerabilities

- For Systematic Study – classify security problems in software into categories that one can dissect for systematic study.
- For SS Tools Evaluation – a taxonomy of security vulnerability that the SA community would agree upon will be essential for evaluating Software Security (SS) tools and classifying SA functions.
- For SRD Development – Classes of software security flaws and vulnerabilities is one of resources to drive a standard reference dataset, which, in simply put, is a benchmark test suite for Software Security tools.

Possible Goals of Classifying Software Security Flaws & Vulnerabilities

- A taxonomy that has classification categories with the satisfactory characteristics as possible.
- Incorporate commonly used terms in security vulnerabilities that occurred in modern days.
- Consensus from the SA community.
SSATM

Information Technology Laboratory
Software Diagnostics and Conformance Testing Division

Workshop on
Software Security Assurance Tools, Techniques, and Metrics

PROGRAM

November 7, 2005
8:30 – 9:00 : Welcome – Paul E. Black
9:00 – 10:30 : Tools and Metrics - Liz Fong
- Where do Software Security Assurance Tools Add Value? – David Jackson, David Cooper
- Metrics that Matter – Brian Chess
- The Case for Common Flaw Enumeration – Robert Martin, Steven Christey, Joe Jarzombek
10:30 – 11:00 : Break
11:00 – 12:30 : Flaw Taxonomy and Benchmarks - Robert Martin
- Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors – Katrina Tsipenyuk, Brian Chess, Gary McGraw
- A Taxonomy of Buffer Overflows for Evaluating Static and Dynamic Software Testing Tools – Kendra Kratkiewicz, Richard Lippmann
- ABM – A Prototype for Benchmarking Source Code Analyzers – Tim Newsham, Brian Chess

[edit]
Goal of the Common Weakness Enumeration Initiative

- To improve the quality of software with respect to known security issues within source code
  - define a unified measurable set of weaknesses
  - enable more effective discussion, description, selection and use of software security tools and services that can find these weaknesses
Clarifying software weaknesses: Enabling communication (1 of 2)

- Systems Development Manager Issue Areas:
  - What are the software weaknesses I need to protect against
    - Architecture, design, code
  - Can I look through the issues by technologies, risks, severity
  - What have the pieces of my system been vetted for?
    - COTS packages, organic development, open source
  - Identify tools to vet code based on tool coverage
    - How effective are the tools?

- Assessment Tool Vendors Issue Areas:
  - Express what my tool does
  - Succinctly identify areas I should expand coverage
Clarifying software weaknesses:

Enabling communication (2 of 2)

- COTS Product Vendor Issue Areas:
  - What have I vetted my applications for?
  - What do my customers want me to vet for?
- Researcher Issue Areas:
  - Quickly understand what is known
  - Easily identify areas to contribute/refine/correct
- Educator Issue Areas:
  - Train students with the same concepts they’ll use in practice
- Operations Manager Issue Areas:
  - What issues have my applications been vetted for? (COTS/Organic/OS)
  - What types of issues are more critical for my technology?
  - What types of issues are more likely to be successfully exploited?
CWE Launched March 2006 with draft 1, now at draft 5
Building Consensus About A Common Enumeration

Common Weakness Enumeration (CWE)
- call & count the same
  ● enable metrics

- Previously Published Vulnerability Taxonomy Work
- CVE's Checklist and Taxonomy
- Secure Software's John Viega's CLASP and Taxonomy
- Microsoft's Mike Howard's Work and Taxonomy
- OWASP's Checklist and Taxonomy
- Cigital's Gary McGraw's Work and Taxonomy
- Fortify's Brian Chess's Work and Taxonomy
- Klocwork's Checklist and Taxonomy
- Ounce Lab's Checklist and Taxonomy
- Gramma Tech's Checklist and Taxonomy
- Watchfire's Security Institute's Checklist and Taxonomy
- SPI Dynamics' KDM Analytics' Checklist and Taxonomy
- Core Security's JMU's Checklist and Taxonomy
- SEI's IBM's Checklist and Taxonomy
- NSA/CTC's MIT LL's Checklist and Taxonomy
- Unisys's Kestrel Technology's Checklist and Taxonomy
- Cenzi's Coverity's Checklist and Taxonomy
- Oracle's Parasoft's Checklist and Taxonomy
- GMU's Stanford's Checklist and Taxonomy
- UC Berkeley's Purdue's Checklist and Taxonomy
- Common Weakness Enumeration (CWE)

 Dictionary
CVE Growth

Status (as of Feb 1, 2007)
• 21,990 unique CVE names
Vulnerability Type Trends: A Look at the CVE List (2001 - 2006)

• 15% "other"
But…

- What about the 15% “Other” in 2006?
  - What is up-and-coming? What’s important but below the radar?
- Variants matter in evaluating software quality
  - Example: obvious XSS vs. non-standard browser behaviors that bypass filters
- Bug X might be “resultant from” or “primary to” Bug Y, yet both are thought of as vulnerabilities
  - E.g. integer overflows leading to buffer overflows
  - How can we tell if things are improving?
- Maybe some issues are symptoms of deeper problems
  - Error: Couldn’t open file “lang-
    <SCRIPT>alert(‘XSS’)</SCRIPT>.txt”
Removing and Preventing the Vulnerabilities Requires More Specific Definitions…

Cross-site scripting (XSS):
- Basic XSS
- XSS in error pages
- Script in IMG tags
- XSS using Script in Attributes
- XSS using Script Via Encoded URI Schemes
- Doubled character XSS manipulations, e.g. ‘<script’
- Invalid Characters in Identifiers
- Alternate XSS syntax

Buffer Errors
- Unbounded Transfer (‘classic overflow’)
- Write-what-where condition
- Boundary beginning violation (‘buffer underwrite’)
- Out-of-bounds Read
- Wrap-around error
- Unchecked array indexing
- Length Parameter Inconsistency
- Other length calculation error
- Miscalculated null termination
- String Errors

Relative Path Traversal
- Path Issue - dot dot slash - ‘..//filedir’
- Path Issue - leading dot dot slash - ‘/..//filedir’
- Path Issue - leading directory dot dot slash - ‘/directory/..//filename’
- Path Issue - directory doubled dot dot slash - ‘directory/..//filename’
- Path Issue - dot dot backlashslash - ‘..\filename’
- Path Issue - leading dot dot backlashslash - ‘..\filename’
- Path Issue - leading directory dot dot backlashslash - ‘directory\..\filename’
- Path Issue - directory doubled dot dot backlashslash - ‘directory\..\filename’
- Path Issue - triple dot - ‘…’
- Path Issue - multiple dot - ‘….’
- Path Issue - doubled dot dot slash - ‘..../’
- Path Issue - doubled triple dot slash - ‘.../.../’
... which led to the Preliminary List of Vulnerability Examples for Researchers (PLOVER)

- Initial goal: extend vulnerability auditing checklist
- Collected extensive CVE examples
  - Emphasis on 2005 and 2006
  - Reviewed all issues flagged "other"
- 300 weakness types, 1500 real-world CVE examples
- Identified classification difficulties
  - Primary vs. resultant vulns
  - Multi-factor issues
  - Uncategorized examples
  - Tried to separate attacks from vulnerabilities
- Beginning vulnerability theory
  - Properties
  - Manipulations
  - Consequences

- One of the 3 major sources of CWE
PLOVER:
300 “types” of Weaknesses, 1500 real-world CVE examples

<table>
<thead>
<tr>
<th>Code</th>
<th>Category Description</th>
<th>Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>[BUFF]</td>
<td>Buffer overflows, format strings, etc.</td>
<td>10 types</td>
</tr>
<tr>
<td>[SVM]</td>
<td>Structure and Validity Problems</td>
<td>10 types</td>
</tr>
<tr>
<td>[SPEC]</td>
<td>Special Elements (Characters or Reserved Words)</td>
<td>19 types</td>
</tr>
<tr>
<td>[SPECM]</td>
<td>Common Special Element Manipulations</td>
<td>11 types</td>
</tr>
<tr>
<td>[SPECTS]</td>
<td>Technology-Specific Special Elements</td>
<td>17 types</td>
</tr>
<tr>
<td>[PATH]</td>
<td>Pathname Traversal and Equivalence Errors</td>
<td>47 types</td>
</tr>
<tr>
<td>[CP]</td>
<td>Channel and Path Errors</td>
<td>13 types</td>
</tr>
<tr>
<td>[CCC]</td>
<td>Cleansing, Canonicalization, and Comparison Errors</td>
<td>16 types</td>
</tr>
<tr>
<td>[INFO]</td>
<td>Information Management Errors</td>
<td>19 types</td>
</tr>
<tr>
<td>[RACE]</td>
<td>Race Conditions</td>
<td>6 types</td>
</tr>
<tr>
<td>[PPA]</td>
<td>Permissions, Privileges, and ACLs</td>
<td>20 types</td>
</tr>
<tr>
<td>[HAND]</td>
<td>Handler Errors</td>
<td>4 types</td>
</tr>
<tr>
<td>[UI]</td>
<td>User Interface Errors</td>
<td>7 types</td>
</tr>
<tr>
<td>[INT]</td>
<td>Interaction Errors</td>
<td>7 types</td>
</tr>
<tr>
<td>[INIT]</td>
<td>Initialization and Cleanup Errors</td>
<td>6 types</td>
</tr>
<tr>
<td>[RES]</td>
<td>Resource Management Errors</td>
<td>11 types</td>
</tr>
<tr>
<td>[NUM]</td>
<td>Numeric Errors</td>
<td>6 types</td>
</tr>
<tr>
<td>[AUTHENT]</td>
<td>Authentication Error</td>
<td>12 types</td>
</tr>
<tr>
<td>[CRYPTO]</td>
<td>Cryptographic errors</td>
<td>13 types</td>
</tr>
<tr>
<td>[RAND]</td>
<td>Randomness and Predictability</td>
<td>9 types</td>
</tr>
<tr>
<td>[CODE]</td>
<td>Code Evaluation and Injection</td>
<td>4 types</td>
</tr>
<tr>
<td>[ERS]</td>
<td>Error Conditions, Return Values, Status Codes</td>
<td>4 types</td>
</tr>
<tr>
<td>[VER]</td>
<td>Insufficient Verification of Data</td>
<td>7 types</td>
</tr>
<tr>
<td>[MAID]</td>
<td>Modification of Assumed-Immutable Data</td>
<td>2 types</td>
</tr>
<tr>
<td>[MAL]</td>
<td>Product-Embedded Malicious Code</td>
<td>7 types</td>
</tr>
<tr>
<td>[ATTMIT]</td>
<td>Common Attack Mitigation Failures</td>
<td>3 types</td>
</tr>
<tr>
<td>[CONT]</td>
<td>Containment errors (container errors)</td>
<td>3 types</td>
</tr>
<tr>
<td>[MISC]</td>
<td>Miscellaneous WIFFs</td>
<td>7 types</td>
</tr>
</tbody>
</table>
Vulnerability Theory:
Problem Statement and Rationale

- With 600+ variants, what are the main themes?
- Why is it so hard to classify vulnerabilities cleanly?
  - CWE, Pernicious Kingdoms, OWASP, others have had similar difficulties
- Same terminology used in multiple dimensions
  - Frequent mix of attacks, threats, weaknesses/faults, consequences
  - E.g. buffer overflows, directory traversal

- Goal: Increase understanding of vulnerabilities
  - Vocabulary for more precise discussion
  - Label current inconsistencies in terminology and taxonomy
  - Codify some of the researchers’ instinct

- One possible application: gap analysis, defense, and design recommendations
  - “Algorithms X and Y both assume input has property P. Attack pattern A manipulates P to compromise X. Would A succeed against Y?”
  - “Technology Z has properties P1 and P2. What vulnerability classes are most likely to be present?”
  - “Why is XSS so obvious but so hard to eradicate?”
Some Basic Concepts, By Example

Buffer overflow using long DNS response

1) Attacker (as user) sends directive over Telnet channel: “Log me in”
2) Server (the target) sends directive over DNS channel: “Tell me IP’s hostname”
3) DNS consultant (controlled by attacker) returns hostname with property “>300 BYTES”
4) Buffer overflow activated
Artifact Labels

- **Interaction Point**
  - A relevant point within the product where a user interacts with the product
- **Intermediate Fault**
  - A behavior by the product that has not yet affected correctness, but will
- **Control Transfer Point**
  - The point where the program’s behavior changes from correct to incorrect
- **Activation Point**
  - The point where the “payload” is activated and performs the actions intended by the attacker
- **Resultant Fault**
  - A fault after a “Primary” fault that is also where incorrect behavior occurs
Artifact Labels - Example

1. \texttt{print HTTPResponseHeader;}
2. \texttt{print \textasciitilde\textasciitilde<title>Hello World</title>\textasciitilde\textasciitilde;}
3. \texttt{ftype = HTTP_Query_Param\textasciitilde\textasciitilde(type);}
4. \texttt{str = \\textasciitilde/tmp\	extasciitilde;}
5. \texttt{strcat(str, ftype); strcat(str, \textasciitilde..dat\textasciitilde;};}
6. \texttt{handle = fileOpen(str, \textasciitilde"read"\textasciitilde;);}
7. \texttt{while((line=readFile(handle)))}
8. \{ 
9. \texttt{line=stripTags(line, \textasciitilde"script"\textasciitilde;);}
10. \texttt{print line;}
11. \texttt{print \textasciitilde<br>
12. \texttt{close(handle);}
Building Consensus About A Common Enumeration

Common Weakness Enumeration (CWE)
- call & count the same
  ● enable metrics
Where Did We Start?

★ Objective: To identify, integrate and effectively describe common software weaknesses known to the industry and software assurance community

★ Leveraging taxonometric approach for list integration
  – Identify and review dozens of existing taxonomies
    ■ Academic and professional (Aslam, RISOS, Landwehr, Bishop, Protection Analysis, etc)
    ■ High level lists
      – OWASP Top 10, 19 Deadly Sins, WASC, etc.
    ■ In-depth practical
      – PLOVER, CLASP, 7 Pernicious Kingdoms
  – Create visualizations for effective comparison and analysis
  – Integrating taxonomies
    ■ Normalizing and deconfliction
    ■ Finding a proper balance between breadth & depth
Formalizing a Schema for Weaknesses

**Identifying Information**
- CWE ID
- Name

**Describing Information**
- Description
- Alternate Terms
- Demonstrative Examples
- Observed Examples
- Context Notes
- Source
- References

**Scoping & Delimiting Information**
- Functional Area
- Likelihood of Exploit
- Common Consequences
- Enabling Factors for Exploitation
- Common Methods of Exploitation
- Applicable Platforms
- Time of Introduction

**Prescribing Information**
- Potential Mitigations

**Enhancing Information**
- Weakness Ordinality
- Causal Nature
- Related Weaknesses
- Taxonomy Mapping
- Research Gaps
CWE-79  Cross-site scripting (XSS)

[CWE-79 Cross-site scripting (XSS) from cwe.mitre.org/data/definition/79.html]
CWE Cross-Section: 20 of the Usual Suspects

- Absolute Path Traversal (CWE-36)
- Cross-site scripting (XSS) (CWE-79)
- Cross-Site Request Forgery (CSRF) (CWE-352)
- CRLF Injection (CWE-93)
- Error Message Information Leaks (CWE-209)
- Format string vulnerability (CWE-134)
- Hard-Coded Password (CWE-259)
- Insecure Default Permissions (CWE-276)
- Integer overflow (wrap or wraparound) (CWE-190)
- OS Command Injection (shell metacharacters) (CWE-78)
- PHP File Inclusion (CWE-98)
- Plaintext password Storage (CWE-256)
- Race condition (CWE-362)
- Relative Path Traversal (CWE-23)
- SQL injection (CWE-89)
- Unbounded Transfer ('classic buffer overflow') (CWE-120)
- UNIX symbolic link (symlink) following (CWE-61)
- Untrusted Search Path (CWE-426)
- Weak Encryption (CWE-326)
- Web Parameter Tampering (CWE-472)
CWE Cross-Section: 22 More Suspects

- **Design-Related**
  - High Algorithmic Complexity (CWE-407)
  - Origin Validation Error (CWE-346)
  - Small Space of Random Values (CWE-334)
  - Timing Discrepancy Information Leak (CWE-208)
  - Unprotected Windows Messaging Channel ('Shatter') (CWE-422)
  - Inherently Dangerous Functions, e.g. gets (CWE-242)
  - Logic/Time Bomb (CWE-511)

- **Low-level coding**
  - Assigning instead of comparing (CWE-481)
  - Double Free (CWE-415)
  - Null Dereference (CWE-476)
  - Unchecked array indexing (CWE-129)
  - Unchecked Return Value (CWE-252)
  - Path Equivalence - trailing dot - 'file.txt.' (CWE-42)

- **Newer languages/frameworks**
  - Deserialization of untrusted data (CWE-502)
  - Information leak through class cloning (CWE-498)
  - .NET Misconfiguration: Impersonation (CWE-520)
  - Passing mutable objects to an untrusted method (CWE-375)

- **Security feature failures**
  - Failure to check for certificate revocation (CWE-299)
  - Improperly Implemented Security Check for Standard (CWE-358)
  - Failure to check whether privileges were dropped successfully (CWE-273)
  - Incomplete Blacklist (CWE-184)
  - Use of hard-coded cryptographic key (CWE-321)

... and about 550 more
Where Are We Today?

Quality
- “Kitchen Sink” – In a good way
  - Many taxonomies, products, perspectives
  - Varying levels of abstraction
    - Directory traversal, XSS variants
- Mixes attack, behavior, feature, and flaw
  - Predominant in current research vocabulary, especially web application security
  - Complex behaviors don’t have simple terms
  - New/rare weaknesses don’t have terms

Quantity
- Draft 5 - over 600 entries
- Currently integrating content from top 15 – 20 tool vendors and security weaknesses “knowledge holders” under NDA

Accessibility
- Website is live with:
  - Historical materials, papers, alphabetical full enumeration, taxonomy HTML tree, CWE in XML, ability to URL reference individual CWEs, etc
Using A Unilateral NDA with MITRE to Bring in Info

Purpose:
- Sharing the proprietary/company confidential information contained in the underlying Knowledge Repository of the Knowledge Owner’s Capability for the sole purpose of establishing a public Common Weakness Enumeration (CWE) dictionary that can be used by vendors, customers, and researchers to describe software, design, and architecture related weaknesses that have security ramifications.
- The individual contributions from numerous organizations, based on their proprietary/company-confidential information, will be combined into a consolidated collection of weakness descriptions and definitions with the resultant collection being shared publicly.
- The consolidated collection of knowledge about weaknesses in software, design, and architecture will make no reference to the source of the information used to describe, define, and explain the individual weaknesses.
Coverage of CWE
Covered CWEs - By Number of Tools

- 67% covered CWEs
- 20% covered CWEs
- 9% covered CWEs
- 2% covered CWEs
- 1% covered CWEs
- 1% covered CWEs

Legend:
- red: one
- yellow: two
- green: three
- blue: four
- orange: five
- brown: six
Current Community Contributing to the Common Weakness Enumeration

- AppSIC
- Cenzic
- CERIAS/Purdue University
- CERT/CC
- Cigital
- CodescanLabs
- Core Security
- Coverity
- DHS
- Fortify
- IBM
- Interoperability Clearing House
- JHU/APL
- JMU
- Kestrel Technology
- KDM Analytics
- Klocwork
- McAfee/Foundstone
- Microsoft
- MIT Lincoln Labs
- MITRE
- North Carolina State University
- NIST

- NSA
- Oracle
- Ounce Labs
- OWASP
- Palamida
- Parasoft
- PolySpace Technologies
- proServices Corporation
- SecurityInnovation
- Secure Software
- Security University
- Semantic Designs
- SofCheck
- SPI Dynamics
- UNISYS
- VERACODE
- Watchfire
- WASC
- Whitehat Security, Inc.
- Tim Newsham

To join send e-mail to cwe@mitre.org
Planned Improvements - Content

- Metadata tagging
  - Language, OS, etc.
  - Time of Introduction
  - Vulnerability theory
  - Other ideas?

- Content cleanup
  - Consistent naming
  - Structural refactoring
  - Attack-centric wording (align to CAPEC)

- Formalization
  - SBVR
Planned Improvements - Site Usability

- **Search**
  - Select a subset of the catalog using any of the metadata
  - Display results and make available as XML
  - Predefined searches

- **Graphical Visualization**
  - Dynamic adjustment and navigation
  - Alternate taxonomies
Building Consensus About A Common Enumeration

Previously Published Vulnerability Taxonomy Work

Dictionary

Common Weakness Enumeration (CWE)
- call & count the same
  ● enable metrics

CVE-based PLOVER Work

Fortify’s Brian Chess’s Work and Taxonomy

CVE-based

Ounce Lab’s Checklist and Taxonomy

OWASP’s Checklist and Taxonomy

Gramma Tech’s Checklist and Taxonomy

Secure Software’s John Viega’s CLASP and Taxonomy

Microsoft’s Mike Howard’s Work and Taxonomy

Klocwork’s Checklist and Taxonomy

Core Security

GMU

Stanford

Purdue

Kestrel Technology

Oracle

KDM Analytics

Core Security

IBM

SEI

NSA/CTC

VERACODE

UC Berkeley

SPI Dynamics

Parasoft

Watchfire

Security Institute

KDM Analytics

JMU

Core Security

MIT LL

Unisys

Cenizc

UMD

NCSU

IBM

SEI

NSA/CTC

VERACODE

UC Berkeley

Purdue

SPI Dynamics

Parasoft

Watchfire

Security Institute

KDM Analytics

JMU

Core Security

MIT LL

Unisys

Cenizc

UMD

NCSU
CWE Compatibility and Effectiveness Program Launched

The CWE Compatibility and Effectiveness Program provides for a product or service to be reviewed and registered as officially "CWE-Compatible" and "CWE-Effective," thereby assisting organizations in their selection and evaluation of tools and/or services for assessing their acquired software for known types of weaknesses and flaws, for learning about the various weaknesses and their possible impact, or to obtain training and education about these issues. Organizations with products and services still working towards compatibility and effectiveness are also listed.

CWE-Compatible Products and Services must meet the first four (4) of the six (6) requirements below, while CWE-Effective Products and Services must meet all six (6) requirements. Please review the complete set of requirements to fully understand CWE compatibility and effectiveness.

- **CWE Searchable**: users may search security elements using CWE identifiers
- **CWE Output**: users may obtain security elements presented to users includes, or allows users to obtain, associated CWE identifiers
- **Mapping Accuracy**: security elements accurately linked to the appropriate CWE identifiers
- **CWE Documentation**: capability’s documentation describes CWE, CWE compatibility, and how CWE-related functionality is used
- **CWE Coverage**: the CWE identifiers that the capability is effective at locating in software
- **CWE Test Results**: results of assessing software for the CWEs are posted on the CWE Web site

See the [CWE Compatibility and Effectiveness Program](http://cwe.mitre.org/compatible/index.html) or email cwe@mitre.org for information on how to register your product(s) or service(s) as CWE-compatible or CWE-effective.
CWE Compatibility and Effectiveness Process Posted

CWE Compatibility and Effectiveness Program

Introduction
The CWE Compatibility and Effectiveness Program is a formal review and evaluation process for organizations wishing to declare their information security products and services as CWE-Compatible and CWE-Effective and have them formally evaluated.

Compatible and Effective products and services, as well as those working towards compatibility and effectiveness, will be posted on the "CWE-Compatible and Effective Products and Services" page on the CWE Web site and included on handouts at information security and related tool/tradeshow and events at which MITRE exhibits CWE (see the CWE Calendar).

The formal CWE Compatibility and Effectiveness Program includes three phases: Declaration, Evaluation, and Effectiveness.

Phase 1 – Declaration Phase
The Declaration Phase requires the completion of a short informational "CWE Compatibility Declaration Form" used to register an organization's declaration of intent with respect to CWE compatibility and effectiveness. In this phase you are asked to verify the compatibility and effectiveness requirements and then make a statement regarding whether your organization believes that its product or service currently fulfills the compatibility requirements, or if your organization is working towards fulfilling the requirements. This phase of the CWE compatibility and effectiveness program does not result in an official evaluation or assessment by MITRE; rather, MITRE only reviews the declaration. As long as the products or services are commercially or publicly available, the declaration and an endorsement quote from you (if desired) is posted on the CWE Web site.

Phase 2 – Evaluation Phase
The Evaluation Phase requires completion of Phase 1 with "yes" as the answer for support of CWE output, CWE searchable, and CWE documentation. You must also complete an extended "CWE Compatibility Requirements Evaluation Form" that is a more extensive CWE-compatible formal review and includes several evaluation activities. You will also receive the "Compatible Product/Service Organization Welcome Kit" with items for your Web site.

This formal evaluation process includes a "branding program" and logo to indicate successful completion of the compatibility portion of the compatibility and effectiveness evaluation. A major component of this phase requires specific details about how your organization has satisfied each of the mandatory requirements in the Requirements and Recommendations for CWE Compatibility and CWE Effectiveness Document. The Phase 2 "CWE Compatibility Requirements Evaluation Form" also requires the signature
CWE Compatibility and Effectiveness Requirements Posted

http://cwe.mitre.org/compatible/requirements.html
CWE-Compatible & CWE-Effective

CWE Compatible:
1. CWE-compatible “intent” declared
   - vendor with shipping product declares intent to add support for CWE ids
2. CWE-compatible “output and searchable” declared
   - vendor declares that their shipping product provides CWE ids and supports searching
3. CWE-compatible “mapping accuracy” compatibility questionnaire posted
   - questionnaire for mapping accuracy posted to CWE web site
4. CWE-compatible means it meets the following requirements:
   - Can find items by CWE id (CWE searchable)
   - Includes CWE id in output for each item (CWE output)
   - Explain the CWE functionality in their item’s documentation (CWE documentation)
   - Provided MITRE with “weakness” item mappings to validate the accuracy of the product or services CWE ids
   - Makes a good faith effort to keep mappings accurate

CWE-Effective:
1. CWE-effectiveness list posted
   - CWE ids that the tool is declaring “effectiveness for” is posted to CWE web site
2. CWE-effectiveness test results posted
   - CWE test cases obtained from NIST reference data set generator by tool owner
   - Scoring sheet for requested CWE test cases provided to MITRE by NIST
   - Tool results from evaluating CWE-based sample applications (CWE test cases) provided to MITRE for processing and posting
The Road Ahead for the CWE effort

- Finish the strawman dictionary/taxonomy
- Create a web presence
- Get NDAs with knowledgeable organizations
- Merge information from NDA’d sources
- Get agreement on the detailed enumeration
- Dovetail with test cases (NIST/CAS)
- Dovetail with attack patterns (Cigital)
- Dovetail with coding standards (SEI CERT/CC)
- Dovetail with BSI, CBK, OMG SwA SIG, ISO/IEC,...
- Create alternate views into the CWE dictionary
- Establish CWE Editorial Board (roles & members)
- Establish CWE Compatibility Requirements
- Collect CWE Compatible Declarations