What Do The Building Blocks for Measuring Assurance Look Like?

• Standard ways for **enumerating** “things we care about”

• **Languages/Formats** for encoding/carrying high fidelity content about the “things we care about”

• **Repositories** of this content for use in communities or individual organizations
The Building Blocks Are:

- **Enumerations**
  - Catalog the fundamental entities in Software Assurance
    - Vulnerabilities (CVE), configuration issues (CCE), software packages (CPE), attack patterns (CAPEC), weaknesses in code/design/architecture (CWE)

- **Languages/Formats**
  - Support the creation of machine-readable state assertions, assessment results, and messages
    - Configuration/vulnerability/patch/asset patterns (XCCDF & OVAL), software security patterns (SBVR), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), config risk (CCSS), weakness risk (CWSS), information messages (CAIF & *DEF)

- **Knowledge Repositories**
  - Packages of assertions supporting a specific application
    - Vulnerability advisories & alerts, (US-CERT Advisories/IAVAs), configuration assessment (NIST Checklists, CIS Benchmarks, NSA Configuration Guides, DISA STIGS), asset inventory (NIST/DHS NVD), code assessment & certification (NIST SAMATE, DoD DIACAP & eMASS)
Common Weakness Enumeration (CWE)

• Weaknesses are characteristics of software that may lead to vulnerability
• Existence of weaknesses in software can be objectively measured through the use of various techniques and tools
• Software assurance is determined by the absence of weaknesses identified as relevant for a given context and assurance level

• CWE is an effort targeted at standardizing the capture and description of weaknesses and providing a useful collection to be leveraged by the community
• Community effort developed from dozens of sources
• CWE version 1.1 was released December 2008
• Already being used in education, tools, software risk assessment, policy, etc.

http://cwe.mitre.org
What is the Common Attack Pattern

• Effort targeted at:
  – Standardizing the capture and description of attack patterns
  – Collecting known attack patterns into an integrated enumeration that can be consistently and effectively leveraged by the community
  – Classifying attack patterns such that users can easily identify the subset of the entire enumeration that is appropriate for their context

• http://capec.mitre.org
• Sponsored by DHS
• Led by Cigital
Mitigating Risk Exposures

- Asset Inventory
- Configuration Guidance Analysis
- Vulnerability Analysis

Responding to Security Threats

- Threat Analysis
- Intrusion Detection
- Incident Management

Operations Security Management Processes

- Centralized Reporting
- Enterprise IT Asset Management

Knowledge Repositories

- System & Software Assurance Guidance/Requirements
- Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation

Operational Enterprise Networks

- DNS Server
- Mail Server
- Web Servers
- Desktop Systems
- Application Servers
- Database Systems

Enterprise IT Change Management

Mitigating Risk Exposures

- Asset Definition
- Configuration Guidance
- Vulnerability Alert

Responding to Security Threats

- Threat Alert
- Intrusion Detection

CAIF/IDMEF/IODEF/CVE/CWE/CVSS/CPE/CME/MAEC/CEE/CRF

Enterprise IT Change Management

CWE/CAPEC/SBVR/MAEC

CVE/CWE/CVSS/CCE/OVAL/XCCDF/CPE/CME/CAPEC/MAEC/CEE/CRF
Making Security Measurable

MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through enumerating baseline security data, providing standardized languages as means for accurately communicating the information, and encouraging the sharing of the information with users by developing repositories.

The other activities and initiatives listed here have similar concepts or compatible approaches to MITRE's. Together all of these efforts are helping to make security more measurable by defining the concepts that need to be measured, providing for high fidelity communications about the measurements, and providing for sharing of the measurements and the definitions of what to measure.

Measurable security pertains at a minimum to the following areas:
- Vulnerability Management
- Asset Security Assessment
- Intrusion Detection
- Asset Management
- Configuration Guidance
- Patch Management
- Malware Response
- Incident Management
- Threat Analysis

Enumerations
- Common Vulnerabilities and Exposures (CVE™) - common vulnerability identifiers
- Common Weakness Enumeration (CWE™) - list of software weakness types
- Common Attack Pattern Enumeration and Classification (CAPEC™) - list of common attack patterns
- Common Malware Enumeration (CME™) - common identifiers for viruses, worms, and other malicious code
- Common Platform Enumeration (CPE™) - common platform identifiers
- OWAS Top Ten - 10 most critical Web application security flaws
- WASC Web Security Threat Classification - list of Web security threats

Languages
- Open Vulnerability and Assessment Language (OVAL™) - standard for describing vulnerability and configuration issues
- Common Result Format (CRF™) - standard assessment result format for conveying findings based on common names and naming schemes
- Common Event Expression (C3E™) - standardizes the way computer events are described, logged, and exchanged
- OVAL Interpreter™ - free tool for collecting information for testing, carrying out OVAL Definitions, and presenting results of the tests
- Benchmark Editor™ - free tool that enhances and simplifies creation and editing of benchmark documents written in XCCDF and OVAL
- Extensible Configuration Checklist Description Format (CCE™) - specification language for uniform expression of security checklists, benchmarks, and other configuration guidance
- Common Vulnerability Scoring System (CVSS™) - open standard that conveys vulnerability severity and helps determine urgency and priority of response
- Common Vulnerability Scoring System (CVSS™) - open standard that conveys vulnerability severity and helps determine urgency and priority of response
- OVAL-Encoded Business Vocabulary and Business Rules (OEBVBR™) - language for interchange of business vocabularies and rules among organizations and software tools

Repositories
- National Vulnerability Database (NVD™) - U.S. vulnerability database based on CVE that integrates all publicly available vulnerability resources and references
- SCAP Security Content Automation Protocol (SCAP™) - security content for automating technical control compliance activities, vulnerability checking, and security measurement
- Red Hat Repository - OVAL Patch Definitions corresponding to Red Hat Errata security advisories
- Center for Internet Security (CIS) Benchmarks - best-practice security configurations accepted for compliance with FISMA, the ISO standard, CIL, SOx, HIPAA, and FIPPA, and other regulatory requirements for information security
- DISA Security Technical Implementation Guides (STIGS™) - U.S. Defense Information Systems Agency's (DISA) STIGs are configuration standards for DOD information assurance and information assurance-enabled devices and systems

View the current collection of organizations, activities, and initiatives.

Disclaimer

This Web site is hosted by The MITRE Corporation. © 2008 The MITRE Corporation. CVE is a registered trademark and the Making Security Measurable logo, CCE, CME, CWE, CPE, and OVAL are trademarks of The MITRE Corporation. All other trademarks are the property of their respective owners. Contact us: measuresecurity@mitre.org

Page Last Updated: January 17, 2008
Practical Measurement Framework

- Harmonized with five prevailing system/software and security measurement approaches
- Provides basic measures development and implementation processes
- Provides general measures examples
- Integrates with existing measurement programs
- Incorporates Making Security Measurable products
- Provides an overarching framework for summarizing SwA measures and communicating them to stakeholders
What Is Measurable Today?

• Enumerations of Things That We Want to Know About:
  – Common Weakness Enumeration (CWE)
  – Common Attack Pattern Enumeration and Classification (CAPEC)
  – Common Vulnerabilities and Exposures (CVE)
  – Common Configuration Enumeration (CCE)

• Ways of Expressing Details About Enumerated Items:
  – Open Vulnerability and Assessment Language (OVAL)
  – XML Configuration Checklist Data Format (XCCDF)
  – Common Platform Enumeration (CPE)
  – Common Vulnerabilities Scoring System (CVSS)
  – Common Configuration Scoring System (CCSS)
  – Common Weakness Scoring System (CWSS)

• Repositories of Content with Measurement Criteria
  – SCAP (Secure Content Automation Protocol)

Other measurable items include quality and project management measures which are well developed and available for use