MAKING SECURITY MEASURABLE AND MANAGEABLE

Robert A. Martin
The MITRE Corporation
Bedford, MA

ABSTRACT

The security and integrity of information systems is a critical issue within most types of organizations. Finding better ways to address the topic is the objective of many in industry, academia, and government. One of the more effective approaches gaining popularity in addressing these issues is the use of standard knowledge representations, enumerations, exchange formats and languages, as well as sharing of standard approaches to key compliance and conformance mandates. By standardizing and segregating the interactions amongst their operational, development and sustainment tools and processes organizations gain great freedom in selecting technologies, solutions and vendors. These "Making Security Measurable" initiatives provide the foundation for answering today's increased demands for accountability, efficiency and interoperability without artificially constraining an organization's solution options.

INTRODUCTION

Over the last decade, MITRE and others have developed a number of information security standards that are increasingly being adopted by vendors and forming the basis for security management and measurement activities across wide groups of industry and government. This paper explores how these standards are facilitating the use of automation to assess, manage, and improve the security posture of enterprise security information infrastructures while also fostering effective security process coordination across the adopting organizations.

The basic premise of the "Making Security Measurable" effort is that for any enterprise to measure and manage the security of their cyber assets they are going to have to employ automation. For an enterprise of any reasonable size that automation will have to come from multiple sources and so to make the finding and reporting issues consistent and composable across different tools there has to be an underlying set of standard definitions of the things that are being examined, reported and managed by the different tools. That standardization is what comprises the "Making Security Measurable" collection.

Information security measurement and management, as currently practiced, is complex, expensive, and fraught with unique activities and tailored approaches. Solving the variety of challenges currently facing enterprises with regards to incident and threat management, patching, application security, and compliance management requires fundamental changes in the way vendor technologies are adopted and integrated. These changes include the way enterprises organize and train to utilize these capabilities. Likewise, to support organizational discipline and accountability objectives while enabling innovation and flexibility, the security industry needs to move to a vendor neutral security management and measurement strategy that is agnostic to the specific solution providers while also flexible enough to work with several different solutions simultaneously. Finally, the new approach should enable the elimination of duplicative and manual activities while also improving the ability of organizations to leverage outside resources and collaborate with other organizations facing the same threats and risks.

These objectives can be met by bringing architecturally driven standardization to the scoping and organization of the information security activities that our enterprises practice. By acknowledging the "natural" groupings of activities, often referred to as domains, that all information security organizations address—independent of the tools and techniques they use—a framework can be established within which organization's can organize their work independent of their current technology choices and flexible enough to adapt to tomorrows offerings. Likewise, by examining these domain groupings and the types of practices of coordination and cooperation that persist across and between them it is possible to improve interoperability and independence of these groups by standardizing common concepts in the information that flows across and between the different domains. These shared concepts are sometimes referred to as boundary objects and are a phenomenon known to those that study inter-community communications[1] but one that had not been leveraged explicitly for information security standardization.

[1] Bowker and Star, "*Sorting Things Out",* ISBN 0262522950, MIT Press, 1999.

978-1-4244-2677-5/08/$25.00 ©2008 IEEE

RECASTING CYBER SECURITY PRACTICES USING ARCHITECTURE AND SYSTEMS ENGINEERING PRINCIPALS

In this paper we will discuss how by leveraging the practices of systems engineering we can recast our current cyber security solutions into a launching point for standard functional decomposition-based security architectures that provide a flexible, logical, and expandable approach to building and operating cyber security solutions for the enterprise and one that is more supportive of security measurement, management, and sharing goals.

We will look at the collection of cyber security related activities that most enterprises practice including inventorying assets; analysis of system configurations; analysis of systems for vulnerabilities; analysis of threats; studying intrusions; reporting and responding to incidents; change management; assessing systems development, integration, and sustainment activities; and certification and accreditation of systems being deployed into the enterprise. (Note that this is a integrated list that includes activities tied to the operation of systems in the enterprise as well as those the create, deploy, and update those systems.)

We will also examine the different types of information that have been identified to support these activities. Finally, we will identify the key activities and information that needs to be sharable and unambiguous in and amongst the different functions of today's cyber security environment. By identifying and collecting these functional components as standard reusable concepts, we will illustrate one of the major benefits that architecture brings to the study of security in the enterprise information technology landscape.

ARCHITECTING SECURITY

By looking at security measurement and management as an architecture issue and using a systems engineering approach to functionally decompose it and identifying the basic functions and activities that need to be done and then getting appropriate technology to support the functions and activities, we can lay the foundation for architecting measurable security.

Through the development and adoption of standard enumerations, the establishment of languages and interface standards for conveying information amongst tools and organizations, and by sharing guidance and measurement goals with others by encoding them in these standard languages and concepts, organizations across the world can dramatically change the options available to address security of the enterprise's cyber environment.

The U.S. federal government and commercial enterprises are already starting to deploy new approaches to security measurement and management that leverage interoperability standards and enable enterprise-wide security measurement and policy compliance efforts by leveraging several of the ongoing security architecture driven measurement and management initiatives [1]. These standards are providing ways for these organizations to create test rules about their organization's minimum secure configurations, mandatory patches, and/or unacceptable coding practices that can be assessed, reported, and any subsequent remediation steps planned, executed, and confirmed using commercial tools. At the same time they also provide a basis for repeatable, trainable processes and sharing along with the enabling of automation-based testing methods for deployment validation and regression testing throughout the operational life-time of the systems.

Maybe more importantly, the establishment of architectural methods within the cyber security community will help open the doors to better, faster, and more coordinated approaches to dealing with the next set of security problems. There is little doubt that each and every one of the current solutions being implemented to fight today's threats will in-turn be attacked by advances in the methods used to subvert the systems in our enterprises. But with a more consistent basis for considering these new threats and methods, solutions can be leveraged faster and applied in more predictable time frames and with more understanding for the risks that remain.

BUILDING BLOCKS FOR ARCHITECTING MEASURABLE SECURITY

We believe there are four basic building blocks for architecting measurable security:

- Standardized enumerations of the common concepts that need to be shared.
- Languages for encoding high-fidelity[2] information about how to find the common concepts and communicating that information from one human to another human, from a human to a tool, from one tool to another tool, and from a tool to a human.

[2] High fidelity refers to the level of detail of the information encoded in a language that is sufficient to convey the understanding and knowledge of the one encoding the information to the one who decodes the information. If a person writes a test for how to check a configuration setting in a language then that language needs to be able to convey the specifics of the test so that another person or a tool reading the check as written in the language understands enough about the check to actually perform the test that was intended by the original author. If a language cannot retain the fidelity of the information to support this then it is not of sufficient fidelity.

- Sharing the information through repositories of content[3] in languages for use in broad communities or individual organizations in a way that minimizes loss of meaning when content is being exchanged between tools, people, or both.
- Uniformity of adoption achieved through branding and vetting programs to encourage the tools, interactions, and content remain standardized and conformant.

The following sections discuss these building blocks in more detail.

ENUMERATIONS

Enumerations catalog the fundamental entities and concepts in information assurance, cyber security, and software assurance that need to be shared across the different disciplines and functions of these practices. The June 2007 National Academies report on the state of cyber security and cyber security research, "Towards a Safer and More Secure Cyberspace," highlighted that metrics and measurements particularly rely on enumerations. As an example the report cited the Common Vulnerabilities and Exposures (CVE®) [2] list run by MITRE Corporation under funding from the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security (DHS), as an enumeration that enables all kinds of measurement by providing unique identifiers for publicly known vulnerabilities in software. There are a number of enumerations in the information assurance, cyber security, and software assurance space. Some examples are shown in Table 1.

Table 1. Enumerations

Name	Topic
Common Vulnerabilities and Exposures (CVE®)	Standard identifiers for publicly known vulnerabilities
Common Weakness Enumeration (CWE™)	Standard identifiers for the software weaknesses in architecture, design or implementation that lead to vulnerabilities
Common Attack Pattern Enumeration and Classification (CAPEC™)	Standard identifiers for attacks
Common Configuration Enumeration (CCE™)	Standard identifiers for configuration issues
Common Platform Enumeration (CPE™)	Standard identifiers for platforms, operating systems, and application packages
SANS Top-20	Consensus list of the most critical vulnerabilities that require immediate remediation
Open Web Application Security Project's (OWASP) Top Ten	List of the ten most critical web application security flaws
Web Application Security Consortium's (WASC) Threat Classification	List of web security attack classes

Table 1. Enumerations (concluded)

LANGUAGES

Standardized languages and formats allow uniform encoding of the enumerated concepts and other high-fidelity information for communication from human to human, human to tool, tool to tool, and tool to human. For example, a configuration benchmark document written in the XCCDF and OVAL languages [3, 4] would be readable by a human and it would be consumable by an assessment tool, in that the tool would be able to directly import the tests and checks that are expressed in the document. As with the enumerations, there are a number of information assurance, cyber security, software assurance measurement and management oriented languages and formats. Some examples are shown in Table 2.

Table 2. Languages

Name	Topic
Extensible Configuration Checklist Description Format (XCCDF)	An XML specification language for writing security checklists, benchmarks, and related kinds of documents
Open Vulnerability and Assessment Language (OVAL™)	An XML state expression language for writing assessment tests about the current state of an asset and expressing the results
Common Vulnerability Scoring System (CVSS)	A method for conveying vulnerability related risk and risk measurements

[3] Content repositories are currently envisioned to be collections of tests to verify settings, patches, and installed software on systems to comply with organizational policies about their information technology systems and processes. Repositories are typically meant to be understandable by humans but used by tools to automate checking for compliance with the tests in the repository. Many different organizations are hosting public and private repositories already and we anticipate that to continue and grow as the need to share grows.

Table 2. Languages (concluded)

Common Result Format (CRF™)	A standardized IT asset assessment result format that facilitates the exchange and aggregation of assessment results
Semantics of Business Vocabulary and Business Rules (SBVR)	A vocabulary and rules for documenting the semantics of an area of business's vocabulary, facts, and processes
Common Event Expression (CEE™)	A language and syntax for describing computer events, how the events are logged, and how they are exchanged
Malware Attribute Enumeration and Characterization (MAEC)	A language for describing malware in terms of its attack patterns, detritus, and actions
Common Announcement Interchange Format (CAIF)	An XML-based format for storing and exchanging security announcements

REPOSITORIES

Repositories allow common, standardized content to be used and shared, whether across broad communities or within individual organizations. The sharing of content has been done for some time but doing so in standard machine-consumable languages and formats using standard enumerated concepts is fairly recent. Most of the listed repositories are in the midst of converting their content into machine-consumable form. Examples are shown in Table 3.

Table 3. Repositories

Name	Topic
Department of Defense Computer Emergency Response Team (DoD-CERT)	Information Assurance Vulnerability Alerts (IAVAs) and Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGS)
The Center for Internet Security (CIS)	CIS Security Configuration Benchmarks
National Security Agency (NSA)	NSA Security Guides
National Vulnerability Database (NVD)	US-CERT advisories, US-CERT Vuln Notes, CVE and CCE Vulnerabilities, Checklists, OVAL Definitions, and U.S. Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP) content
Red Hat Repository	OVAL Patch Definitions for Red Hat Errata security advisories
OVAL Repository	OVAL Vulnerability, Compliance, Inventory, and Patch Definitions

These are all examples of very public repositories with a variety of types of content that will be recast into standardized machine-consumable form using some of the Languages identified in Table 2 and the Enumerations in Table 1, but there are also closed repositories where, for instance, a company may write a tailored set of policies about what they want to do to comply with Sarbenes-Oxley or something similar. They don't necessarily want to share with the world, but they want to be standard across all of the different elements of their company and they want it available for their auditors and possibly their partners.

UNIFORMITY OF ADOPTION

Uniform adoption of standards by the community is best achieved through branding/vetting programs that can help the tools, interactions, and content remain conformant with the accepted standards.

MITRE's CVE project has employed a highly successful CVE Compatibility Program that has vetted numerous information security products and services to ensure they are "CVE Compatible," that is, that they can interoperate with other products that are also compatible and that they each have correctly mapped their capabilities concept of a particular vulnerability to the correct CVE Identifier for that vulnerability. Similarly, OVAL has employed an OVAL Compatibility Program and CWE has begun a CWE Compatibility Program. NIST has also initiated a SCAP Validation Program for those vendors that currently provide, or intend to provide, SCAP-validated tools.

All of these programs, and others that may be developed in the future, will help ensure consistency within the security community regarding the use and implementation of the standards and to assure users of the tools, services, and information from those supporting the standards are doing so correctly and there is a high confidence that they will work correctly together.

HOW THE ARCHITECTURAL BUILDING BLOCKS COME TOGETHER

The building blocks of architecting for measurable security are already in use. The creation of benchmark documents is one example. An OMB memo dated June 1, 2007, entitled "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" [5] references the content in NVD. This guidance is also referred to as part of the Federal Desktop Core Configuration (FDCC) [6] and is intended to bring consistency in the specific secure system software configuration of Microsoft XP and VISTA used in the federal government. The part of the memo that is directed at VISTA directly points to a set of content that uses the XCCDF and OVAL languages along with the CPE and CCE enumerations [7, 8]. A year later, another OMB memo, dated August 22, 2008, entitled "Guidance on the Federal Desktop Core Configuration (FDCC)" [9] reinforced the earlier guidance, the utilization of SCAP for FISMA, and it highlights the FAR changes that made FDCC compliance a mandatory requirement of selling software to the U.S. Government. The SCAP and FDCC content hosted by NIST are examples of benchmark documents in a public repository using these standard languages and enumerations.

Figure 1 below shows how an organization can utilize a tool-consumable benchmark document from a knowledge repository for configuration guidance, like the OMB VISTA guidance from NVD, to provide the checking logic for a commercial tool that is used by the organization to conduct their configuration guidance analysis to assess the configuration compliance of the organization's computer systems.

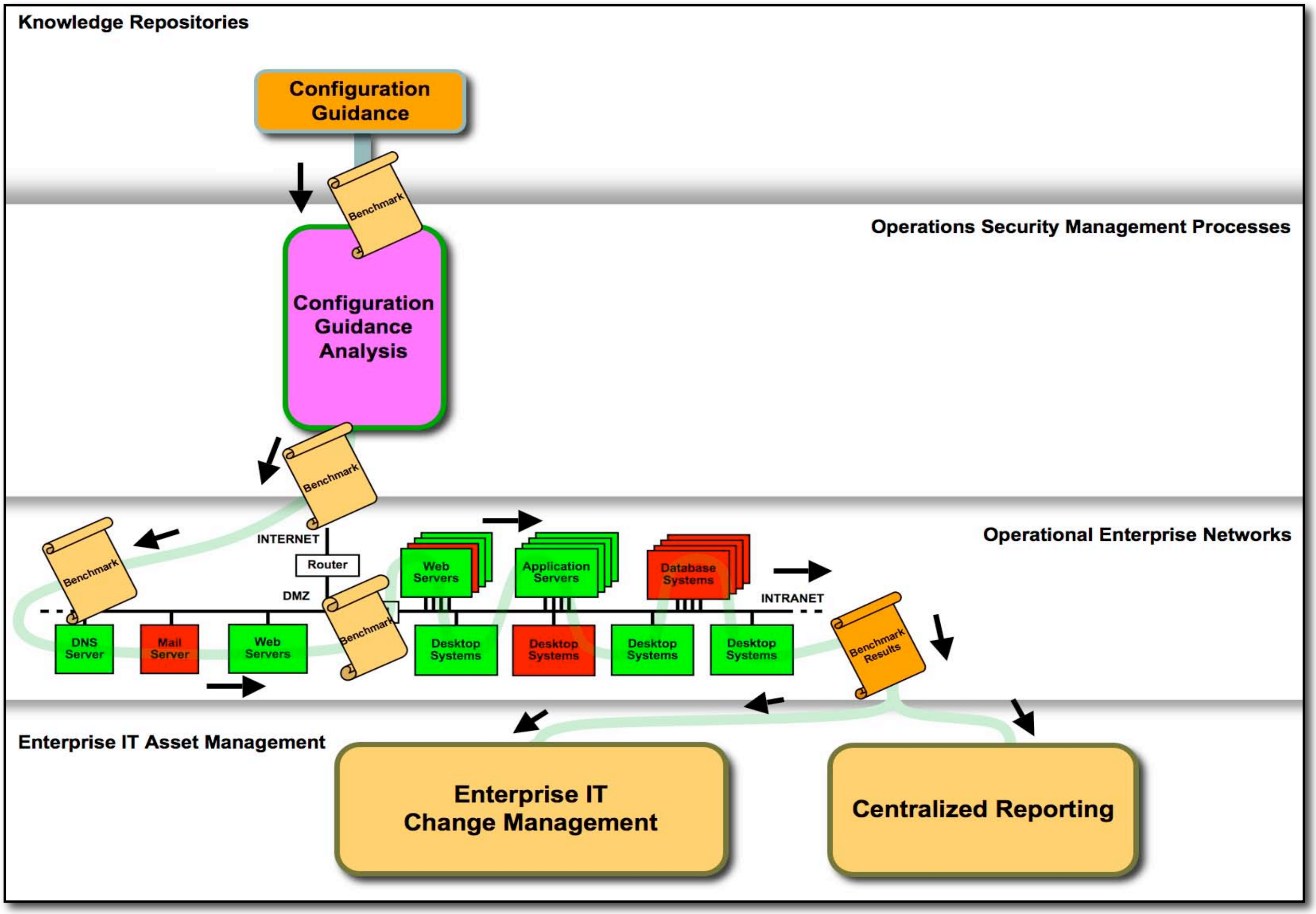


Figure 1: Assessment of Configuration Compliance Using Standards

As shown in Figure 1, the results of the benchmark examination are also provided in standard language and enumeration terms as it is fed to the enterprise's IT change management and central reporting processes. The configuration guidance analysis, enterprise IT change management, and centralized reporting activities depicted in Figure 1 are three of the security measurement and management activities abstracted by taking a systems engineering analysis view of some of the different security activities of an organization.

This same process of abstraction can be used to identify and define the other security measurement and management activities that an organization conducts. Figure 2 contains a current cut at these additional processes including an inventory asset activity, analysis of systems for vulnerabilities, analysis of threats, studying intrusion activities, notifications about incidents, assessment of systems development, integration, and sustainment activities as well as certification and accreditation of systems being deployed into the enterprise. Those can all be functional pieces to which you could manage.

Furthermore, Figure 2 illustrates how the different security measurement and management activities are tied together through standards-based data interfaces that utilize the standard enumerations and standard languages discussed earlier. By utilizing these abstracted activities and enforcing the use of the standards-based interactions between them, an organization can bring commercially available technologies and tools to bear on their security problems but still keep control of the processes and activities rather than ending up with activities that are defined by the scope of the tools being used and are coupled together by proprietary mechanisms.

Standard repositories of governance and guidance can help drive the business value of these standard measurement and management activities.

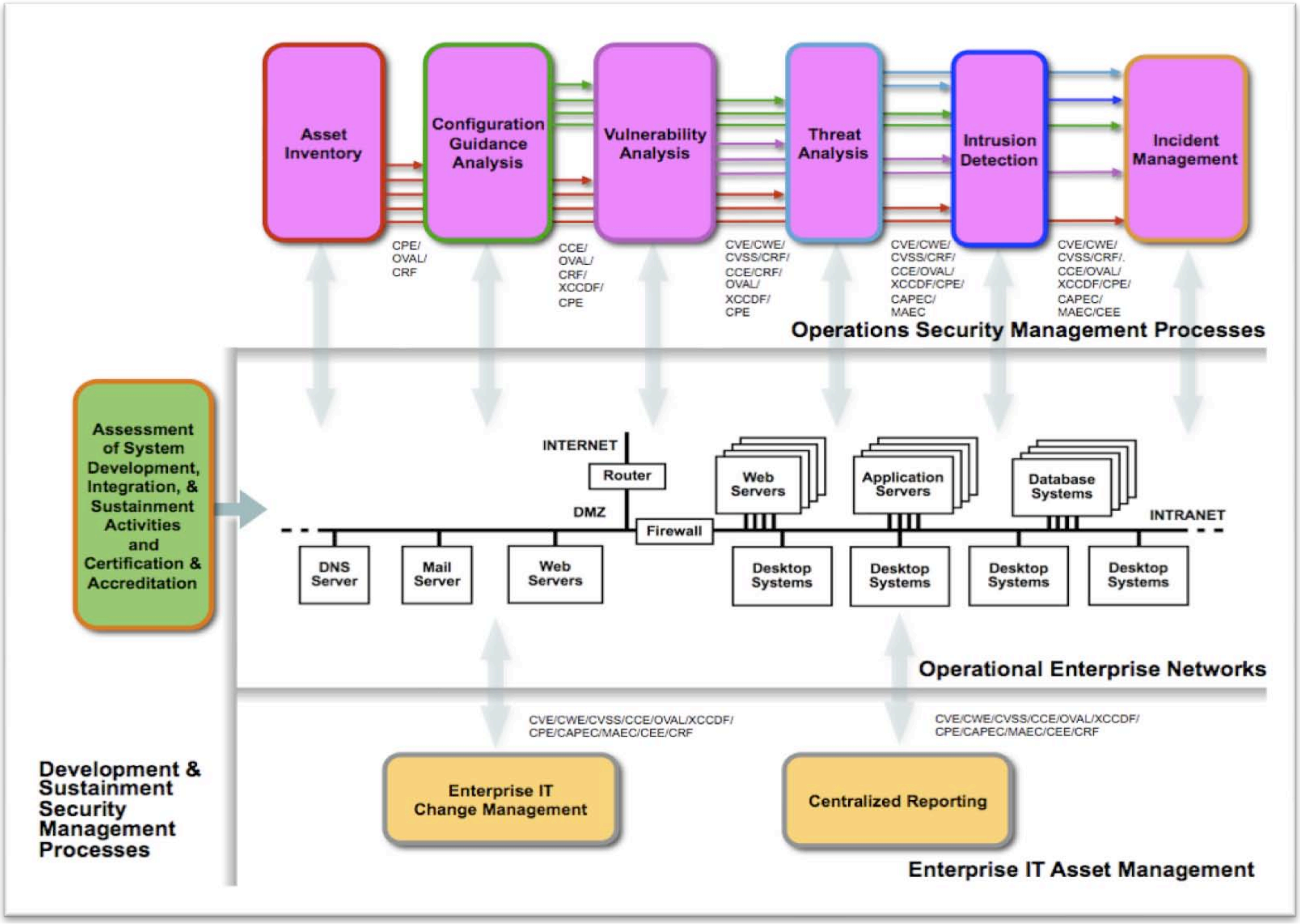

Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ CRF
CCE/ OVAL/ CRF/ XCCDF/ CPE
CVE/CWE/ CVSS/CRF/ CCE/CRF/ OVAL/ XCCDF/ CPE
CVE/CWE/ CVSS/CRF/ CCE/OVAL/ XCCDF/CPE/ CAPEC/ MAEC
CVE/CWE/ CVSS/CRF/. CCE/OVAL/ XCCDF/CPE/ CAPEC/ MAEC/CEE
Operations Security Management Processes
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/OVAL/XCCDF/ CPE/CAPEC/MAEC/CEE/CRF
CVE/CWE/CVSS/CCE/OVAL/XCCDF/ CPE/CAPEC/MAEC/CEE/CRF
Development & Sustainment Security Management Processes
Enterprise IT Change Management
Centralized Reporting
Enterprise IT Asset Management

Figure 2: Decomposition of Security Measurement and Management Activities

As shown in the OMB guidance examples, the information about how systems should be patched and configured is captured by CVE, OVAL, XCCDF, CCE, CVSS, and CPE. To leverage this standardization, the DoD requires support for these standards in its procurements of commercial capabilities [10,11,12].

REUSABLE AND SHARED REPOSITORIES

Similarly, as shown on the left side of Figure 3, these same standards can be used to capture how your organization has configured and set up a new system when it has been approved for use in your enterprise. By using these standards that information can go right into your operational network management so that you can make sure the new system continues to be configured the way it was approved. You can also include standard guidance about which weaknesses from CWE [13] you want to be reviewed in your own development activity or in your supplier's development activity. In addition, the common attack patterns from CAPEC [14] can be used to define and document the types of penetration testing and attack scenarios your development team thought about defending against when they were doing their development and penetration testing.

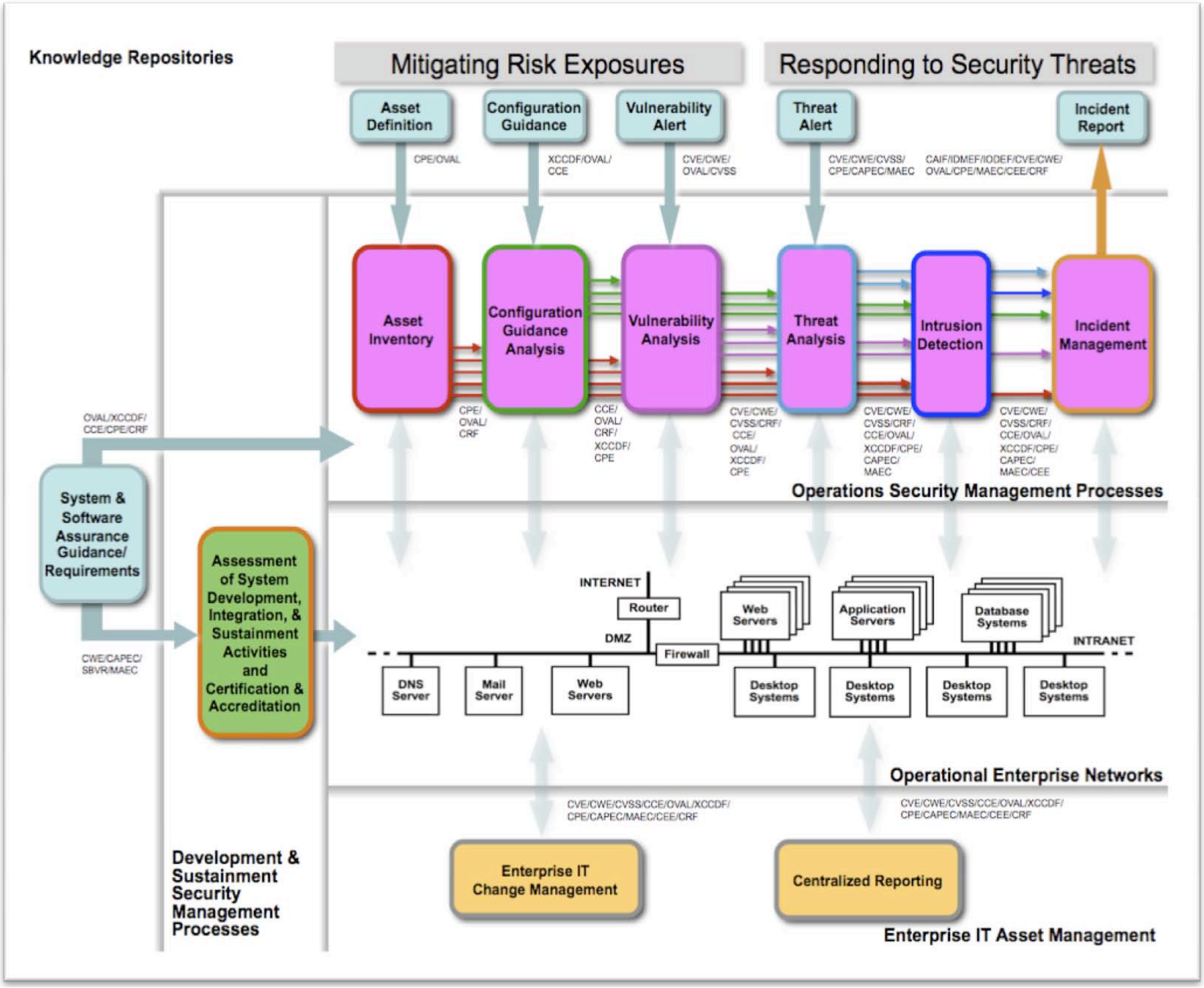

Knowledge Repositories
Mitigating Risk Exposures
Responding to Security Threats
Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE
CVE/CWE/ OVAL/CVSS
CVE/CWE/CVSS/ CPE/CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CEE/CRF
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ CRF
CCE/ OVAL/ CRF/ XCCDF/ CPE
CVE/CWE/ CVSS/CRF/ CCE/ OVAL/ XCCDF/ CPE
CVE/CWE/ CVSS/CRF/ CCE/OVAL/ XCCDF/CPE/ CAPEC/ MAEC
CVE/CWE/ CVSS/CRF/ CCE/OVAL/ XCCDF/CPE/ CAPEC/ MAEC/CEE
Operations Security Management Processes
OVAL/XCCDF/ CCE/CPE/CRF
System & Software Assurance Guidance/ Requirements
CWE/CAPEC/ SBVR/MAEC
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/OVAL/XCCDF/ CPE/CAPEC/MAEC/CEE/CRF
CVE/CWE/CVSS/CCE/OVAL/XCCDF/ CPE/CAPEC/MAEC/CEE/CRF
Development & Sustainment Security Management Processes
Enterprise IT Change Management
Centralized Reporting
Enterprise IT Asset Management

Figure 3: Repositories Feeding Standard Measurement and Management Activities

For asset inventory, standards-based information utilizing CPE and OVAL will let an organization know exactly what assets they have in a manner that is tool independent and usable in the other standard activities like configuration analysis. Similarly, if you know exactly how your assets are configured it's much easier to perform vulnerability analysis based on CVE, CWE, OVAL, and CVSS. Likewise, if you know what you have, and how it's configured, and what it's vulnerable to, that will change the context and framework of how you do threat analysis.

Vulnerability alerts, for example those in NVD, are another case in point. Sometimes these are standardized already, depending which source they come from. Errata from Red Hat, Inc. for example are regularly posted with CVEs, OVAL Definitions, and CVSS scores. In this area particularly, the standards have already been adopted by industry.

Threat alerts, however, are not yet as standardized. This is an area where standardization could happen, and efforts like MAEC are aimed at enabling that. Similarly, in incident reporting there are a lot of different ideas about what should be standardized and to what extent it should be standardized.

Finally, like any new area there are many aspects of usage that are still evolving. For example, the correct approach to managing changes, updates, or new content for shared repositories is evolving. The question of whether the repositories should be enabled as services, as static collections, or both is also open. Similarly, as new insights are made with respect to vulnerabilities, weaknesses, threats, and attacks there will surely be changes needed in how the different aspects of these types of information are knitted together and used. By bringing the various aspects of cyber security, information assurance, and software assurance into a consistent security architecture framework there will be many new opportunities and much faster responses to new threats and new information.

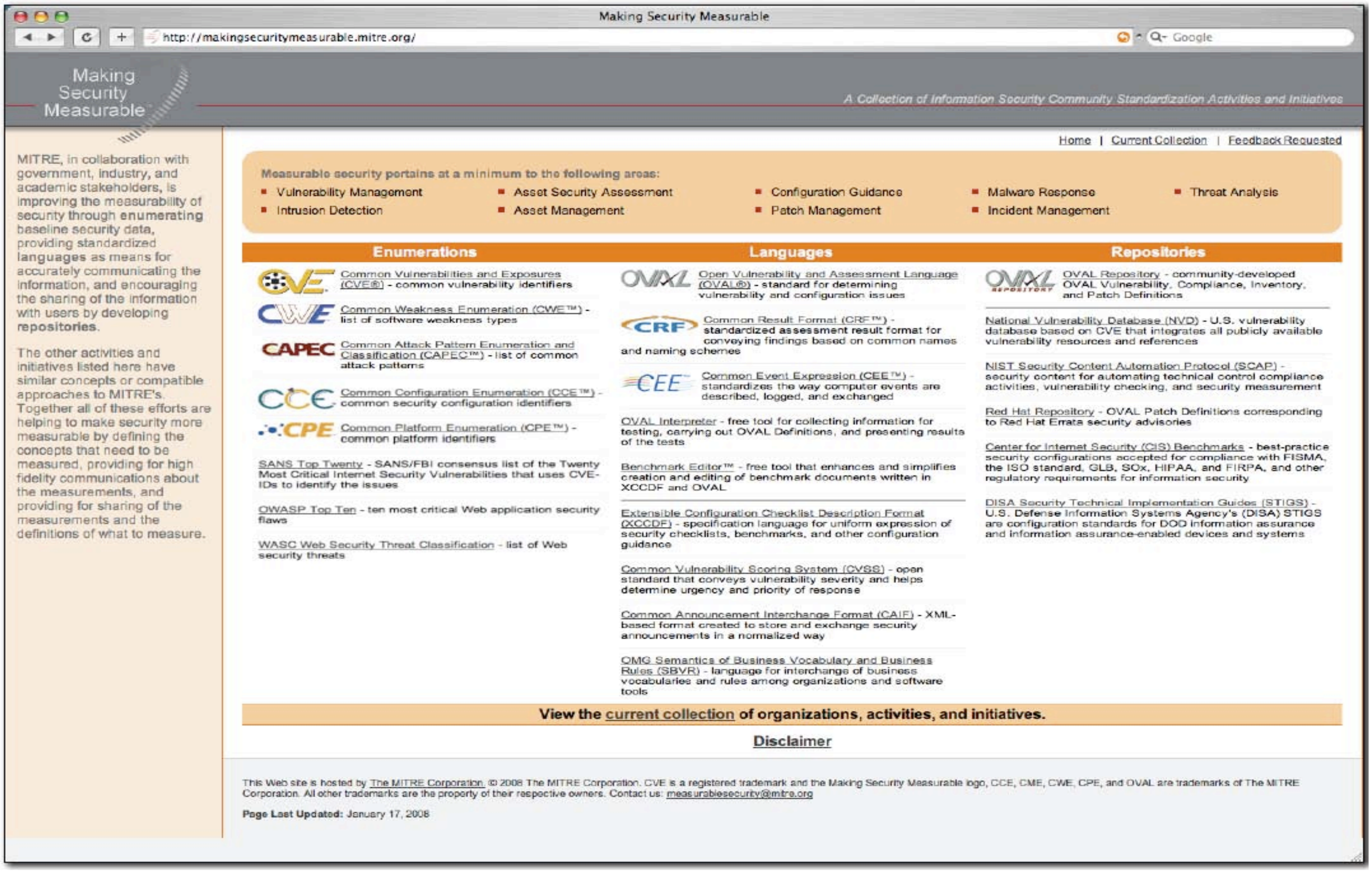
CONCLUSION

Measurable security and automation can be achieved by having government and the public efforts holistically address information security during the creation, adoption, operation, and sustainment in a holistic manner; use common, standardized concepts; communicate this information in standardized languages; share the information in standardized ways; and adopt tools that adhere to the standards.

A lot has been done to transform the way security measurement and management is conducted but there is still plenty of work that needs to be addressed. The use of architecture and systems engineering principals has been shown to be effective and enabling. Ongoing efforts to address and evolve all of the activities in this arena will greatly benefit from the continued application of this methodology and we are very interested in ideas for additional areas and functions that should be added into the Making Security Measurable efforts to ensure that collectively we address the key capabilities our enterprises and community need to transform the way we deal with security of our information resources and capabilities. Like most architecture efforts today the true value of architecture is not apparent or appreciated until its enabling properties start to manifest themselves as shown here. With the changes in security practices and technologies outlined in this paper we hope to show specific and measurable changes that can be directly related to the use of architectural methods on security of information technologies in government and private industry and the benefits in sharing that standardized information can bring.

By creating and evolving these types of standards and new approaches to security measurement and management each of us will need to step away from the traditional focus on local and enterprise issues and realize that much more powerful and productive solutions to these issues can be fostered through an emphasis on community-wide examinations of each of the technical areas where a multitude of concerns and needs are balanced and considered. The increased insights and ability to leverage the collective knowledge about what vulnerabilities and attacks affect us and what can be done to address them by leveraging everyone's insights and experience and being able to find out about new attacks and issues from those who encounter them first are valuable benefits to trading off local concerns against community-wide concerns.

To further the goal of making security measurable and encourage participation and adoption of the different aspects of this work, MITRE has established a public "Making Security Measurable" web site, shown in Figure 4, that informally collects all of the efforts listed in this paper, as well as others we know about, which together are helping or will help to make security more measurable. If you are aware of additional areas, or ways to better incorporate those already being addressed, we welcome your comments and suggestions and we would especially welcome participation of interested individuals and organizations that wish to contribute to these efforts.


Making Security Measurable
http://makingsecuritymeasurable.mitre.org/
Google
Making Security Measurable
A Collection of Information Security Community Standardization Activities and Initiatives
Home | Current Collection | Feedback Requested

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
- Intrusion Detection
- Asset Security Assessment
- 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 Configuration Enumeration (CCE™) - common security configuration identifiers

Common Platform Enumeration (CPE™) - common platform identifiers

SANS Top Twenty - SANS/FBI consensus list of the Twenty Most Critical Internet Security Vulnerabilities that uses CVE-IDs to identify the issues

OWASP Top Ten - ten 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 determining vulnerability and configuration issues

Common Result Format (CRF™) - standardized assessment result format for conveying findings based on common names and naming schemes

Common Event Expression (CEE™) - 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 (XCCDF) - 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 Announcement Interchange Format (CAIF) - XML-based format created to store and exchange security announcements in a normalized way

OMG Semantics of Business Vocabulary and Business Rules (SBVR) - language for interchange of business vocabularies and rules among organizations and software tools

Repositories

OVAL Repository - community-developed OVAL Vulnerability, Compliance, Inventory, and Patch Definitions

National Vulnerability Database (NVD) - U.S. vulnerability database based on CVE that integrates all publicly available vulnerability resources and references

NIST 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, GLB, SOx, HIPAA, and FIRPA, 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: measurablesecurity@mitre.org

Page Last Updated: January 17, 2008

Figure 4: Making Security Measurable web site (measurablesecurity.mitre.org)

REFERENCES

[1] Martin, R. A., “Transformational Vulnerability Management Through Standards”, CrossTalk: The Journal of Defense Software Engineering, May, 2005, (www.stsc.hill.af.mil/crosstalk/2005/05/0505Martin.html)

[2] “The Common Vulnerabilities and Exposures (CVE) Initiative”, MITRE Corporation, (cve.mitre.org)

[3] Ziring, N., Quinn, S., “The Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4.”, National Institute of Standards and Technology, January 2008, (csrc.nist.gov/publications/nistir/ir7275r3/NISTIR-7275r3.pdf)

[4] “The Open Vulnerability and Assessment Lanugage (OVAL) Initiative”, MITRE Corporation, (oval.mitre.org)

[5] Evans, K. S., “OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations”, 1 June, 2007.

[6] “The Federal Desktop Core Configuration (FDCC) Effort”, National Institute of Standards and Technology, (nvd.nist. gov/fdcc/index.cfm)

[7] “The Common Platform Enumeration (CPE) Initiative”, MITRE Corporation, (cpe.mitre.org)

[8] “The Common Configuration Enumeration (CCE) Initiative”, MITRE Corporation, (cce.mitre.org)

[9] Evans, K. S., “OMB Memorandum for Chief Information Officers: Guidance on the Federal Desktop Core Config-uration (FDCC)”, 22 August 2008.

[10] DISA IASSURE contract 2004 Task Order 232 (www.ditco.disa.mil/public/discms/IASSURE/00232_00.doc), Jun. 3, 2004.

[11] DISA IASSURE contract 2004 Task Order 254, (www.ditco.disa.mil/public/discms/IASSURE/00254_00.doc), Sep. 24, 2004.

[12] DISA “Asset Configuration Compliance Module” RFI, Solicitation Number ACCMRFI, (www.fbo.gov), Aug. 5, 2008.

[13] “The Common Weakness Enumeration (CWE) Initiative”, MITRE Corporation, (cwe.mitre.org)

[14] “The Common Attack Pattern Enumeration and Classification (CAPEC) Initiative”, MITRE Corporation, (capec.mitre.org)