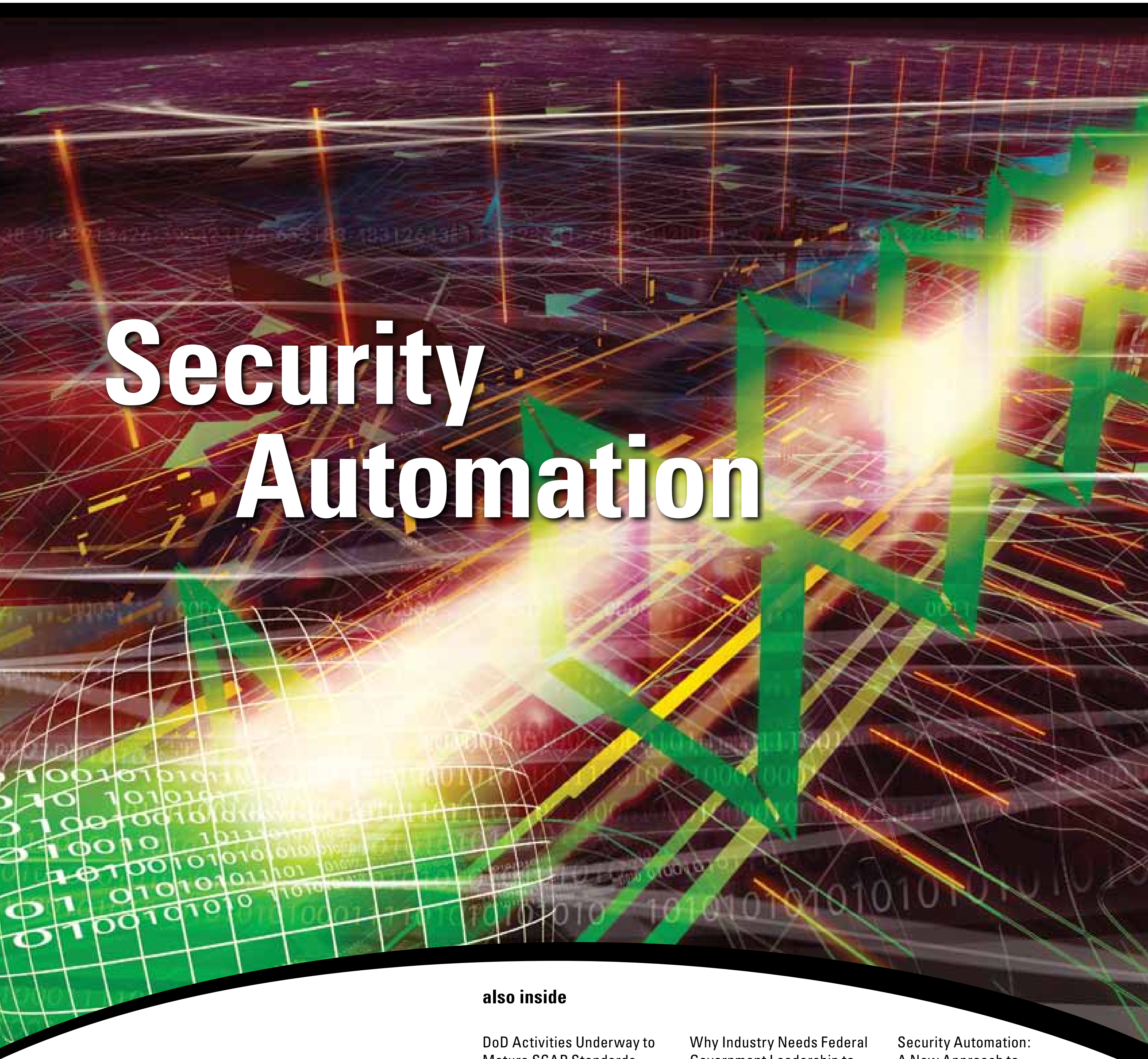
13/1

Volume 13 Number 1 • **Winter 2010**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



Security Automation

also inside

DoD Activities Underway to Mature SCAP Standards

The Security Content Automation Protocol (SCAP)

Ask the Expert

Secure Configuration Management (SCM)

Why Industry Needs Federal Government Leadership to Gain the Benefits of Security Automation

Practicing Standards-Based Security Assessment and Management

The DoD IA Policy Chart

Security Automation: A New Approach to Managing and Protecting Critical Information

Subject Matter Expert

DoDTechipedia Happenings

IATAC Spotlight on a University

IATAC

contents

About IATAC and the *IAnewsletter*
The *IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Director, Defense Research and Engineering (DDR&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, DTIC, or DDR&E. The mention of commercial products does not imply endorsement by DoD or DDR&E.

Inquiries about IATAC capabilities, products, and services may be addressed to—

IATAC Director: Gene Tyler
Inquiry Services: Peggy O'Connor

***IAnewsletter* Staff**
Art Director: Don Rowe
Copy Editor: Lindsay Marti
Designers: Kathryn Littlehale
Lacey Olivares
Brandi Samchisen
Editorial Board: Dr. Ronald Ritchey
Angela Orebaugh
Gene Tyler
Kristin Evans
Al Arnold

***IAnewsletter* Article Submissions**
To submit your articles, notices, programs, or ideas for future issues, please visit *http://iac.dtic.mil/iatac/IA_newsletter.html* and download an "Article Instructions" packet.

***IAnewsletter* Address Changes/Additions/Deletions**
To change, add, or delete your mailing or email address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road
Suite 6031
Herndon, VA 20171

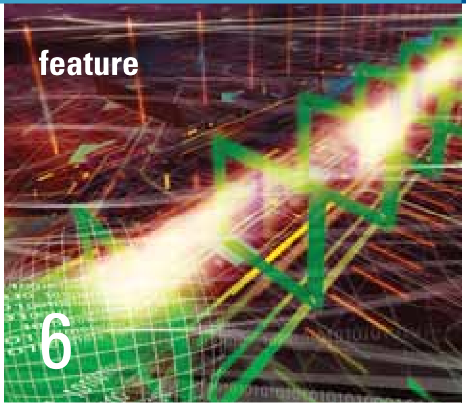
Phone: 703/984-0775
Fax: 703/984-0773

email: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*

Deadlines for Future Issues
Summer 2010 May 8, 2010

Cover design: Lacey Olivares
Newsletter design: Donald Rowe

Distribution Statement A:
Approved for public release;
distribution is unlimited.



in every issue

IATAC Chat

Gene Tyler, IATAC Director

I read a newspaper article that reinforced some of the information assurance (IA) issues I believe are most relevant today. It described the frustration Pakistani officials expressed because they did not receive actionable intelligence from U.S. agencies that might facilitate Pakistan's ability to target al Qaeda terrorists within its borders. The article discussed the same IA challenges that North Atlantic Treaty Organization scientist Brian Bottesini discussed in our last edition of the *IAnewsletter:* in order to collaborate on an international level, IA is transitioning from a "need to know" to a "need to share" environment. But what type of information, and how much information, can we share safely?

To provide the IA community with greater insight on IA and supply chain functions, IATAC is proud to announce the development of its *Security of the Supply Chain State of the Art Report* (SOAR).

The challenges we face on an international level, both in sharing information and maintaining information security, shed additional light on how difficult it really is for our first-line defenders to maintain a strong cyber defense.

This topic is the focus of this edition. Through security automation, how can we develop a stronger, more secure line of cyber defense for our first-line defenders? In his introduction, National Security Agency (NSA) veteran Tony Sager sets the stage for how the IA community is answering this question.

Of course, the IA challenges our warfighters face are widespread. A while back, the media exposed how the U.S. was outsourcing the manufacturing of its electronic U.S. passports. This issue raised additional questions about how secure our supply chain for U.S. information technology really is. As a result, the overall security of our supply chains has warranted more intense focus within the IA community. Is it safe for our warfighters to use technologies manufactured by our potential adversaries?

The Information Assurance Technology Analysis Center (IATAC) understands the importance of analyzing this question. To provide the IA community with greater insight on IA and supply chain functions, IATAC is proud to announce the development of its *Security of the Supply Chain State of the Art Report* (SOAR). This SOAR focuses on security over the entire life cycle of the supply chain, and addresses both insider and external threats during development, delivery, and maintenance of the supply chain. It provides information essential to maintaining high levels of information security from the early developmental stages of the technologies we use. Stay connected for future updates on this topic—the SOAR is due out this summer.

President Obama's announcement in December that 30,000 more troops will deploy to Afghanistan is reason enough for the IA community to focus on how we can best provide our front-line defenders with the information they need without sacrificing our information security. I hope that with each edition of this publication, you learn more about how critical IA is to our national security as well as to the security and safety of the brave men and women who proudly serve our country. I know many of you have family, friends, and other loved ones serving our great nation and want to ensure we operate in a safe and secure environment; IATAC helps achieve this goal! I encourage you to help us keep this dialogue going. We always look forward to your comments and recommendations. We are interested in knowing how IA research and development will change the way we share information in the future, and what IA solution will better protect our warfighters, industries, and national interests at large. Please send us your thoughts, comments, or potential *IAnewsletter* articles. Feel free to contact us at *iatac@dtic.mil* with the next chapter to this IA story! ■

Gene Tyler

Security Automation Introduction

by Tony Sager

It's no secret—the Department and the Nation at large are struggling with the problems of cyber defense. In cyberspace, the bad guys have the upper hand: speed, anonymity, high leverage, stealth, global information sharing, and rapid adoption of new technology. They disrupt our operations, steal our intellectual property, force us to spend vast amounts of money and manpower, and raise our uncertainty *via* a fog of botnets, criminality, and subverted Web sites.

And here is the really disturbing fact: the vast majority of our defenders are in effect pinned down by relatively mundane technical problems: poorly engineered software; missing patches; unenforced policies; poor configuration choices; and inconsistent security controls.

Does this mean that our front-line defenders are not working hard enough, aren't competent, or just don't care? In the vast majority of cases, the answer is no. Consider our own problems: outdated, inconsistent, and/or conflicting policies; slow acquisition of new defensive tools; lack of coordinated Department-wide defensive action; untrained operators; and incomplete sharing of threat and vulnerability information. In such an environment, it is not rational to expect every front-line defender of our systems to take complex, unpatched, known-flaw software out of the box and cobble together a secured mission environment.

These are problems that are not as *technically* hard as they are *operationally* hard.

All of this speaks to a need for much greater use of automation and standardization. And not just technology, but technology that is built directly into the architecture, made a natural part of acquisition, linked to policies, supported by training, and adaptable to new information. We need all of this at a reasonable cost, built into commercial off-the-shelf products, and based on open industry standards.

There is hope on the horizon for both the Department and the nation. More than a generic public-private partnership, we've seen a "confederacy" emerge to include security practitioners, buyers, operators, educators, IT and security vendors, and policymakers. The early use cases include the Air Force's desktop standardization and the Federal Desktop Core Configuration (FDCC), supported by the Security Content Automation Protocols (SCAP) from National Institute of Standards and Technology (NIST). But we think these stories are just the starting point. In this issue, we summarize this important collaboration, how it is being used to solve operational problems for the DoD, and then provide some glimpses of what the future might hold.

Challenges

Despite the progress, there is a lot of heavy lifting ahead. There are still plenty of technical challenges. And many of the ideas still need to be institutionalized in standards, commercial tools, business processes, and governance.

But once we have the basic "plumbing" in place for large-scale patch/configuration/vulnerability/compliance management, an even larger target is within reach. We need to move from managing information technology to managing information. To regain the information advantage, we must be able to rapidly collect, correlate, and use information of many types and from many sources (*e.g.,* IT components, network devices, specialty security tools, threat data.) in order to assess the current risks to our operations and manage changes in real time. This issue will provide some ideas and inspiration to start us down this path. ■

About the Author

Tony Sager | is the chief of the Vulnerability Analysis and Operations (VAO) Group within the Information Assurance Directorate at the National Security Agency. During his 30 years at the NSA, Tony has held a number of positions in computer/network security and software analysis. He received a BA degree in mathematics from Western Maryland College and an MS in computer science from the Johns Hopkins University. He has received numerous awards for his work in the IT security community.

Dr. Sanjay Goel

by Angela Orebaugh

This article continues our profile series of members of the IATAC Subject Matter Expert (SME) program. The SME profiled in this article is Dr. Sanjay Goel at the University at Albany, State University of New York (UAlbany).

Dr. Goel is an associate professor in the Information Technology Management Department of the UAlbany School of Business. He teaches several classes, including Computer Networking & Security, Information Security Risk Analysis, Security Policies, Enterprise Application Development, Database Design, and Java Language Programming. He is also the director of research at the New York State Center for Information Forensics and Assurance. His research group at UAlbany is engaged in several projects, including investigation of computer security threats such as botnets and malware propagation, risk analysis, information classification, business continuity, disaster recovery, security modeling, and self-organization in complex systems. His latest research on self-organizing systems includes traffic light coordination, nano-bio computing, and social networks. He and his team have worked with the New York State Office of Cyber Security & Critical Infrastructure Coordination in developing the state's information classification policy.

Dr. Goel won the promising Inventor's Award in 2005 from the SUNY Research Foundation. In 2006, he was awarded the SUNY Chancellor's Award for Excellence in Teaching, the UAlbany Excellence in Teaching Award, and the Graduate Student Organization Award for Faculty Mentoring. He was recently named one of the three AT&T Industrial Ecology Faculty Fellows for 2009–2010.

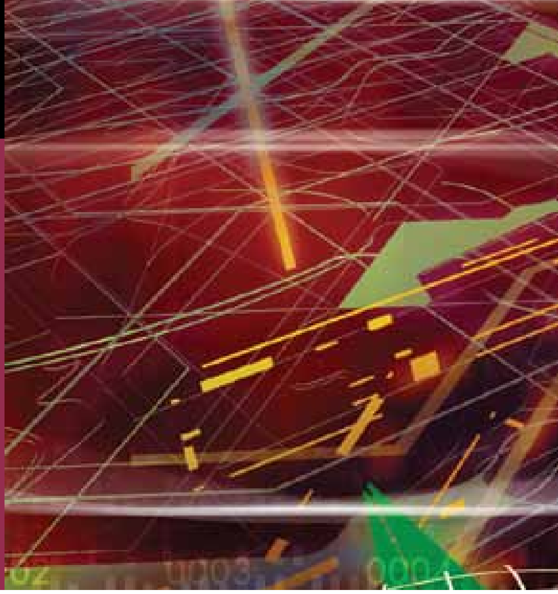
Dr. Goel's current research interests include self-organized systems for modeling of autonomous computer security systems using biological paradigms of immune systems, epidemiology, and cellular regulatory pathways. His current research also includes the use of machine learning algorithms to develop self-learning adaptive optimization strategies and use of information theoretic approaches for classification of data for use in applications such as portfolio analysis and information assurance. [1]

Dr. Goel's research in security combines the following four streams—

- **Intrusion detection**—Dr. Goel's research on intrusion detection involves developing security models inspired by biological systems. He currently is developing a simulation for a distributed immune system on the network. He also is developing an epidemiological model based on Poisson Point Processes for arrival of threats to computers in a network. A model is also being developed based on cellular processes to determine the interactions among the network components and to detect anomalies in the network. Dr. Goel is performing botnet research involving analysis of network traffic data collected from different sources on the network that is intelligently mined to identify infected machines, sources of attacks, and other anomalies on the network.
- **Resilient self-organizing networks**—Dr. Goel's work in resilient self-organizing networks has developed an alternate computing model to resist failures. This architecture consists of services that can be easily discovered on the network in real-time so that if one service fails, another can take its place. This architecture was used to support engineering design at General Electric.
- **Economics of security**—Dr. Goel's work on economics of security focuses on three aspects: 1) Information security risk modeling, 2) Development of security policy metrics and, 3) Valuating the impact of security breaches on financial returns. The new risk model developed as part of this work simplifies the risk analysis process and makes it more transparent. Research on security policies is focused on developing metrics to characterize policies. The work is using natural language processing to determine the attributes of the security policies. These metrics can then be correlated with the success and failure of policies.

▷▷ continued on page 31

Security Automation: A New Approach to Managing and Protecting Critical Information



by Daniel Schmidt

Information technology (IT) data about asset, vulnerability, and threat is assaulting those charged with managing and defending our critical IT networks at an ever-increasing rate. For example, the National Institute of Standards and Technology (NIST) published 17 new vulnerabilities a day in the National Vulnerability Database (NVD). [1] According to Chris Roland, chief technology officer at IBM, when Storm Worm, a broadband virus affecting mobile users spread, it infected nearly 17% of all broadband users. [2] A telling statistic recently provided by Greg Garcia of the Department of Homeland Security (DHS), the number of reported cyber incidents rose 1,700% over the past three years. [3] In response, the DHS National Cyber Security Division Fiscal Year 2009 budget has grown to $313 million, a 400% increase from 2004. [3] As a nation, we cannot sustain the continually increasing rates of budget, latency, and complexity of employing manual security responses. In today's manual processes, management practice typically involves the employment of text-based security guidance and policy that requires manual implementation. The employment of Security Content Automation Protocols (SCAP) and SCAP-validated tools will automate security, asset, and configuration management functions and transform how we manage and defend our critical IT infrastructure and data. To achieve automation, security guidance will be expressed in SCAP, consumed, and implemented within leading IT industry products that use common asset, vulnerability, and threat data models to enable common naming and format. This strategy will automate many security and configuration management, compliance, and network defense functions and give our system administrators and network defenders a chance to succeed.

Objectives and Motivations for a Security Automation Strategy

In today's IA operations, communicating vulnerability, configuration, and threat information in a consistent and timely manner is critical to secure operations. The Department of Defense (DoD), National Security Agency (NSA), and NIST initiated a strategy involving the creation of security standards and data models to identify and standardize vulnerability, configuration, and threat information. The objective was to enable several key IA-related functions targeted at shoring up the defense of the DoD IT architecture while transforming many of the configuration management, policy compliance enforcement, measurement, and reporting processes. An enterprise as large as the DoD has somewhere around six million IT assets. The truth is, the manually intensive processes in place today are incapable of supporting accurate tracking and management necessary to truly protect these assets. A component of security automation is achieving a fairly precise understanding of the computing environment and its compliance with policy. To do so requires the ability to accurately account for installed hardware, software, and more importantly, the actual configuration of these assets. To facilitate this, the SCAP standards were developed. The individual components of SCAP are described in Table 1. SCAP is a collection of open, interoperable standards that support automated vulnerability management, measurement, and policy compliance evaluation. More specifically, SCAP is a suite of standards that are used to—

- Establish common enumerations for software flaws, security-related configuration issues, and product names
- Determine if specific software flaws, configuration issues, patches, or products are present on a system
- Accurately and consistently communicate the impact of security issues while providing transparency regarding how the score was derived
- Enable integration and management of critical Computer Network Defense and IT configuration information.

Security Content Automation Protocol (SCAP)		
CPE	Common Platform Enumeration	Standard nomenclature and dictionary of product names
CCE	Common Configuration Enumeration	Standard nomenclature and dictionary of security-related configurable items
CVE	Common Vulnerabilities & Exposures	Standard nomenclature and dictionary of security-related software flaws
CVSS	Common Vulnerability Scoring System	Standard for measuring the impact of a vulnerability
OVAL	Open Vulnerability and Assessment Language	Standardized XML testing language to assess system state
XCCDF	Extensible Checklist Configuration Description Format	Standard XML for specifying checklists and for formatting results of checklist evaluation

Table 1 SCAP Standards.

SCAP

One of the challenges faced when attempting to identify assets affected by emerging threats is to determine which assets are affected, their criticality to the mission, and whether the vulnerability detected yesterday is different than the one that is being exploited today. As discussed previously, the volume of vulnerabilities and threats and diverse nature of the typical enterprise IT architecture is beyond the ability of a human to manage on a per-threat, per-asset basis. Machine-consumable standards to uniformly describe asset, vulnerability, and threat data in a fashion that can be consumed and correlated automatically, in near real time is the only realistic option. To start with, all hardware and software assets must share a common naming scheme. This was achieved by development of the Common Platform Enumeration (CPE) specification and CPE dictionary that is now hosted in the NVD, where it is available to the global community. The Uniform Resource Identifier (URI) structure of a CPE is—

CPE Example

```
cpe:/{part} : {vendor} : {product} : {version} : {update}
: {edition} : {language}
```

The Part field indicates whether the CPE represents hardware, an operating system, or an application. The vendor field provides the product vendor. The product field holds the name of installable software products, and the last four optional fields allow specification of additional, commonly available product details. The NVD-hosted CPE dictionary provides CPE in an XML format and provides known relationships between component parts of known CPE names (*e.g.,* Linux is distributed by Red Hat, Suse, and Caldera).

Many software products have a variety of security-related configuration settings. On some platforms such as Microsoft Windows XP, there are around 800 individual settings. The traditional approach has been for product vendors and agencies to analyze a product and define recommended security settings in a textual document. The job of the system administrator is to then take each of these prose documents and manually implement each of these recommended, or in some cases, mandatory, settings. Further, mandated settings typically require some form of compliance reporting to attest that settings have been implemented as prescribed. It is not uncommon for these settings, once implemented, to be changed simply by installation of another software product. As new threats emerge, the only response may be to implement an enterprise-wide, host-based configuration change. This is an impossible task on even modestly sized networks. Achieving automation requires that each unique configurable security setting along with the allowable range of parameters be assigned a unique identifier, referred to as a common enumeration. The name of this security standard is the Common Configuration Enumeration (CCE). CCE provides product vendors, users of the product, and security guidance providers a standard way to describe each individual configurable item, the range of settings, the desired setting, and the technical mechanism for implementing the setting and evaluating the status of the setting.

CCE Example

CCE-3260-7
Definition: The "Log Dropped Packets" option for the Windows Firewall should be configured correctly for the Domain Profile.

Parameter: Enabled or Disabled.

Technical Mechanisms:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Paramters\FirewallPolicy|Domain Profile|Logging\LogDroppedPackets
- Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Allow Logging – Log Dropped Packets
- Control Panel\Windows Firewall\Advanced\Security Logging\Logging Options\ Log dropped packets

Example taken from "An Introduction to the Common Configuration Enumeration, V 1.7, dated July 24, 2008, by David Mann at *http://cce.mitre.org/about/documents.html.*

Software coding flaws are another source of software vulnerability exploited daily. As indicated previously, new threats are emerging at astounding rates. Any of these vulnerabilities provide a potential entry point that may enable exploitation of critical assets and exfiltration of data. As with the previously described SCAP enumerations, a common method for naming software flaws was necessary to ensure that, as a new vulnerability emerged, security practitioners are all discussing and responding to the same vulnerability. Too often, differences in vulnerability names and description create confusion and hinder effective response. To address this, the Common Vulnerabilities and Exposures (CVE) standard was created.

CVE Example

CVE-1999-0091

Description: Buffer overlow in AIX writesrv command allows local users to obtain root access. Status: Entry Reference: ERS:ERS-SVA-E01-1997:005I.1

Example from CVE (Version 20061101) at *http://cve.mitre.org/data/downloads/allcves.html.*

The Common Vulnerability Scoring System (CVSS) provides a metrics-based assessment of a software vulnerability to provide uniformity in describing the risk posed by a specific vulnerability. CVSS is comprised of three components: a base score, which is consistent across environments and time; an environmental score that is determined by risk based upon the physical and logical environment of an IT system; and a temporal score based on common events in exploitation process of a vulnerability (*e.g.*, vulnerability discovered, vulnerability disclosed, exploit code developed, and exploits discovered on operating networks). The combination of the three components allows scores to be tailored to an individual environment at a point in time. For example, a CVSS score will be lower when the vulnerable software is not installed within the environment and it is a new vulnerability that malware has not yet been designed to exploit. [4]

The Open Vulnerability and Assessment Language (OVAL) is a language for expressing how a configuration item, software flaw, or patch is checked on a given operating system. The acronym refers to both the language and the MITRE repository of OVAL definitions. The three OVAL XML Schemas are: the System Characteristics schema, which describes objects and states on a given operating system; the OVAL definition schema, which defines how objects and states on a system can be assessed; and an OVAL Results schema, which is used for reporting the outcome of applying a Definition to a System Characteristics file. [5] OVAL allows interoperability between security assessment tools in that they can use the same OVAL content to assess a product. An example XML excerpt of an OVAL definition that tests for the presence of a Microsoft Windows Office product is provided as follows—

OVAL Example

```
<definition id="oval:org.mitre.oval:def:663" version="2"
class="inventory">
=<metadata>
<title>Microsoft Office 2002 is installed</title>
=<affected family="windows">
<platform>Microsoft Windows 2000</platform>
<platform>Microsoft Windows XP</platform>
<platform>Microsoft Windows Server 2003</platform>
</affected>
<reference source="CPE" ref_id="cpe:/
a:microsoft:office:xp" />
<description>The application Microsoft Office 2002 is
installed.</description>
=<oval_repository>
=<dates>
=<submitted date="2006-07-25T12:05:33">
<contributor organization="ThreatGuard, Inc.">Robert
L. Hollis</contributor>
</submitted>
<status_change date="2006-10-07T09:15:51.244-
04:00">INTERIM</status_change>
<status_change date="2006-10-
24T09:15:58.62804:00">ACCEPTED</status_change>
```

Example from MITRE at *http://oval.mitre.org/repository/data/ViewDefinition?id=oval%3aorg.mitre.oval%3adef%3a663.*

The Extensible Configuration Checklist Description Format (XCCDF) is a standard that groups together security policy and settings in a single document or checklist for a particular software product. [6] A checklist includes the basic criteria for security hardening an IT system through configuration settings. The XCCDF specification supports configuration compliance testing and reporting as shown in Figure 1.

For example, an XCCDF checklist provides the mapping between security policy and individual system level checks, providing the framework to enable automation of the Federal Information Security Management Act (FISMA). FISMA mandates a set of processes and requirements to define and document a system to include its components, the roles of those components within the system, the information it contains, and the vulnerability and threats to systems based on their composition, placement, and configuration. This allows the IT minimum security controls and settings

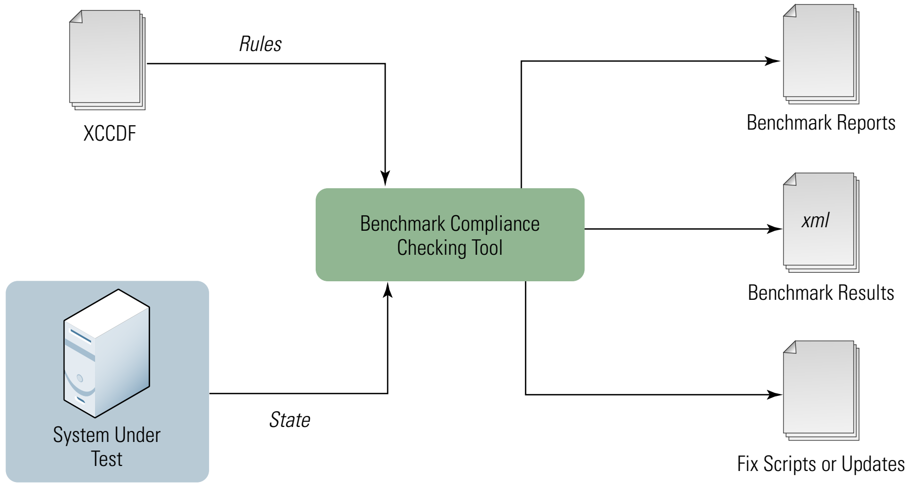


Figure 1 Workflow for Checking Benchmark Compliance.

based on mission impact of the system to be described to support complex, risk-based certification and accreditation processes. An XCCDF checklist in combination with CPE, CVE, CCE, and OVAL provides the XML to allow system configuration(s) to be assessed, and vulnerabilities based on software flaw or configuration identified and checked against policy with detailed mapping to higher level policy or legislation such as a NIST special publications, the Privacy Act of 1974, or Health Insurance Portability and Accountability Act (HIPAA) to facilitate compliance reporting activities.

SCAP represents a fundamental transformation of IT security management. Vulnerabilities are identified in a uniform manner; the risk posed by each vulnerability is assessed for each environment. Assets are uniformly identified by a group of CPEs, which enables software flaws (CVE) and configuration settings (CCE) to be uniquely identified for each individual software and hardware component. The configurations (CCE) for a particular platform (CPE) can be tested (OVAL) and packaged in a checklist (XCCDF) that can be consumed by a SCAP-validated tool to manage a platform and enable transformation of many FISMA requirements, such as risk assessment-based certification and accreditation activities.

Figure 2 demonstrates the overlapping functionality of the various SCAP components to integrate asset, vulnerability, configuration, and compliance reporting under a comprehensive and interoperable set of standards, consumable by tools, and therefore enabling an automated response to network security threats.

Governance Challenge

Achieving technical and process uniformity across the federal government will require governance and acquisition policy that provides strategic management and vision. The first step was a series of policy memoranda from the Office of Management and Budget (OMB) Chief Information Officer (CIO) Karen Evans. The policy memoranda are M-07-11 issued in March 2007 and M-08-22 issued August 2008 [7]. These federal policy documents mandated a Federal Desktop Core Configuration (FDCC) for Microsoft Windows XP, Vista, and the usage of SCAP content and SCAP-validated tools to manage the FDCC configuration. To further enable this strategy, the General Services Administration (GSA) established a GSA SmartBuy Blanket Purchase Agreement for SCAP-enabled FDCC scanning tools. These two initiatives have significantly advanced the adoption of SCAP. It is anticipated that further policy to mandate the standardization of other operating system, application, and IT products will be forthcoming over the next several years. In response, SCAP will require governance to establish broader oversight and funding stability from other agencies and industry organizations.

Governance should provide a structured framework for maturing the standards and support the widest range of user requirements. SCAP organizational roles and responsibility should be defined through policy to ensure long-term stability and structure. SCAP governance should have oversight and control from the very top of the federal government to provide a mechanism to address and adjudicate

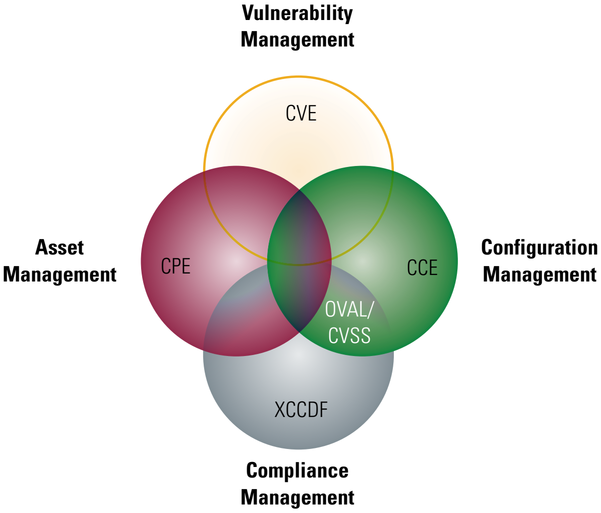


Figure 2 SCAP—A New Approach.

diverse interests and needs. The approach under discussion is formalization of a working group subordinate to the recently established federal CIO councils Technical Infrastructure Subcommittee. The working group is called the Information Security Automation Program (ISAP) Working Group (WG). The current composition of this group is DoD, NIST, NSA, Defense Information Systems Agency, Department of Energy, and DHS. The initial goal is to expand membership by 2010 to include more diverse federal agency representation. The ISAP WG is being structured to be the body that accepts change proposals from the public and private sector security community through a series of subworking groups that assess the technical, process, and financial implications of the change. One of the challenges of this WG is to manage expanding fiscal requirements in response to emerging standard requirements as participation and involvement grow.

Industry Strategy

Another challenge is developing and maintaining a strong strategic relationship with the IT industry leaders as vendor adoption is considered key to the success of SCAP. For example, when a major operating system vendor releases a new software product, the goal is to have that vendor enumerate, in SCAP, the security-related configuration items and recommended settings for its product. FDCC is a recent example of what can be achieved through federal government and industry partnership. The NSA and DoD worked closely with Microsoft to define a standard security configuration for Microsoft Vista and several other commonly used Microsoft applications. Once the security settings where identified, the SCAP content was encoded in XCCDF and made available to every user of these products *via* the NVD. The United States Air Force took this a step further and negotiated a contract with a major desktop PC vendor to deliver all Microsoft Vista based platforms configured in compliance with FDCC from the factory. Further, they deployed SCAP-validated tools to test this configuration to ensure each host conformed to FDCC and streamlined DoD and OMB compliance reporting. This is a successful example of how standardization saves resources and ultimately simplifies defense of these assets. This partnership is rapidly expanding to include the full range of operating system and application product vendors.

Summary

SCAP standards and the security automation, enabled by the processes and tools that employ SCAP, provide critical security management functionality, efficiency, and principles that are applicable to the nation's federal and private IT sectors. For the first time, senior leadership can express IT security policy that can be captured in standards and employed in tools at every level within the enterprise to ensure implementation, enforcement, and compliance. Security automation is a very real strategy that will allow the nation's brightest federal and private sector security professionals to collaborate and develop SCAP content to mitigate emerging vulnerabilities and employ a wide range of interoperable IA tools and trusted security content to mitigate threats as they develop. The next challenge is to establish the policy, procedures, and governance to mature the security automation strategy to enable the widest possible employment of standards such as SCAP and secure implementations such as FDCC. ■

References

1. National Vulnerability Database (NVD), Retrieved November, 2, 2008 from *http://nvd.nist.gov/*
2. Georgia Tech Information Security Center (GTSIC) "Georgia Tech Information Security Center Emerging Cyber Threat Report for 2008", Retrieved October 31, 2008, from *http://64.233.169.104/search?q=cache:UU5T7itlYkoJ:www.gtisc.gatech.edu/pdf/GTISC%2520Cyber%2520Threats%2520Report.pdf+cyber+threats&hl=en&ct=clnk&cd=2&gl=us*
3. Remarks by Cybersecurity and Communications Assistant Secretary Greg Garcia at the 2008 National Cyber Secuirty Awareness Month Kick-Off event at the Washington, D.C., National Press Club, Retrieved October, 31, 2008 from *http://www.dhs.gov/xnews/speeches/sp_1223058336863.shtm*
4. Mell, P., Scarfone, K., & Romanosky, S. "CVSS" A complete Guide to the Common Vulnerability Scoring System, Version 2.0, Forum of Incident Response and Security Teams, June 2007. Retrieved November, 6, 2008 from *http://www.first.org/cvss/cvss-guide.html#i2.1*
5. MITRE. "An Introduction to the OVAL Language, v 5.0". Retrieved November, 7, 2008 from *http://oval.mitre.org/oval/about/documents.html#language*
6. Ziring, N. "Specification for the Extensible Configuration Checklist Description Format (XCCDF)", *http://nvd.nist.gov/scap/xccdf/docs/xccdf-spec-1.0.pdf.*
7. Office of Management and Budget (OMB). (2008). Memoranda. Washington, DC. Retrieved November, 4, 2008 from *http://www.whitehouse.gov/omb/memoranda/*

About the Author

Mr. Daniel J. Schmidt | is a computer scientist serving as the technical director of the NSA Information Assurance Directorate Vulnerability Analysis and Operation Mission Integration and Technology Office. Mr. Schmidt spent 20 years as a cryptologist while serving in the Navy from 1980 to 2000. Upon retirement from the Navy, Mr. Schmidt immediately transitioned to NSA as a federal government employee.

During his time with NSA, Mr. Schmidt has performed in a variety of technical leadership roles, focusing on the design and development of IT-based systems with a special emphasis on large-scale, high-volume data and information management and automation.

The University at Albany– State University of New York

by Angela Orebaugh

The State University of New York (SUNY) was founded in 1816 and officially established in 1948 to create a state university system. SUNY initially represented a consolidation of 29 unaffiliated institutions, including 11 teachers colleges. Today, SUNY consists of 64 geographically dispersed campuses that comprise the nation's largest comprehensive system of public higher education. SUNY provides access to almost every field of academic or professional study within the system *via* 7,669 degree and certificate programs.

Located in the state capital of New York, the University at Albany (UAlbany) serves 18,000 undergraduate and graduate students and offers over 100 undergraduate majors and minors and over 120 graduate programs. UAlbany offers several options for studying information assurance and security, including—

- The School of Business Master of Business Administration (MBA) program offers concentrations in information assurance and information technology management.
- The School of Business offers courses on information security, risk analysis, security policies, and computer forensics. It is developing an IA certificate program that is going through the university approval process.
- The College of Computing and Information's (CCI) Department of Informatics hosts a multidisciplinary Ph.D. program with a specialization in IA.

UAlbany courseware meets National Training Standards for Information Systems Security Professionals and is certified for Committee on National Security Systems (CNSS) 4011 and 4012.

UAlbany also hosts the New York State Center for Information Forensics and Assurance (CIFA), a partnership of UAlbany, SUNY, New York State Office of Cyber Security and Critical Infrastructure Coordination, and the New York State Police. Its mission is research and education to better enable practitioners to address real problems in information forensics and assurance, especially in the area of public protection. Specifically, CIFA—

- Targets the public sector workforce in an effort to build knowledge resources and practical skills within state and local government
- Develops and deploys courseware for academic and professional education programs in related disciplines
- Provides a home for multidisciplinary researchers and practitioners developing workable approaches to emerging information forensics and assurance issues and effective methods to facilitate learning and dissemination of these approaches. [1]

CIFA was founded in 2003 through funding by federal and state government grants, including those from the National Science Foundation, the United States Department of Education, and the National Institute of Justice. As of 2004, CIFA also participates in the activities of the Northeast Regional Forensic Institute, a collaborative partnership between UAlbany and the New York State Police Forensic Investigation Center designed to address a nationwide shortage of forensic scientists, which has created critical casework backlogs in labs across the nation. In 2005, the Capital Region Cyber Crime Partnership (CRCCP) was created, comprised of the New York State Police, district attorneys from eight counties in the Capital Region, the New York Prosecutors Training Institute, and members of CIFA. CRCCP works specifically to reduce computer crime case backlog through research in the computer forensics field and creation of training materials. CIFA's operation emulates that of a teaching hospital [2] where educational cases based on real problems provide learning opportunities for students and

▷▷ continued on page 29

The Security Content Automation Protocol (SCAP)

by John Banghart

To support the broad security automation vision, it is necessary to have both trusted information and a standardized means to store and share it. Through close work with its government and industry partners, the National Institute of Standards and Technology (NIST) has developed the Security Content Automation Protocol (SCAP), providing the standardized technical mechanisms to share information between systems. Through the National Vulnerability Database (NVD) and the National Checklist Program (NCP), NIST is providing relevant and important information to the areas of vulnerability and configuration management.

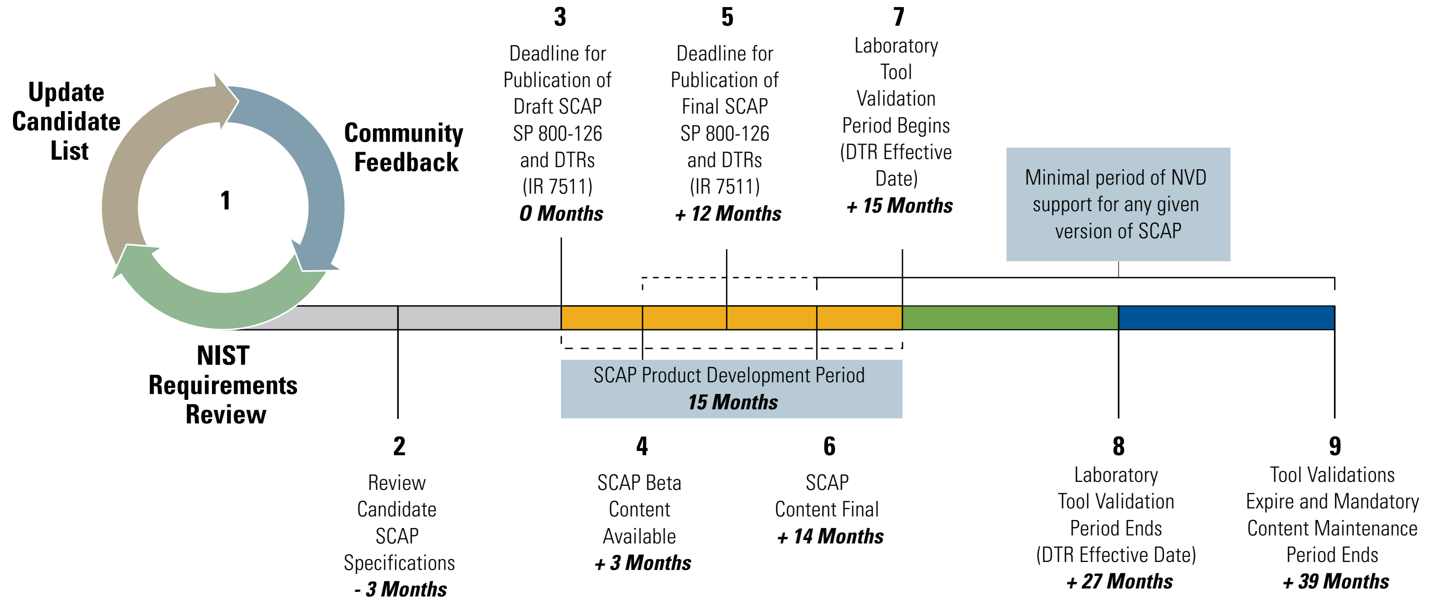
Combined, SCAP and the programs that leverage it are moving the IA industry in a direction of being able to standardize communications, collect and store relevant data in standardized formats, and provide automated means for the assessment and remediation of systems for both vulnerabilities and configuration compliance.

SCAP

SCAP is a suite of specifications that use the eXtensible Markup Language (XML) to standardize the format and nomenclature by which security software products communicate information about software flaws and security configurations.

SCAP is achieving widespread adoption by major software and hardware manufacturers and has become a significant component of large information security management and governance programs. The protocol is expected to evolve and expand in support of the growing need to define and measure effective security controls, assess and monitor ongoing aspects of that information security, remediate non-compliance, and to successfully manage systems in accordance with the risk management framework described in NIST Special Publication 800-53. To manage that evolution, a timeline has been constructed to balance progress against stability, as seen in Figure 1.

Figure 1 SCAP Timeline (*http://scap.nist.gov/timeline.html*).



Update Candidate List
1
Community Feedback
NIST Requirements Review
3
Deadline for Publication of Draft SCAP SP 800-126 and DTRs (IR 7511)
0 Months
5
Deadline for Publication of Final SCAP SP 800-126 and DTRs (IR 7511)
+ 12 Months
7
Laboratory Tool Validation Period Begins (DTR Effective Date)
+ 15 Months
Minimal period of NVD support for any given version of SCAP
SCAP Product Development Period
15 Months
2
Review Candidate SCAP Specifications
- 3 Months
4
SCAP Beta Content Available
+ 3 Months
6
SCAP Content Final
+ 14 Months
8
Laboratory Tool Validation Period Ends (DTR Effective Date)
+ 27 Months
9
Tool Validations Expire and Mandatory Content Maintenance Period Ends
+ 39 Months

At its core, the timeline allows for new specifications to be added to SCAP and the SCAP Validation Program, while ensuring vendors and users have a 15-month window to update their products and/or processes to accommodate the changes.

Specifications have both intrinsic and synergistic value. They have intrinsic value in that the specification demonstrates value on its own merits. For example, XCCDF is a standard way of expressing checklist content. XCCDF also has a synergistic value when combined with other specifications such as CPE, CCE, and OVAL to create a SCAP-expressed checklist that can be processed by SCAP-validated products. Likewise, CVE has use cases that could simply be a consistent way to enumerate vulnerabilities for tracking purposes; however, when combined with CPE and OVAL, CVE is elevated to formulate a greater use case, namely that of automated checks for vulnerabilities that can be processed by SCAP-validated products.* These relationships are captured in SP 800-126; however, it is important to recognize that specifications can and should demonstrate value in their own right without being SCAP specifications. To address this, NIST will explore the possibility of implementing separate but related validation programs for individual specifications. For example, NIST is in the process of implementing an OVAL Validation Program whose purpose is to allow products to be tested for OVAL functionality that may not be used in SCAP use cases.

It is expected that new specifications will be developed on an ongoing basis. In response, NIST has established an email list and Web page specifically for emerging specifications. More information can be found at *http://scap.nist.gov/emerging-specs/index.html*.

Currently, NIST is leveraging SCAP in multiple areas to support its own mission and to enable other agencies and private sector entities to meet their goals. For NIST, SCAP is a critical component of the SCAP Validation Program, the NVD, and the NCP.

National Checklist Program

There are many threats to users' computers, ranging from remotely launched network service exploits to malicious code spread through emails, malicious Web sites, and download of infected files. Vulnerabilities in information technology (IT) products are discovered daily, and many ready-to-use exploitation techniques are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security configuration controls are usually not enabled by default, so many out-of-the-box IT products are immediately vulnerable. In addition, identifying a reasonable set of security settings for many IT products is a complicated, arduous, and time-consuming task, even for experienced system administrators.

To facilitate development of security configuration checklists for IT products and to make checklists more organized and usable, NIST established the NCP. The goals of the NCP are to—

- Facilitate development and sharing of checklists by providing a formal framework for vendors and other checklist developers to submit checklists to NIST
- Provide guidance to developers to help them create standardized, high-quality checklists that conform to common operations environments
- Help developers and users by providing guidelines for making checklists better documented and more usable
- Encourage software vendors and other parties to develop checklists
- Provide a managed process to review, update, and perform maintenance of checklists
- Provide an easy-to-use repository of checklists
- Provide checklist content in a standardized format

* SCAP components are discussed in detail on pages 7–8 of this publication.

- Encourage the use of automation technologies for checklist application such as SCAP.

Checklists can take many forms, including files that can automatically set or verify security configurations. Having automated methods has become increasingly important for several reasons, including the complexity of achieving compliance with various laws, executive orders, directives, policies, regulations, standards, and guidance; the increasing number of vulnerabilities in information systems; and the growing sophistication of threats against those vulnerabilities. Automation ensures that the security controls and configuration settings are applied consistently within an information system, and that the controls and settings can be effectively verified.

The SCAP program addresses these needs by enabling standards-based security tools to automatically perform configuration checking using NCP checklists. Security products and checklist authors assemble content from SCAP data repositories to create viable SCAP-expressed security guidance. A security configuration checklist that documents desired security configuration settings, installed patches, and other system security elements using SCAP in a standardized format is known as an SCAP-expressed checklist. Such a checklist would use XCCDF to describe the checklist, CCE to identify security configuration settings to be addressed or assessed, and CPE to identify platforms for which the checklist is valid. The use of CCE and CPE entries within XCCDF checklists is an example of a SCAP convention—a requirement for valid SCAP usage. Another example of a SCAP convention is the mapping of individual checks within a checklist to external requirements such as security controls from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. Organizations producing SCAP content should adhere to these conventions to ensure the highest degree of interoperability.

There are 128 checklists posted on the Web site; 17 of the checklists are SCAP-expressed and can be used to SCAP-validate products. It is anticipated that 26 more SCAP-expressed checklists will be added in Fiscal Year 2010. This allows organizations to use checklists obtained from the NCP Web site (*http://checklists.nist.gov)* for automated security configuration and patching without vendor interaction. Some vendors, including Microsoft Corporation and Red Hat, provide SCAP checklist content to the NCP, while most of the checklists come from government organizations, not-for-profits, and Federally Funded Research and Development Centers (FFRDC). NCP currently has SCAP checklists for Internet Explorer 7.0, Office 2007, Red Hat Linux, Symantec AntiVirus, Windows 2000, Windows 2003 Server, Windows Vista, Windows XP, and other products.

To assist users in identifying automated checklist content, NCP groups checklists into tiers, from tier I to tier IV. NCP uses the tiers to rank checklists according to their automation capability. Tier IV checklists are considered production-ready and have been validated by NIST or a NIST-accredited independent testing laboratory to ensure, to the maximum extent possible, interoperability with SCAP-validated products. Tier III checklists have not been validated, but have gone through a minimum acceptance testing process to ensure that they are able to run in SCAP-validated products. Tier II checklists document their recommended security settings in a machine-readable but non-standard format, such as a proprietary format or a product-specific configuration script. Tier I checklists are prose-based and contain no machine-readable content.

Checklists are sorted by default according to tier, from tier IV to tier I. Users can browse the checklists based on the checklist tier, IT product, IT product category, or authority, and also through a keyword search that searches the checklist name and summary for user-specified terms. The search results show the detailed checklist metadata and a link to any SCAP content for the checklist as well as links to any supporting resources associated with the checklist.

Although checklists are encouraged for use in both the private and public sectors, federal agencies are required to use security configuration checklists from the NCP. In February 2008, revised Part 39 of the Federal Acquisition Regulation (FAR) was published. Paragraph (d) of section 39.101 states, "In acquiring information technology, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations available from the NIST Web site at *http://checklists.nist.gov.* Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated." In Memorandum M08-22, the Office of Management and Budget (OMB) mandated the use of SCAP-validated products for continuous monitoring of Federal Desktop Core Configuration (FDCC) compliance.

The NCP is defined in NIST SP 800-70 Rev 1, which can be found at *http://csrc.nist.gov.*

SCAP Validation Program

The SCAP Validation Program performs conformance testing to ensure that products correctly implement SCAP. Conformance testing is necessary because SCAP is a complex specification consisting of six individual specifications that work together to meet various use cases. A single error in product implementation could result in undetected vulnerabilities or policy non-compliance within agency and industry networks.

The SCAP Validation Program was created on request by OMB to support the FDCC. It works with the NIST National Voluntary Laboratory Accreditation Program (NVLAP) to set up independent conformance testing laboratories that conduct the testing based on NIST IR 7511, *Rev 1: DRAFT Security Content Automation Protocol (SCAP) Version 1.0 Validation Program*

Test Requirements. When testing is completed, the laboratory submits a test report to NIST for review and approval. Product validations are currently active for one year, at which time vendors have the option to renew their validation by submitting the product for testing. SCAP validation testing has been designed to be inexpensive, yet effective. The SCAP conformance tests are either easily human verifiable or automated through NIST-provided reference tools. To date, the program has accredited 10 independent laboratories and validated 25 products from 19 different vendors.

While FDCC SCAP testing is an important part of the program, it is only one of several SCAP capabilities that vendors can apply to test their products. The others cover product capabilities such as configuration scanning, vulnerability scanning, patch checking, and remediation capabilities, all within the SCAP context.

Another new area, currently in its early stages, is the SCAP Content Validation Program, whose purpose will be to ensure that SCAP content available through the NCP is assured to work in SCAP Validation products within the same use case. As the use of SCAP continues to grow into mission-critical areas, it is increasingly important that users of the technology can be assured that it will function as expected. This means that when SCAP content is processed by a SCAP Validation product, it should work without error. Achieving this goal requires the creation of the SCAP Content Validation Program, which is currently in the early stages of development. Working in conjunction with the SCAP Product Validation Program and the NCP, the SCAP Content Validation Program will ensure that content designed to meet a specific use case, such as configuration compliance, can be processed fully and accurately by SCAP Validation products for that same use case. The NCP, using a tiered structure, will highlight SCAP Validation content by placing it in the highest tier, Tier IV. This provides end users and fast and simple way to identify the content they need, pair it with their SCAP Validation products, and achieve their mission goals.

National Vulnerability Database

The NVD is the federal government repository of standards-based vulnerability management reference data. The NVD contains information regarding vulnerabilities (software flaws and misconfigurations), including impact measurements, detection techniques, remediation assistance, and security control mappings.

NVD search and publication capabilities provide access to all publicly available federal vulnerability resources and references to industry resources. NVD also contains a statistics engine to enable users to gain a deeper scientific understanding of the nature of published vulnerabilities and associated trends. NVD supports SCAP by making SCAP standard reference data readily available to industry and government agencies.

Vulnerability Search Engine

NVD currently contains over 38,000 vulnerability advisories with an average of 14 new vulnerabilities added daily. NVD provides basic and advanced online searching capabilities. The basic search allows users to search for vulnerabilities containing specific words or phrases of interest with the ability to limit results to vulnerabilities published within the "Last 3 Months" or "Last 3 Years." The basic search criteria can also be tailored to retrieve vulnerabilities associated with United States Computer Emergency Readiness Team (US-CERT) Technical Cyber Security Alerts or Vulnerability Notes or vulnerabilities for which SCAP automated check content is available. The NVD "Advanced Search" option provides additional search capabilities, including searching by—

- CVE identifier
- CPE vendor or product name
- Category (*e.g.*, buffer errors, cross-site scripting, input validation)
- Date of publication or last modification
- CVSS Version 2 Impact Metrics
- NVD CVE Publication.

NVD also provides the ability for Web download of vulnerability XML files that contain the core vulnerability data as well as CVSS impact metrics and CPE identifiers for affected products. The CVE XML files are available by year—

- Vulnerabilities by year (2003–2008)
- Vulnerabilities prior to and including 2002

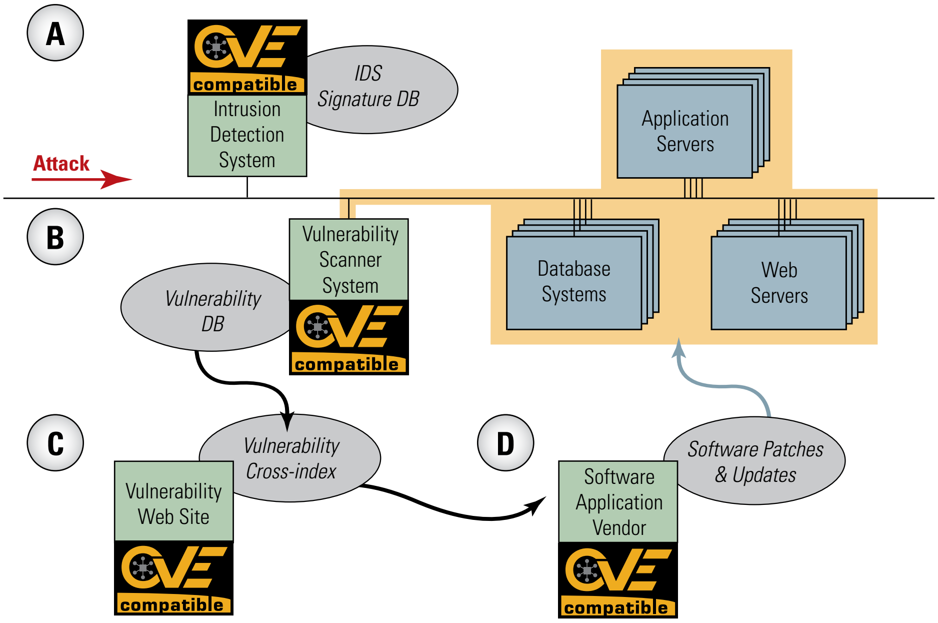


Figure 2 CVE utilization after detecting attack.

- All recently published or recently updated vulnerabilities.

In addition to the Web download, NVD provides two RSS 1.0 data feeds. The first feed provides information on all recent CVE vulnerabilities. The second feed provides only those CVE vulnerabilities that have been fully analyzed by the NVD analysis team.

The diagram in Figure 2 shows how CVE is utilized across the security infrastructure following the detection of a potential attack. The NVD plays a critical role in providing the necessary information for parts "B" and "C" of the process by providing access to vulnerability information used by scanning tools and vendors to assess and remediate the problem.

NIST SP 800-53 controls to CCE Mapping

Currently under development at the time of this writing is the NIST SP 800-53 controls to CCE Mapping.

NIST has the chartered authority to provide controls and guidance for the Federal Information Security Management Act (FISMA) and to work with the Centers for Medicare and Medicaid Services (CMS) to create a framework for the Health Insurance Portability and Accountability Act (HIPAA) security compliance. Achieving these goals requires that framework controls be fully and accurately mapped to checklist level guidance in the form of specific system settings such as password length and disabling ports. CCE provides the pointers to these settings, so in mapping them to the higher level controls in NIST SP 800-53, agencies are able to achieve and report real success with their FISMA compliance efforts. Further, NIST and CMS have been working to create authoritative mappings between NIST SP 800-53 and the HIPAA frameworks. This provides a transitive association to CCE, which in turn enables the use of SCAP Validation products to collect FISMA and HIPAA compliance information down to the individual host level.

CVSS Impact Metrics

The CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. NVD provides CVSS scores for almost all publicly known vulnerabilities.

In particular, NVD supports the CVSS version 2 standard for all CVE vulnerabilities. NVD provides CVSS "base scores," which are derived from the innate, immutable characteristics of each vulnerability. NVD does not currently assign 'temporal scores' (scores that change over time due to events external to the vulnerability); however, NVD provides a CVSS score calculator to allow a user to add temporal data and to calculate environmental scores (scores customized to reflect the impact of the vulnerability on an organization). This calculator contains support for government agencies to customize vulnerability impact scores based on FIPS 199 System ratings.

Official Vendor Statements on CVE Vulnerabilities

NVD provides an open forum to industry to allow comments to be submitted regarding CVE vulnerabilities affecting their products. Product vendors possess a great depth of knowledge regarding their products and are uniquely positioned to comment on the nature and scope of these vulnerabilities. Organizations can use the service in a variety of ways. For example, they can provide configuration and remediation guidance, clarify vulnerability applicability, provide deeper vulnerability analysis, dispute third-party vulnerability information, and explain vulnerability impact. The set of "official vendor statements" is available as an XML feed from the NVD Data Feed page.

Official CPE Dictionary

CPE is a structured naming scheme for information technology systems, software, and packages. The NVD CPE Product dictionary is a list of over 17,805 official CPE product names. The dictionary is provided in XML format and is available to the public *via* Web download. Generation of the CPE dictionary is currently performed on a daily basis as needed to add new products to the dictionary or update existing dictionary entries.

Future Capabilities

The NVD team currently is designing and developing the following capabilities:

- CCE repository that includes core system configuration settings, metadata, and impact metrics
- CCE search, data feeds, and Web service capabilities
- CPE search, data feeds, and Web service capabilities
- Publication of authoritative mappings of CCE and NIST SP 800-53 controls to various frameworks (*e.g.*, HIPAA, PCI) to realize compliance automation using SCAP validated tools.

NVD is maintained by the NIST Information Technology Laboratory's Computer Security Division with sponsorship from the DHS National Cyber Security Division and the NSA. ■

About the Author

John Banghart, NIST | has spent over 15 years in the IT/IS fields, both in the private and public sectors. Currently, he is the SCAP Validation Program manager at NIST. As part of the broader security automation initiative, this program develops software requirements and accredits laboratories for the purpose of validating that products are correctly implementing SCAP. Mr. Banghart is currently the NIST representative to the Interagency Security Automation Program Working Group, where he works with other agency representatives and external stakeholders to develop and promote security automation initiatives across the federal government and private sector.

The DoD IA Policy Chart

by John Dittmer, Tony Robey, and Rick Aldrich

Building, operating, and securing the Global Information Grid (GIG) for the DoD is a complex and ongoing challenge. To meet this challenge, a wide range of directives, instructions, manuals, and other policies have been published. Unfortunately, the breadth and scope of these policies are such that being able to locate the appropriate policy and the latest version of that policy is not always easy. To make that a little easier for the DoD's IA professionals, the Deputy Assistant Secretary of Defense for Cyber Identity and Information Assurance (CIIA) requested that the Defense-wide Information Assurance Program (DIAP) develop a chart that pulled together all of the IA policies into a single document. (See page 18.) It is built upon the creation of the similar Acquisition Security Policy Chart by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. The goal of the IA Policy Chart is to capture the tremendous breadth of applicable policies, some of which many IA practitioners may not even be aware, in a helpful organizational scheme. The use of color, hatching, fonts, and hyperlinks (in the electronic version) are all designed to provide additional assistance to IA professionals navigating their way through policy issues in order to build, operate, and secure the GIG.

Navigating around the IA Policy Chart

Essentially, the Chart is designed around the four CIIA goals—

1. Organize for unity of purpose and speed of action (shortened to "Organize" in the chart)
2. Enable secure, mission-driven access to information and services (shortened to "Enable" in the chart)
3. Anticipate and prevent successful attacks on data and networks (shortened to "Anticipate" in the chart)
4. Prepare for and operate through cyber degradation or attack (shortened to "Prepare" in the chart).

These four goal areas are subdivided into activities supporting each goal. In the center of the chart is a legend that identifies the originator of each policy by a color-coding scheme. On the right-hand side of the IA Policy Chart, there are boxes that cover the legal authority for the policies, the federal/national level of IA policies, and operational level documents that provide details on securing the GIG and its assets.

Because IA Policy development is a wide-ranging and ongoing process, we ask for input from all who download this chart, advising us of any policies that may have been overlooked, but should be included. In addition, we ask for any policy updates that may not be properly reflected on the IA Policy Chart or any suggestions to improve the chart. Please send suggestions, comments, or questions about the chart to *iatac@dtic.mil*. If you have questions about the content of any particular policy, please directly contact the point of contact for that policy. ■

About the Authors

Rick Aldrich | is the senior computer network operations policy analyst for IATAC. He has taught cyberlaw at the collegiate level and has presented at several national and international conferences. He received a BS degree in computer science from the Air Force Academy, a JD from UCLA, and an LLM from the University of Houston. He is also a CISSP.

John Dittmer | currently supports the DoD Computer Network Defense (CND) Architect through IATAC. He was stationed in Denmark, Cuba, Italy, Bosnia, San Diego, and the Washington, DC, area while serving as a Navy reservist. John received an MA degree in information resources management from Webster University and BA degrees in political science and history from Marquette University, and he is a graduate of the Naval War College. John has CISSP-ISSMP and PMP certifications.

Tony Robey | currently supports the DoD CND Architect through IATAC. He is a recent graduate from Radford University and received a BS degree in computer science with concentrations in networks and network security. Tony has a Security+ certification.

Build and Opera

Cyber, Identity, & Inf

- DoD Cyber, Identity & Information Assurance Strategic Plan
- DoDD 8100.01 Global Information Grid (GIG) Overarching Policy
- DoDD 8500.01E Information Assurance (IA)
- ASD(NII)/DoD CI DoD GIG

CIIA Goal 1: Organize

1.1 Lead and Govern in Uncertainty

- DODD 8115.01 IT Portfolio Management
- *ASD(NII)DoD CIO DoD FISMA Guidance–Fiscal Year 2009*
- DODI 8115.02 IT Portfolio Management Implementation
- SP 800-18 Guide for Developing Security Plans for Federal Information Systems
- DODD 7045.20 Capability Portfolio Management
- SP 800-30 Guide for Conducting Risk Assessments
- DoDI 7000.14 Financial Management Policy and Procedures (PPBE)
- CJCSI 3170.01G Joint Capabilities Integration and Development System (JCIDS)

1.2 Design for the Fight

- DODD 5000.01 The Defense Acquisition System
- DODI 8580.1 Information Assurance (IA) in the Defense Acquisition System
- DODI 5000.02 Operation of the Defense Acquisition System
- DODI 8510.01 DOD IA Certification and Accreditation Process (DIACAP)
- NTISSP-11 National Informatin Assurance Acquistion Policy
- *IA Component of the GIG Integrated Architecture, v1.1*
- *Overview and Summary Info (AV-1) DoD CND Architecture, v0.1*
- *ASD(NII)/DoD CIO G&PM 12-8430 Acquiring Commercial Software*
- DNI CIO Memo Intelligence Community (IC) Enterprise Software Licensing
- ASD(NII)/DoD CIO Memo DOD Support for the SmartBUY Initiative
- DFARS Subpart 208.74 Enterprise Software Agreements
- CJCSI 6212.01E Interoperability and Supportability of IT and National Security Systems
- *Alignment Framework for the GIG IA Architecture (AFG) version 1.1*
- Common Criteria Evaluation and Validation Scheme (CCEVS)
- DoDD 4630.05 Interoperability and Supportability of IT and National Security Systems (NSS)
- DIACAP Knowledge Service

1.3 Develop the Workforce

- DODD 8570.01 IA Training, Certification, and Workforce Management
- DOD 8570.01-M Information Assurance Workforce Improvement Program
- NSTISSD-501 National Training Program for INFOSEC Professionals
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard for Systems Administrators (SA)
- CNSSI-4014 National IA Training Standard for Information Systems Security Officers
- CNSSI-4015 National Training Standard for Systems Certifiers
- CNSSI-4016 National IA Training Standard for Risk Analysts
- *NSTISSI-4000 COMSEC Equipment Maintenance and Maintenance Training*

1.4 Partner for Strength

- NSTISSI-1000 National Information Assurance (C&A) Process (NIACAP)
- CNSSP-14 National Policy Governing the Release of IA Products/Services...
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
- SP 800-37 Guide for the Secuirty Authorization of Federal Information Systems
- SP 800-39 Managing Risk from Information Systems: An Organizational Perspective
- SP 800-53A Recommended Security Controls for Federal Information Systems
- SP 800-53 R3 Recommended Security Controls for Federal Information Systems
- *CNSSI-1253 Security Controls Catalog (SCC) (Draft)*
- ICD 503 IT Systems Security Risk Management, Certification, and Accreditation
- *DoD Strategic Plan for Defense Industrial Base Cyber Security and Information Assurance*
- *DoDI 5205.ff Defense Industrial Base Cyber Security / IA Activities (Draft)*

CIIA Goal 2: Enable

2.1 Secure Data in Transit

- DODD 8521.01E Department of Defense Biometrics
- DODI 8523.01 Communications Security (COMSEC)
- *DODI S-5200.16 Objectives and Min Stds for COMSEC Measures used in NC2 Comms*
- DODI 4650.1 Policy and Procedures for Mgt and Use of the Electomagnetic Spectrum
- DODD 4640.13 Mgt of Base and Long Haul Telecomms Equipment and Services
- *CJCSI 6510.02C Cryptographic Modernization Plan*
- CNSSI-5000 Guidelines for Voice Over Internet Protocol (VoIP) Computer Telephony
- *CJCSI 6510.06A Communications Security Releases to Foreign Nations*
- CNSSI-5001 Type-Acceptance Program for VoIP Telephones
- NAMCSI-6002 National COMSEC Instruction Protection of Gov't Contractor Telecomm's
- NCSC-5 Nat'l Policy on Use of Cryptomaterial by Activities Operating in High Risk Environments
- NSTISSP-101 National Security Policy on Securing Voice Communications
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
- NTISSI-7003 Protective Distribution Systems (PDS)
- CNSSP-17 National Information Assurance Policy on Wireless Capabilities
- FIPS 140-2 Security Requirement for Cryptographic Modules
- CNSSP-19 National Policy Governing the Use of HAIPE Products
- CNSSP-15 National Policy on teh Use of the AES to Protect National Security Systems...
- ASD(NII)/DoD CIO Memo Use of Commercial Wireless LAN Devices, Systems, and Technologies...
- CNSSP-25 National Policy for PKI in National Security Systems
- *NACSI-2006 Foreign Military Sales of COMSEC Articles and Services to Foreign Govt's and Int'l Orgs*
- *NACSI-2005 Communications Security (COMSEC) End Item Modification*
- *NSTISSI-4006 Controlling Authorities for COMSEC Material*
- *DoDD 8100.2 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG*

2.2 Manage Access

- DOD 1000.25 DOD Personnel Identify Protection (PIP) Program
- DODI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- HSPD-12 Policy for a Common ID Stanard for Federal Employees and Contractors
- DoD Strategic Plan for Identity Management
- M-05-24 Implementation of HSPD-12
- *ASD(NII)/DoD CIO Memo Approval of External Public Infrastructures*
- FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors
- NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
- *CNSSP-10 Nat'l Policy Governing the Use of Approved Security Containers in Info Sys Security Apps*
- CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
- *NSTISSI-4005 Safeguarding COMSEC Facilities and Materials*
- *NSTISSI-4010 Keying Material Management*
- *NSTISSI-4001 Controlled Cryptographic Items*
- *NSTISSI-4003 Reporting and Evaluating COMSEC Incidents*
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- NSA/CSS Policy 3-9 Crypto Modernization Initiative Req's for Type 1 Classified Products

2.3 Assure Information Sharing

- DODD 8320.02 Data-Sharing in a Net-Centric Department of Defense
- *CJCSM 3213.02 Joint Staff Focal Point*
- *ASD(NII)/DoD CIO Memo Use of Peer-to-Peer File Sharing Applications Across DoD*
- *Cross Domain Community Roadmap*
- United States Intelligence Community Information Sharing Strategy
- DoD Information Sharing Strategy
- DTM-08-027 Security of Unclassified DoD Information on Non-DoD Info Systems
- CJCSI 6211.02C Defense Information System Network: Policy and Responsibilities

CIIA Goal 3:

2.1 Secure D

- FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
- SPP 800-60 Guideline for Mapping Types of Info and Info Systems to Security Categories

3.2 Prevent and Delay Attackers...

- DODD C Computer Networ
- DODD C Support to Computer N
- DODD O- CND Service Provider Certificat
- DODI Ports, Protocols, and Servi
- DODI 8 Use of Mobile Code Technologi
- CJCSI 6 Information Assurance (IA) and C
- CJCSM 6 Information Assurance (IA) and C
- *ASD(NII)/DoD CIO Memo Federal Desktop Core Configuration (FDCC)*
- FIPS 200 Minimum Security Requirements for Federal Information Systems
- DTM 08-060 Policy on Use of DoD Info Sys—Std Consent Banner and User Agreement

Cyber, Identity & Information A
Policies and IssuancesDevelop

Last Updated: November 10, 20

Send questions/suggestions to

Download the latest version

About this Chart

- This chart organizes information assu show all IA or IA-related policies a C
- No priority is intended by the arrang
- Policies in hatched boxes represent
- In the electronic version, each polic
- Policies in italics indicate the docur
- For printing, this chart is best viewe

Color Key–OPRs

🟧	ASD(NII)/DoD CIO
🟨	CNSS
🟦	DISA
🟫	DNI

te a Trusted GIG

formation Assurance

- O G&PM 11-8450 Computing
- DoDI 8500.2 Information Assurance Implementation
- *DoD CIIA Campaign Plan*
- DoDD 8000.01 Management of the DOD Information Enterprise

: Anticipate

ata in Transit

- SP 800-59 Guideline for Identifying an Information System as a NSS
- *OUSDI(I) Memo Battlespace Awareness (BA)– Capability Area Deep Dives*

3.3 Prevent Attackers from Staying...

-)-8530.1 rk Defense (CND)
-)-8530.2 etwork Defense (CND)
- 8530.1-M tion and Accreditation Program
- 8551.1 ices Management (PPSM)
- 8552.01 es in DOD Information Systems
- 510.01E omputer Network Defense (CND)
- 6510.01A omputer Network Defense (CND)
- *ASD(C31) Policy Memo Guidance for CND Response Actions*
- *ASD(NII)/DoD CIO Memo Protection of Sensitive DoD Data at Rest on Portable Computing Devices*
- ASD(NII)/DoD CIO Memo Encryption of Sensitive Unclass DAR on Mobile Computing Devices and Removable Storage Media
- ASD(NII)/DoD CIO Memo DoD Guidance on Protecting Personally Identifiable Information (PII)

CIIA Goal 4: Prepare

4.1 Develop and Maintain Trust...

- *Globalization Risk Management Strategic Plan (Draft)*

4.2 Strengthen Cyber Readiness

- DODI 8560.01 COMSEC Monitoring and Information Assurance Readiness Testing
- DODD 8581.1 IA Policy for Space Systems Used by the DoD
- DODD 3100.10 Space Policy
- NSTISSD-600 Communications Security (COMSEC) Monitoring
- CNSSP-12 National IA Policy for Space Systems Used to Support NSS
- *DoDD O-5100.30 Department of Defense (DoD) Command and Control (C2)*
- *DODD S-5100.44 Defense and National Leadership Command Capability (DNLCC) (U)*
- DODD 3020.40 Defense Critical Infrastructure Protection Program

4.3 Sustain Missions

- *DODD C-5200.19 Control of Compromising Emanations*
- CNSSI-1001 National Instruction on Classified Information Spillage
- *CNSSI-4004, Destruction and Emergency Protection Procedures for COMSEC and Class. Material*
- CNSSP-18 National Policy on Classified Information Spillage
- *CNSSP-6 National Policy for C&A of National Security Telecom and Info Systems*
- CNSSP-22 IA Risk Management Policy for National Security Systems
- CNSSP-21 National IA Policy on Enterprise Architectures for NSS
- DoDD 3020.44 Defense Crisis Management
- DoDD 3020.26 Department of Defense Continuity Programs
- CNSSP-300 National Policy on Control of Compromising Emanations
- DoDD 5144.1 ASD for Networks and Information Integration/DoD CIO
- *NSTISSI-7001 NONSTOP Countermeasures*
- *CNSSI-7000 TEMPEST Countermeasures for Facilities*
- Defense Acquisition Guidebook Section 7.5 Information Assurance
- *NSTISSI-7002 TEMPEST Glossary*
- DoDI 8410.02 NetOps for the Global Information Grid (GIG)
- *NSA IA Directorate (IAD) Management Directive MD-10 Cryptographic Key Protection*

Authorities

- Title 10 Armed Forces [§3010(b), §5013(b), §8013(b)]
- Title 14 Cooperation with other Agencies (Ch. 7: §141, §144, §145, §148, §149, §150)
- Title 32 National Guard (§102)
- Title 40 Public Building, Property, and Works (Ch. 113: §11302, 11315, 11331)
- Title 44 Public Printing and Documents (Ch. 35: §3541, §3504)
- Title 50 War and National Defense (§§401, 1801)
- Federal Information Security Management Act, 44 U.S.C. §3541 et seq
- Clinger-Cohen Act, Pub. L. 104-106
- UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

National/Federal

- CNSSI-4009 National Information Assurance Glossary
- *NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems*
- CNSSD-502 National Directive on Security of National Security Systems
- *NSPD 54/HSPD 23 Computer Security and Monitoring*
- CNSDD-900, Governing Procedures of the Committee on National Security Systems (CNSS)
- A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Info Sys
- CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Insuance System
- National Security Strategy
- *NSTISSI-4002 Classification Guide for COMSEC Information*
- FAR Federal Acquisition Regulation
- National Defense Strategy (NDS)
- National Strategy to Secure Cyberspace
- National MIlitary Strategy (NMS)
- National Military Strategic Plan for the War on Terrorism
- *National Military Strategy for Cyberspace Operations (NMS-CO)*
- Quadrennial Defense Review (QDR) Report
- National Military Strategy to Combat Weapons of Mass Destruction
- *Guidance for Development of the Force (GDF) for 2010–2015*
- Executive Order 12958 Classified National Security Information
- Executive Order 13231 Critical Infrastructure Protection in the Information Age
- Presidential Memo, "Classified Information and Controlled Unclassified Information," 27 May 09
- Computer Fraud and Abuse Act Title 18 (§1030)
- Federal Wiretap Act Title 18 (§2510 et seq.)
- Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
- Stored Communications Act Title 18 (§2701 et seq.)
- Pen Registers and Trap and Trace DevicesTitle 18 (§3121 et seq.)

Operational

- *STRATCOM OPLANs*
- *STRATCOM CONPLAN 8039-08*
- *SI 504-04 Readiness Reporting*
- *SI 507-01 NetOps Community of Interest (NCOI) Charter*
- *SD 527-01 DoD INFOCON System Procedures*
- SI 701-01 NetOps Reporting
- *Computer Network Directives (CTO, FRAGO, WARNORD)*

Subordinate Policy

- Security Technical Implementation Guides (STIGs)
- *Component-level Policy(Directives, Instructions, Publications, Memoranda)*
- Security Checklists
- Security Readiness Review Scripts (SRRs)
- DISA FSO Whitepapers
- Security Configuration Guidelines (SCGs)

ssurance (CIIA) Related
bed by DASD-CIIA
09
iatac@dtic.mil

of the IA Policy Chart from: *http://iac.dtic.mil/iatac/ia_policychart.html.*

urance policies and guidance by CIIA Strategic Goal and Office of Primary Responsibility (see Color Key). It is intended to
Component may need to comply with and direct users to the full text
gement of the guidance boxes.
new or updated drafts with a release scheduled in the near future.
y is hyperlinked to its full text online. To use the hyperlink, simply click on the box.
ment is marked for limited distribution or no public-facing hyperlink is currently available.
ed on 22"x17" (Size C) paper.

🟩	JCS	🟪	OSD	⬜	USD(I)
🟪	NIAP	🟪	STRATCOM	🟨	USD(P)
🟦	NIST	🟥	USD(AT&L)	🟧	USD(P&R)
🟩	NSA	🟩	USD(C)	🟦	Other Agencies

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

Secure Configuration Management (SCM)

by Marcia E. Weaver

As the Global Information Grid (GIG) expands and the number and complexity of devices on it continue to increase, those who manage the enterprise and its networks are challenged to maintain the components of the GIG in secure configurations. There are millions of assets within the DoD installed with numerous types of operating systems and applications—involving thousands of security-related settings—where settings for the same software often need to be secured and configured differently on multiple hosts. Defining and maintaining a secure standard baseline for each application and operating system on the GIG infrastructure is a mammoth task—but even this is not sufficient to protect the GIG. Daily vulnerabilities are publicly announced, and attacks attempting to exploit those vulnerabilities are ever increasing.

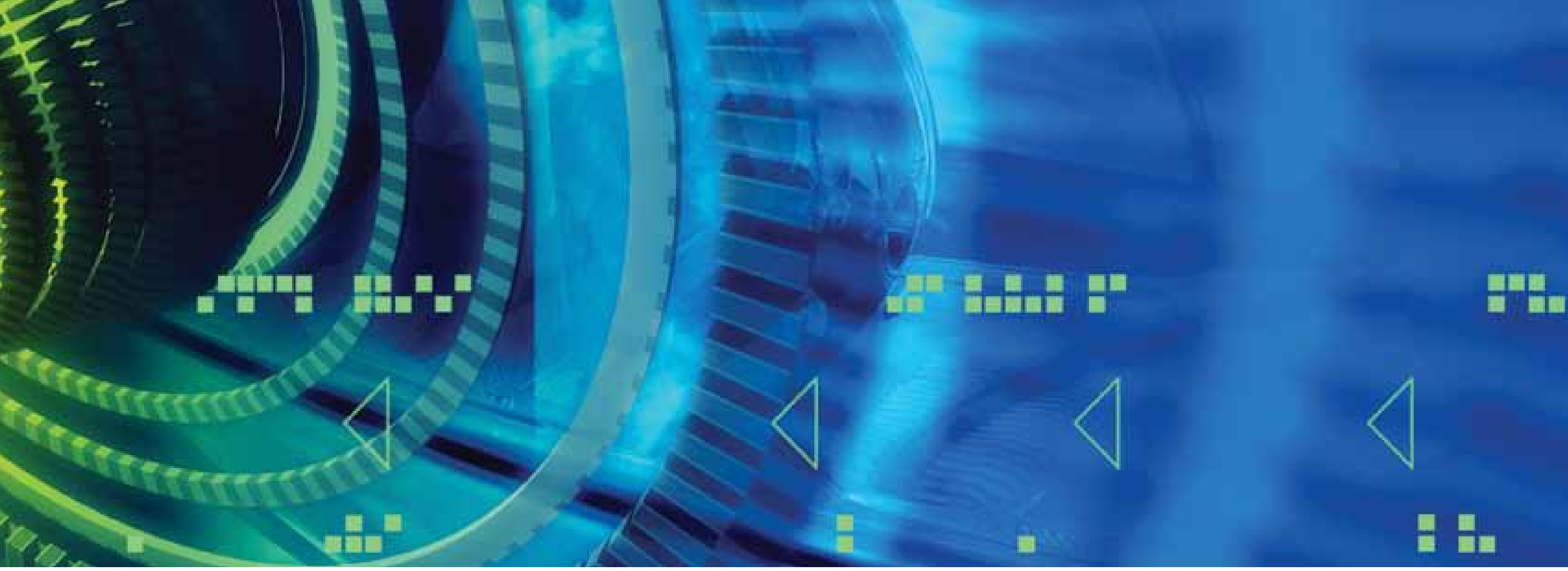
To win the fight against those vulnerabilities, standardized IA best practices must be consistently implemented, new countermeasures must be rapidly directed, and most critically, secure configuration compliance must be vigilantly verified. The dynamic nature of today's DoD missions means that computers are often disconnected and reconnected to new domains, new software applications are installed, and changing administrators and users may alter security features deemed inconvenient. Organizations require a standardized, automated way of regularly collecting the configuration state of security settings and patches of assets under their authority and producing compliance evidence. Once standardized, configuration information can be easily shared and correlated across disparate domains to enable better situational awareness of the overall security posture of the enterprise. When the information is further correlated with standardized vulnerability information, the DoD is able to rapidly and accurately assess risk posed by new vulnerabilities or non-compliant assets and identify, prioritize, and direct countermeasures. Today, organizations typically employ a variety of tools for security management that use proprietary data formats, nomenclature, and interface—preventing interoperability, creating inconsistencies in reports for the same findings, and causing significant delays in decision making.

Increasing interest and adoption of the Security Content Automation Protocols (SCAP) is about to change all of that. SCAP comprises a suite of specifications for organizing and expressing security-related information in standardized ways as well as related reference data such as identifiers for software flaws and security configuration issues. SCAP can be used for maintaining the security of enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise. [1] Federal acquisition officials have already begun embedding requirements for SCAP-validated products in their procurements. The DoD is on target to deploy enterprise-wide SCAP assessment tools in early Fiscal Year 2010. This article addresses current security configuration challenges facing the DoD and the strategy to evolve to a SCAP-based Secure Configuration Management (SCM) capability that significantly improves situational awareness of the security posture of the GIG—and ultimately enables well-informed decision making and rapid implementation of changes to that posture.

The Challenge

Managing the security of DoD systems continues to challenge the DoD on a number of fronts, such as—

- The number of complex and disparate operating systems and applications that must be secured. The DoD enterprise is a complex infrastructure of classified and unclassified networks, new and legacy systems, and commercial off-the-shelf (COTS) and government off the shelf (GOTS) software. Every system in this environment needs to be protected—the required level of protection may vary based on the value of the system and its data as well as the operational environment in which the system functions. Security managers have the



time-consuming task of determining what operating systems and applications are in use across the enterprise and verifying that the thousands of settings on each system are secured in accordance with the governing security controls. Managing large numbers of modern systems and networks is not achievable using manual techniques.

- The increasing number of mandates to which compliance must be demonstrated. There are many high-level sets of requirements that drive the implementation of security controls; however, the process of mapping the security requirements to specific controls is highly subjective based on individual interpretation of the intent of the requirement. Compliance evidence based on independent manual mapping and interpretation is largely unreliable.
- The daily emergence of new vulnerabilities. The National Vulnerability Database (NVD) contains over 33,000 vulnerabilities with approximately 20 new vulnerabilities added per day. With so many new vulnerabilities coming out each day, the DoD is finding it increasingly difficult to understand enterprise-wide impacts and to prioritize critical fixes.
- The static certification and accreditation status of changing systems. Networks change on an almost daily basis, and yet the certification and accreditation of systems on those networks remain static and inadequate to understand the impact of those changes on the accreditation.

As a result of these challenges, organizations have amassed a collection of security management tools, where each tool typically focuses on automation and communication within a single discipline such as vulnerability management or asset management. The tools use proprietary interfaces, data formats, and mechanisms that create significant inconsistencies in how these tools assess and report the security state of an asset.

Complying with required countermeasures (*e.g.,* Information Assurance Vulnerability Management [IAVM], security technical implementation guides, Communications Tasking Orders [CTO], and information operations condition changes) is equally laborious and inefficient. With limited automated assistance, security managers must determine which systems are affected by new security policies and manually execute the remediation actions using existing proprietary mechanisms. In general, once an asset is patched or configured to a new baseline, it is assumed that the settings will be maintained. There is little ongoing verification of proper configuration maintenance.

The Approach

To better protect their IT systems, security managers must be able to accurately and consistently assess the security state of their networks and institute consistent and repeatable mitigation policies throughout the enterprise. The DoD is implementing SCM as a means to gain greater control over and ensure the integrity of IT systems—by providing a standardized, automated way of securing software. At the heart of SCM are the SCAP specifications and content developed by the National Institute of Standards and Technology (NIST) and industry partners for expressing security-related information in standardized ways. Common identifiers are assigned to platform types, software flaws, and security configuration issues, enabling organizations to share and correlate information referencing the same vulnerability or configuration issue. In addition, SCAP includes standard assessment languages that provide an unambiguous way to communicate what and how software, patches, software flaws, and individual security settings will be checked. The result is consistent and repeatable checks for configuration concerns such as compliance with policy, evidence of system compromise, and vulnerability to emerging exploits. Where previous IA content was proprietary to the tool, SCAP enables the separation of the IA content from the specific tool implementation to—

- Improve data correlation

- Enable interoperability
- Foster automation
- Ease the gathering of metrics for use in situational awareness and IT security audits.

Inventory and configuration information from multiple tools can be easily correlated through standard SCAP enumerations and checklists, and emerging standardized reporting capabilities. The correlated results can be aggregated within a single organization or across the entire enterprise to provide uniform, shareable, and consumable decisioning information on what networks exist; what devices, circuits, and people are resident on the networks; and how these assets are configured.

The SCM initiative will extend the current SCAP specifications to go beyond collecting the security posture of DoD assets, to identifying and implementing recommended countermeasures. IAVMs, CTOs, and other policy changes will become machine-readable files consumed by configuration assessment tools for automated identification of affected assets, and consumed by remediation tools for automated implementation of required remediation actions.

SCM will be enterprise-deployable and operational in a multi-tiered infrastructure environment. As illustrated in Figure 1, national-level security configuration policies and associated system security checklists such as those embodied in the Office of Management and Budget Federal Desktop Core Configuration will serve as the basis for DoD systems, but will be tailored as appropriate at each tier to meet specific organizational and operational requirements. SCAP checklists are documented in standard XML so checks can be easily added, deleted, or modified. Organizations will employ SCAP-validated tools to use the checklists on a regular basis to confirm that systems are secured as intended. Mappings to high-level security controls are maintained and distributed by NIST, which allow the tools to automatically generate compliance evidence. Compliance evidence and inventory configuration assessment results will flow up through the DoD infrastructure, providing an increasingly broader view of the security posture of DoD systems.

The Assessment

The DoD requires the ability to fully discover and compile inventories of devices on its networks and to assess the configuration of those devices. These assessments will enable security managers to check system security settings for compliance with policy, verify the installation of patches, determine if vulnerabilities exist, and examine for signs of compromise such as the presence of malware files. SCAP provides an emerging specification, Open Checklist Interactive Language, for the standardization of non-automated checks.

Consistent with these limitations, the DoD will deploy persistent assessment agents to devices as part of the DoD Host-Based Security System. The configuration compliance assessment agent on an individual device can fully assess dynamic and static configuration attributes without requiring those attributes to be exposed externally where they may be exploited by adversaries.

For devices where persistent agents cannot be deployed, the DoD will conduct assessments with a network-based assessment tool. Finally, some devices may be added to DoD networks that are not capable or intentionally implemented in such a way that they do not register as part of network domains and receive assessment agents, nor do they respond to network-based discovery scans. To discover and assess these devices, the DoD will deploy a Passive Device Characterization Capability that will collect an inventory of all device addresses that access the wide area network from an internal network. The assessment capabilities will serve as the initial basis for providing enclave-level situational awareness of the security configuration of base/post/camp/station level networks.

The Reporting

Situational awareness of the security posture of the GIG is required at every level throughout the DoD—but not every tier requires the same granularity of detail or breadth of coverage. Inventory and configuration information reporting may begin at the Service (*e.g.,* network operations center) or enclave level of the infrastructure, depending upon where the network assessments are initiated and managed. SCM will consolidate the outputs of the different SCAP-validated assessment tools to provide aggregated, correlated, and de-conflicted detailed, per-device data on every system characteristic or finding of interest. This fused inventory of data will be organized into logical networks and associated with contextual information, such as which people and organizations are charged with operating, maintaining, and defending which devices, networks, and circuits. Once collected locally, this information may be shared with other local applications, such as certification and accreditation processes and security information management tools.

To support this fusion of data, it is necessary for the assessment tools report data to be in a standard results format. An emerging SCAP standard, Assessment Results Format (ARF), has been developed to provide SCM with a standardized reporting expression of the types of data that can be reported. Ultimately, SCM capabilities will issue tasking that will provide direction on the frequency and content of data to be collected, acted on, and reported to higher levels for complete enterprise assessments. Although ARF is capable of pushing detailed per device results to higher tiers, the DoD will continue to refine which data elements are required to meet enterprise management needs at each tier in the infrastructure. For example, do analysts need details about a specific asset, or are they more likely to use summary data such as platform type groupings to determine courses of action? SCM capabilities will include the ability to roll up per-device results into summary reports that include statistical

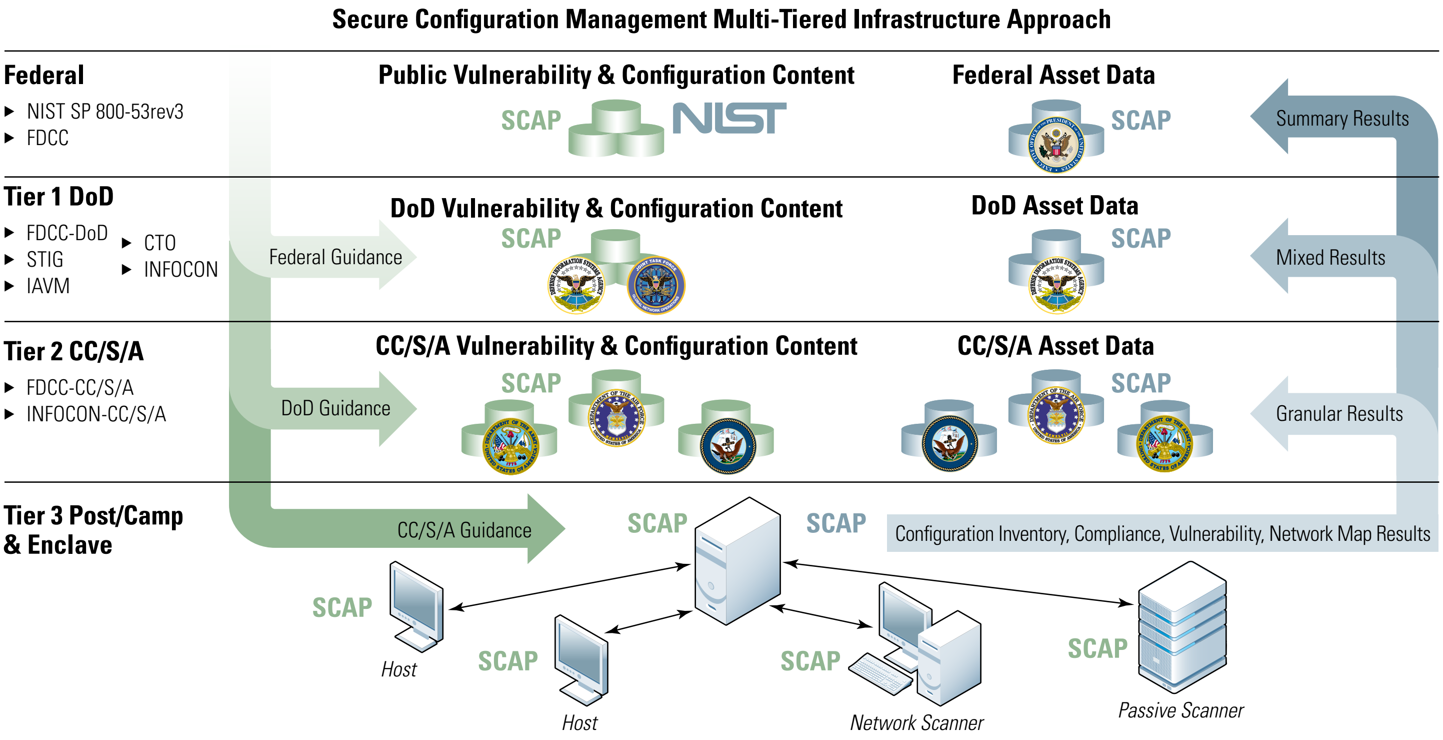


Figure 1 Secure Configuration Management Multi-Tiered Infrastructure Approach.

information about groups of devices, such as counts or lists of device identifiers for devices meeting certain conditions. Authoritative data repositories used to store the reported data will be discoverable across the enterprise by consuming for compliance tracking.

The Remediation

Finally, secure configuration management capabilities need to address the entire problem space—namely, imposing remedies to fix the problems found. In the case of SCM, remediation is the act or process of mitigating non-compliant findings or implementing recommended changes contained in new policies or orders. Remediation actions may consist of changes to the asset itself such as applying patches, installing software, and changing operating system and/or application settings. Alternatively, there are also remediation actions that may not involve the asset at all, such as changes to firewall rules or deployment of group policy objects. The SCM remediation capability will consist of a suite of solutions where the remediation can be executed on local asset drives, on centrally deployed policy deployment tools, or on existing COTS network management tools. Currently, SCAP standards for remediating vulnerabilities in a standardized and transparent way are under development through a NIST-led community effort.

The Summary

SCM resolves many of the current inefficiencies in information security through transparency, interoperability, repeatability, uniformity, and ultimately, automation. Standardization and automation enables SCM to bring the asset management, vulnerability management, compliance management, and configuration management worlds together. It unifies all this information across a diverse environment into a uniform, accurate, and current picture of the security posture of the DoD.

The linchpin to the SCM capability is the availability of both SCAP-validated tools and SCAP content for DoD deployed technologies. As SCAP content continues to mature, it will be extended into additional technologies such as firewalls and intrusion detection systems—further expanding the breadth and depth of visibility into the secure configuration posture of the entire DoD enterprise. For more information on the SCAP Program, visit the NIST SCAP Web site at *http://scap.nist.gov/*. ■

References

1. NIST SP 800-117, Draft, Guide to Adopting and Using the Security Content Automation Protocol (SCAP), May 2009

Acknowledgement

A team of configuration management experts contributed to this paper, including Joseph Wolfkiel, Daniel Schmidt, James Shelton, and Laurie Montano.

About the Author

Marcia E. Weaver | is the chief of the Enterprise Security Management Special Program Office at the National Security Agency (NSA), Department of Defense. She possesses 25 years of work experience at NSA, 12 of those years within the IA field, and four years in IT management.

DoD Activities Underway to Mature SCAP Standards

by Kevin Bingham and Scott Messick

In support of the Network Operations mission to defend and operate the Department of Defense (DoD) Global Information Grid (GIG), current Computer Network Defense (CND) strategies are focused on protecting DoD information systems and limiting an adversary's ability to impact the network on which those information systems reside. Figure 1 from the National Information Assurance Engagement Center (NIAEC) shows the basic objectives an adversary must achieve to gain the ability to impact a network and its resources. The CND mission is to limit an adversary's ability to get in, stay in, and act, therefore reducing impact to DoD networks. In order to penetrate a network, an adversary targets assets (any network-connected device) that possess hardware or software configurations with known vulnerabilities that can be exploited to enable them to get in and act within the network. To negate these malicious activities, timely configuration management processes, like applying patches, are necessary to address vulnerabilities to create a hardened network that prevents an intruder's ability to get in and stay in. Adversaries that are able to stay in and act within the network are detected and identified by analyzing the events that are generated by intrusion detection and network monitoring systems. Although these processes and tools exist to protect DoD networks, today's capabilities rely on human-centric processes that result in incomplete configuration management, questionable policy compliance, and lengthy manual processes for detecting and responding to malicious activity.

Each CC/S/A has dissimilar processes and supporting technologies for tracking and maintaining information about assets on the network, events occurring on the network, and assessing the impact and potential risk of known vulnerabilities. In many organizations, CND data is currently stored in disparate, disconnected systems that do not easily share information. Net-centric processes enabled by machine-to-machine communications can accelerate protective measures to reduce the window of exposure and ensure timely protection of networks.

Machine-to-machine communication is enabled by standardizing how information is represented and exchanged. The National Institute of Standards and Technology (NIST) is developing the Security Content Automation Protocol (SCAP) that combines a number of open standards that are used to enumerate software flaws and configuration issues related to security. With mature and effective SCAP standards comes the ability to measure, report, analyze, and take response actions through machine-to-machine automation—supporting all pillars of CND defensive measures (protect, detect, respond, and sustain). The result: significant improvements to GIG situational awareness, response speed, and interoperability in tools and vendor products. As we look forward to the future of CND, the SCAP standards become a critical foundation for measurement and automation across the GIG.

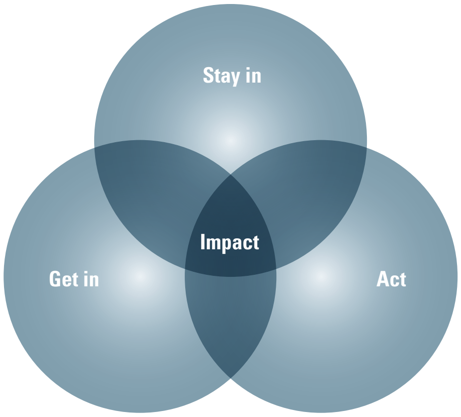
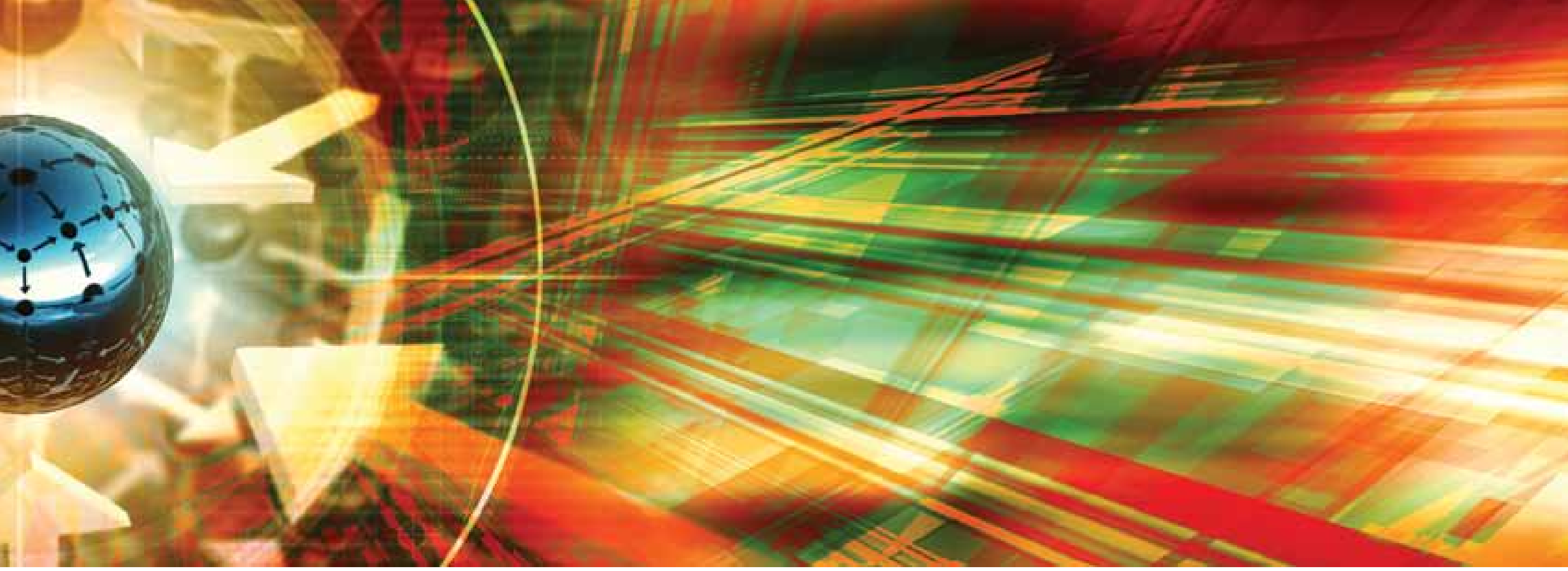


Figure 1 Adversary's ability to impact computer networks.

The CND Data Strategy Pilot, sponsored by the Office of Assistant Secretary of Defense for Networks and Information Integration (OASD NII) and the National Security Agency (NSA) Information Assurance Directorate, is focused on applying the net-centric data strategy to the CND mission to make CND data quickly visible, accessible, and understandable to people and systems across the DoD. The CND pilot works to achieve these goals by: 1) Building upon



NIST SCAP data standards to create schemas that define how data is represented; 2) Defining the interfaces through which data is exchanged; and 3) Validating the standards ability to support DoD missions and operations. The establishment and validation of CND data exchange standards is a necessary initial step in the transformation of a stove-piped, reactive, and manual problem-solving environment to a flexible, powerful, and net-centric environment. (See Figure 2).

The initial intent of the pilot was to validate that SCAP and DoD standards can help reduce the processing time required for vulnerability risk analysis. As new vulnerabilities emerge, they are uniquely identified by the Common Vulnerability Enumeration (CVE) SCAP standard. Vulnerable configurations are indicated by the Common Platform Enumeration (CPE) SCAP standard. Vulnerable CPEs can be compared to the CPEs of DoD assets to identify the target distribution and collateral damage potential for a given vulnerability, and the severity of the vulnerability is captured by using the SCAP Common Vulnerability Scoring Standard (CVSS). Events can be related to assets *via* IP addresses and also be related to vulnerabilities *via* event signatures that

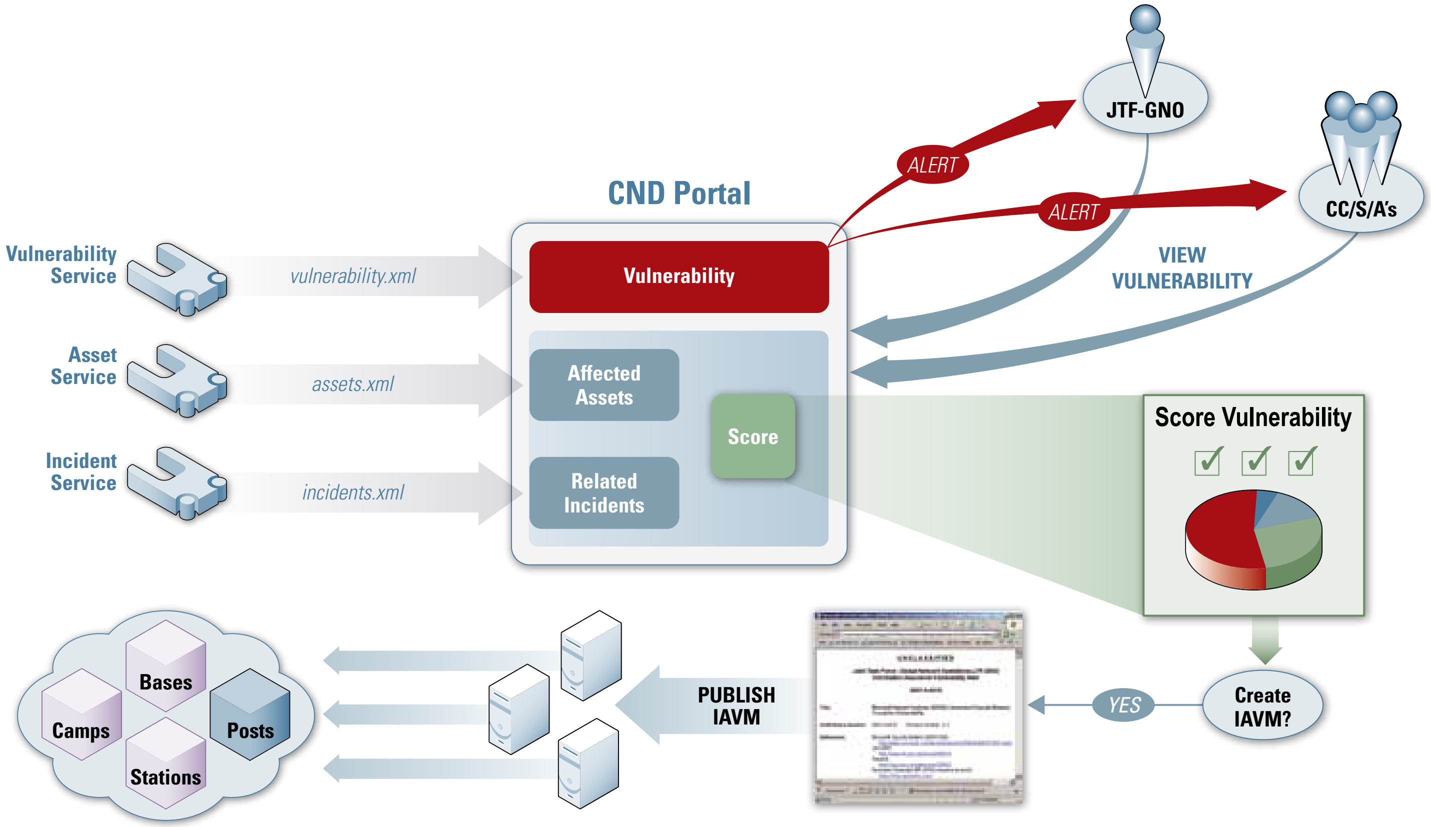
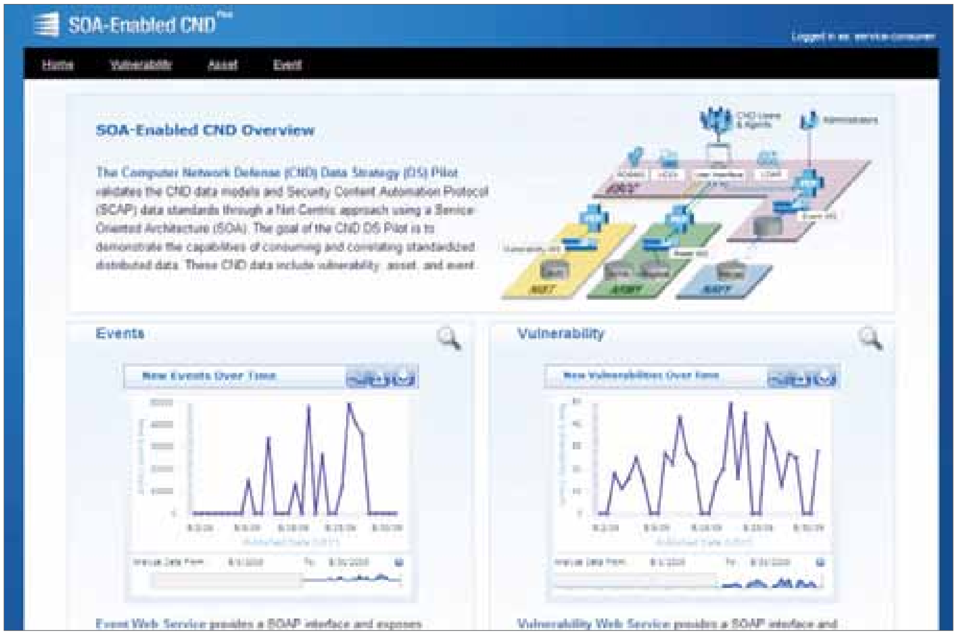


Figure 2 Automating and accelerating the IAVM creation and dissemination process using SCAP and DoD data exchange standards.

include references to CVEs. By employing these SCAP standards, assets, events, and vulnerabilities can be quickly related to determine if configuration management modifications in the form of Information Assurance Vulnerability Alerts (IAVA) are needed.

To realize this use case, the pilot identified authoritative data sources for vulnerabilities, assets, and events and then instrumented them with Web service interfaces to expose their data in accordance with CND data exchange standards. NIST's National Vulnerability Database (NVD) provides vulnerability data. The Army's Asset and Vulnerability Tracking Resource (A&VTR) provides asset and configuration data. The Navy's Prometheus repository provides event data. Data from each of the sources is consumed and correlated within a lightweight Web-based CND workspace to provide authorized users visibility into the relationships between vulnerability, asset, and event data. The pilot correlates data from a variety of data sources and provides tailored views without manipulating the original data and without replicating the diverse data sets into a centralized repository.

Authorized users can view a summary of newly identified vulnerabilities over time, browse vulnerability summaries, view vulnerability details, identify the assets that are potentially vulnerable, and determine the criticality of events that are occurring due to the vulnerability (Figure 3). Authorized users can determine the distribution of assets across geographical regions and Mission Assurance Category (MAC) levels, view the details of any given asset, and identify all of the vulnerabilities to which the asset may be vulnerable (Figure 4). Authorized users can also see a summary of event counts over time, identify the top occurring events, determine the severity of events, and review the details of the vulnerabilities that are related to the event signatures (Figure 5). These activities, which used to take days or months to complete, can now be accomplished within a matter of minutes with a series of mouse clicks.



SOA-Enabled CND Overview

The Computer Network Defense (CND) Data Strategy (DS) Pilot validates the CND data models and Security Content Automation Protocol (SCAP) data standards through a Net-Centric approach using a Service Oriented Architecture (SOA). The goal of the CND DS Pilot is to demonstrate the capabilities of consuming and correlating standardized distributed data. These CND data include vulnerability, asset, and event

Event Web Service provides a SOAP interface and exposes

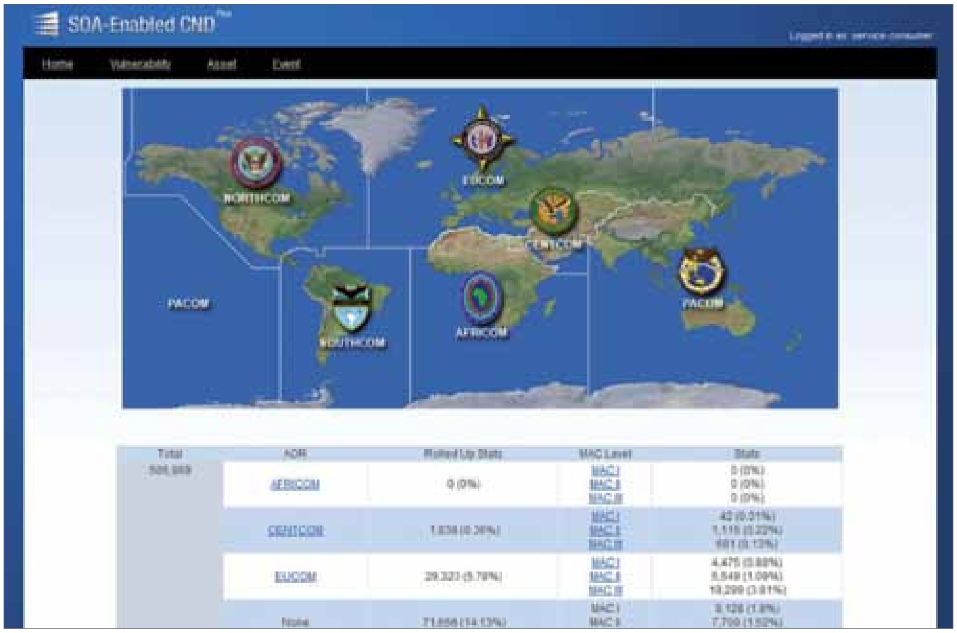
Vulnerability Web Service provides a SOAP interface and

Figure 3 Event and Vulnerability Trends.

The CND Data Strategy Pilot is bringing confidence and validity to the SCAP data standards, Web Service specifications, and the supporting architecture developed to realize the objectives of security measurement and automation. Powered by machine-to-machine communications, this net-centric CND environment demonstrates the ability for standards to automate and accelerate the process of correlating events and vulnerabilities to assets within DoD networks. The effort demonstrates the capability to integrate data from several diverse data sources distributed across the GIG and is an example of the type of powerful composite applications that can quickly be created given the availability of shared information, common data specifications, and contemporary Web service technologies. Efforts are ongoing to add more data sources and validate additional standards related to remediation, systems, missions, and operations as the CND Data Strategy Pilot matures and more components join in the effort.

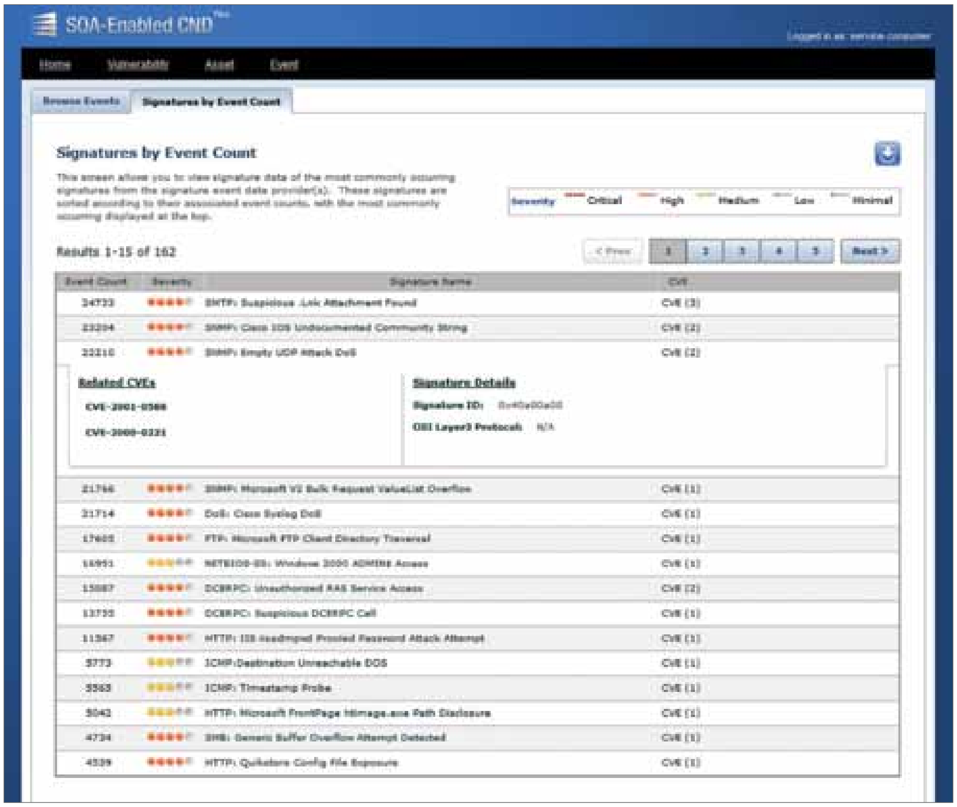
Based on the successes of the data strategy and piloting efforts, there are a number of operational deployment activities focused on establishing the foundation of an integrated set of interoperable CND systems—

- The Host Based Security System (HBSS) baseline has been expanded to include an asset Web service that publishes asset data to the enterprise in accordance with CND data standards. This Web service will help CND analysts obtain a greater degree of situational awareness of what is happening with the DoD enterprise networks at the asset level. The service will enable an enterprise catalog of assets on DoD networks.
- The Information Assurance Vulnerability Management (IAVM) system is being enhanced based on the successes of the CND data strategy pilot. Vulnerability assessment teams will use this enhanced knowledge of how vulnerabilities, assets, and events relate to make informed decisions about the creation of configuration management policies. Leveraging SCAP data standards, such as Open Vulnerability and Assessment Language (OVAL) and eXtensible Configuration Checklist Description Format (XCCDF), this IAVM system will enable creation and dissemination of machine-readable



Total	AOR	Rolled Up Stats	MAC Level	Stats
506,869	AFRICOM	0 (0%)	MAC I MAC II MAC III	0 (0%) 0 (0%) 0 (0%)
	CENTCOM	1,838 (0.36%)	MAC I MAC II MAC III	42 (0.01%) 1,115 (0.22%) 681 (0.13%)
	EUCOM	29,323 (5.79%)	MAC I MAC II MAC III	4,475 (0.88%) 5,549 (1.09%) 19,299 (3.81%)
	None	71,656 (14.13%)	MAC I MAC II	9,128 (1.8%) 7,700 (1.52%)

Figure 4 Vulnerable Assets Across COCOM and MAC Level.



Signatures by Event Count

This screen allows you to view signature data of the most commonly occurring signatures from the signature event data provider(s). These signatures are sorted according to their associated event counts, with the most commonly occurring displayed at the top.

Results 1-15 of 162

Event Count	Severity	Signature Name	CVE
34733	★★★★☆	SMTP: Suspicious .Lnk Attachment Found	CVE (3)
23204	★★★★☆	SNMP: Cisco IOS Undocumented Community String	CVE (2)
22210	★★★★☆	SNMP: Empty UDP Attack DoS	CVE (2)

Related CVEs

CVE-2001-0566

CVE-2000-0221

Signature Details

Signature ID: 0x40a00a00

OSI Layer3 Protocol: N/A

Event Count	Severity	Signature Name	CVE
21766	★★★★☆	SNMP: Microsoft V2 Bulk Request ValueList Overflow	CVE (1)
21714	★★★★☆	DoS: Cisco Syslog DoS	CVE (1)
17605	★★★★☆	FTP: Microsoft FTP Client Directory Traversal	CVE (1)
16951	★★★☆☆	NETBIOS-SS: Windows 2000 ADMIN$ Access	CVE (1)
15087	★★★★☆	DCERPC: Unauthorized RAS Service Access	CVE (2)
13755	★★★★☆	DCERPC: Suspicious DCERPC Call	CVE (1)
11367	★★★★☆	HTTP: IIS isadmpwd Proxied Password Attack Attempt	CVE (1)
5773	★★★☆☆	ICMP:Destination Unreachable DOS	CVE (1)
5563	★★★☆☆	ICMP: Timestamp Probe	CVE (1)
5042	★★★☆☆	HTTP: Microsoft FrontPage htimage.exe Path Disclosure	CVE (1)
4734	★★★★☆	SMB: Generic Buffer Overflow Attempt Detected	CVE (1)
4539	★★★★☆	HTTP: Quikstore Config File Exposure	CVE (1)

Figure 5 Top Occurring Event Signatures & Related vulnerabilities.

policies across the DoD. By employing a Web service, these policies can be directly injected into existing systems and business processes, resulting in a major reduction in the time between vulnerability identification and compliance.

- The Joint Incident Management System (JIMS) is evolving the capabilities for incident response, incident reporting, incident metrics, and incident correlation. CND and SCAP standards establish a common language for the exchange of incident information across the enterprise. The result will be faster incident response times and the reduction of duplicative efforts due to the increases in incident visibility and collaboration across the enterprise.

The early stages of building this environment are underway with several efforts focused on maturing the standards and proving the architecture to achieve future objectives stated throughout this issue. Efforts are IA-related initiatives aimed at supporting improved protection, detection, and response within CND. Configuration management (CM) activities are defining the flexible enterprise baselines for DoD networks. IA best practices and Federal Desktop Core Configuration (FDCC) efforts establish those baselines to harden the network core and provide assured information protection. Network sensors, audit logs, and detection signatures provide the insight required to ensure the network's ability to support operations and measure the effectiveness of decisions and actions. Definition and adoption of data exchange standards enable automated reporting across diverse data sets to strengthen situational awareness. The orchestration of the initial set of asset, event, vulnerability, IAVM, and incident services automates the vulnerability and incident management processes, resulting in a reduction in the "window of exposure" (identification to remediation for a given vulnerability or incident) from months down to days or hours.

Building on the SCAP foundation, relatively near-term expectations of the SCAP standards to support CND architectural strategies are being realized. Strong and flexible configurations can be achieved through FDCC, NIST SCAP tool validations, and best practice configuration efforts. Effective IA command and control will be enabled through strong situational awareness, rapid reporting, and automated remediation. Supporting these end states will require measurement and correlation of disparate data elements at all tiers within the GIG—measurements that will support detection (network sensor, log/audit data, node confidence data, and detection signatures) and protection of GIG resources (compliance validations and automated remediation capabilities) able to validate secure configurations and enable rapid mitigation against new threats. Standards-based data will be available to feed numerous systems—some will be focused on technical system details, and others will be focused on high-level system health status within a commander's common operating picture. Measurements and improved situational awareness, coupled with strong IA command and control, will create an automated and dynamic environment able to anticipate, prevent, and reduce the impact of cyber attacks. ■

About the Authors

Kevin Bingham | has served in the role of CND architect for the DoD since October 2007. He supports the DoD and the Enterprise Solutions Steering Group with CND strategy and architectural issues—working closely with NSA, JTF-GNO, and DISA. His current CND Architect efforts are heavily focused on supporting the CND Data Strategy and CND Data Strategy Pilot—an effort to demonstrate operational applicability of SCAP and CND Data Standards to support NetOps by enhancing CND situational awareness and enabling automated CND processes.

Previously, Mr. Bingham spent six years with the NSA Red Team, serving in positions as on-net operator, wireless LAN vulnerabilities team lead, assessment team lead, and operations branch chief. He spent 10 years in the Air Force as a C-130 navigator in the Pacific and as an instructor at the Air Force Undergraduate Navigator Training School at Randolph AFB, TX. He received a BS degree in mechanical engineering from Texas Tech University and an MS degree in computer information systems from St. Mary's University in San Antonio, TX.

Scott Messick | supports NSA, OSD/NII, and JTF-GNO on a number of Computer Network Defense data strategy efforts. Mr. Messick has over 13 years of professional IT consulting experience and is an expert in the areas of net-centricity, service oriented architecture, data strategy, and full life-cycle software development of Web services and rich Internet applications. Earlier in his career Mr. Messick provided consulting, architecture, and IA support to Industry 500 companies.

Letter to the Editor

Q ***I subscribe to several of IATAC's electronic mailings. I know IATAC sends the IA Digest out in HTML and plain text formats. At my organization, I am not allowed to view HTML emails. Is that a standard email policy across DoD? Or is that policy determined at the organizational level?***

A A lot of IATAC customers often inquire about why they are unable to view our IA Digest in Hyper Text Markup Language (HTML) format. To answer your question, the Department of Defense (DoD) has not issued a Department-wide mandate for email configurations; instead, it is left up to the individual combatant commanders, services, and agencies to set their own policies regarding items such as email presentations and attachments.

In many cases, responsibility for defining this type of policy devolves further down to the individual sites. It is the system administrator who configures the individual site's email servers and firewalls in accordance with the site policy. As one of IATAC's residential subject matter experts states, "The differentiation between different sites' policies no doubt reflects a difference in the level of Web application security awareness between one site's policy maker and the next." (Web application security is an issue because HTML is a Web markup language.)

HTML format can introduce some security risks. One risk is that HTML allows the email sender to include easy-to-click, embedded links to external Web sites rather than the full Universal Resource Locators (URL) for those sites. Because they don't see the URLs, trusting recipients of such messages may simply click on the embedded links without first using browser features to reveal the actual URLs. In some cases, the links may be invalid, and may point to malicious Web pages from which malicious code such as spyware is automatically downloaded to the recipient's computer. Another risk is that use of HTML tags such as <APPLET> or <EMBED> enable the automatic loading of large executable objects within the email message itself; the result can be a denial of service to the email client or browser (for email viewed *via* a Webmail application).

The best method of avoiding these risks altogether is to configure the email server or firewall to block messages that are not in plain text; this means that messages that contain HTML or XML will be blocked. Sites with this level of security awareness often disallow certain types of attachments, too, such as compressed attachments (*e.g.*, Zip archives), executable attachments (*e.g.*, .exe files), and others that increase the risk that malicious code may be introduced to the site's network. ■

DoDTechipedia Happenings

by Rogelio Raymond

In some undisclosed military deployment location, a service member logs onto a social networking Web site to say "hello" to family and friends back in the United States. He notices he has an email that seems to be from a relative back home. The email contains a link to a Web site that offers free products. All he has to do is give his login credentials to get into the Web site for these products. This gentleman was just "phished," and if the attempt was successful, he may have just compromised his local computer network. DoDTechipedia can help heighten our awareness of the dangers of these social networks.

DoDTechipedia is still keeping the Research & Development and Science & Technology communities in the federal government and DoD on the cutting edge of technology in what's new and in the news in information assurance (IA) and information warfare (IW).

The use of social networking sites on DoD and federal government computer networks currently is a hot topic in the news. Browse the blog spaces for DoDTechipedia's IA and IW Web portals, and you will find several blogs on the topic of vulnerabilities with social networking sites such as Twitter, Facebook, LinkedIn, and MySpace. Blog titles such as "Koobface Worm hits Twitter," "DoS attacks on Social Media sites," and "Social networkers' risky behavior" illustrate how the increasing usage of social networking Web sites by federal government and DoD employees creates possibilities of social engineering, denial-of-service attacks, Trojan Horse exploitation, and phishing.

Help keep the DoD community well informed and connected by logging onto DoDTechipedia and sharing your experience and expertise on the use of social networking technology in your organization. You can do this by posting blogs or by creating or contributing to an existing technology page.

To access DoDTechipedia, visit *https:// www.dtic.mil.* ■

▷ continued from page 11

IATAC SPOTLIGHT ON A UNIVERSITY

practitioners to hone their skills under the guidance of seasoned experts. [3]

UAlbany co-hosts the Annual New York State Cyber Security Conference and the Annual Symposium on Information Assurance. UAlbany's School of Business also co-hosted the first International Conference on Digital Forensics and Cyber Crime (ICDF2C). ICDF2C brought together law enforcement, prosecutors, private industry employees, government officials, and academics in the area of digital forensics and cyber crime. The conference was the first to encompass both traditional computer and information security concerns (*e.g.,* Internet crimes against children) as well as money laundering and accounting fraud detection (both of which have become increasingly electronic). Topics included continuous auditing, digital evidence in fraud detection, smart phone forensics, cell phone camera fingerprint recognition, instant messaging authorship identification, removable device data exfiltration prevention, botnet investigation, digital evidence standards, and a mock direct and cross-examination of a computer forensics examiner. ■

References

1. *http://www.albany.edu/cifa/*
2. Goel, S., Pon, D., & Bloniarz, P., Bangert-Drowns, R., Berg, G., Delio, V., Iwan, L., Hurbanek, T., Schuman, S., Gangolly, J., Baykal, A., and Hobbs, J. Innovative Model for Information Assurance Curriculum: A Teaching Hospital. ACM Journal on Educational Resources in Computing, Special Issue on Support for the Computer Security Currículum, 6 (3), 2006.
3. *http://www.albany.edu/cifa/about/index.html*

Why Industry Needs Federal Government Leadership to Gain the Benefits of Security Automation

by Alan Paller

Software interoperability is fundamental to automation of security. Without effective interoperability, network defense is a hit-and-miss game that takes too many people, too much money, and too much time—

- If the intrusion detection system cannot communicate with the inventory system, then attacks that are critical (because they are rare but highly targeted) may get too little attention, while harmless attacks (common attacks but aimed at systems without the target vulnerability) may get too much attention.
- If the vulnerability management system cannot interact fully with the configuration management system, then days or weeks of manual patch testing may be required before patches can be installed. On the other hand, if they can communicate, the configuration management system can verify that the vulnerability being tested is in a system that has a configuration that matches the standard, so it can be patched immediately.

There are many more examples that other writers in this issue illuminate. I include these just to support the theme that security will be far too expensive and ineffective without software interoperability.

This article describes why the structure and incentives in the software industry mean that software interoperability will not come to critical infrastructure businesses and to colleges, cities, and states unless the federal government takes a strong leadership role.

Switching Costs

Software companies get 90% of their profits from existing customers. Beyond their initial outlay for software, existing customers pay for maintenance (at prices that rise almost every year), upgrades, training, and add-ons, all of which add up to much more than the initial outlay. In addition, when a software company creates (or buys) a completely new product, it finds that selling to an existing customer costs one fifteenth of what it costs to sell to a new customer. Because marketing and sales costs consume around 50 cents out of every dollar spent by software companies, holding onto customers is the winning strategy—maybe the only winning strategy.

You might well assume that product quality and customer service are the ways that software companies hold onto customers, and you would be right, in part. But usually, software companies look for an edge, something that makes it very hard for a customer to shift to a replacement product. The academics call them "switching costs" and define them as "those one-time inconveniences or expenses a customer incurs in order to switch over from one product to another." If, for example, one vendor holds all your historical data, and to switch to a different vendor you would have to spend weeks reconstructing the database, it might not be worth switching.

Standards lower switching costs. Because they make switching easier, standards are deeply distrusted by software marketers and developers. One exception occurs when a dominating vendor can make its own technology into a standard, but in the security software field there are no dominating vendors. That means that regardless of the vendors' claims, most software vendors will work diligently to delay the creation, vetting, or deployment of standards for software interoperability that might make it easier for their clients to switch. The vendor representatives may even come to meetings and act as if they are helping, all the while looking for ways to delay the process. A second exception is sometimes perplexing. When one vendor has gotten a strong foothold in a huge client organization, other vendors—especially small ones—will sometimes champion open standards in order to have a chance to bid on replacement contracts.

Client Control and Isolation

Software vendors have very limited teams of advanced development engineers, so they jealously guard the priorities placed on those engineers. Clients who ask for new product features that make it easier for them to switch to other vendors' products usually get a friendly "thank you" and a statement something like, "You are the first organization to suggest

that, but it is really a good idea. I'll take it back to our development team." They say that even when dozens of customers have asked for the same thing—like interoperability. And you probably will never hear from them again on that topic.

The One Incentive that Trumps all the Others

When a very big customer comes to a vendor and says, "We need this particular feature in order to buy your product or continue using your product," the natural defenses disappear. The sales staff has direct access to the development staff and those few advanced development engineers are assigned to make it happen. But you have to be a extremely large client in order to have a real impact.

Even the largest corporations are, individually, very small buyers of any one product. When they try to gather other users together to speak with one voice, the vendor will offer special incentives (free upgrades or discounts or training, for example) to get them to act individually. It is very hard to hold the line on demanding open standards when a vendor is offering your boss a 40% discount if he agrees to select the current, proprietary product instead.

That is why federal leadership, especially Department of Defense (DoD) leadership, is the key to enabling rapid adoption of security automation. The U.S. government is a large enough buyer of technology to provide the incentives for security vendors to adopt open standards. If the DoD establishes a policy that all software licenses after a date certain must include a specific list of open standard capabilities, the vendors will build the interoperable products. Once they are built, industry can buy them, too. ■

About the Author

Alan Paller | is responsible for SANS' consensus research initiatives and Internet Storm Center. He chairs the Application Security Summit and the SCADA Security Summit and edits NewsBites, the bi-weekly security news summary sent to 200,000 people. President Bill Clinton named Mr. Paller one of the original members of the National Infrastructure Assurance Council, and the Federal CIO Council gave him its Azimuth Award, recognizing his "singular vision and outstanding service to federal information technology."

▷ *continued from page 5*

SUBJECT MATTER EXPERT

- **Security Education**—Dr. Goel's security education work involves developing innovative models for information security education. A "teaching hospital" model was created that envisages using information security problems from industry and abstracting them into living-cases to be used for education of students and public workforce. [2]

Dr. Goel organizes and presents at several conferences in information security with topics such as wireless security, hacking, and botnets, and has several publications in leading conferences and journals. He is the conference chair of the International Conference on Digital Forensics and Cyber Crime, the Annual Symposium on Information Assurance, and Nanosensors 2010.

Before joining the university, Dr. Goel worked at the General Electric Global Research Center. He received his Ph.D. in mechanical engineering in 1999 from Rensselaer Polytechnic Institute. ■

References

1. *http://www.albany.edu/~goel*
2. *http://www.albany.edu/~goel/research/infosec.shtml*

Practicing Standards-Based Security Assessment and Management

by Robert Martin

Over the past 10 years, MITRE, in collaboration with government, academia, and industry has developed a number of information security standards. While still evolving, several of these efforts in standardization have made their way into commercial solutions and government, industry, and academic usage. Perhaps most visible of these has been the Federal Desktop Core Configuration (FDCC) that leveraged the Security Content Automation Program (SCAP). SCAP utilizes mature standardization efforts to clearly define common security nomenclature and evaluation criteria for vulnerability, patch, and configuration measurement guidance and is intended for adoption by automated tools.

For an enterprise to measure and manage its cyber assets, it will need to employ automation techniques and typically use products from different vendors. To make the finding and reporting issues consistent and composable across different tools, there has to be a set of standard definitions of the things that are being examined, reported, and managed by those tools. 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 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 tools and some areas like SCAP and FDCC, there is more that individuals can do to allow even greater capabilities to emerge. We feel that those who buy software products, create organizational security policies, and create security guidance and benchmarks can help us all get to these greater capabilities faster by adopting some of the following practices.

Procurement Guidance for Software

As a procurement officer, you can make sure that the products being offered are compliant with the new FAR provision, *FAR Case 2007-004, Common Security Configurations,* specifying compliance with FDCC and that end users should make sure the products they are considering are compliant with FDCC. Additionally, procurement officers can levy requirements on the software providers to—

- Provide a public address (email and/or Web) for reporting security-relevant issues with the provider's software
- Provide a publicly available statement of the time frame and process the software provider's organization follows in addressing reports of security relevant issues with the provider's software
- Provide 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 of 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 CVSS rating for the flaw, misconfiguration, or incorrect default settings as part of the initial public advisory.

Government Organizations

As a government organization decides how systems should be set up for operational use, standards can be used to convey a "blessed" configuration. Specifically, government organizations can levy requirements on their user communities to—

- Express policies and guidelines in the XCCDF/OVAL standard languages so that tool technologies can use these machine-readable descriptions directly to evaluate the

status of information technology with regards to those policies and guidelines

- Adopt the use of automated methods to directly use the machine-readable XCCDF/OVAL policies and guidelines for assessing, reporting, and directing action on exceptions to the policies and guidelines.

Specifically, these types of products and services should—

- Include the appropriate CVE Identifier for security-related 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 results from flaw, patch, and configuration check assessments that are written in conformance with the OVAL Results schema
- As appropriate to the functionality of the tool, incorporate support for the different severity score portions of the CVSS rating for the flaw or incorrect default settings.

It is strongly recommended that 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 SCAP.

Procurement Guidance for Security Assessment and Management Tools

In general, procurement and end users should request/require that security product vendors that deal with security flaws, configuration settings, policies, or patches support the SCAP standards. It is strongly recommended that 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 SCAP.

- 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

Additional areas of standardization are emerging (*e.g.,* application weaknesses, events, malware attributes, attack patterns, remediation actions) that in the future will benefit those working to secure their enterprises. ■

About the Author

Robert A. Martin | is a principal engineer in MITRE's Information and Computing Technologies Division. For the past nine years, he has focused on the interplay of enterprise risk management, cybersecurity standardization, critical infrastructure protection, and the use of software-based technologies. Mr. Martin is a member of the ACM, AFCEA, and the IEEE Computer Society. He received bachelor and master degrees in electrical engineering from Rensselaer Polytechnic Institute, and an MBA from Babson College.

Cloud Assurance Still Missing

by Allan Carey

As with virtualization, organizations are flocking to cloud computing by the allure of lower costs. Instead of investing to purchase infrastructure and software, organizations and agencies are attracted by the idea of getting infrastructure, platforms, and software as a "pay per use" service.

Along with lower fixed costs, however, use of cloud computing brings with it a loss of control and an exposure to various risks, particularly security risks. Practitioners are advised to—

- Understand exactly what cloud computing means, which includes understanding the taxonomy and layers
- Assess where cloud computing might make sense and which model of cloud computing, public *vs.* private, is the most appropriate
- Understand the risks faced, conduct a gap analysis, and develop plans to address the risks. Often these plans entail focusing on the basics by matching the business and security requirements against the most appropriate cloud models.
- Take actions such as classifying data and assets, conducting a risk assessment, evaluating vendors, educating their organization, and participating in the evolution of cloud computing.

When people refer to "the cloud," they are typically talking about the SPI model, which includes software (S), platform (P), and infrastructure (I) as a service. The following taxonomy describes the components and layers of these services. These different services and their many layers mean that organizations can pick and choose the different pieces of the SPI model that meet their needs—

1. **Infrastructure as a service (IaaS)**—This includes the physical facilities, the hardware, an abstraction layer, a core connectivity and delivery layer, and application program interfaces. Vendors in this space include Amazon EC2, GoGrid, and FlexiScale.
2. **Platform as a service (PaaS)**—This is the middleware that integrates the infrastructure and the resources that sit on top of it. It can include identity and access management, databases, and authentication. PaaS vendors are Force.com, Google AppEngine, and Coghead.
3. **Software as a service (SaaS)**—This is the data and the applications. Examples of SaaS vendors are Salesforce.com, GoogleApps, and Oracle on Demand.

There are many similarities between cloud computing and virtualization. Virtualization is an enabler of cloud computing, as the new de facto atomic unit of the digital infrastructure is now a virtual machine.

A reality of virtualization is that organizations have rushed to adopt it without solving many of its attendant security, privacy, and management challenges. And now, without having solved the problems associated with virtualization—problems that are within an organization's own control—organizations are moving to the cloud, where they have even less control.

The security problems that organizations face related to cloud computing are the same as those related to virtualization—but even more so. The abstraction of infrastructure points to the need for information centricity and, consequently, information assurance.

Steps that security practitioners should take to decrease the risks associated with cloud computing involve common sense. Information assurance practitioners already have most of what is needed to make an informed set of decisions about cloud computing. The challenge is to match the organization's business and security requirements against the various cloud "service" (aaS) models. Among the requirements: not being a speed bump to business operations and achieving and maintaining compliance. Activities that practitioners should engage in include conducting a cloud computing risk assessment and a gap analysis. An organization can assess security for each layer in the cloud and can identify any shortcomings. Some additional resources include the Cloud Security Alliance, cloud computing Google groups, and attending a local CloudCamp. ■

FREE Products Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not a registered DTIC user, you must do so prior to ordering any IATAC products (unless you are DoD or Government personnel). To register online: *http://www.dtic.mil/dtic/registration*. The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name ____________________ DTIC User Code ____________________

Organization ____________________ Ofc. Symbol ____________________

Address ____________________ Phone ____________________

____________________ Email ____________________

____________________ Fax ____________________

Please check one: □ USA □ USMC □ USN □ USAF □ DoD □ Industry □ Academia □ Government □ Other

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: ____________________

____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)

- □ **Firewalls**
- □ **Intrusion Detection**
- □ **Vulnerability Analysis**
- □ **Malware**

Critical Review and Technology Assessment (CR/TA) Reports

- □ Biometrics (soft copy only)
- □ Data Mining (soft copy only)
- □ Wireless Wide Area Network (WWAN) Security
- □ Computer Forensics (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)
- □ Configuration Management (soft copy only)
- □ IA Metrics (soft copy only)
- □ Defense in Depth (soft copy only)
- □ Network Centric Warfare (soft copy only)
- □ Exploring Biotechnology (soft copy only)

State-of-the-Art Reports (SOARs)

- □ Measuring Cyber Security and Information Assurance
- □ The Insider Threat to Information Systems (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)
- □ Software Security Assurance
- □ A Comprehensive Review of Common Needs and Capability Gaps
- □ IO/IA Visualization Technologies (soft copy only)
- □ Modeling & Simulation for IA (soft copy only)
- □ Malicious Code (soft copy only)
- □ Data Embedding for IA (soft copy only)

UNLIMITED DISTRIBUTION

IAnewsletters hardcopies are available to order. Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 11 □ No. 1 □ No. 2 □ No. 3 □ No. 4
Volumes 12 □ No. 1 □ No. 2 □ No. 3 □ No. 4
Volumes 13 □ No. 1

SOFTCOPY DISTRIBUTION

The following are available by email distribution::

□ IADigest
□ IA/IO Scheduler
□ Research Update

Fax completed form to IATAC at 703/984-0773

Calendar

February

2010 Information Assurance Exposition
2–5 February 2010
Nashville, TN
http://www.informationassuranceexpo.com/

The Network and Distributed System Security Symposium (NDSS) 2010
28 February–3 March 2010
San Diego, CA
http://www.isoc.org/isoc/conferences/

March

RSA Conference
1–5 March 2010
San Francisco, CA
http://www.emc.com/microsites/rsa-conference/index.htm

Mid-Atlantic Information Security Forum
16–17 March 2010
Washington, DC
http://www.ianetsec.com

DTIC 2010
22–25 March 2010
Alexandria, VA
http://fbcinc.com

April

IAPP Global Privacy Summit
19–21 April 2010
Washington, DC
http://www.privacysummit.org/

May

DISA Customer Partnership Conference
3–7 May 2010
Nashville, TN
http://www.disa.mil/conferences/

IEEE Symposium on Security and Privacy
16–19 May 2010
Oakland, CA
http://oakland31.cs.virginia.edu/index.html

To change, add, or delete your mailing or email address (soft copy receipt), please contact us at the address below
or call us at: 703/984-0775, fax us at: 703/984-0773, or send us a message at: iatac@dtic.mil

IATAC

Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171