Systems Assurance as a Team Sport

Robert A. Martin
The MITRE Corporation

It is time for individual procurement officers—and those who work with the vendors and software developers creating or delivering our day-to-day mission software-based systems—to contribute to, and accelerate the adoption of, standards-based cybersecurity. This article outlines several practical and straightforward steps that professionals can take to speed the adoption of the enterprise security initiatives currently under way, and to make those efforts have a greater and quicker impact.

Many exciting and important changes are happening within the marketplace of cybersecurity capabilities and the way organizations address compliance, assurance, and security. As documented in [1, 2, 3, 4], MITRE has collaborated with industry, government, and academia throughout the last 10 years. They have fostered the creation and adoption of a number of information security standards that are changing the concepts of compliance, assurance, and security in enterprises, products, and practices.

While still evolving, several of these standardization efforts have made their way into commercial solutions and government, industry, and academic use. Perhaps the most visible of these have been the:

- Common Vulnerabilities and Exposures (CVE) initiative.
- Executive Office of the President–Office of Management and Budget (EOP-OMB)-mandated (see [5, 6, 7, 8, 9]) Federal Desktop Core Configuration (FDCC) effort that leverages the Security Content Automation Protocol (SCAP).
- Consensus Audit Guidelines [10].
- Build Security In (BSI) initiative.

CVE is utilized by the majority of the vulnerability-related information providers and tool vendors. The SCAP utilizes CVE and the other mature standardization efforts to clearly define common security nomenclature and evaluation criteria for vulnerability, patch, and configuration measurement guidance; it is intended for adoption by automated tools. By specifying and measuring compliance in terms of these standardized concepts, the community is moving towards *compliant all the time* based on automated measurement. This method takes an annual or tri-annual activity that had questionable insights about the current security posture of an enterprise and makes it into a consistent way of *knowing* both how and that your enterprise is secured.

Similar to the transformation in operational security measurement (motivated by the CVE initiative, FDCC, and the SCAP) are the changes under way in assuring the resilience and code security of the software making up the applications and systems software bought and built in organizations and government entities. The BSI initiative is a software assurance effort that provides practices, tools, guidelines, rules, principles, and other resources software developers, architects, and security practitioners can use to build security into software in every phase of its development. BSI leverages the Common Weakness Enumeration (CWE) and the Common Attack Pattern Enumeration and Classification (CAPEC) efforts.

> *"While still evolving, several of these standardization efforts have made their way into commercial solutions and government, industry, and academic use."*

To measure and manage their cyber assets, an enterprise will need to employ consistent approaches that are supported by automation techniques, typically using products from a variety of different vendors. To make the finding and reporting of issues consistent and composable across different groups of practitioners and tools, there has to be a set of standard definitions of the things that are being examined, reported, and managed [4].

To reach this level of capability, the standardization has to make sense to commercial industry so that it will be adopted in baseline products and practices, and to the academic world so that research will continue to advance the state of the art in a complementary manner.

While there has been great progress in bringing standardization to some activities and tools in some areas like the CVE initiative, the SCAP/FDCC, and BSI, there is still more that individuals can do. Those buying software products, creating organizational policies related to the security and resiliency of systems, or creating security guidance and benchmarks can help us all get to these greater capabilities faster by taking the actions outlined in this article.

Procurement Guidance for Purchasing Software

As a procurement officer, you can make sure that the products being offered are compliant with the new Federal Acquisition Regulation provision [11], specifying compliance with the FDCC. Additionally, procurement officers can levy requirements on the software providers to:

- Submit a Common Platform Enumeration (CPE) name for each new release of the provider's software.
- Have a public address (e-mail and/or Internet) for the reporting of security relevant issues with the provider's software.
- Have a publicly available statement of the time frame and process that the software provider's organization follows in addressing reports of security relevant issues with the provider's software.
- Have public advisories of relevant security-related issues and their resolution.
- Include a CVE Identifier for security-related issues when the issues are related to a software flaw or default setting that constitutes a security shortcoming in the provider's software (as part of the initial public advisory).
- Include an initial Open Vulnerability and Assessment Language (OVAL) definition(s) as a machine-readable description of how to tell if the flaw,

misconfiguration, or incorrect default settings are present and whether any of the known resolutions have been taken as part of the initial public advisory.
- Include the base and initial temporal severity score portions of the Common Vulnerability Scoring System (CVSS) rating for the flaw or incorrect default settings as part of the initial public advisory.
- Provide advice to customers on how to securely configure their software and do so utilizing the standards within the SCAP. Specifically, offer eXtensible Configuration Checklist Description Format (XCCDF) and OVAL documents representing the vendor's recommendations on secure configuration. Include the appropriate Common Configuration Enumeration (CCE) identifiers for the configuration controls that they recommend settings for and CPE names for the software packages discussed.
- Identify and discuss the assurance activities that their software products go through—in terms of the CWE names that are reviewed and tested for and the CAPEC names utilized in the analysis and evaluation activities performed on their software.

Government Organizations

As a government organization decides how systems should be set-up for operational use, standards can be used to convey this *blessed* configuration. This is referred to in [12] as a SCAP-expressed checklist. Specifically, government organizations can levy requirements on their user communities to:
- Express policies and guidelines in the XCCDF/OVAL languages so that tool technologies can use these machine-readable descriptions to evaluate the status of information technology with regards to those policies and guidelines.
- Adopt automated methods utilizing the machine-readable XCCDF/OVAL policies and guidelines for assessing, reporting, and directing action on exceptions to the policies and guidelines.

Similarly, as a government organization establishes its approach to gaining assurance about the robustness, integrity, and secureness of the software its systems contain, standards can be used to clarify and specify the types of evidence and insights needed to gain sufficient software assurance. Specifically, government organizations can require their user communities to:
- Express policies and guidelines about the assurance of a capability by discussing the security weaknesses that have been vetted for in terms of CWE names and methods used to verify and test for security issues in terms of CAPEC names.
- Adopt the use of automated assessment methods that utilize CWE and CAPEC for assessing, reporting, documenting, and directing action on weaknesses and exceptions to the assurance policies and guidelines. This way, issues can be tracked and managed in a vendor-neutral and consistent manner.

Procurement Guidance for Purchasing Security Tools

In general, procurement and end-users should request or require that the vendors of security products that deal with security flaws, configuration settings, policies, or patches support the SCAP standards. It is strongly recommended that the automated tools used to implement or verify security controls employ SCAP (or similar standardization) efforts for clearly defined nomenclature and evaluation criteria not covered by the SCAP. Specifically, these types of products and services should:
- Include the appropriate CVE Identifier for security information that is related to a software flaw or a non-secure default setting.
- Provide for the searching of security-related information by CVE Identifier.
- Incorporate the machine-readable tests for flaws, patches, and configuration checks written in conformance with the OVAL Definition Schema.
- Generate machine-readable assessment results from tests for flaws, patches, and configuration checks in conformance with the XCCDF and OVAL Results Schema. In the near future, expect products to produce results in the Assessment Results Format, which is an emerging SCAP specification that describes an XML Schema for sharing per-device assessment results of devices on IP-routed networks.
- Incorporate the machine-readable results from flaw, patch, and configuration check assessments that are written in conformance with the OVAL Results Schema.
- Incorporate, as appropriate to the functionality of the tool, support for the different severity score portions of the CVSS rating for the flaw or incorrect default settings.

An *assurance ecosystem* has emerged around these various types of enumerative and language-based standardization and has been adopted in various ways by government and commercial industry[1]; it continues to provide the framework to the academic world for continued research and to industry in advancing the state of the art in a complementary, interoperable manner.

While there has been great progress in bringing standardization to many practices and tools, there is more that individuals can do to push even greater capabilities to emerge in a timely manner. Procurement officials and consumers of software products, as well as organizational security policy makers, should take more deliberate action to demand secure products and create security guidance and benchmarks, in turn helping to get to these greater capabilities faster; [12] addresses many aspects of this issue. Similar adoption endorsement initiatives and efforts—to move forward and support other useful standards initiatives—

Table 1: *Emerging Standardization Efforts*

Activity	Focus	Web site
Assessment Results Format	Result Reporting	<http://msm.mitre.org/incubator>
Common Event Expressions	Security Events	<http://cee.mitre.org>
Policy Language for Assessment Results Reporting	Result Reporting	<http://msm.mitre.org/incubator/plarr>
Malware Attribute Enumeration and Characterization	Malware Attributes	<https://buildsecurityin.us-cert.gov/swa/malact.html>
Common Remediation Enumeration	Remediation Actions	<http://msm.mitre.org/incubator>
Common Remediation Language	Remediation Actions	<http://msm.mitre.org/incubator>
Open Checklist Interactive Language	Interactive Survey Questions	<http://scap.nist.gov/specifications/ocil>
Open Checklist Reporting Language	Interactive Survey Answers	<http://ocrl.mitre.org>

Software Defense Application

The rollout of efforts like SCAP-enabled operational measurement is setting the stage for higher levels of assurance in cybersecurity, but it must be balanced with similar levels of assurance in the software products themselves. Additionally, all of the other commercial and open source applications and capabilities fielded in the DoD must participate in these efforts. This article describes how the federal government and the commercial industries working our nation's critical industries and infrastructure can—by embracing and accelerating the adoption of these standards efforts into all the procurement and development efforts in defense—make the promises of greater assurance and resiliency happen faster and more completely.

will be important in creating needed changes to their operational use and in bringing discipline and repeatability into security measurement [13, 14].

While already making many useful and needed changes possible, these common enumerations and languages will continue to evolve and grow to cover additional areas of standardization. Some of the emerging areas already being worked as standardization efforts are for security events, malware attributes, attack patterns as operational model templates, remediation actions, and interactive survey questions and result reporting (as shown in Table 1, previous page).

These new standardization areas (like those outlined in this article) have the potential to evolve into similarly beneficial standards efforts for those working to secure their enterprises. The key to realizing the promise of these new efforts are the communities working on them and the inclusiveness and fair-handedness of the process surrounding these efforts. The growth and maturity of these new areas should be monitored and evaluated against today's threats and operational challenges. This way, organizations can leverage the ideas and processes as soon as possible and anyone with insights and interests in these areas can get involved.◆

References

1. Martin, Robert A. "The Vulnerabilities of Developing on the Net." CrossTalk Apr. 2001 <www.stsc.hill.af.mil/crosstalk/2001/04/martin.html>.
2. Martin, Robert A. "Transformational Vulnerability Management Through Standards." CrossTalk May 2005 <www.stsc.hill.af.mil/crosstalk/2005/05/0505Martin.html>.
3. Martin, Robert A. "Being Explicit About Security Weaknesses." CrossTalk Mar. 2007 <www.stsc.hill.af.mil/crosstalk/2007/03/0703Martin.html>.
4. Martin, Robert A. "Making Security Measurable and Manageable." CrossTalk Sept. 2009 <www.stsc.hill.af.mil/crosstalk/2009/09/0909Martin.html>.
5. Evans, Karen. "Managing Security Risk By Using Common Security Configurations." *EOP-OMB Memorandum for Chief Information Officers and Chief Acquisition Officers*. 20 Mar. 2007 <www.cio.gov/documents/Windows_Common_Security_Configurations.doc>.
6. Johnson, Clay. "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems." *EOP-OMB Memorandum for Chief Information Officers and Chief Acquisition Officers*. M-07-11. 22 Mar. 2007 <www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-11.pdf>.
7. Evans, Karen S., and Paul A. Denett. "Ensuring New Acquisitions Include Common Security Configurations." *EOP-OMB Memorandum for Chief Information Officers and Chief Acquisition Officers*. M-07018. 1 June 2007 <www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-18.pdf>.
8. Evans, Karen S. "Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations." *EOP-OMB Memorandum for Chief Information Officers and Chief Acquisition Officers*. 31 July 2007 <www.cio.gov/documents/FDCC_memo.pdf>.
9. Evans, Karen S. "Guidance on the Federal Desktop Core Configuration." *EOP-OMB Memorandum for Chief Information Officers and Chief Acquisition Officers*. M-08-22. 11 Aug. 2008 <www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf>.
10. "Twenty Critical Security Controls for Effective Cyber Defense: The Consensus Audit Guidelines." SANS Institute. Vers. 2.3. 13 Nov. 2009 <www.sans. org/critical-security-controls/cag.pdf>.
11. DoD – General Services Administration, and NASA. "Federal Acquisition Regulation; FAR Case 2007–004, Common Security Configurations." 28 Feb. 2008 <http://download.microsoft.com/download/7/6/c/76c0483d-425e-4d99-8d08-15414cf504a2/FAR%202007-004.pdf>.
12. Barrett, Matthew, et al. "Guide to Adopting and Using the Security Content Automation Protocol (Draft)." *NIST SP 800-117*. May 2009 <http://csrc.nist.gov/publications/drafts/800-117/draft-sp800-117.pdf>.
13. "The MITRE Corporation – Information Security Data Standards." *Making Security Measurable*. 10 Sept 2009 <http://makingsecuritymeasurable.mitre.org/list/>.
14. Information Assurance Technology Analysis Center. *Measuring Cyber Security and Information Assurance – State-of-the-Art Report*. 8 May 2009 <http://iac.dtic.mil/iatac/download/cybersecurity.pdf>.

About the Author

Robert A. Martin is a principal engineer in MITRE's Information and Computing Technologies division. For the past nine years, his efforts have been focused on the interplay of enterprise risk management, cybersecurity standardization, critical infrastructure protection, and the use of software-based technologies and services. Martin is a member of the Association for Computing Machinery, Armed Forces Communications and Electronics Association, IEEE, and the IEEE Computer Society. He has bachelor's and master's degrees in electrical engineering from Rensselaer Polytechnic Institute, and an MBA from Babson College.

The MITRE Corporation
202 Burlington RD
Bedford, MA 01730-1420
Phone: (781) 271-3001
E-mail: ramartin@mitre.org

Note

1. The Web sites for these main standardization efforts are: CVE <http://cve.mitre.org>, SCAP <http://scap.nist.gov>, FDCC <http://fdcc.nist.gov>, BSI <http://buildsecurityin.us-cert.gov>, CWE <http://cwe.mitre.org>, CAPEC <http://capec.mitre.org>, CPE <http://cpe.mitre.org>, OVAL <http://oval.mitre.org>, CVSS <www.first.org/cvss>, XCCDF <http://nvd.nist.gov/xccdf.cfm>, CCE <http://cce. mitre.org>.