Transformational Vulnerability Management Through Standards

Robert A. Martin
MITRE Corporation

The Department of Defense's new enterprise licenses for vulnerability assessment and remediation tools [1,2] call for use of capabilities that conform to both the Common Vulnerabilities and Exposures (CVE) [3] and Open Vulnerability and Assessment Language (OVAL) [4] standards efforts, as does a new Air Force enterprise-wide software agreement with Microsoft [5]. These contracting activities are part of a larger transformation of the Department of Defense's (DoD's) management and measurement of the information assurance posture of their network-enabled systems with respect to vulnerabilities, configuration settings, and policy compliance. In combination with procedural changes, the adoption of these [6] and other standards, such as the National Security Agency's (NSA's) Extensible Markup Language (XML) Configuration Checklist Data Format (XCCDF) [7], are making it possible to radically improve the accuracy and timeliness of the DoD's remediation and measurement activities which are critical to ensuring the network and systems integrity of their network-centric warfare capabilities.

Introduction

The basic process for addressing unexpected security-relevant flaws in any commercial or open source software used in any organization, including the DoD, starts with the discovery of a security-relevant flaw in that software. The discoverer could be the software creator themselves, an outside researcher, or a user of the software. The next step is usually for the software creator to be informed of the potential security-relevant flaw in order to start evaluating the flaw and looking for potential resolutions.

Eventually, a fix and possible workarounds to the flaw(s), if it turns out to be real, is released to the customers of the software. This is usually done through a security advisory or bulletin from the software creator, and/or by the researcher that discovered the flaw. Subsequently, the community of security tool developers that check for security flaws in deployed software start the task of figuring out how to check for this new public security flaw and its fixes. For the majority of these developers the only information they have to start with is the narrative from the security advisory or bulletin. In short order most security assessment tool developers will update their tools to look for and report the status of systems with respect to this new security-relevant flaw. Exactly how each tool checks for the flaw and its possible resolutions is usually not known to the tool users.

DoD's Current Flaw Management and Measurement Process

In the DoD there is keen interest in ensuring that critical security-relevant flaws are sought out and addressed in a timely manner. Not all flaws that are discovered and made public will be relevant to the DoD, only those that involve the specific platforms, operating systems, and applications in use in the DoD are of interest. The DoD process of identifying which publicly known flaws need to be addressed and the timeframe for addressing them results in one of three notifications, called Information Assurance Vulnerability Alerts (IAVAs), Information Assurance Vulnerability Bulletins (IAVBs), and Information Assurance Vulnerability Technical Advisories (IATAs) [8,9]. Depending on the potential impact of the flaw it will be included in one of these three notifications – unless the impact is thought to be insignificant.

DoD organizations are responsible for addressing the flaws discussed in these different notifications and for recording their progress and completion in resolving the flaws. Collectively, this is referred to as the "IAVA Process." A new flaw that must be assessed, reported upon, and remediated can be referred to as a new "IAVA Requirement."

Today that process is very dependent on manual reporting methods, as illustrated in figure 1, which starts with a known "compliant" system that has addressed all known flaws. The figure shows how the discovery of a new flaw proceeds to the assessment for that flaw, followed by the reporting of the status with respect to that flaw, and the remediation of the flaw, with the subsequent return to a known "compliant" state.

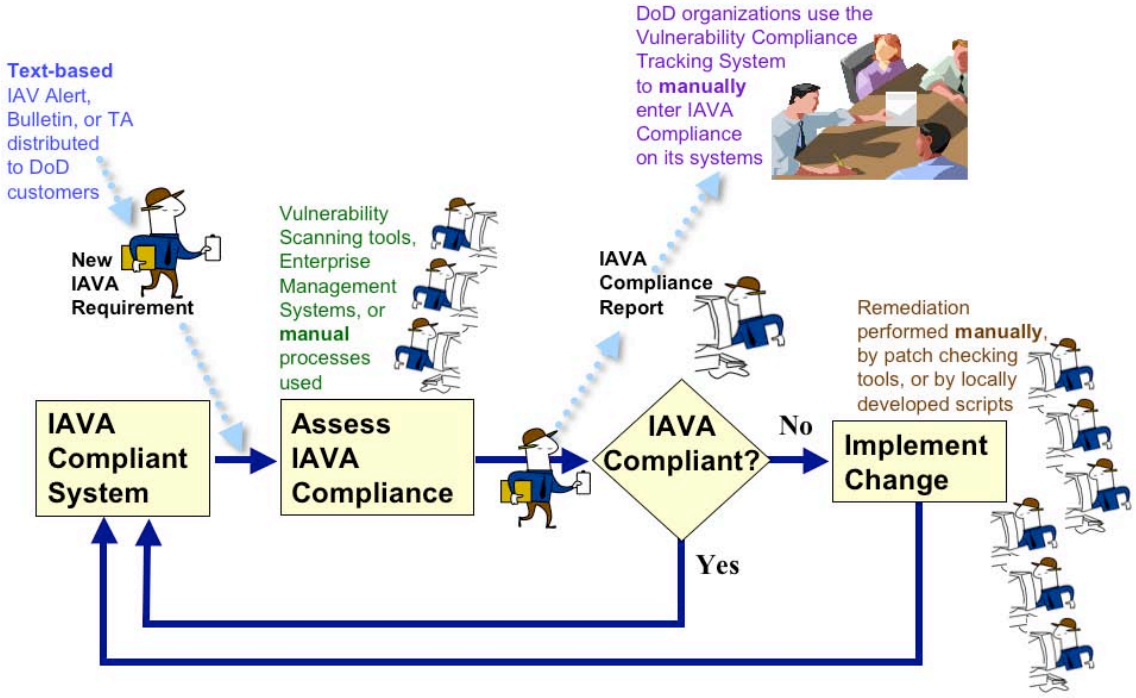


Figure 1: IAVA Process

Quick, Complete, and Dependable Knowledge

There are many opportunities for improving the original IAVA Process and the information sources upon which it relies. Some of the most striking opportunities are improving the quality of the information contained in the original announcements about new flaws; improving the accuracy, completeness, and timeliness of security tool vendor's incorporation of tests for new flaws; minimizing the dependence on manual reporting within the enterprise; overcoming the difficulty in combining reports and findings from various tools due to differences in their format, test criteria, and test methods; and eliminating the need for reassessment as part of the remediation process. The opportunity for improvements in all of these areas comes from the lack of standardization in the vulnerability management arena.

Standard Machine-Readable Flaw Definitions

Why do we tolerate having each security tool developer recreate the knowledge of how to identify a new flaw, when the organization that tells everyone about it has much more knowledge about the flaw since they are usually studying it and its possible remediation methods for some time while they prepare to make the flaw public? If the discoverer could pass its knowledge along to the tool developers in a quick and precise way wouldn't we all benefit, especially if it was done in a non-exploit manner? Most advisory/bulletin writers try to explain how to determine if you have the flaw they are writing about – but they do it in narrative English and without any consistency. The OVAL Initiative is an xml-based language standard that is specifically designed to address this issue.

Different Criteria

Why do we put up with different tools using different methods for determining whether a particular flaw exists on one of our systems? Currently you can be running one assessment tool that examines the banner reply from a networked service and then determines whether you have the flawed software based on the banner contents. Another tool may try an exploit over the network to see if the flaw is there. A third tool may authenticate itself to the system so that it can gain access to the file system-level information and determine whether the flawed version of the software is installed, and then check for whether the appropriate patch or service pack is there. Finally, a fourth tool may do these system-level checks and then also check whether other remediation approaches, like changing the ownership of the flawed software to root (which makes it unavailable for general users to run), could make the flaw un-exploitable.

If an organization has different tools using different testing methods – with most of the test criteria being hidden – it is easy to see that combing results of tools together may not be straightforward. Additionally, not knowing how a tool is checking for a flaw can make it very difficult to determine whether systems are safe or exploitable. With such a large variety of test methods and results, most remediation tools treat the results of assessment tools as good suggestions of where to start looking for flaws and then end up doing their own assessment before making recommendations on remediation approaches. With time being a critical factor why should we being doing assessments for the same flaws more than once? The OVAL Initiative is designed to address these issues. Additionally, most network assessment based tools are adding capabilities to allow for authenticated access to systems so they can produce more definitive findings as to whether a particular flaw exists on a system. This trend allows network tools to use OVAL test definitions for these new checks.

Combining and Communicating Vulnerability Assessment Information

What would the impact be from having a choice of different assessment tools that all were using known testing criteria and each provided standardized results? Assuming that these results contained the minimum necessary information to allow an organization to combine the findings of different tools for creating an organizational status report, we could stop trying to use a single all-encompassing tool but rather select appropriate tools based on what they do well. For instance, one may do well on network components like routers and switches, while another covers security appliances another Windows-based standard applications, another Solaris, and so on. With standard results formats and structures we could get the enterprise insight we need without giving up the power of specialization. The OVAL Initiative's Result Schema is specifically aimed at addressing this. Additionally, with the right type of information being passed along we could eliminate some portion of the redundant assessment work that remediation tools are forced to undertake today.

DoD's Future Flaw Management and Measurement Process

By utilizing the CVE, OVAL, and XCCDF standards the DoD will be able to transform the IAVA Process into one that is predominantly based on machine-to-machine information flows that will improve the accuracy, timeliness, and manpower needed to address the flaws that are found in software. Figure 2 illustrates the revised IAVA Process where: "New IAVA Requirements" include OVAL Definitions on how to identify the new issue; assessment tools are capable of using the OVAL Definitions and they report their findings per the OVAL Results xml standard; and then these same standard-based results are fed into the reporting process and the remediation process. Various procurements have started requiring support for the standards that will enable the transition to this new IAVA Process. Work in transforming current checklists and checking guidelines into these standards is also underway which will set the stage for the formal process to be changed.

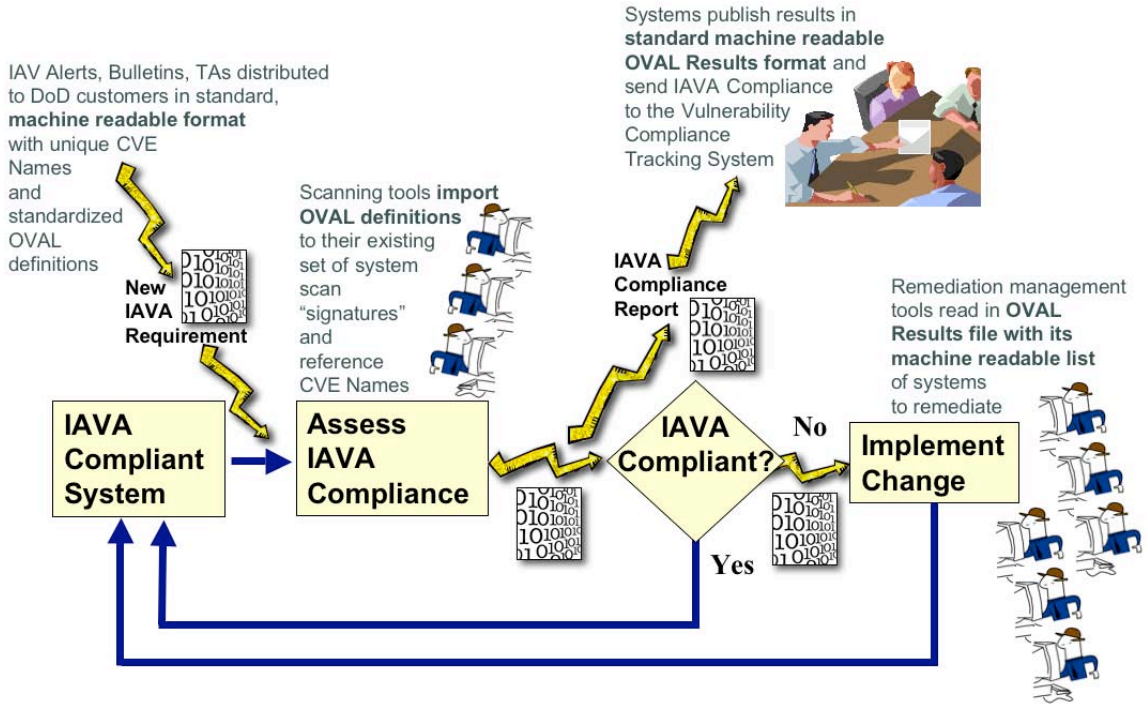


Figure 2: Standard-Based IAVA Process

Dealing With More Than Vulnerabilities

The DoD, like many organizations, has established criteria for how its operating systems and standard applications are configured. These criteria are usually different from the way the software suppliers ship the software from their distribution facility. DoD, through the work of the Defense Information Systems Agency (DISA), the NSA, the Center for Internet Security (CISecurity), and several vendors, has over the past few years come to a consensus on how operating systems and applications can be "locked down" to safer configurations. These settings can be checked by the free tools that CISecurity provides, but in the near future these configuration checks will be available as machine readable xml policy documents that use a combination of NSA's XCCDF and OVAL [10]. Additionally, the DoD's Security Technical Implementation Guidelines' (STIGs) configuration guidance [9] can be expressed as xml documents using XCCDF and OVAL, which would make both of these collections of policy tests on configuration settings usable within commercial and open source security tools that are able to import the xml test definitions.

Similarly, the testable portions of other policy efforts can be expressed as a combination of XCCDF and OVAL xml. Doing so would open the door to increased automation and improved fidelity in enterprise status reporting and management with respect to these efforts. The Director of Central Intelligence Directive (DCID) 6/3 [11], Defense Information Assurance Certification and Accreditation Process (DIACAP), Federal Information Security Management Act (FISMA) [12], and The SANS (SysAdmin, Audit, Network, Security) Institute's Top 20 [13] would all benefit from the clarity and automation that expressing their goals in machine-readable standardized languages provides. It would probably also significantly change the amount of time and labor that organizations dedicate to reporting and managing these efforts, versus adjusting their organization's systems to comply with them. Figure 3 illustrates how adoption of these types of standards could look.

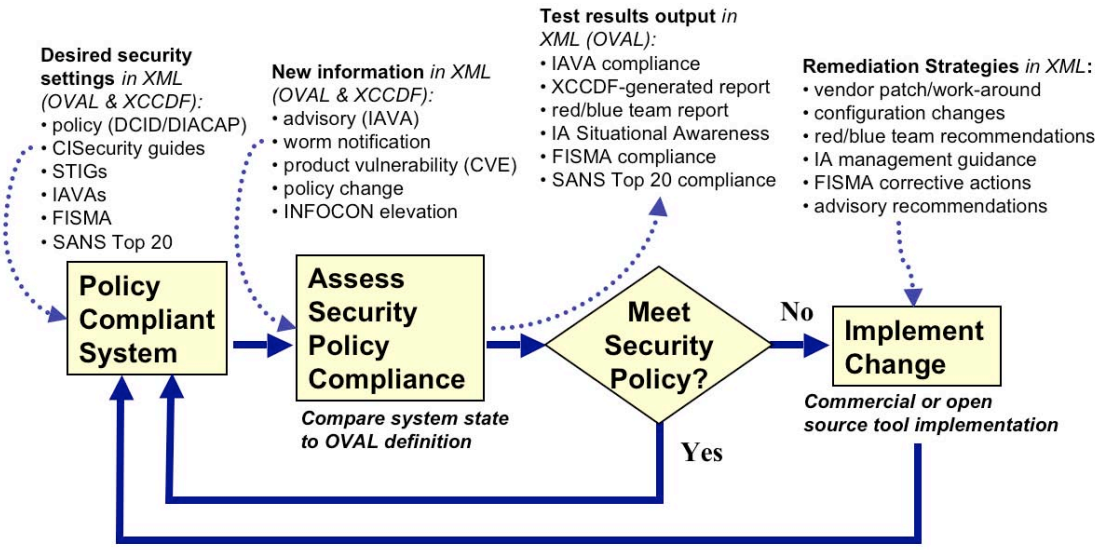


Figure 3: A Standard-Based Security Management Process

Patch Applicability Testing

The same types of information that are used for testing for flawed software, misconfigurations and adherence to stated policies can be used to check whether a particular patch can be applied to a system. The OVAL language includes a patch definition type that will support testing for whether the prerequisites for a patch are fulfilled, allowing an assessment tool to determine whether a particular patch can be applied to a system. Collectively the CVE, OVAL, and XCCDF standards describe a collection of interoperable functionality that will streamline the way security assessment and management are applied in the enterprise, opening the door for more interoperable and composable tool support as shown in Figure 4.

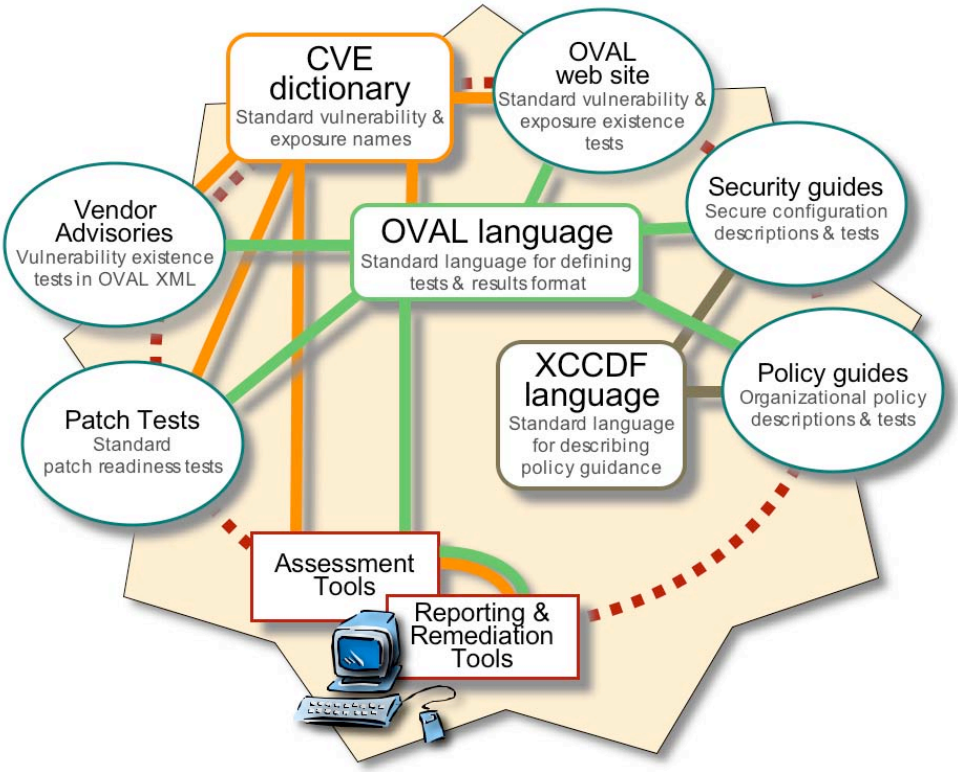


Figure 4: Standard-Enabled Information Security Automation

Conclusion

The DoD's new vulnerability and configuration standardization efforts are focused on the elimination or minimization of manual and non-automated aspects of these areas. The DoD is moving to their new process by requiring the inclusion of CVE names and standardized OVAL xml vulnerability and configuration tests in software supplier's alerts and advisories, and by acquiring tools that can import new and future OVAL xml test definitions and export their findings as standardized OVAL xml results. By also obtaining capabilities that can import the OVAL xml results for remediation, organizational status reporting, and generating certification and accreditation reports, the DoD will have created a focused, efficient, timely, and effective enterprise incident management and remediation process by adopting information security products, services, and methodologies that support the CVE naming standard and use OVAL test definitions and results schemas. By also adopting the XCCDF standard, the DoD will be able take the improvements in these areas onto a fuller set of policy and configuration management arenas. Collectively these changes will dramatically improve the insight and oversight of the security and integrity of the systems and networks underlying tomorrow's network-centric warfare capabilities.

Acknowledgments

The summary work contained in this article is based on the efforts of a large number of individuals, but special thanks is made for the contributions of Julie Connolly.

References

[1] DISA IASSURE contract 2004 Task Order 232 Statement of Work for eEye Digital Security's Retina, https://www.ditco.disa.mil/public/discms/IASSURE/00232_00.doc, Jun. 3, 2004.

[2] DISA IASSURE contract 2004 Task Order 254 Statement of Work for Citadel's Hercules, https://www.ditco.disa.mil/public/discms/IASSURE/00254_00.doc, Sep. 24, 2004.

[3] "The Common Vulnerabilities and Exposures (CVE) Initiative," MITRE Corporation (http://cve.mitre.org).

[4] "The Open Validation and Assessment Language (OVAL) Initiative," MITRE Corporation (http://oval.mitre.org).

[5] Fisher, Dennis, "Microsoft, Dell Snag Air Force Deal," eWeek Enterprise News & Reviews from ZIFF DAVIS MEDIA (http://www.eweek.com/article2/0,1759,1731420,00.asp), Nov. 29, 2004.

[6] DoD Instruction 8500.2, "Information Assurance (IA) Implementation," Section VIVM-1, Vulnerability Management, Mission Assurance Categories I, II, and III, pages 64, 75, 84, http://www.dtic.mil/whs/directives/corres/html/85002.htm, Feb. 6, 2003.

[7] Ziring, Neal and Wack, John, "NISTIR 7188 - Specification for the Extensible Configuration Checklist Description Format (XCCDF)," http://csrc.nist.gov/checklists/xccdf.html, Jan. 2005.

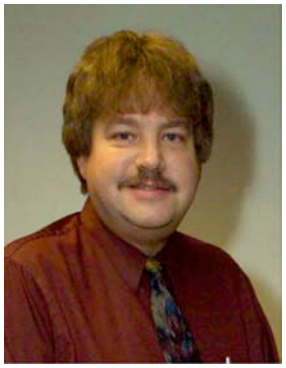
[8] DISA IAVA PROCESS HANDBOOK (http://www.tricare.osd.mil/contracting/healthcare/solicitations/TDP/0000/00_Attachment_16.pdf), Version 2.1, Jun. 11, 2002.

[9] Joint Task Force – Global Network Operations (JTF-GNO) NetDefense [DoD-CERT] web site, http://www.cert.mil/.

[10] Beale, Jay, "Ask the Linux Guru Column – "Big O" for Testing", Information Security Magazine, http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss526_art1075,00.html, Dec. 2004.

[11] Protecting Sensitive Compartmented Information Within Information Systems, Director of Central Intelligence Directives (DCID) 6/3, http://www.fas.org/irp/offdocs/DCID_6-3_20Policy.htm, Jun. 5, 1999.
[12] Federal Information Security Management Act (FISMA), Title III of the E-Government Act (Public Law 107-347), http://csrc.nist.gov/policies/FISMA-final.pdf, Dec. 2002.
[13] The SANS (SysAdmin, Audit, Network, Security) Institute's Top 20, http://www.sans.org/top20/, "The Twenty Most Critical Internet Security Vulnerabilities ~ The Experts Consensus," 2001-2004.

The Author



Robert A. Martin is a Principal Engineer in MITRE's Information Technologies Directorate. For the past five years, Martin's efforts have been focused on the interplay of risk management, cyber security standards, critical infrastructure protection, and the use of software-based technologies and services. Martin joined the MITRE Corporation in 1981 after earning a bachelor's degree and a master's degree in electrical engineering from Rensselaer Polytechnic Institute, subsequently he earned a master's of business degree from Babson College. He is a member of the ACM, AFCEA, IEEE, and the IEEE Computer Society.