
Being Explicit About Weaknesses

Robert A. Martin - MITRE

Sean Barnum - Cigital

Steve Christey - MITRE

1 March 2007



Software Security Assurance

SECURE

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 that antivirus software and intrusion detection systems, although essential to their overall security posture, no longer provide adequate protection. Black-hat hackers and other intruders are increasingly circumventing network security and exploiting loopholes in applications.

These vulnerabilities are costing enterprises a lot of money. The National Institute of Standards & Technology reports that companies are spending about \$60 billion a year on correcting software errors. Exploited software flaws cost the U.S. financial services industry more than \$3 billion per year, according to NIST.

Part of the problem is the changing nature of software development, says Gartner analyst John Pescatore. Databases once kept in centralized data centers and accessed only by apps within the enterprise's security perimeter are now connected to customers, partners and suppliers through the Web.

Another part of the problem is the nature of software development, he says. Application development or testing are rewarded for delivering features and meeting deadlines, so developers tend to focus on those things. Consequently, security becomes an afterthought, and developers address vulnerabilities only if they are discovered after an application has been developed.

Not doing the security work up front can quickly become expensive. Gartner figures it's 50 times more costly to fix a vulnerability after it's been discovered than it is to fix it before the software is released.

www.adtmag.com

The DoD SoftwareTech NEWS

Secure Software Engineering

www.dodmag.com

PHOTO-ILLUSTRATION BY ANN ELLIOTT CUTTING

GCN News 10.10.05

Procurement is key to security, IT execs say

BY PATIENCE WAIT | GCN STAFF

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 strengthen the country's cyber-infrastructure in the process.

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 Purdy, acting director of DHS' National Cyber Security Division.

Vendors will not invest in improving the quality of their software of their own volition, said Priscilla Guthrie, deputy CIO and deputy assistant secretary of Defense for networks and information integration. "We've got to use acquisition organizations to make sure we get the quality we need."

INFORMATION ASSURANCE

"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."

— DOD'S PRISCILLA GUTHRIE

NEWS&ANALYSIS

Update gives developers head start in fixing code

By Paul F. Roberts

A NEW SOFTWARE RELEASE from Secure Software Inc. is designed to make it easier for organizations doing software development to spot and resolve security flaws in raw computer code.

Secure Software, based in McLean, Va., planned to release in late June CodeAssure 2.0, the latest edition of its automated code security auditing technology. The upgrade includes CodeAssure Management Center, a tool that will make it easier to open-source IDE (integrated development environment) from the Eclipse Foundation Inc.

Microsoft Corp. said in June that it was working with SPI Dynamics to integrate its DevInspect and SecureObjects into Visual Studio 2005 and Visual Studio 2005

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

SC AWARDS 2006

Nominations are now open, click here to

Go to - SC Magazine Asia Pacific

Latest News

Software quality, FISMA top federal CISO concerns

by Marcia 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.

- Home
- News
- Products
- Features
- White Papers
- Events
- Advertising
- Working with SC

26 WEEK ■ JUNE 27/JULY 4, 2005

Software Assurance



OSD
DoD Software Assurance Initiative
Mitchell Komaroff, OASD (NII)/DCIO
Kristen Baldwin, OUSD(AT&L)/DS

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 Acquisitions, 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

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.

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, 5000.2, 5000, 3170, 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's or an old risk changes, contractor must be notified



Basis for SwA Technology

- Offensive side
 - Pedigree problem
 - Interconnectivity
 - Value of IT information
 - Many adversaries
- Defensive side
 - Fragmented efforts
 - Immature science
 - Lack of resources

Software Assurance: A Strategic Initiative of the U.S. Department of Homeland Security to Promote Integrity, Security, and Reliability in Software

Sept 7, 2005

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
US Department of Homeland Security

Driving Needs for Software Assurance

- Software vulnerabilities jeopardize intellectual property, business operations and services, infrastructure operations, and consumer services
- Growing awareness and concern over the ability of an adversary to subvert the software supply chain
 - Federal Government relies on COTS products and commercial development from foreign and non-vetted domestic suppliers to meet majority of IT requirements
 - Software development offers opportunities to insert malicious code and design and build software enabling exploitation
- Growing concern about inadequacies of suppliers' capabilities and deliver secure software with requisite levels of integrity
 - Current education & training provides too few practitioners with requisite 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-the-art on software capabilities of the nation
- Processes and technologies are required to build trust into software acquired and used by Government and critical infrastructure

Strengthen operational resiliency



Main Page - SAMATE

Information Technology Laboratory
Software Diagnostics and Conformance Testing Division

SAMATE - Software Assurance Metrics and Tool Evaluation

Welcome to the home page of the NIST Software Assurance Metrics and Tool Evaluation (SAMATE), pronounced sub-mate, rhymes with sadate) project. The project leader is Paul C. Stapp.

Upcoming Workshop:
Software Security Assurance Tools, Techniques, and Methods (7-8 Nov 2005)

This project is in support of the Department of Homeland Security's 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.

A definition of Software Assurance is:
...the planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures.

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.

NIST SAMATE Workshop: Defining the State of the Art in Software Assurance Tools (10-11 Aug 2005)

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.

SSATTM - SAMATE

http://samate.nist.gov/index.php/SSATTM

AFC Home MII Home Search Map/Ph/Weather/Travel Bob's Bookmarks CVEnOVAL SPAMmngt

Create an account or log in

article discussion edit history

SSATTM

Information Technology Laboratory
Software Diagnostics and Conformance Testing Division

Workshop on Software Security Assurance Tools, Techniques, and Metrics

[edit]

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

SE

navigation

- Main Page
- Project Plan
- Tools
- Resources
- Bibliography
- Recent changes
- Past Workshops
- Group Pages
- Help

search

Go Search

toolbox

- What links here
- Related changes
- Special pages



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

The screenshot shows the homepage of the Common Weakness Enumeration (CWE) website. The browser address bar displays <http://cwe.mitre.org/>. The page features a navigation menu on the left with sections for **CWE List**, **About**, **Community**, **News**, **Compatibility**, and **Contact Us**. The main content area includes a central diagram titled "Building CWE & Consensus" which illustrates the process of gathering information from various sources like "Publicly Available Security Taxonomies" and "Other Work Available in Security Taxonomies, Research, and Checklists" into the central "CWE" database. To the right, a "News" section lists recent updates, including "CWE Draft 5 Released" and "Important Message about CWE Web Site Availability, January 13-16". Below the news is an "Upcoming Event" section for the "CWE booth at RSA 2007" and a "Status Report" section.

CWE List
Full Dictionary View
Classification Tree
Other Views

About
Sources
Process
Documents

Community
Related Activities

News
Calendar

Compatibility
Program
Requirements
Make a Declaration

Contact Us
Search the Site

Building CWE & Consensus

Publicly Available Security Taxonomies, Research, and Checklists

Other Work Available in Security Taxonomies, Research, and Checklists

CWE

News

- [CWE Draft 5 Released](#)
- [Important Message about CWE Web Site Availability, January 13-16](#)
- ["CWE Compatibility and Effectiveness" Section Added to CWE Web Site](#)
- [CWE Information Included in Article in SC Magazine](#)
- [Vulnerability Type Distributions White Paper Now Available](#)

[...more](#)

Upcoming Event

- [CWE booth at RSA 2007, February 5-8, 2007](#)
- [CWE booth at 2007 IA Workshop, February 12-16, 2007](#)

[...more](#)

Status Report

Recent

Fifth draft posted December 15, 2006. Changes include (1) additional descriptions and mitigations for about 40 of the items, (2) minor revisions and updates to approximately 100 items based on the donated information, and (3) revisions to the names and structure of the hierarchical view to reflect the new and revised CWE content.

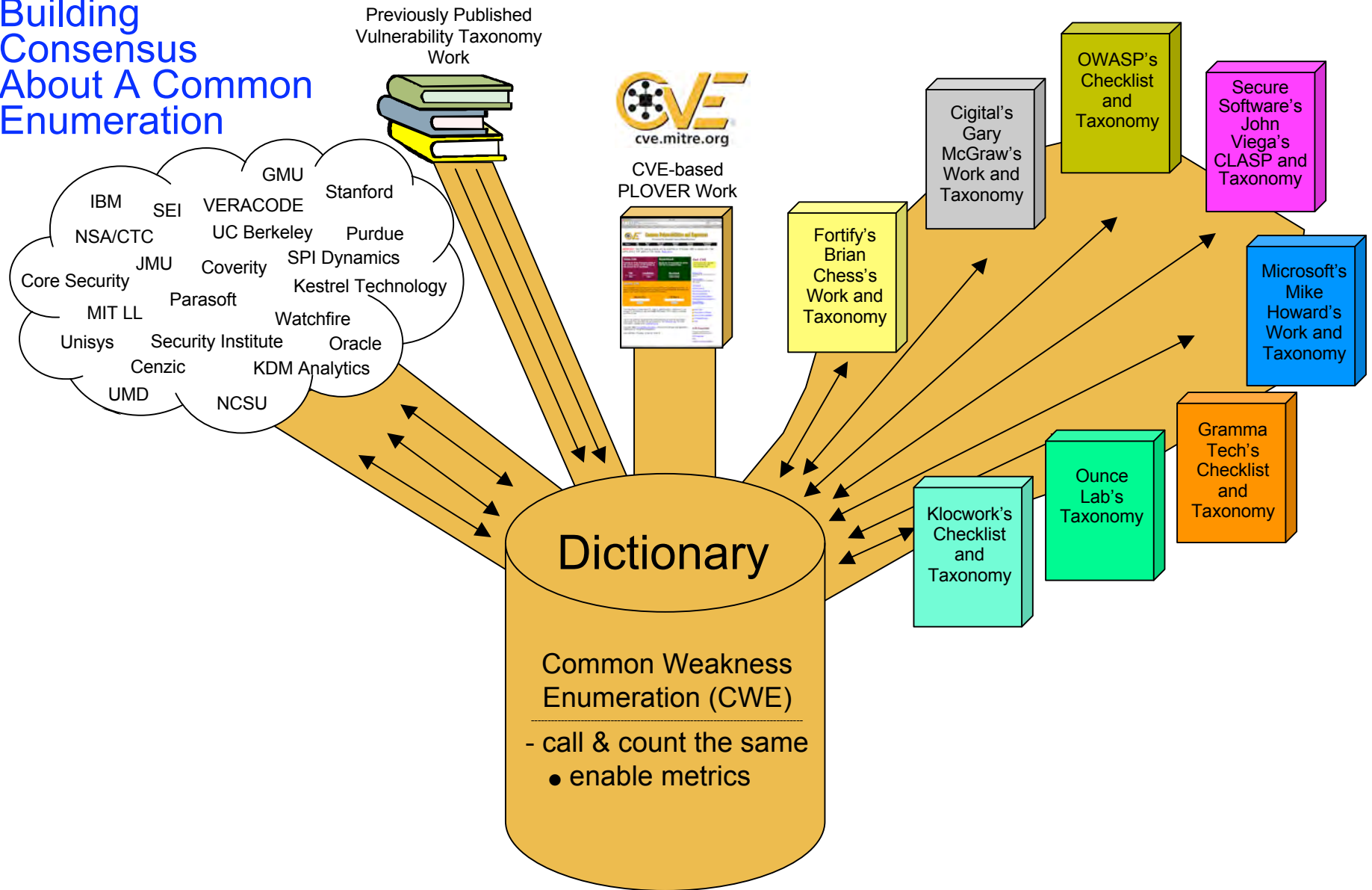
Next Step

We are gathering data about weaknesses from the sixteen tool and knowledge sources that are participating in CWE and then merging this new data into the current list to create a sixth draft.

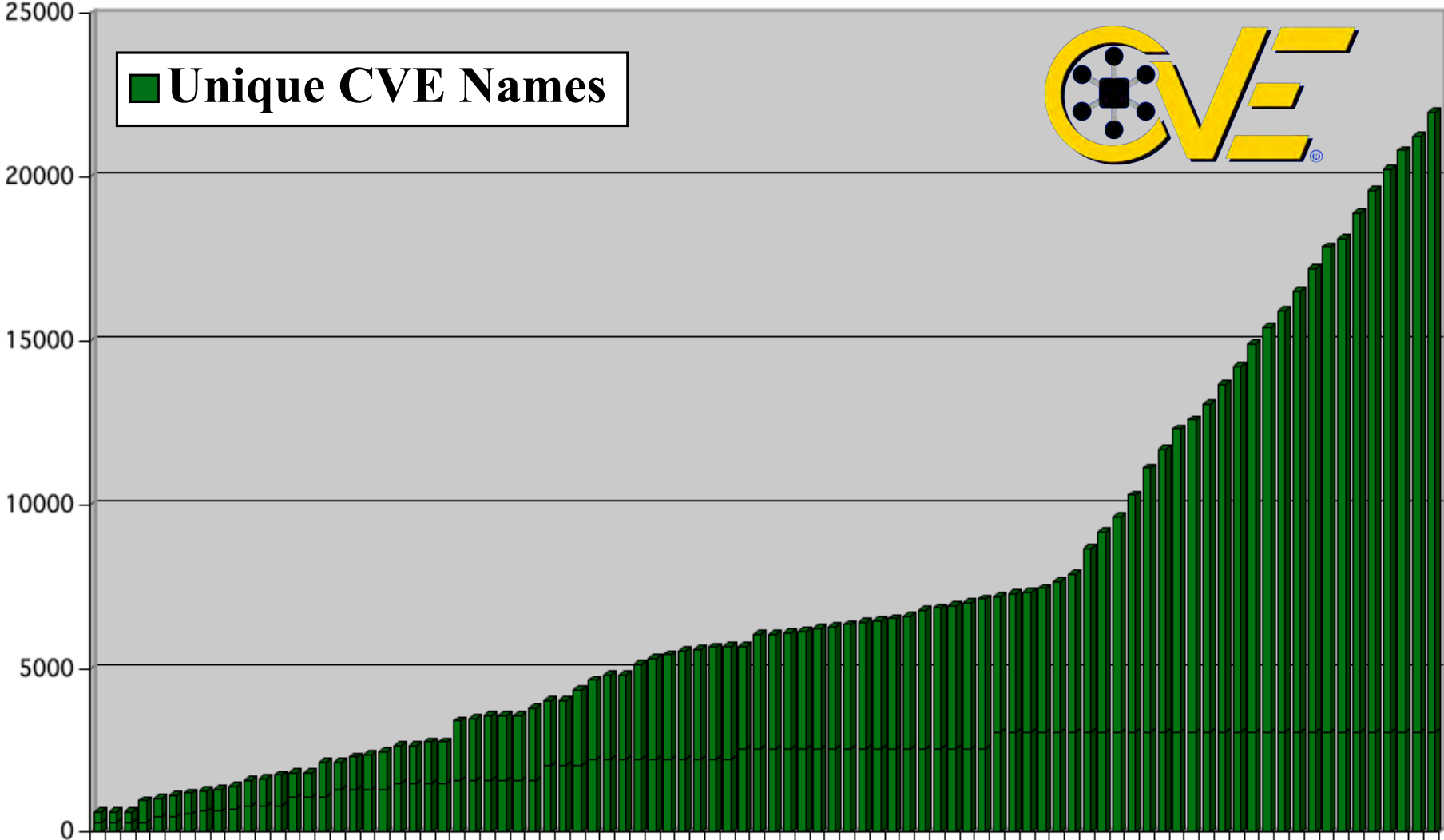
More Information
cwe@mitre.org

[cwe.mitre.org]

Building Consensus About A Common Enumeration



CVE Growth

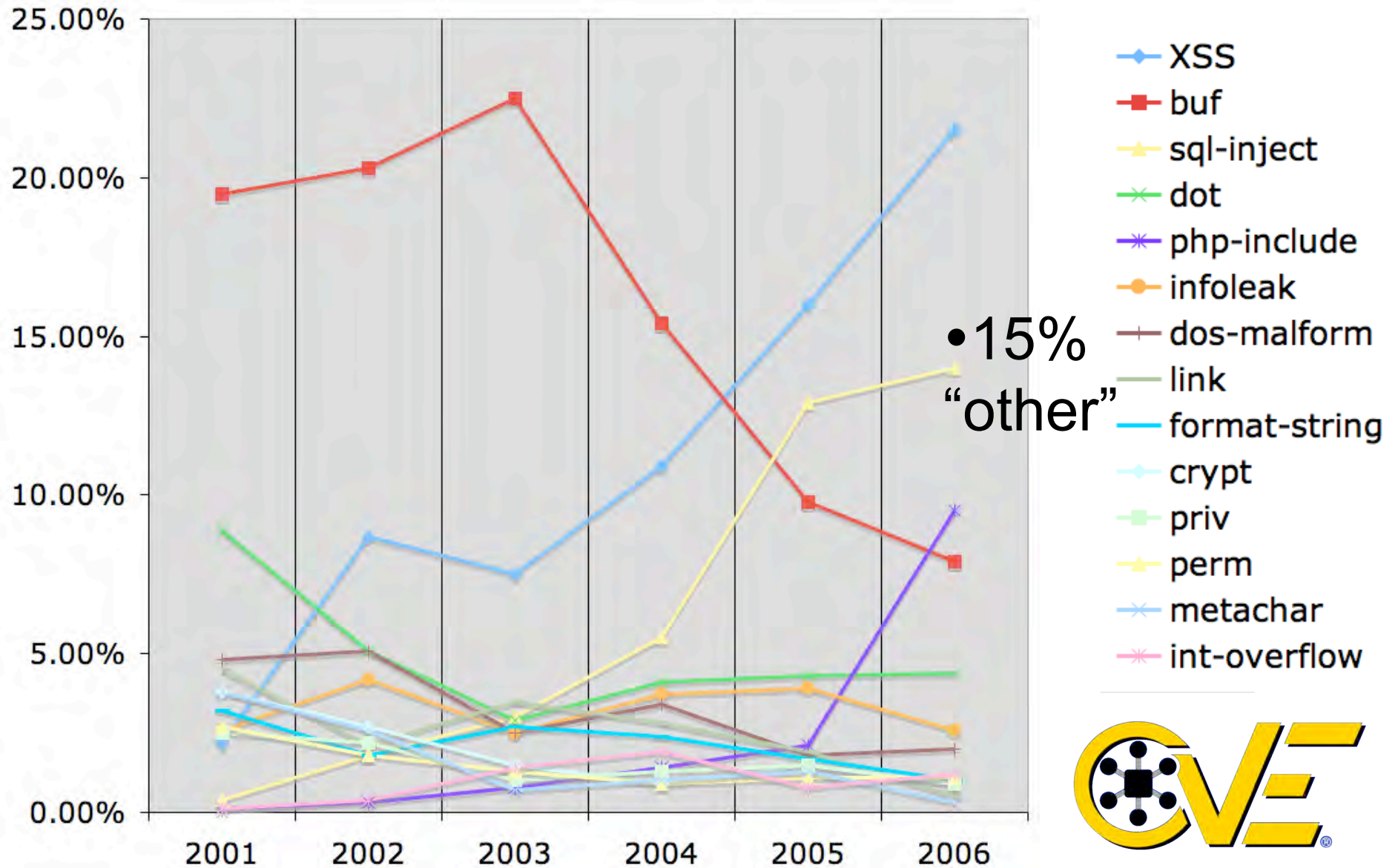


Status

(as of Feb 1, 2007)

• 21,990 unique CVE names

Vulnerability Type Trends: A Look at the CVE List (2001 - 2006)



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...

◆ XSS

■ buf

◆ sql-inject

◆ dot

◆ php-include

◆ infoleak

◆ dos-malform

◆ link

◆ format-string

◆ crypt

◆ priv

◆ perm

◆ metachar

◆ int-overflow

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

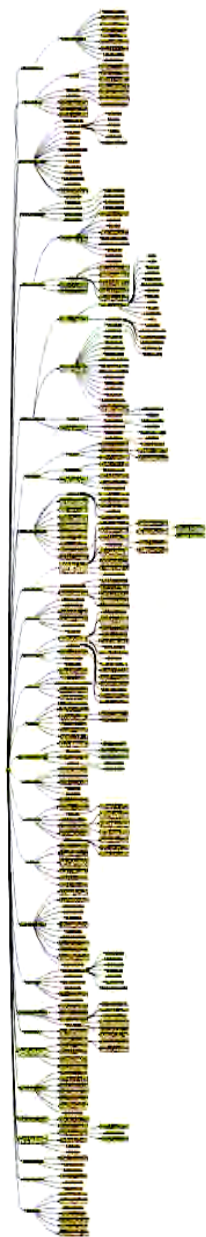
- Path Issue - dot dot slash - '../filedir'
- Path Issue - leading dot dot slash - './../filedir'
- Path Issue - leading directory dot dot slash - '/directory/../filename'
- Path Issue - directory doubled dot dot slash - 'directory/../../filename'
- Path Issue - dot dot backslash - '..\filename'
- Path Issue - leading dot dot backslash - '\..\filename'
- Path Issue - leading directory dot dot backslash - 'directory..\filename'
- Path Issue - directory doubled dot dot backslash - '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



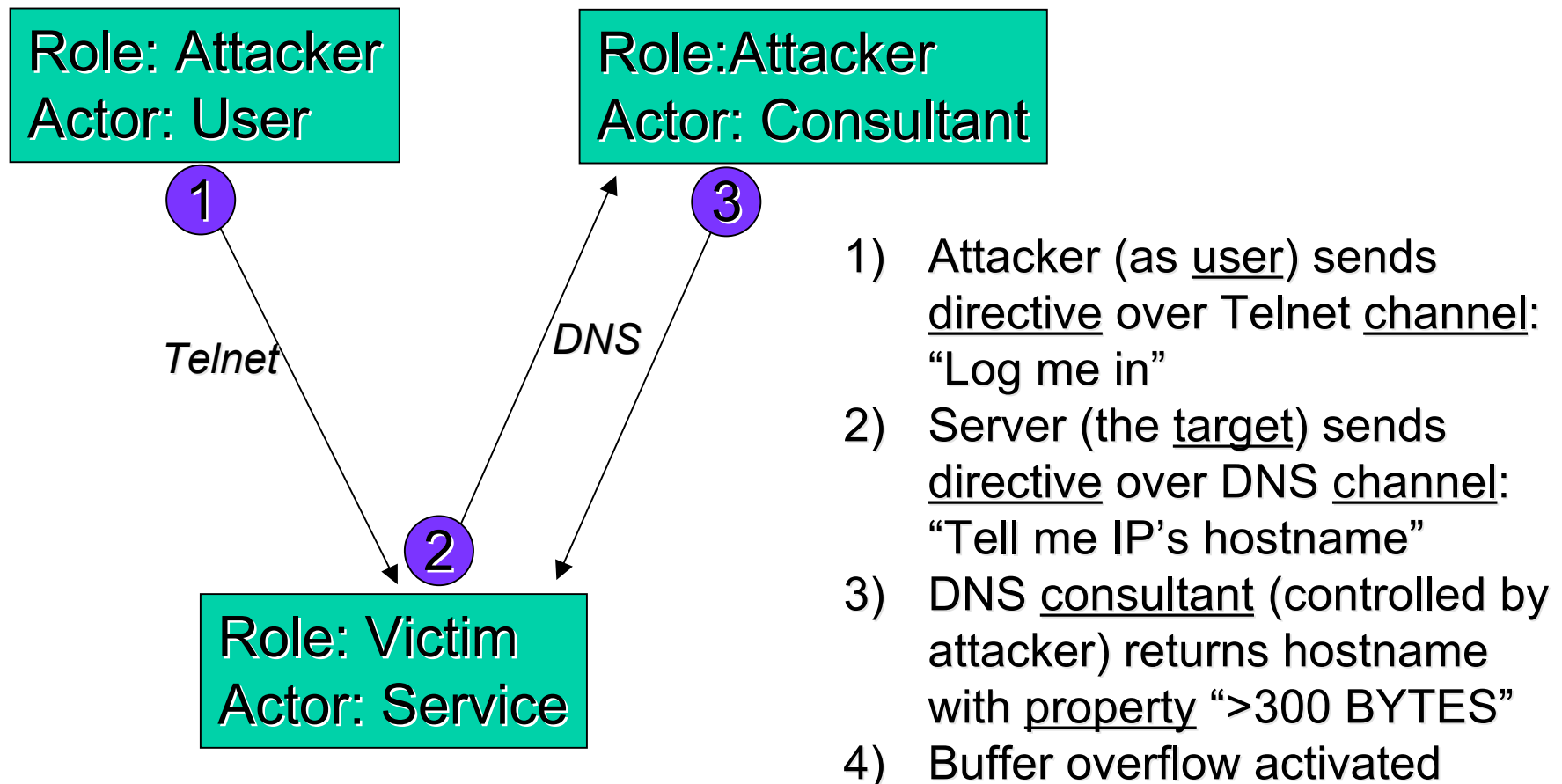
[BUFF] Buffer overflows, format strings, etc.	10 types
[SVM] Structure and Validity Problems	10 types
[SPEC] Special Elements (Characters or Reserved Words)	19 types
[SPECM] Common Special Element Manipulations	11 types
[SPECTS] Technology-Specific Special Elements	17 types
[PATH] Pathname Traversal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

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



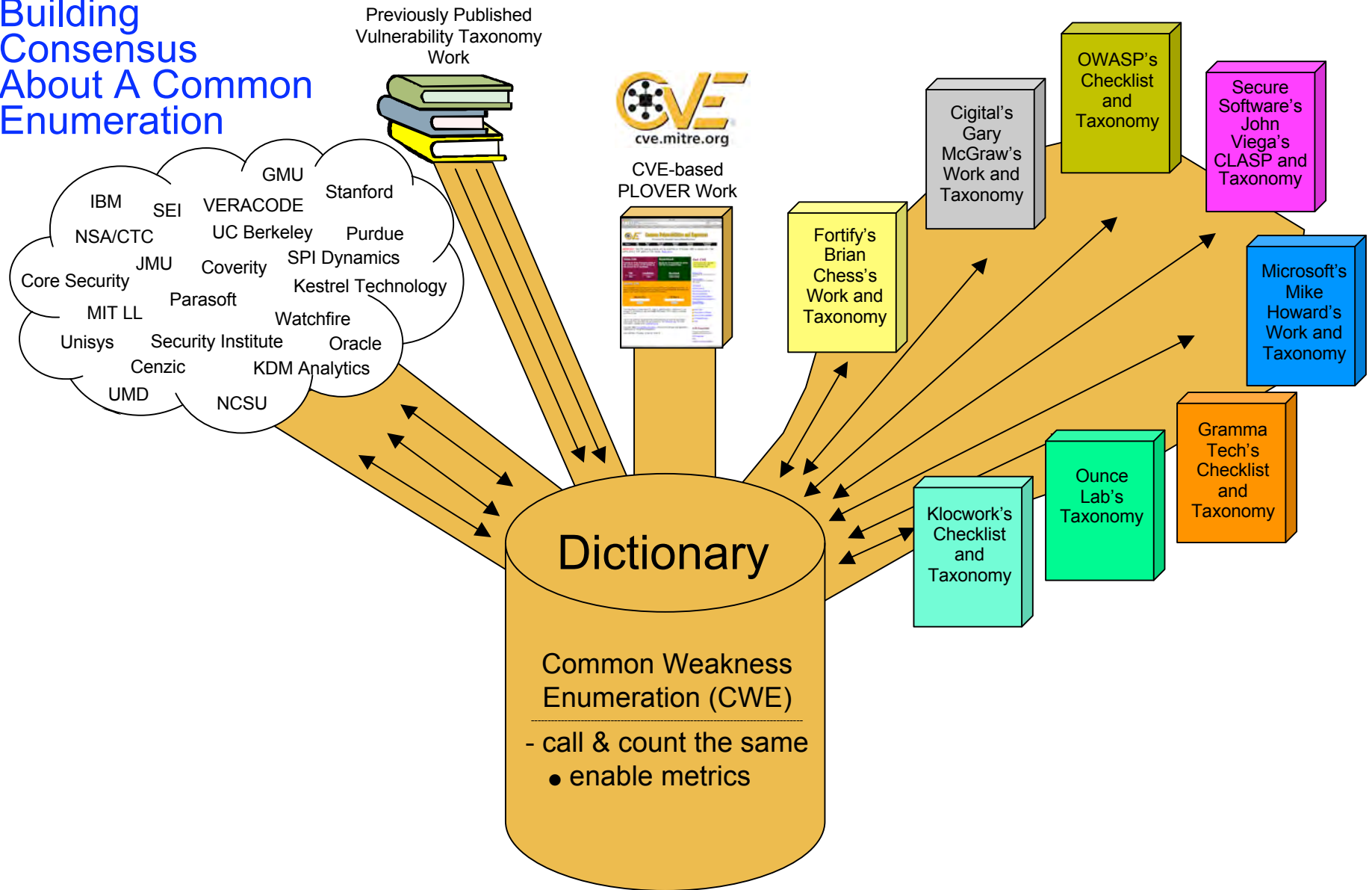
Artifact Labels

- 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

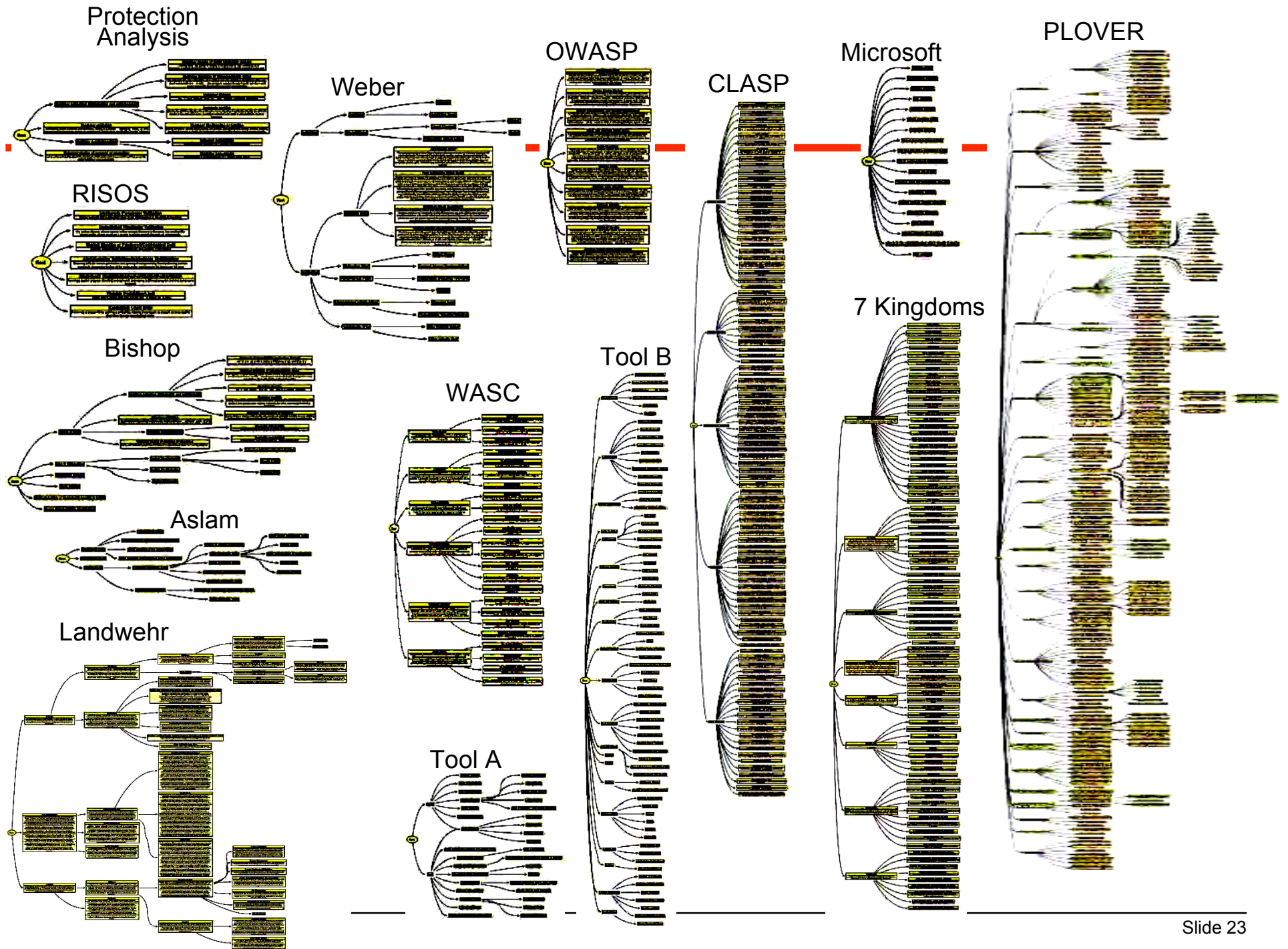
```
1   print HTTPResponseHeader;
2   print "<title>Hello World</title>";
3   ftype = HTTP_Query_Param("type");
4   str = "/tmp";
5   strcat(str, ftype); strcat(str, ".dat");
6   handle = fopen(str, "r");
7   while((line=fread(handle)))
8   {
9       line=stripTags(line, "script");
10      print line;
11      print "<br>\n";
12  }
13  fclose(handle);
```

Building Consensus About A Common Enumeration



Where Did We Start?

- Objective: To identify, integrate and effectively describe common software weaknesses known to the industry and software assurance community
- Leveraging taxonomic 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.mitre.org/data/definition/79.html]

Individual CWE Dictionary Definition (draft 5)

Cross-site scripting (XSS)	
CWE ID	79
Description	Cross-site scripting weakness occurs when dynamically generated web pages display input, such as login information, that is not properly validated, allowing an attacker to embed malicious scripts into the generated page and then execute the script on the machine of any user that views the site. If successful, Cross-site scripting vulnerability can be used to steal sensitive session cookies, create requests on behalf of the user, compromise data, and execute code on the end user's machine.
Alternate Terms	"CSS" was once used but caused confusion with the "C" in "Cross-site" significantly, and its use is discouraged.
Likelihood of Exploit	High to Very High
Weakness Ordinality	Resultant (Weaknesses Resultant)
Causal Nature	Explicit (This is an explicit developer error)
Common Consequences	Confidentiality: The weakness involves the disclosure of sensitive information. Access control: In some cases, an attacker can execute code on a victim's computer, bypassing other flaws.
Potential Mitigations	Carefully check each input against the specification (white list). All input should be sanitized to specify, but all data headers, the URL itself, and any continuing XSS vulnerabilities.
References	M. Howard and D. LeBlanc. Writing Secure Code. 2nd edition. Microsoft, 2003.
Node Relationships	Child Of - Injection (74) Results In - Mobile Code: Invoking untrusted mobile code (494) Parent Of - Basic XSS (80) Parent Of - XSS in error pages (81) Parent Of - Script in IMG tags (82) Parent Of - XSS using Script in Attributes (83) Parent Of - XSS using Script Via Encoded URI Schemes (84) Parent Of - Doubled character XSS manipulations, e.g. '<<script' (85) Parent Of - Invalid Characters in Identifiers (86) Parent Of - Alternate XSS syntax (87) Parent Of - Mobile Code: Invoking untrusted mobile code (494)
Source Taxonomies	PLOVER - Cross-site scripting (XSS) 7 Pernicious Kingdoms - Cross-site Scripting CLASP - Cross-site scripting
Applicable Platforms	C C++ Java .NET

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

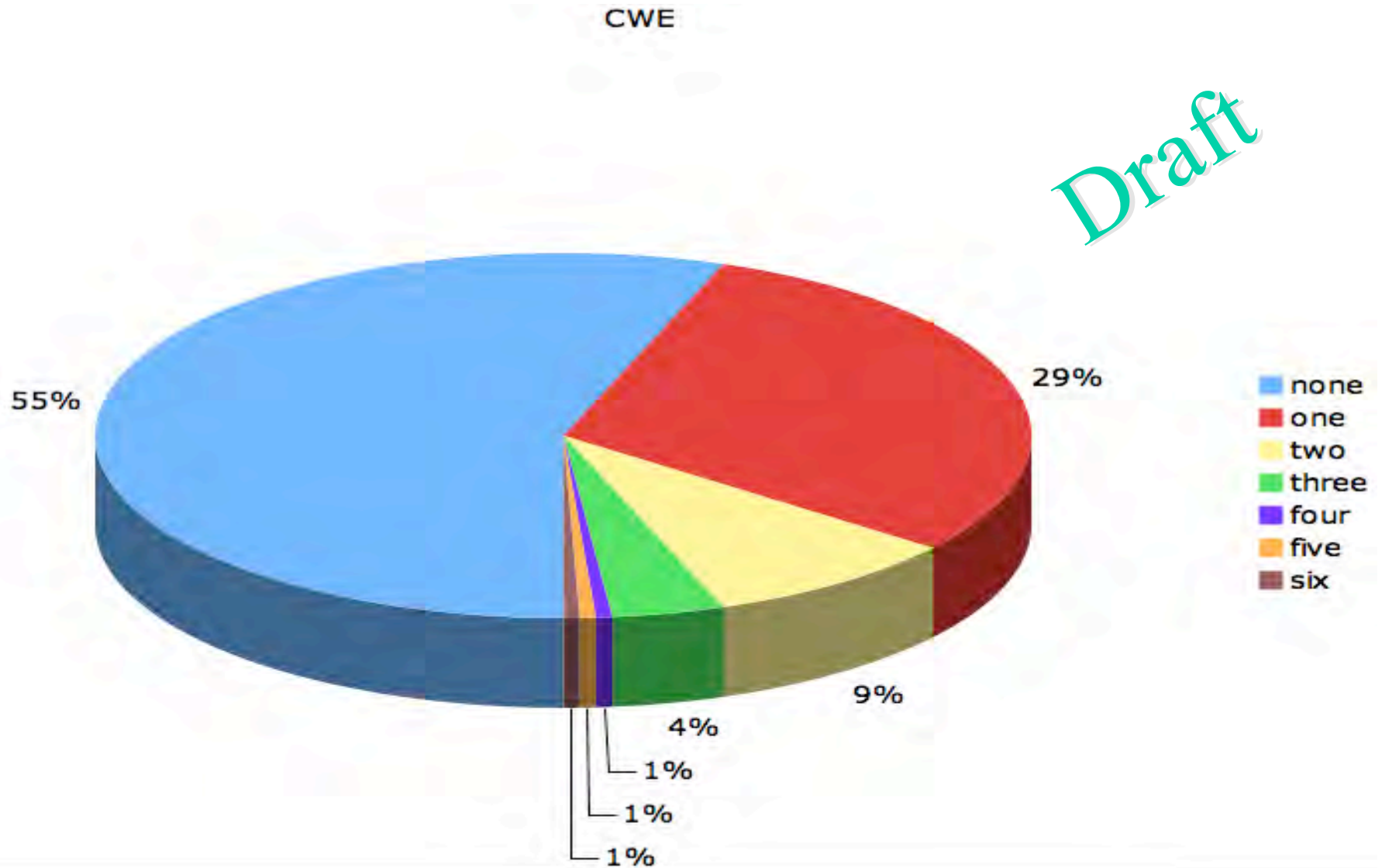
Using A Unilateral NDA with MITRE to Bring in Info

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.



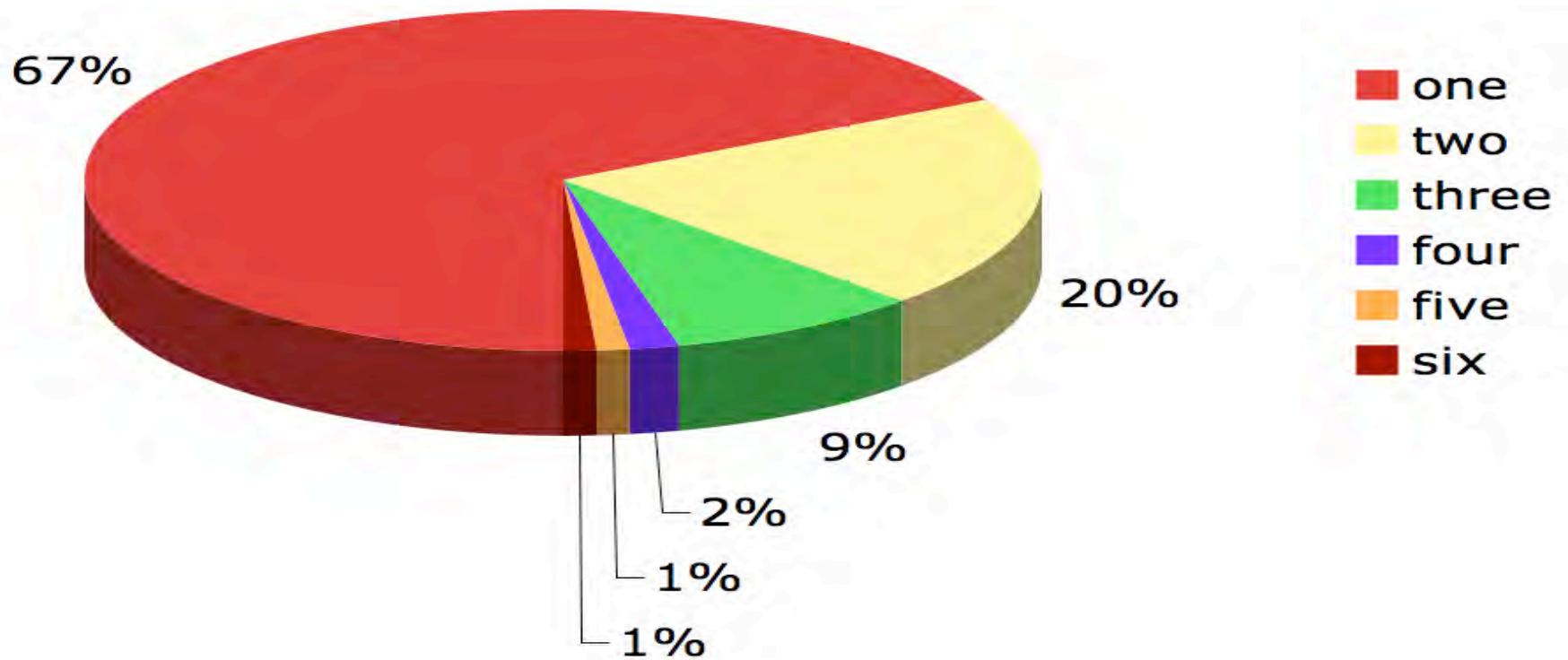
Coverage of CWE



Covered CWEs - By Number of Tools

Covered CWEs

Draft



Current Community Contributing to the Common Weakness Enumeration

- AppSIC
- Cenxic
- 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

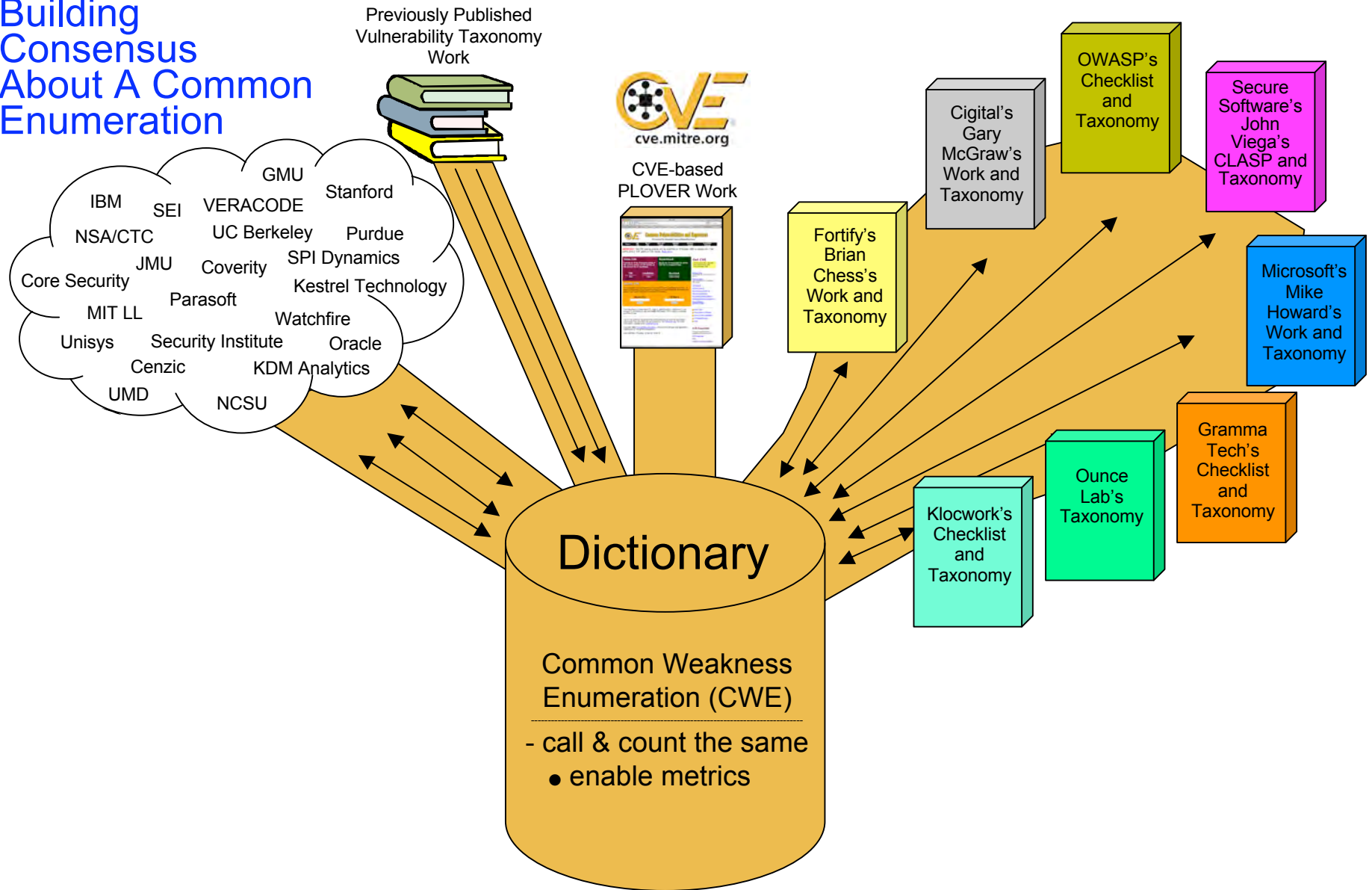
Planned Improvements - Content

- 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

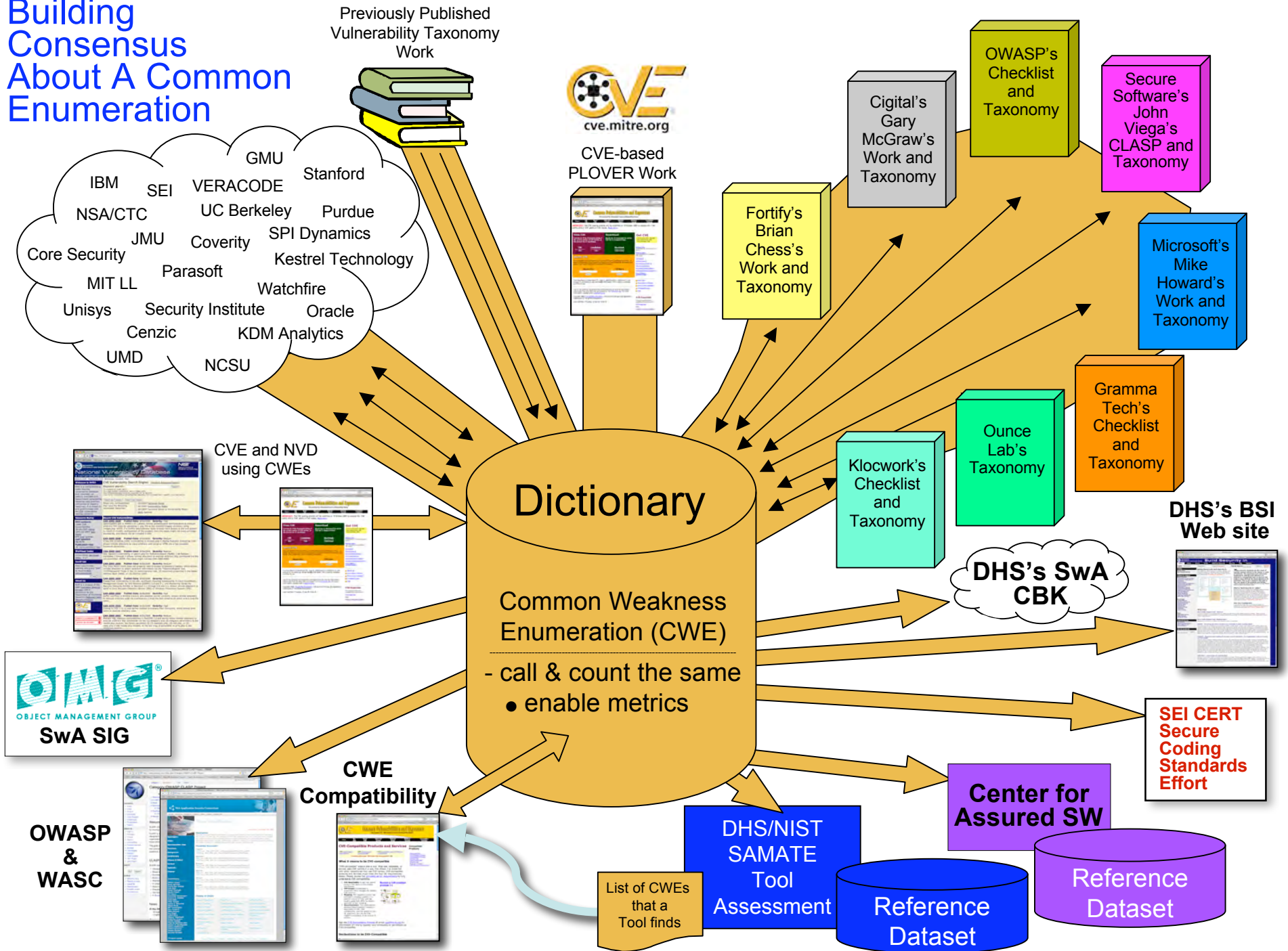
Planned Improvements - Site Usability

- 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



Building Consensus About A Common Enumeration



CWE Compatibility and Effectiveness Program Launched

The screenshot shows a web browser window with the URL <http://cwe.mitre.org/compatible/index.html>. The page features the CWE logo and the title "Common Weakness Enumeration: A community-developed dictionary of common software weaknesses". The main content area is titled "CWE Compatibility" and includes a paragraph explaining the program's purpose, a list of requirements for compatibility and effectiveness, and a list of program goals. A sidebar on the left contains navigation links, and a sidebar on the right contains a "Section Contents" menu. The footer includes the U.S. Department of Homeland Security logo, the MITRE Corporation logo, and contact information.

CWE Compatibility

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** — security elements presented to users includes, or allows users to obtain, associated CWE identifiers
- Mapping Accuracy** — security elements accurately link to the appropriate CWE identifiers
- CWE Documentation** — capability's documentation describes CWE, CWE compatibility, and how CWE-related functionality in the capability is used
- CWE Coverage** — for CWE-Effectiveness, capability's documentation explicitly lists the CWE identifiers that the capability is effective at locating in software
- CWE Test Results** — for CWE-Effectiveness, test results from the capability showing the results of assessing software for the CWEs are posted on the CWE Web site

See the [CWE Compatibility and Effectiveness Program](#) or email cwe@mitre.org for information on how to register your product(s) or services(s) as CWE-compatible or CWE-effective.

Section Contents

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

U.S. Department of Homeland Security

MITRE Corporation

CWE is sponsored by the U.S. Department of Homeland Security.
This Web site is hosted by The MITRE Corporation.
Copyright 2007, The MITRE Corporation. CWE and the CWE logo are trademarks of The MITRE Corporation.
Contact cwe@mitre.org for more information.

Page Last Updated: December 29, 2006
[Privacy policy](#)
[Terms of use](#)
[Contact us](#)

CWE Compatibility and Effectiveness Process Posted

The screenshot shows a web browser window displaying the "CWE - CWE Compatibility and Effectiveness Program" page. The browser's address bar shows the URL "http://cwe.mitre.org/compatible/program.html". The page features a navigation menu with links for "Introduction", "Declaration Phase", "Evaluation Phase", "Effectiveness Phase", and "Contact Instructions". The main content area is titled "CWE Compatibility and Effectiveness Program" and includes an "Introduction" section. The introduction states that the 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. It also mentions that compatible and effective products and services will be posted on the "CWE-Compatible and Effective Products and Services" page. The page is divided into three phases: Declaration, Evaluation, and Effectiveness. The "Phase 1 - Declaration Phase" section describes the requirements for the Declaration Phase, including the completion of a "CWE Compatibility Declaration Form" and the submission of a statement regarding the organization's belief in its product or service's compliance with the requirements. The "Phase 2 - Evaluation Phase" section describes the requirements for the Evaluation Phase, including the completion of a "CWE Compatibility Requirements Evaluation Form" and the submission of a "Compatible Product/Service Organization Welcome Kit".

CWE List
Full Dictionary View
Classification Tree
Other Views

About
Sources
Process
Documents

Community
Related Activities

News
Calendar

Compatibility
Program
Requirements
Make a Declaration

Contact Us
Search the Site

Section Contents
Compatibility
Program
Requirements
Make a Declaration

CWE Compatibility and Effectiveness Program

[Introduction](#) [Declaration Phase](#) [Evaluation Phase](#) [Effectiveness Phase](#) [Contact Instructions](#)

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 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

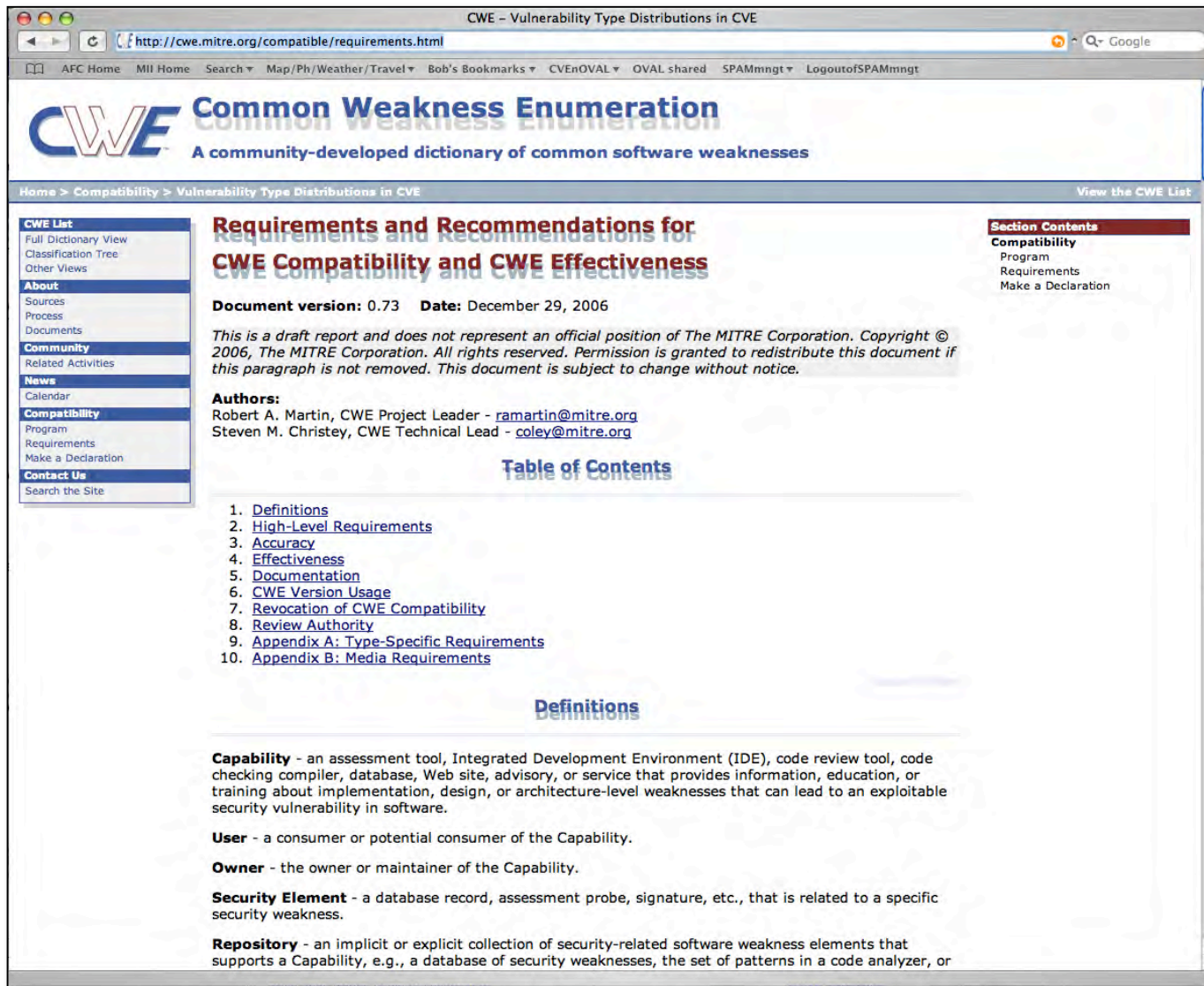
The Declaration Phase requires the completion of a short informational "CWE Compatibility Declaration Form" used to register an organization's declaration of intent with respect to CWE compatibility and effectiveness. In this phase you are asked to review the compatibility and effectiveness requirements 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 process 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



The screenshot shows a web browser window displaying the page "Requirements and Recommendations for CWE Compatibility and CWE Effectiveness" on the MITRE CWE website. The browser's address bar shows the URL "http://cwe.mitre.org/compatible/requirements.html". The page features a navigation menu on the left with categories like "CWE List", "About", "Community", "News", "Compatibility", and "Contact Us". The main content area includes a title, document version (0.73), date (December 29, 2006), a disclaimer, authors (Robert A. Martin and Steven M. Christey), a table of contents, and a section titled "Definitions" with entries for Capability, User, Owner, Security Element, and Repository.

Requirements and Recommendations for CWE Compatibility and CWE Effectiveness

Document version: 0.73 **Date:** December 29, 2006

This is a draft report and does not represent an official position of The MITRE Corporation. Copyright © 2006, The MITRE Corporation. All rights reserved. Permission is granted to redistribute this document if this paragraph is not removed. This document is subject to change without notice.

Authors:
Robert A. Martin, CWE Project Leader - ramartin@mitre.org
Steven M. Christey, CWE Technical Lead - coley@mitre.org

[Table of Contents](#)

1. [Definitions](#)
2. [High-Level Requirements](#)
3. [Accuracy](#)
4. [Effectiveness](#)
5. [Documentation](#)
6. [CWE Version Usage](#)
7. [Revocation of CWE Compatibility](#)
8. [Review Authority](#)
9. [Appendix A: Type-Specific Requirements](#)
10. [Appendix B: Media Requirements](#)

Definitions

Capability - an assessment tool, Integrated Development Environment (IDE), code review tool, code checking compiler, database, Web site, advisory, or service that provides information, education, or training about implementation, design, or architecture-level weaknesses that can lead to an exploitable security vulnerability in software.

User - a consumer or potential consumer of the Capability.

Owner - the owner or maintainer of the Capability.

Security Element - a database record, assessment probe, signature, etc., that is related to a specific security weakness.

Repository - an implicit or explicit collection of security-related software weakness elements that supports a Capability, e.g., a database of security weaknesses, the set of patterns in a code analyzer, or

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

DONE
DONE
DONE
In Process
In Process
In Process
In Process
In Process
In Process
In Process
Pending
In Process
Drafted
Started