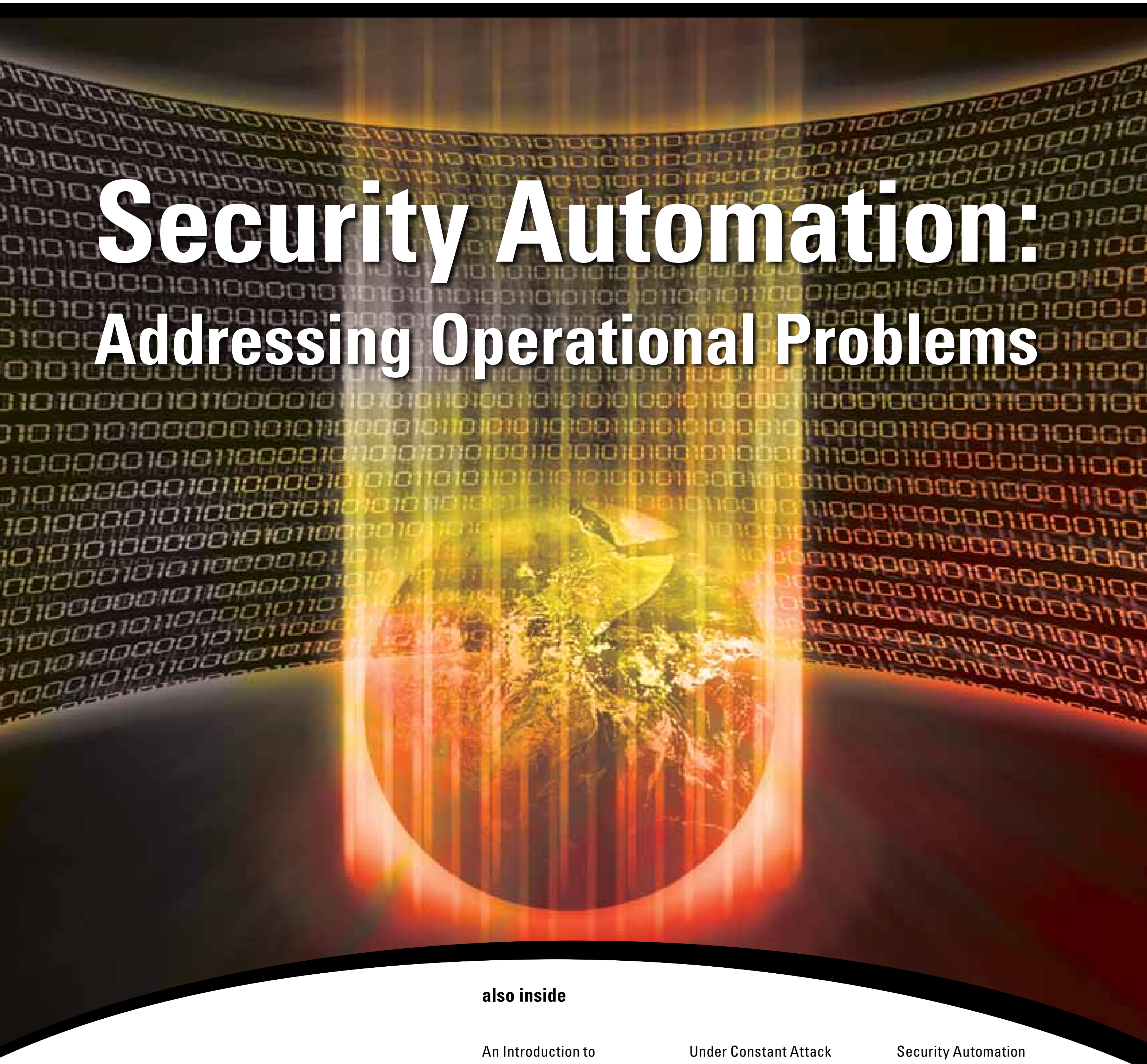
14/4

IAnewsletter

Volume 14 Number 4 • Fall 2011

The Newsletter for Information Assurance Technology Professionals



Security Automation: Addressing Operational Problems

also inside

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 Assistant Secretary of Defense for Research & Engineering ASD(R&E).

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

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

IATAC Director:	Gene Tyler
Inquiry Services:	Yida Li

If you are interested in contacting an author directly, please e-mail us at *iatac@dtic.mil*.

***IAnewsletter* Staff**

Chief Editor	Gene Tyler
Assistant Editor	Kristin Evans
Art Director:	Tammy Black
Copy Editor:	Alexandra Sveum
Editorial Board:	Al Arnold
	Angela Orebaugh
	Dr. Ronald Ritchey
Designers:	Tammy Black
	Michelle Deprenger
	Lacey Olivares

***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 e-mail 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
E-mail:	*iatac@dtic.mil*
URL:	*http://iac.dtic.mil/iatac*

Deadlines for Future Issues

Spring 2012	Jan 27, 2012

Cover design:	Tammy Black
Newsletter design:	Donald Rowe

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

in every issue

IATAC Chat

Gene Tyler, IATAC Director

On 14 July 2011, the Honorable William J. Lynn, III, Deputy Secretary of Defense, gave a speech at National Defense University outlining the Department of Defense (DoD) Strategy for Operating in Cyberspace. In this speech, Mr. Lynn acknowledged that today, "bits and bytes can be as threatening as bullets and bombs," and then stressed the importance of military, government, international, private sector, and individual citizen participation in securing cyberspace. He stated, "Because cyberspace is composed of many interwoven networks that perform many different functions, ensuring its peaceful use will require efforts on many fronts. The men and women of the military, other government agencies, our allies, the private sector, and indeed, the citizens of cyberspace must all play a role." [1]

The importance of encouraging cooperation and collaboration across public and private organizations is a daunting task. This edition of the *IAnewsletter* showcases how key stakeholders and organizations have worked together to advance security automation through the development of the Security Content Automation Protocol (SCAP). In short, this edition highlights how one of the core principles Mr. Lynn outlines has been put into action.

This edition provides high-level perspectives from individuals within the Department of Homeland Security, Department of Commerce's National Institute of Standards and Technology (NIST), U.S. Cyber Command, and the National Security Agency, and focuses on security automation as an imperative to furthering solutions to cyberspace's operational problems. Bruce McConnell, Director for Cyber Strategy at the Department of Homeland Security, provides an overview in his article of how developing security standards enable "dissimilar devices to collectively perform agreed upon security functions" that advance DHS's aims in cybersecurity. John Banghart explains SCAP and its capabilities from a NIST and technology perspective, and David O'Berry details an example of how SCAP advanced the security of South Carolina prison networks through true collaborative efforts.

Besides this variety of government perspectives, this edition also features articles by several key players in the commercial sector and in academia. Companies that have played an integral role in security automation discuss how SCAP has impacted their commercial innovations. This edition features articles from Juniper, Triumfant, and Harris Corporation. Dr. Ehab Al-Shaer of the University of North Carolina Charlotte, and Dr. Soumyo Moitra of Carnegie Mellon University, also discuss their research and innovations in this area.

The 13/1 edition of the *IAnewsletter* first introduced our readers to security automation and the importance of collaboration in developing standards that allow network defenders to focus on managing information instead of information technologies. [2] Almost two years later, this edition showcases tangible evidence of how security automation and true collaboration across the government, industry, and academia has resulted in powerful information assurance advancements. More importantly, this collection of articles demonstrates that when everyone plays an active role, enhanced network defense while operating in cyberspace is achievable.

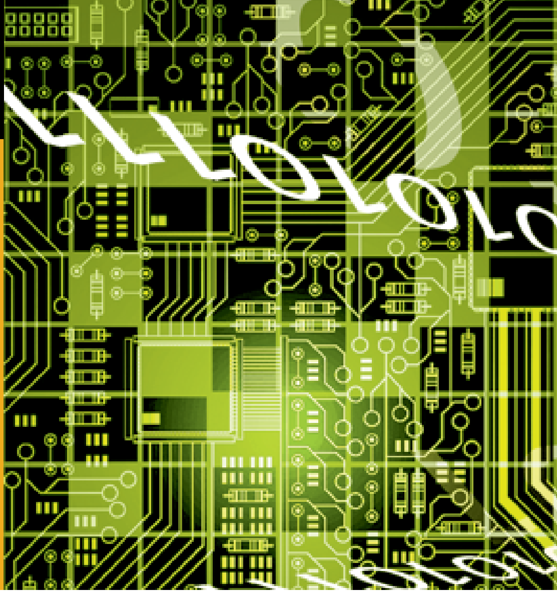
I always encourage our readers to submit articles sharing their perspectives. What other IA advancements have resulted from collaboration in which you, our readers, play a part? We're interested in learning about other examples! Please feel free to contact us with your ideas at *iatac@dtic.mil*. I look forward to continuing this dialogue with the IA community.

Gene Tyler

References

1. *http://www.defense.gov/speeches/speech.aspx?speechid=1593*
2. Sager, Tony. "Security Automation Introduction." *IAnewsletter,* vol. 13, no. 1, winter 2010, p. 4.

A special thanks to Tony Sager and Betsy Hudson for their vision and support for this edition of the *IAnewsletter*. We truly appreciate it!



An Introduction to Security Automation

by MG David B. Lacquement, Tony Sager, and Paul Bartock

United States Cyber Command (USCYBERCOMMAND) is little over a year old, and I believe that we have made major strides in defending, securing and improving the operations of Department of Defense (DoD) networks. We have accomplished a great deal in a relatively short time with help from our key mission partners like the National Security Agency and Defense Information Systems Agency. This has been a challenge, given that DoD's networks are complex and constantly changing, with multiple network "owners" and "operators" and often no one actively securing and defending components of the network. We have very little visibility and situational awareness of the states of our networks or activity on the networks. Our adversaries have taken advantage of the current limitations to see and defend our networks and have been able to maneuver too freely inside our networks.

Cyberspace is a Warfighting domain and just like the other Warfighting domains the mission is about reconnaissance, maneuvers, and fires. Cyberspace is different from the other domains primarily due to the global nature of the networks, the network speed of cyber activity, the sheer volume of cyber events and rapid development, and planning and decision cycle of our adversaries. We must dramatically tighten up our own decision-action cycle. This implies much more standardization and automation; we must counter and mitigate as much of the adversary activity of vulnerabilities within our networks automatically whenever possible. Automation will free up the finite defender forces to focus on the critical threats to our key cyber terrain.

This is also impacted by the reality that we are and will be operating in a constrained fiscal environment that will force us to be incredibly efficient and maximize the use of scalable, enterprise-level technology.

All of this will require advances in technology, standards, tactics, procedures, processes, *etc*. But, at the end of the day, this is all about solving large-scale, complex operational problems. The problems that we need to solve for DoD should drive the priorities.

Here are a few examples from my "operational wish list" for USCYBERCOMMAND. We must be able to—

- Know that systems are configured as securely as possible, focused on systems associated with key cyber terrain, and when this is not so;
- Rapidly assess the technical risk of a newly found vulnerability in technology (*e.g.*, how many systems of this type are out there, which of them are configured in an exploitable way) so that technical risk can be weighed with other factors in determining operational risk;
- Rapidly query the environment to find system artifacts evidence of potential adversary actions;
- Apply the findings from our own operations and testing (*e.g.*, Red Teams) to find and mitigate similarly vulnerable systems;
- Rapidly share information across the entire enterprise in machine-readable, standard forms;
- Quickly formulate and implement policy across the enterprise, and know when systems go out of compliance; and
- Effectively measure the value of countermeasures as we put them in place (*e.g.*, the Unified Gold Master image for the DOD). ■

About the Author

MG David B. Lacquement, USA, | is the Director Operations, J-3, for United States Cyber Command in Fort Meade, MD. As the Director of Operations, he is responsible for planning, executing, coordinating, and managing forces for DoD computer network attack and computer network defense as directed by USSTRATCOM. MG Lacquement holds a B.A. in History from Western Maryland College, and M.S. degrees in Strategic Intelligence from the Joint Military Intelligence Training College, Military Art and Science from the United States Army Command and Staff College, and National Security Strategy Studies from the National Defense University. He can be contacted at *iatac@dtic.mil.*

The Winter 2010 edition of the *IAnewsletter* focused on security automation—the compelling need, the applicable standards, and the key Department of Defense programs—and also offered some hints of the roadmap ahead. The basic premise was that cyber defenses are being overwhelmed by mostly mundane, well-understood problems; therefore, we need a much greater focus on standardization and automation to allow humans to get out of the loop of manual defense and focus instead on human-worthy activities. The Winter 2010 edition laid out the basic groundwork of standards, processes, and issues that partners across government and industry have been working for several years.

In this edition of the *IAnewsletter*, we follow up with use cases—the operational problems that we need to solve. Standards are essential, and compatible tools are great, but in the final analysis, this is about solving problems. In addition, we will offer insight from a wide variety of stakeholders, from national to tactical, and from government to industry. This is a problem that cuts across all of cyberspace, and our solutions must do the same. ■

Standards are essential, and compatible tools are great, but in the final analysis, this is about solving problems.

About the Author

Tony Sager | is the Chief Operating Officer for the Information Assurance Directorate (IAD) at the National Security Agency (NSA). IAD's vision is to be the decisive defensive advantage enabling America and its allies to outmaneuver network adversaries. During his 30+ year NSA career, Mr. Sager has held technical and managerial positions in Computer/Network Security and software analysis. He holds a B.A. in Mathematics from Western Maryland College and an M.S. in Computer Science from Johns Hopkins University. He can be contacted at *iatac@dtic.mil.*

Just Opened…the TNC & SCAP Demonstration Center (DC)

The NSA has been undertaking an effort to create an external unclassified DC to support the development, integration, and demonstration of security automation use cases involving TNC and SCAP. The DC, located in Hanover, MD, allows rapid prototyping and the demonstration of enhanced security automation techniques and efficiencies that will lay the foundation for advancements in risk scoring, proactive network defenses, compliance enforcement, and network health situational awareness.

The development of security automation standards is truly a grass-roots partnership between government and industry. As such, the DC provides a space within which commercial vendors can be actively and easily engaged. Within the DC, vendors are able to quickly set up their equipment and interface it to existing demonstration lab networks and other required hardware.

We are currently pursuing the following seven use cases for integrating Security Content Automation Protocol (SCAP) with Trusted Network Connect (TNC) in the TNC & SCAP Demonstration Center (DC)—

1. **Continue the Comply to Connect network visibility effort with additional features**—We are performing an SCAP-based assessment using TNC protocols, enabling a requirement for SCAP compliance to gain network access or to ensure that the administrator knows the compliance state of all the devices on the network. Several vendors have implemented this use case using the IF-IMC and IF-IMV APIs to connect SCAP client and server software to a TNC system.
2. **External scan/request for investigation**—The Policy Decision Point notifies network security devices (*eg.*, external SCAP scanners) when a new device enters the network, enabling the scanner to quickly find and scan new devices. This is achieved through features in IF-MAP 2.0 and IF-MAP Metadata for Network Security 1.0.
3. **Network sensing and response**—Security sensors detect suspicious activity (*e.g.*, traffic sent to a known bad Internet Protocol [IP] address) and publish this information to IF-MAP, which triggers further investigations, such as checking domain name system (DNS) caches on endpoint devices (*e.g.*, workstation, server, printer, *etc.*) to see if they have that IP address in their DNS cache. Vendors can implement this use case through IF-MAP 2.0.
4. **Trends**—Administrators get visibility into warning by viewing activity on a console. IF-MAP 2.0 enables this use case, but a vendor has not yet implemented it. We plan to reach out to commercial vendors (*e.g.*, SourceFire, RedSeal, and other networking monitor vendors) to prototype this within their commercial products. Some vendors are already interested in doing the prototyping of this use case.
5. **Rescan for New Policy**—When SCAP policies change, endpoints should be rescanned and their network access modified accordingly. Non-compliant endpoints might be quarantined until remediation can be completed. A good use case is INFOCON/CYBERCON changes.
6. **Information sharing across administrators**—The IF-MAP provides a single shared database that allows administrators to have a common view of what is happening on their networks. Tricky and interesting issues arise when sharing information across trust boundaries (*i.e.*, from one organization to another). Information may be summarized.
7. **Dashboard**— Commanders and Executives often want a global view of security issues. Which areas of the world are seeing the most attacks or the most compliance or non-compliance? They also want to drill down to get more information. IF-MAP collects and exchanges this sort of data among security systems in a standard way. Executives generally view issues from a risk perspective (*i.e.*, infections on a critical system are more important than those on a less critical one), which actually builds upon the above activities as they are completed. ■

Commanders and executives often want a global view of security issues. Which areas of the world are seeing the most attacks or the most compliance or non-compliance?

About the Author

Paul Bartock | is the Technical Leader for Mitigations in the Information Assurance Directorate at the National Security Agency (NSA). He is responsible for working with Department of Defense (DoD), federal government, and private industry stakeholders to promote the use of security standards and best practices to protect DoD and federal computer networks. He partners with the leading operating system vendors to encourage participation in government standards activities. For 12 years, he provided technical guidance on the government consensus work groups to influence the development of security baseline configurations, which led to the Office of Management and Budget-mandated Federal Desktop Core Configuration. Drawing on his extensive knowledge of networks, he developed and published countermeasure guidance to mitigate vulnerabilities in DoD and government networks. Mr. Bartock is a graduate of the University of Maryland and is a Certified Information Systems Security Professional and a Network Certified Engineer. In 2008, he received the Exceptional Civilian Service Award and Federal 100 Award for his work developing the federal security baselines. In 2009, he was elevated to the Senior Executive Service. He can be contacted at *iatac@dtic.mil.*

University of North Carolina at Charlotte

by Angela Orebaugh

Founded in 1946, the University of North Carolina at Charlotte (UNCC) is a research intensive university in Charlotte, NC. UNCC offers 92 Bachelor's, 59 Master's, and 19 Doctoral degree programs to over 25,000 students. [1]

The College of Computing and Informatics, one of seven colleges at UNCC, includes the Computer Science, Software and Information Systems, and Bioinformatics and Genomics departments. The Software and Information Systems Department is responsible for information technology (IT) research and education, emphasizing designing and deploying IT infrastructures that deliver integrated, secure, reliable, and easy-to-use services. The National Security Agency recognizes the department's Information Security and Privacy program as a National Center of Academic Excellence in Information Assurance Education. Students earn a certificate from the Information Security and Privacy program that requires 12 hours of course work in one of the following topics—

- Information Security and Privacy
- Vulnerability Assessment and System Assurance
- Computer Forensics
- Access Control and Security Architecture
- Information Infrastructure Protection
- Applied Cryptography
- Information Technology: Ethics, Policy, and Security
- Network-based Application Development
- Computer Communication Networks
- Network Security
- IT Internship Project
- Software Testing and Quality Assurance
- Software Assurance. [2]

Through the Federal Cyber Corps Scholarship for Service, UNCC also offers the Carolina Cyber Defender Scholarship Program, which provides up to 2 years tuition, fees, books, and salary for students seeking a degree in information assurance. The scholarship is in exchange for a match of 1-to-1 years of employment in an information assurance position at a government agency or laboratory after graduation. [3] Since 2001, the Carolina Cyber Defender Scholarship Program has provided approximately 100 full scholarships.

The Software and Information Systems Department also houses the Cyber Defense and Network Assurability (CyberDNA) Center. "The CyberDNA offers a unique environment to facilitate joint research and development programs (consortia, seminars, and workshops) with the industry, financial institutions, utility service providers, and government agencies. The main objective of CyberDNA is to enable assurable and usable security and privacy for a smart, open society by making cyber defense provable, enforceable, measurable, and automated. CyberDNA has a unique vision and approach among other national centers including promoting automated analytics and synthesis of designing, configuration, and evaluation of mission-oriented security systems; offering leap-ahead research by integrating multidisciplinary research from security, networking, reliability, risk management, economical, behavioral, and physical world communities; and developing deployable tools to facilitate technology transfer and workforce education and preparation." CyberDNA is led by Dr. Ehab Al-Shaer and includes faculty from different colleges and external collaborators who cover a wide range of security expertise. [4] ■

References

1. *http://publicrelations.uncc.edu/information-media-kit*
2. *http://sis.uncc.edu/?q=content/certificate-information-security-and-privacy*
3. *http://cci.uncc.edu/?q=news/carolinas-cyber-defender-scholarship-0*
4. *http://www.arc.uncc.edu/*

Enabling Distributed Security in Cyberspace

by Bruce McConnell

The Department of Homeland Security (DHS) has the lead for the federal government to secure federal civilian executive branch computer systems, to work with industry to defend privately-owned and -operated critical infrastructure, and to work with state, local, tribal, and territorial governments to secure their information systems. In March 2011, DHS published a white paper that explores the idea of a future cyber ecosystem in which cyber devices collaborate in near-real time in their own defense. [1] The cyber ecosystem is global and includes U.S. government and private sector information infrastructure; the full variety of interacting persons, processes, information, and communications technologies; and the conditions that influence their cybersecurity. In this future, devices are able to anticipate and prevent attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state.

To realize this future, security capabilities must be built into cyber devices in a way that allows preventive and defensive courses of action to be coordinated among communities of devices. Near-real time coordination would be enabled by combining the innate capabilities of individual devices with trusted information exchanges and shared, configurable policies.

The white paper suggests three interdependent building blocks are needed for distributed security—

- **Authentication—**Enable a network to know if it can trust a request to connect;
- **Automation—**Enable immediate response to intrusions and anomalies; and
- **Interoperability**—Enable standards-based devices to share information.

Properly combining these three building blocks would permit automated collective action in response to malicious activity, including financial fraud, identity theft, and advanced persistent threats that exploit access to intellectual property and sensitive information.

Identified by the Quadrennial Homeland Security Review last year, safeguarding and securing cyberspace is one of DHS's five core security missions. [2] The white paper lays out part of DHS's vision for carrying out this mission, which we believe requires the creation of a fundamentally safer and more secure cyber environment. To do this, we must change the way people and devices work together.

The Current Cyber Ecosystem

Security capabilities are naturally distributed in cyberspace, and substantial expertise resides in the private sector and at all levels of government.

In general, these security capabilities operate independently. Security products, such as vulnerability scanners, intrusion detection systems, and anti-virus software, do not exchange data and have inconsistent security policies. Competing manufacturers develop this technology and have little incentive to share information or enable a coordinated response. The result is an environment where security products protect a single community, a single user, or even a single aspect of a single user's experience. Mutual defense is almost by accident.

A Future Cyber Ecosystem

To create a safe, secure, and resilient cyberspace, we must leverage the expertise that exists across the enterprise and use the distributed nature of cyberspace in its own protection. There is no prospect that an external boundary defense can do the job. Instead, standards-based products and services can be used to strengthen local and individual capabilities and unite those capabilities in collective actions to realize shared security interests.

There are potentially many benefits to automated collective action. If cyber devices communicated in near-real time with each other about incidents and

took coordinated protective measures consistent with defined policies, even zero day attacks could be contained. Decision making would be optimized, and automated defenses could be effective at the earliest, least costly stages of an incident.

Automated courses of action (ACOA) are methods chosen to bring about a technical solution to a threat. Potential ACOAs include—

- Taking infected devices offline;
- Changing the configuration of healthy devices to harden them against intrusion;
- Blocking incoming malware;
- Filtering or re-routing traffic;
- Cordoning off portions of the network or of applications; and
- Changing access levels.

Immediately upon detection of an incident, a digital policy (*i.e.,* machine instruction) could deploy to alert others and begin sharing information in a format that could be authenticated and automatically fed into cyber devices in other communities.

Transition

The transition to a healthy cyber ecosystem will be gradual. It will be facilitated by the following activities:

Development of International Standards

Interoperability and authentication standards are critical for dissimilar devices to collectively perform agreed-upon security functions. Government and private sector stakeholders must work with industry and standards bodies to mature existing standards and create new ones.

Many security- and configuration-related data specifications already exist. These include, for example, the Open Vulnerability and Assessment Language, the Common Vulnerabilities and Exposures identifiers, and the Security Content Automation Protocol. [3] These data specifications provide an excellent foundation for the development of future international standards.

Authentication of Individuals, Devices, and Processes

A healthy cyber ecosystem must be able to appropriately authenticate user identities, devices, and processes. Authentication must be secure, affordable, easy to use, scalable, and interoperable.

Production of Trustworthy Hardware and Software

Industry must produce hardware and software that provides increasing levels of safety, security, resiliency, reliability, privacy, and usability. Each product must be able to sense, react to, and communicate changes in its security or its surroundings in a way that preserves or enhances the security posture of the ecosystem. In addition, the software must have strong feed forward and feedback signaling mechanisms.

Resolution of Policy and Governance Issues

Government must work with the private sector to collectively develop a framework for identifying and resolving political and legal issues related to automated collective defense.

Key policy questions include the following—

- What distributed behaviors would be effective and thus should be automated?
- What decisions should be delegated to machines?
- What elements of trust would be required?
- Who is accountable when unintended consequences occur?

DHS envisions a healthy cyber ecosystem having five maturity levels characterized by increasing levels of information sharing, interaction, and decision rights. The white paper outlines these maturity levels, and participation at each level is voluntary. The existence of multiple maturity levels takes into account the diversity of participants in the ecosystem and enables better risk-based security decisions across systems and organizations.

Government Role

DHS intends to lead the evolution of the healthy cyber environment and is working with its partners in the public and private sector to complete the tasks detailed below.

Develop Requirements and Use Cases

The white paper describes 25 functions that security content automation and exchange could transform. The white paper organizes the functions into two phases: Pre-incident Detection and Post-incident Detection. The Pre-incident Detection phase includes asset inventory, configuration guidance analysis, vulnerability analysis, and threat analysis. The Post-incident Detection phase includes intrusion detection and incident management and is currently less standards-based than the Pre-incident Detection phase.

Identify Early Adopters

An early example of security automation is continuous monitoring. System managers use a variety of software products to automatically detect and report known security vulnerabilities in network nodes. In some cases, system managers further configure their systems to automatically remediate detected (*i.e.,* known) security deficiencies. DHS is working with its partners to highlight other early adopters.

Conduct Pilots and Demonstrations

In Fiscal Year 2012, DHS will undertake several pilots related to automation and interoperability, including the following—

- Continuous monitoring within the ".gov" space
- Threat information sharing
- Software assurance.

Pilots can be an effective methodology to demonstrate how devices work together, determine whether there are improvements in security, identify gaps and challenges, and help recommend ways to mitigate weaknesses. Pilots can also help identify in a systematic way whether or not standards are mature enough and properly implemented in various devices.

DHS welcomes the collaboration of other government and private sector stakeholders in implementing pilots and demonstrations.

Move the Public Discussion Forward

DHS has begun meeting with stakeholders to discuss leveraging security automation, authentication, and interoperability to build a healthy and resilient cyber ecosystem. This dialogue is helping to improve ecosystem concepts, identify opportunities to pilot near-term capabilities, and help identify gaps in technologies, standards, and policies.

To broaden our audience, DHS plans to establish a cyber ecosystem wiki to encourage comments on the *Enabling Distributed Security in Cyberspace white paper.*

In addition, DHS intends to publish three follow-on white papers. The first white paper will summarize feedback submitted on the ecosystem concept and provide a coordinated action plan. The second white paper will provide a more detailed vision and operational construct for authentication of devices. The third white paper will report early results of pilots and governance activities against the action plan.

Finally, DHS is nearing publication of its *Cybersecurity Strategy for the Homeland Security Enterprise*. The strategy is designed to protect the critical systems and assets that are vital to the U.S., and, over time, to foster stronger, more resilient information and communication technologies to enable government, business, and individuals to be safer online. DHS will publish the strategy in 2011 and will describe the capabilities needed to ensure the phased implementation of a healthy cyber ecosystem.

DHS invites you to be an active participant in refining requirements and use cases, identifying early adopters, and participating in pilots and demonstrations. We welcome your feedback and comments to the e-mail address *CyberFeedback@dhs.gov*. ■

About the Author

Bruce W. McConnell | has served as the Senior Counselor and Director for Cyber+Strategy at the National Protection and Programs Directorate of DHS since June 2009. Prior to DHS, Mr. McConnell served on the Obama-Biden Presidential Transition Team, working on a variety of open government and technology issues. From 2000 to 2008, he created, built, and sold McConnell International and Government Futures, which were boutique consultancies that provided strategic and tactical advice in technology, business, and government markets. From 1999 to 2000, Mr. McConnell was the Director of the International Y2K Cooperation Center, where he coordinated regional and global critical information technology infrastructure organizations to promote information sharing and joint action. From 1993 to 1999, Mr. McConnell was Chief of Information Policy and Technology in the U.S. Office of Management and Budget. He holds an M.P.A. from the University of Washington and a B.S. from Stanford University. He can be contacted at *iatac@dtic.mil.*

References

1. DHS. "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action." 2011. *http://blog.dhs.gov/2011/03/enabling-distributed-security-in.html.*
2. *http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf*
3. NIST SP 800-126, The Technical Specification for the Security Content Automation Protocol. *http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf.*

Security Automation: Commercial Sector Perspectives and Contributions

by Steve Hanna and Jim Ivers

Editors Note: to highlight commercial sector innovation in security automation, NSA invited all of the companies who have participated with them in SCAP efforts to present their perspectives in the *IAnewsletter*. The following articles present perspectives from two companies.

Juniper is committed to furthering the development of standards for Security Automation within standards bodies such as the Trusted Computing Group (TCG), Internet Engineering Task Force (IETF), and others.

Juniper Networks (Juniper) has been a long-time supporter of Security Automation using open standards. Industry employees co-chair several key standards groups especially regarding the Trusted Network Connect (TNC) standards for network security automation. Juniper worked to create the TNC standards and architecture back in 2005; we were the first company to ship products that implement the TNC standards and to have our products certified as implementing the TNC standards. Juniper worked with partners to support new capabilities such as the TNC and Security Content Automation Protocol integration.

As described elsewhere in this *IAnewsletter* edition, the greatest potential for Security Automation is still ahead. Many new use cases have been laid out. The key to making them work, however, is to ensure that all security systems are working together using open standards, permitting customers to deploy the ideal tool for each problem (or the tool that they have at hand) without requiring expensive, manual integration.

Juniper is committed to furthering the development of standards for Security Automation within standards bodies such as the Trusted Computing Group (TCG), Internet Engineering Task Force (IETF), and others. We are also committed to implementing these standards across our product lines, recruiting other vendors to implement them, and working with customers to ensure their use cases are addressed in the standards. Through open standards, Security Automation is strategic to Juniper and we look forward to many more years of exciting progress in this area. ■

Disclaimer: The IAnewsletter is a vendor-neutral publication. The publication of this article does not imply a recommendation or endorsement by IATAC or DTIC for the commercial products or services identified.

About the Author

Steve Hanna | is a distinguished engineer at Juniper. As co-chair of the TNC Work Group in the TCG and the Network Endpoint Assessment Working Group in the IETF, Steve has a deep and broad understanding of Network Access Control technology. He is the author of many papers, an inventor/co-inventor on 34 issued patents, and a regular speaker at industry events. He can be contacted at *amylee@juniper.net.*

Continuous monitoring is the ongoing process of assessing information security, vulnerabilities, and threats to maintain a dynamic understanding of organizational risk. Knowing the efficacy of your security controls provides insight into the security readiness of the organization, empowering effective and informed risk decisions in the face of today's highly volatile and advanced threats. Data is the foundational element of any continuous monitoring initiative, just as the lack of data is a limiting factor to effectiveness. The volume of threats and the velocity at which they evolve dictate that scanning must be constant, complete, and free of the assumptions that result from reliance on prior knowledge. Past attempts at continuous monitoring efforts often relied on piecing together data from multiple, task-specific scans that executed at various intervals (weekly, monthly).

Triumfant essentially automates the collection of the base data needed for continuous monitoring with one efficient, continuous, and comprehensive scan. Triumfant's approach of using change detection and patented analytics to detect anomalous activity on host machines necessitates an "assume nothing, scan everything" approach. The technical translation is that Triumfant continuously scans all of the persistent attributes of each machine—files (hash), registry keys, ports, process, services, and more—with over 200,000 attributes per machine. A fortunate by-product of this scanning is a comprehensive data repository of state data at a very granular level. Triumfant collects the data on the server using a fully automated, change-data-capture process between the host machine and the server, keeping the state data current with minimal impact on the host machine and the network. Triumfant is fully Security Content Automation Protocol (SCAP) enabled, allowing the repository to contain SCAP attributes such as Common Configuration Enumeration, Common Platform Enumeration, and Common Vulnerabilities and Exposures data. With all the state data available in one repository, organizations can provide actionable insight into the security readiness of the organization: patch inventories, application inventories, vulnerability data, configuration data, performance data, and insight into the integrity of applications and the operating system. Most important is that this information is available through one automated scanning process.

> The volume of threats and the velocity at which they evolve dictate that scanning must be constant, complete, and free of the assumptions that result from reliance on prior knowledge.

Why is this important? Consider the announcement of a new vulnerability. In the past, an organization would learn about a new vulnerability, prepare their agentless scanning tool, scan the machine population, and consolidate the results. More than one organization has reported that this process takes days or even weeks, creating considerable lag before the organization can accurately assess the risk. Contrast the same scenario with a continuous monitoring process that maintains a current and comprehensive repository of detailed state data. An organization equipped with such a repository can produce a near-real-time picture of the potential threat for most new vulnerabilities with a relatively simple query. Within minutes, the organization has accurate data to assess risk and can then take the steps necessary to mitigate that risk and maintain the highest possible level of security readiness. The breadth and depth of readily available information that results from Triumfant's comprehensive and continuous scanning enables organizations to enjoy the full benefits of continuous monitoring. ■

Disclaimer: The IAnewsletter is a vendor-neutral publication. The publication of this article does not imply a recommendation or endorsement by IATAC or DTIC for the commercial products or services identified.

About the Author

Jim Ivers | is the Chief Security Strategist for Triumfant, where he is responsible for product management and marketing of the Triumfant solution. Mr. Ivers was previously on the executive team of Cybertrust, a worldwide security services company sold to Verizon Business. Mr. Ivers also held roles with Vovici, webMethods, and Information Builders. He has a background in business intelligence and data warehousing. Mr. Ivers holds a B.S. in Computer Science from the University of Central Florida. He can be contacted at *iatac@dtic.mil.*

SCAPVal: Validating Specification Conformance

by Adam Halbardier and Angela Orebaugh

The Security Content Automation Protocol (SCAP) is an umbrella specification developed by the National Institute of Standards and Technology (NIST) along with partners across the federal government. Special Publication 800-126 (SP 800-126): *The Technical Specification for the Security Content Automation Protocol* provides guidance on how to create security automation content by leveraging a variety of other specifications that fall within its domain. [1] Security automation content details how to scan a target host and what to scan it for and specifies detailed rules and checks in a standardized manner that is widely understood. The rules detail policy such as the configuration settings to discover or the vulnerabilities to identify as well as expected values and potentially a weight for each discovery. The checks detail how to discover the specific information necessary to evaluate the policy.

SCAP leverages numerous specifications to accomplish its goal. The Extensible Checklist Configuration Description Format (XCCDF) describes how to represent a checklist of rules describing what an SCAP-compliant tool checks along with how to score the discovered information. [2] The Open Vulnerability Assessment Language (OVAL) describes how to check a host for a desired item in an automated fashion [3], while the Open Checklist Interactive Language (OCIL) describes how to represent a questionnaire that can be presented to a human to answer questions about a host. [4] XCCDF leverages both OVAL and OCIL to gather results and make an assessment related to a particular policy. SCAP defines the expected relationships between XCCDF, OVAL, OCIL, and other specifications that define boundary object formats such as the Common Configuration Enumeration (CCE) [5], Common Vulnerability Enumeration (CVE) [6], and Common Platform Enumeration (CPE). [7] Each of these boundary object specifications describe in a standardized and enumerated manner what specific XCCDF rules and associate OVAL and OCIL checks are describing. SCAP is effectively the specification that ties numerous existing specifications into a cohesive package that wholly solves real-world problems; it is a standard mechanism to do configuration, vulnerability, and inventory scanning of a target host.

With the introduction of the SCAP specification into the security automation domain, there was a need to express common policy in an SCAP-compliant format. The Federal Desktop Core Configuration [8] and the United States Government Configuration Baseline [9] were subsequently developed to represent the U.S. government-wide policy for workstation configuration settings. They are expressed as SCAP bundles for a variety of platforms and products. Each bundle is a ZIP file containing, at minimum, an XCCDF checklist file, an OVAL definitions file, and a CPE dictionary file. Those files, together, represent an SCAP bundle, and the SCAP specification mandates certain relationships between the content in those files. In addition, other agencies and/or vendors may take this content and modify or adapt it for their specific needs as well as create brand new SCAP content. This need to distribute the content creation process led NIST to develop an SCAP Content Validation Tool (SCAPVal) to help content creators confirm that their SCAP content is well-structured and compliant with the SP 800-126.

SCAPVal is a command-line Java application that is freely available from NIST's SCAP Website. [10] It allows content developers to provide it as an SCAP bundle. The tool inspects the bundle and performs a series of validation checks against it. First, SCAPVal downloads the latest CPE and CCE feeds from the National Vulnerability Database (NVD) and then performs extensible markup language (XML) schema validation against all of the components in the bundle. SCAPVal then uses an XML validation language, Schematron, to validate all of the individual XML components that have a corresponding Schematron rule set. [11]

▷▷ *continued on page 32*

Security Automation Research: Challenges and Future Directions

by Dr. Ehab Al-Shaer

Configuration complexity imposes a heavy burden on both regular users and experienced administrators. This complexity dramatically reduces overall network assurability. For example, a report from the Center for Strategic and International Studies states that "inappropriate or incorrect security configurations were responsible for 80 percent of United States Air Force vulnerabilities." [1] Juniper Networks report that "human error is blamed for 50 to 80 percent of network outages." [2] It has been widely reported that the cost of system management has been growing exponentially over the years due to increasing complexity of system management including security configuration. [3] It also states that "more than 40 percent of the total IT budget of a $1 billion-plus company going to human labor and IT operations accounting for 80 percent to 90 percent of the budget." [4]

Attribution of Security Configuration Complexity

The increasing complexity of security configuration management can be attributed to the following main challenges—

- **Large-scale yet Heterogeneous**—A typical enterprise network contains thousands of servers and security appliances including firewalls, Internet Protocol Security (IPSec) gateways, intrusion detection systems (IDSs), where each device contains hundreds or thousands of configuration parameters such as rules or variables. For example, a typical enterprise firewall might contain more than 10,000 rules. Additionally, in multi-vender environments, the same configuration parameters might be syntactically different across devices from different vendors. [5]
- **Distributed yet Inter-dependent**—Valid system behavior depends on not only the correctness of individual device configuration but also the global configuration interaction of different devices across the network. There are usually functional and logical dependencies between various devices in the system. For example, traffic should be decrypted (by IPSec) before being inspected by an IDS. Similarly, a flow that is blocked by a firewall should not be allowed by another firewall on a different path (backdoor); therefore, network devices must be configured consistently and uniformly to implement cohesive security policies.
- **Semantic Gap**—Considering this complexity, it is usually not obvious to translate high-level requirements into low-level configurations correctly. Likewise, there is a significant gap between the values of the low-level configuration parameters, like rules and actions, and what they globally mean in the network.
- **Dynamic**—As systems' context, including technologies, vulnerabilities, regulatory requirements, and business relations, evolve over time, configuration must constantly change to accommodate new services and capabilities while considering threat/risk related consequences. The emergence of pervasive and mobile services is another example of such complexity, which requires adaptive configuration based on context changes.
- **Multiple stakeholders**—Large enterprise networks are usually managed by multiple administrators with different mandates, requirements, and skills. The lack of systematic coordination and resolution of actions from different administrators increases the potential of configuration errors.

Unfortunately, this complexity is likely to grow tremendously as the technology evolves toward "smart," "hybrid," and "open" cyber infrastructures such as cyber-physical systems (*e.g.*, tele-health, smart grid,

etc.), cloud computing, and virtual and OpenFlow networking. Future Internet services will be highly configurable to provide agility and flexibility. Due to complex interactions between system configurations parameters, the diagnosability of security violations and failures becomes extremely difficult. We do not have automated decision-making capabilities to detect and respond to cyber attacks in real-time. Additionally, many new game-changing ideas for cyber defense, such as the moving target defense [6], will require robust security automation support. These technical and operational challenges call for much greater use of efficient and cost-effective automation that can be built into commercial, off-the-shelf products based on open industry standards.

State of the Art Overview

Many research and development efforts have been made to address these challenges. Security Content Automation Protocol (SCAP) was proposed to represent a uniform information model for desktop configuration. It enables software flaws (Common Vulnerabilities and Exposures) and configuration settings (Common Configuration Enumeration [CCE]) to be uniquely identified for each individual software and hardware component. It also allows each configuration (CCE) for a particular platform (Common Platform Enumeration) to be tested (Open Vulnerability and Assessment Language) and validated using checklist policy (Extensible Configuration Checklist Description Format) for risk assessment-based certification and accreditation activities. [7] SCAP offers fundamental transformation for information technology (IT) security management by providing basic building blocks for unified security automation and analytics. Additionally, a number of formal configuration analytic tools have been developed using advanced formal methods such as ConfigChecker [8] and ConfigAssure [9] to provide global automated security analysis across network devices. ConfigChecker, for example, creates a model checker for thousands of devices with millions of rules and allows users to define and verify arbitrary logical and temporal security properties across all network devices, including firewall, NAT, routing, IPSec, wireless access point, and others. ConfigChecker supports verification and diagnosis of reachability, security, reliability, and risk-based policy requirements.

Future Directions

Despite this progress, there is a lot of heavy lifting ahead to bridge the gap between security, assurability, and usability. There are still plenty of technical challenges that require fundamental research to move from information collection to information integration, from desktop-centric to network-centric, and from template-based compliance checking to automated analytics for proactive cyber defense. Many of these ideas still need to be institutionalized in standards, commercial tools, business processes, and governance policies. By offering a uniform configuration representation and data collection, SCAP can play an instrumental role to enable transformations from desktop security automation to global security analytics. Figure 1 highlights a number of key challenges and research directions to accomplish this vision.

Architecture and Interfaces

Security Content Query Language (SCQL)

SCAP provides a basis for powerful integration and analytics of configuration information. One of the major incentives behind many Internet innovations (*e.g.,* Web, peer-to-peer communication, and social networking) is not only the accessibility of the information but also the availability of logical interfaces and analytical techniques (*e.g.,* semantic Web, declarative languages, data mining, and graph searching) that enable powerful and scalable search and intelligent reasoning. Creating logic-based interfaces for SCQL will enable developers and administrators to create

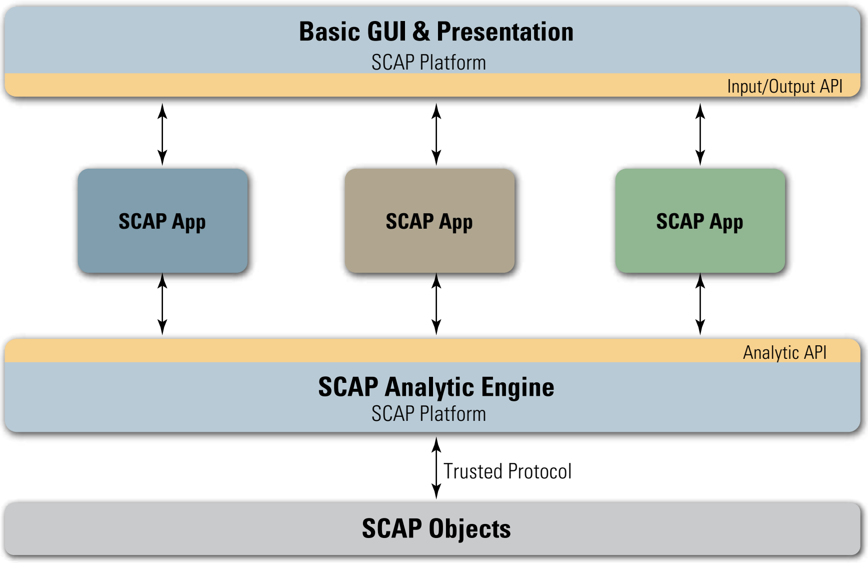


Figure 1 SCAP open platform

their own high-level arbitrary queries to investigate security properties across different devices. Users and vendors can use the SCQL constructs as a building block to develop powerful automated security tools for intelligent security content integration and analysis. SCQL should include intra- and inter-correlation constructs that can be used to define configuration inter-dependencies for arbitrary system invariants (always true) and security properties. For example, someone can define a security control to restrict reachability between hosts based on not only the vulnerability similarities but also accessibility exposure (who can communicate with this host).

Holistic Security Automation for Integrating Network and Desktop Analysis

A comprehensive security assessment requires integrating analyses of configurations of end-systems (*e.g.*, operating system [OS]), network devices (*e.g.*, firewall, IPSec, IDS, routing, mobility) and applications (*e.g.*, authentication, authorization, Web services filtering). Although SCAP components are mainly developed to support compliance checking of the Federal Desktop Core Configuration, this effort can be extended to include network and application security configuration-like access controls. This will allow for creating powerful formal models to define and analyze security controls across multiple devices and enable the creation of novel automated security analytics tools. This is not as simple as it sounds. Creating abstract representation of filtering device configurations will require modeling filtering syntax as well as semantic. Different vendors might use different packet matching control mechanisms. For example, while most firewalls use single-trigger sequential matching based on rule ordering, IPSec performs multi-trigger recursive security transformation to allow the same traffic to be transformed multiple times by the same IPSec gateway.

SCAP Open Platform

Leveraging the above capabilities, SCAP can extend its services to offer an open platform for running security automation tools (SCAP applications) from multiple vendors (refer to Figure 1). The SCAP platform provides analytical primitives commonly needed by most automation tools (SCAP applications) for querying, analyzing, and reporting. SCAP primitives provide the base capabilities for developing sophisticated security management solutions such as automated configuration verification, evaluation, diagnosis, mitigation, visualization, and what-if threat analysis. This will alleviate vendors from the burden of creating interfaces, languages, parsers, and compilers or implementing common analytics techniques, allowing them to focus their effort on providing vendor-specific security analytics capabilities. Additionally, the combination of various SCAP applications can provide additional capabilities by integrating the capabilities and outcome of various tools that use heterogeneous information from different sources (*e.g.*, network devices, risk/threat tools, threat data) within a single SCAP platform.

Novel Security Automation Capabilities

Closing the Security Automation Loop

Security automation is the process of collecting, integrating and analyzing various types of security contents (*e.g.*, configurations, alarms, audit logs, *etc.*) from different sources/locations (*e.g.*, OS, networks, and applications) to verify, diagnose, rectify, monitor, measure, and improve security controls. Security automation must support heterogeneous technology and configurations in a systematic and justifiable manner based on well-defined metrics and preferably through formal method proofs—this constitutes the "automation loop." Security automation tools should be capable of extracting and modeling system configurations (hosts, networks, and applications) and the system security requirements. It should also automatically verify if the system model satisfies the requirements. In case of security violations, automation tools must be able to diagnose the root cause of the violation and produce a remediation plan that identifies the minimum cost configuration changes to restore the security and operational integrity of the system. Recent advances of modern model checking, (*i.e.*, SAT and SMT tools) allow for analyzing networks of thousands of devices and millions of configuration parameters in seconds. [10] [11] Building efficient system abstraction is a key requirement for developing scalable models. [12] To close the loop, security automation tools should continuously monitor system configuration changes, such as addition of new services, new vulnerability postings, or policy modifications and automatically assess the IT security posture, such as defense-in-depth and access control rules accordingly with minimal human intervention.

Although bits and pieces of the overall framework have been developed, there is a pressing need today to close the loop from verification to rectification and from monitoring to remediation. Such close loop automation capabilities are critical to counter sophisticated attacks such as advance persistent threat and stealthy worms.

Automating Security Architecture Design

Most of the research and development activities in this area so far have focused on security configuration automation to address pressing challenges and needs; however, we also face similar fundamental challenges in designing security architectures. Security architectures define the cyber defense posture, which includes security zoning such as demilitarized zone, counter measures, defense perimeters, device placement in the network, defense-in-depth setup, and other issues. Although security architecture design usually follows well-known security principles and common practices such as least-privilege, isolation, defense-in-depth, fail safe, *etc.*, experts usually do the design in a manual or *ad hoc* manner. This has raised many issues about the validity and optimality of the security architecture particularly when the design process requires balancing between many competing factors such as risk, cost, and usability. One of the major challenges in this area is to automate the creation of an optimal security architecture that minimizes risk using security principles while satisfying other system constraints such as usability, performance, and cost. The design process is likely to be an interactive optimization process to give the user a chance to explore various architecture alternatives in the design space and zoom toward the required security architecture systematically using theoretically proven measures.

Configuration Nervous System (CNS)

Although security configuration parameters are highly inter-dependent (within a device and across devices), they are often modified locally without full knowledge of the system. This can easily lead to misconfiguration errors and security violations. CNSs create a virtual nervous network that connects inter-dependent configuration parameters and coordinates the global setting of configuration values (*e.g.*, actions) consistently according to the mission and requirements of the system. CNS also allows system changes to propagate as natural signals to many relevant components of the system for global coordination and automation of security and defense operations; therefore, changing part of the system configuration will automatically result in complete reconciliation with the rest of the system according to the security system requirements. CNS allows for an automated and error-proof change management process in large-scale dynamic networks. For example, blocking traffic to a destination in a single firewall will immediately lead to blocking the same traffic in all firewalls along different paths to the same destination. Another example of proactive cyber defense is the deactivation of access privileges of those users who are performing reckless (risky) configuration actions, such as installing unauthorized services, activating/switching wireless adapter/networks, *etc.*

Security Automation for Supporting Moving Target Defense

Moving target defense (MTD) enables a paradigm shift in proactive cyber defense by randomly and constantly changing the attack surface parameters, such as system configuration, to confuse, distort, or deceive adversaries. An example of an MTD system is Mutable Networks (or MUTE), which enables hosts to have mutable IP addresses and responses to counter network reconnaissance and fingerprinting attacks. [13] MTD, however, might be too expensive and disruptive without efficient security automation support that enables rapid and safe target motion; therefore, security automation tools, specially tailored for supporting MTD and dynamic proactive systems, are required for next-generation defense systems.

Automated Analytics of Smart Critical Infrastructures

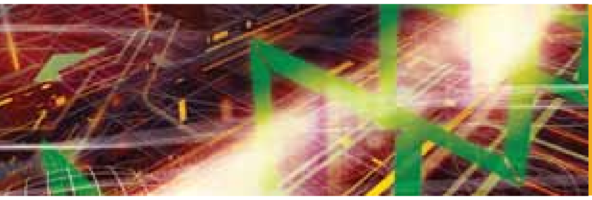
Our future smart critical infrastructures (*e.g.*, Smart Grid) comprise both cyber and physical systems. The integration of hybrid components in a single system greatly increases potential interdependencies of configuration parameters and inevitably introduces new types of threats and attacks against critical infrastructure. For example, misconfiguration of time-driven data delivery between nodes in Advanced Metering Infrastructure of the Smart Grid can flood the communication link, which creates denial of service attacks. Nevertheless, the future of our economy depends on deploying smart critical infrastructure. To mitigate the risk of massive attacks or failures of such systems, we must rely on rigorous formal analysis supplemented by effective visual analytics to understand and model the security and assurability invariants of the systems. Automated verification and continuous monitoring are core requirements for any automated security systems of smart critical infrastructure. ■

About the Author

Dr. Ehab Al-Shaer | is a Professor and the Director of the Cyber Defense and Network Assurability (CyberDNA) Center in the School of Computing and Informatics at University of North Carolina Charlotte. His primary research areas are network security, security management, fault diagnosis, and network assurability. Dr. Al-Shaer edited/co-edited more than 10 books and book chapters and published more than 100 referred journals and conferences papers in his area. Dr. Al-Shaer has been the General Chair and Technical Program Committee Chair of many premier conferences, and he has received many Institute of Electrical and Electronics Engineers and Association of Computing Machinery awards. Dr. Al-Shaer completed his Ph.D. in Computer Science at Old Dominion University, his M.Sc. in Computer Science at Northeastern University, and his B.S. in Computer Engineering at King Fahd U University of Petroleum and Minerals. He can be contacted at *ealshaer@uncc.edu.*

References

1. Center for Strategic and International Studies. Securing Cyberspace for the 44th Presidency. December 2008.
2. What's Behind Network Downtime? Proactive Steps to Reduce Human Error and Improve Availability of Networks, Juniper Networks White Paper, 2008, *http://www-05.ibm.com/uk/juniper/pdf/200249.pdf*
3. "Challenges to Economic Viability and Trustworthiness of Future Internet Applications," Policy and Security Configuration Management Group, PoSecCo European Consortium, 2011, *http://www.posecco.eu/index.php?id=359.*
4. Forrester Research, How To Manage Your Information Security Policy Framework. January 2006.
5. Ehab Al-Shaer and Hazem Hamed, Anomaly Discovery in Distributed Firewalls, IEEE INFOCOM'04, March 2004.
6. *http://www.nitrd.gov/NCOSearch.aspx*
7. *http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf*
8. E. Al-Shaer, W. Marrero, A. El-Atawy, and K. Elbadawi. Network Configuration in a Box: Towards end-to-end verification of network reachability and security. In Proceedings of IEEE International Conference in Network Protocols (ICNP), 2009.
9. S. Narain *et al.* Declarative Infrastructure Configuration Synthesis and Debugging. JNSM 2008
10. *Ibid.*
11. Z3: An Efficient SMT Solver, Leonardo de Moura and Nikolaj Bjørner, Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), Budapest, Hungary, 2008.
12. *Ibid.*
13. Ehab Al-Shaer, "Mutable Networks for Moving Target Defense," ARO Workshop for Moving Target Defense, October 2010.
14. NISTIR 7628: Guidelines for smart grid cyber security. Smart Grid Interoperability Panel- Cyber Security Working Group.
15. Yices: An SMT Solver. *http://yices.csl.sri.com/.*



Letter to the Editor

Q ***Let's say you are hardening a system. Are there any examples that you know of where a standard was implemented to quantify the integrity of a solution?***

A The Security Content Automation Protocol (SCAP) is actually designed to provide interoperability between tools to measure the integrity of a system's secure configuration over time. The SCAP framework enables tools to measure the combination of: 1) a system's compliance with a standard secure configuration, and 2) the known vulnerabilities detected in the system.

SCAP is intended to provide the basis for assessing and measuring a system's compliance and known vulnerabilities for both the initial deployment and periodic reassessments of the deployed system. It also provides the basis for continuous monitoring and assessment whereby each new assessment compares the then-current system configuration and detected vulnerabilities against the original security baseline. This highlights any changes or deviations, which could be considered indications that the *integrity* of the system's security posture has diminished—or, in very rare cases, increased—over time.

Although stakeholders are still working to fully define SCAP, there are a number of security and vulnerability assessment products that have completely implemented the protocol. Some of these products have completed a National Institute of Standards and Technology accredited validation process to become an official SCAP Validated product. SCAP is one concrete example of a set of specifications based on a standardized format that have been implemented to help quantify the integrity of a system or solution. ■

DoDTechipedia Happenings

by Sandy Schwalb

Have you visited DoDTechipedia lately? There are a few new enhancements and features that make sharing information and collaborating with your colleagues much easier. The mission of DoDTechipedia is to increase collaboration across the global Department of Defense (DoD) enterprise; the new enhancements to the wiki make it easier to input information and to find information relevant to the scientific and technical (S&T) community.

The DoDTechipedia team upgraded the rich text editor to include an auto complete function with drop-down menus for links, attachments, macros, and user macros. This feature saves time when moving content from one area of the wiki to the other by offering suggestions based on what you are typing. This is especially helpful if you are linking several pages on a similar topic that you routinely work on because a drop-down menu appears listing these pages.

With a similar look and feel of the auto complete function in the rich text editor, the new link browser makes it easy to link to recently viewed pages within the wiki, recently added attachments, and recently viewed Web pages. When you click the *Insert Link* icon, the *Insert Link* screen appears, displaying four links in the left pane: *Search, Recently Viewed, Attachments,* and *Web Link*. When you click any link, a search field appears; when you begin typing in that field, DoDTechipedia will suggest options for you. Select the text you want or enter the text you want to link, and then click the Insert button. This feature eliminates the need to write code.

In addition to enhanced functions, the DoDTechipedia team is making it easier to find and connect content through two sections on the home page: *DoD S&T Priorities* and *In the News*. Both sections highlight important information for the S&T community.

For example, in April 2011, a memorandum from Secretary of Defense Robert Gates outlined seven S&T investment areas for 2013 through 2017. The DoD S&T Priorities section provides links to information about these areas. You can find overview information for each priority with additional links to research the topic available in the Defense Technical Information Center's (DTIC's) collection of technical reports and research summaries. Information is also available for subcategories related to each priority. These pages are updated frequently to reflect advances in the field.

In the top-right box on the DoDTechipedia Home Page, you will find an *In the News* section. Each week, this section highlights two or three topics from the week's headlines. These links navigate directly to technical reports and research summaries in DTIC's collection and also provide additional links to information within the wiki. The topics change weekly, so visit often to see how S&T research is relevant today. If you are an expert on one of the topics, feel free to expand or update the page.

The recent enhancements and features in DoDTechipedia make finding the information you need to meet your mission a breeze. DoDTechipedia is open to all DoD and federal government employees and contractors. If you have a Common Access Card (CAC), simply visit *https://www.dodtechipedia.mil* and accept the terms and conditions to be automatically registered for DoDTechipedia and several other DTIC resources. If you do not have a CAC, visit *https://www.dtic.mil* and fill out a short Web-based form to complete your registration.

If you have any questions or need assistance while using the wiki, contact *dodtechipedia@dtic.mil*. ■

DoDTechipedia is a project of the Under Secretary of Defense for Acquisition, Technology and Logistics; Assistant Secretary of Defense, Research & Engineering; Defense Technical Information Center; and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer.

On Providing Risk Metrics Using Security Automation, Protocols, and Standards

by James Park and Dayna Harris

Facing an environment where threat actors present increasingly sophisticated and persistent attacks, the U.S. Department of Defense and federal government are working to better understand the threat scope and automate risk assessments to improve the security awareness and cyber defense of our information networks. [1] Efforts are underway to restructure how information systems are secured and accredited, make security controls more visible and manageable, and provide timely and accurate security situational awareness. [2] The federal government's Continuous Monitoring strategy is one such undertaking. [3]

The principle of continuous monitoring leverages the automation of network device security assessments to reduce the cost of security audits, improve visibility, and stimulate a more consistent and effective application of security controls. A key enabler in the implementation of continuous monitoring is the use of Security Content Automation Protocol (SCAP) standards. [4] SCAP makes risks associated with network devices more visible, collectable, and actionable.

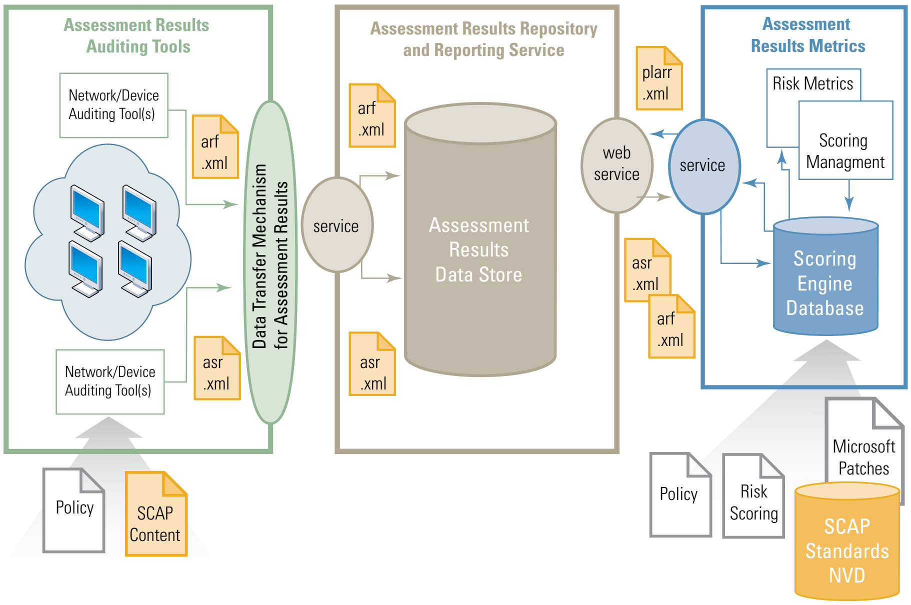

Assessment Results Auditing Tools
Network/Device Auditing Tool(s)
arf .xml
Network/Device Auditing Tool(s)
asr .xml
Data Transfer Mechanism for Assessment Results
Policy
SCAP Content
Assessment Results Repository and Reporting Service
service
arf .xml
Assessment Results Data Store
asr .xml
plarr .xml
web service
asr .xml
arf .xml
Assessment Results Metrics
service
Risk Metrics
Scoring Managment
Scoring Engine Database
Microsoft Patches
Policy
Risk Scoring
SCAP Standards NVD

Figure 1 Integrated Auditing and Risk Metrics System Diagram

Together, security automation and SCAP standards have the potential to transform information technology security policy into a capability at "every level within the enterprise to ensure implementation, enforcement, and compliance." [5]

In an applied research initiative to establish SCAP in a continuous monitoring application, the National Security Agency's (NSA's) Computer Network Defense Research and Technology (CND R&T) Team developed a reference implementation of a standards-based, extensible risk scoring engine as part of an integrated security auditing system. The system diagram shown in Figure 1 highlights (in orange) the areas in this initiative where SCAP was incorporated and leveraged. The objective of this article is to describe the findings and previously unknown, unanticipated, or unforeseen gaps in the process and technology necessary to support an enterprise-wide, standards-based, tool-agnostic information system risk awareness capability.

The initiative employed SCAP standards internally and between each component of the Integrated Auditing and Risk Metrics System: from using SCAP device assessment protocols (eXtensible Configuration Checklist Description Format [XCCDF] and Open Vulnerability Assessment Language [OVAL]), to employing SCAP enumeration (Common Vulnerabilities

Standardized data is more shareable, more collectable, and more easily correlated and combined. Standards by nature enable the community to invest and be invested in its purpose and success.

and Exposures [CVE], Common Configuration Enumeration [CCE], and Common Platform Enumeration [CPE]) [6] [7] [8] and data exchange standards (Assessment Results Format [ARF], Assessment Summary Results [ASR], and Policy Language for Assessment Results Reporting [PLARR]) [9] [10] [11], to storing results in SCAP assessment results relational repositories (Assessment Summary Consumer and Analysis Tool [ARCAT] and Automated Steel Cleanliness Analysis Tool).

Standards Aid Automation and Risk Awareness

Standards enable data to go unencumbered from large supporting structures freely into collection and assessing applications. Standardized data is more shareable, more collectable, and more easily correlated and combined. Standards by nature enable the community to invest and be invested in its purpose and success. But, also by nature, standards must be supported, employed, evolved, and maintained to be successful.

During its incorporation in this initiative, an unprecedented level of scrutiny was given to the employment of SCAP standards. From auditing devices to reporting device assessments to summarizing and correlating risk scores, weaknesses were exposed in SCAP's ability to support a risk-based situational awareness capability.

XCCDF/OVAL Content is Complex and Demanding

Employing SCAP content for the auditing component of this initiative emphasized that XCCDF and OVAL XML documents are very difficult to produce correctly. Content authoring requires advanced technical knowledge of the computing devices for which it is being written and a fundamental understanding of the standard and specification. Variances in format and the absence of validation, field testing, and lack of an authoritative source greatly impacted the initiative at each phase.

Producing the content necessary for risk metrics presented an ongoing challenge. Existing content had to be modified to provide sufficient data, new content had to be assembled from community-submitted checks, and new checks had to be written to accommodate patch metrics. Several iterations of testing and review reinforced the need for content validation and field testing and an authoritative source for reliable checks. The current shortage of standardization and overall guidance does not provide a credible foundation for asserting risk scores.

An authoritative repository for discrete OVAL checks, which have been vetted and tested, could provide an extremely effective appliance for assembling benchmarks to meet the needs of nearly any application. When supplemented with additional governance and directives for risk scoring, it is expected that SCAP content will be a very powerful instrument in the assessment of a network device for risk metrics.

Enumerations Enable Risk Scoring

SCAP enumerations (*e.g.*, CCE, CVE, and CPE) have the potential to make interoperability and risk scoring seamless when properly employed and supported. To avoid ambiguity in

> To provide meaningful metrics that reflect an accurate security posture and highlight critical aspects, some effort must be applied to determining what assessments make sense and what combinations of measurements provide the clearest representation of risk.

applying a risk score for a measure in a metric, each corresponding check must be uniquely identified. Existing content was not written with this objective in mind and in some cases had to be reconstructed to support this approach. As the initiative proceeded with the SCAP enumerations as the identifiers for checks, some checks could not be related to existing enumerations and new ones had to be established. For example, the Windows 7 benchmark included checks for bundled software services (*e.g.,* Telnet Server and TCP/IP Services), which did not have CCEs assigned.

Other weaknesses encountered during this initiative include—

- SCAP does not define a standard for identifying patches.
- Current implementations do not enable results to indicate a value. For example, the password length check results do not indicate the actual length found; only a pass or a fail is returned; therefore, the results lack the context to support risk scoring.
- CPEs are not fully supported by the auditing tool's interpretation of the content or in the reporting of the results.

Of the SCAP suite of standards and protocols, it is likely that the enumerations offer the best chance at measurably improving interoperability, given additional guidance and support.

Data Exchange Standards Have Benefits and Drawbacks

To transfer assessment results from auditing tools into a relational data store and to provide summarized reports for risk assessment, the initiative employed ARF, ASR, and PLARR candidate SCAP data exchange standards. The implementation of data exchange standards proved to be cumbersome and highly resource-consuming. While the development of the software components is facilitated by tightly coupling the producer, consumer, and database to the XML schemas, the perceived amount of maintenance required at each component when changes in the data set are made seem to overshadow the benefits. Follow-on research to this initiative will explore alternative methods to more efficiently transfer assessment results.

Metrics Enhance Situational Awareness and Improve Effective Mitigation

To provide meaningful metrics that reflect an accurate security posture and highlight critical aspects, some effort must be applied to determining what assessments make sense and what combinations of measurements provide the clearest representation of risk. One widely accepted list of protective measures is the SysAdmin, Audit, Network, Security (SANS) Institute's 20 Critical Security Controls, often referred to as Consensus Audit Guidelines (CAG). [12] These controls, however, have not been translated and codified into measures and metrics by which organizations can gauge themselves.

The severity ratings for some types of measures have not been defined. Not all measures are equal as not all patches are equal in terms of the risks alleviated; therefore, each measure should have a varying severity with which it is associated. The SCAP Common Vulnerability Scoring System (CVSS) is a good example of a scoring standard. This model of associating a severity to a risk measure needs to be extended to configurations, patches, applications, *etc.* For configuration measures, the Common Configuration Scoring System (CCSS) standard has been established, yet the values remain unassigned.

Findings and associated severity ratings are not the only drivers in deriving risk scores. Often, findings and ratings are compounded in the risk scoring engine to derive a score that may be heightened or lowered depending on the specifics. One type of risk may be compounded or alleviated by mitigation of another type of risk. In addition, severity ratings allow managers and systems administrators to prioritize the mitigation actions necessary. As concepts for continuous monitoring and risk scoring mature and as metrics become more advanced, the need for severity ratings for numerous other measures will likely increase.

Asset Visibility is Key

Network device visibility and the ability to assess configurations are vital in determining the overall health of a network. Risk metrics pivot on an awareness of the asset population while automation hinges on the ability to assess devices *via* electronic means. Assessing only a subset of network devices provides an ineffectual risk assessment that is at best misleading. The unknown risk contributed to a system by an unmanaged device far outweighs the known risk contributed by a managed device, while unknown devices present an even greater risk. The ability to electronically capture and comprehend an organization's device population may be the foremost attribute of a successful continuous monitoring capability. Only after asset visibility has occurred can security configuration management begin. This very idea is captured by SANS in its first critical control: "An accurate and up-to-date inventory, controlled by active monitoring and configuration management, can reduce the chance of attackers finding unauthorized and unprotected systems to exploit." [13]

Other Un-Assessable Device Attributes and Organizational Structure Gaps Inhibit Rollup

One unexpected challenge encountered during this initiative was the inability to accurately assess who owned a device and who managed that device. This distinction is necessary to assign responsibility and accountability and to be able to aggregate or roll up system risk scores to higher levels. When responsibility cannot be assigned, the ability to drive behavior based on metrics is made more difficult. Due to the complex nature of military hierarchy, organizational structures and the dynamic nature of deployments, an easy work-around was not readily available for this initiative.

Conclusion

Network security continuous monitoring and supporting concepts have become the foundation for many new initiatives in securing this nation's information systems. This strategy can boost risk awareness, prioritize necessary remediation actions, and improve overall security posture. For the government to achieve an enterprise-wide network security continuous monitoring capability, supportive federal, industry, and international processes and governance bodies must be implemented in harmony with the technical solutions.

Real and achievable efforts to target include—

- A focus group to identify a strategy to develop a government-wide organization naming standard;
- Increased support for risk metrics research and development;
- Governance and strategy for public and private sector content management; and
- A working group to increase enumeration interoperability and wider adoption.

Attention to and resourcing in these areas will provide incentive, guidance, and support for continuous monitoring as well as a better foundation on which to deliver more viable standards-based risk assessment solutions. ■

About the Authors

James Park | is a CND R&T project manager at NSA Information Assurance Directorate. Mr. Park has a diverse background from being an engineer on nuclear powered submarines, to information technology systems engineer, to Computer Network Operations planner while on active duty with the Navy. Since retirement from the Navy, Mr. Park has been focusing on research activities supporting network security continuous monitoring. He can be contacted at *iatac@dtic.mil*.

Dayna Harris | is a computer scientist on the CND R&T team in the Security Automation Office of NSA. Since joining the NSA team, she has been working on SCAP-related initiatives, contributing to the emerging data exchange standards and developing the ARCAT and Assessment Results Measure of Risk (ARMOR) Continuous Monitoring initiatives. Ms. Harris has 15+ years of software engineering experience leading design and development for database-driven, web-based software systems. She received her B.S. in Computer Science from Hawaii Pacific University and is currently pursuing her MSCS at Johns Hopkins University. She can be contacted at *iatac@dtic.mil*.

References

1. The Comprehensive National Cybersecurity Initiative. Retrieved July 1, 2011, from *http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative*.
2. Department of State, Information Resource Management, Office of Information Assurance, iPost: Implementing Continuous Risk Monitoring at the Department of State, Version 1.5, May 2010.
3. NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, Appendix G, Continuous Monitoring.
4. NIST Special Publication 800-126 Revision 1, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1.
5. Schmidt, D. (2010, Winter) Security Automation: A New Approach to Managing and Protecting Critical Information, IAnewsletter, 6-10, Volume 13 Number 1.
6. *http://cve.mitre.org/*
7. *http://cce.mitre.org/*
8. *http://cpe.mitre.org/*
9. *http://measurablesecurity.mitre.org/incubator/arf/*
10. *http://measurablesecurity.mitre.org/incubator/asr/*
11. *http://measurablesecurity.mitre.org/incubator/plarr/*
12. 20 Security Controls. Retrieved Jun 28, 2011, from *http://www.sans.org/critical-security-controls/*.
13. SANS Critical Control 1: Inventory of Authorized and Unauthorized Devices. *http://www.sans.org/critical-security-controls/control.php?id=1*.

Under Constant Attack

by Will Pelgrin

A recent survey that the Ponemon Institute conducted confirmed that organizations of all sizes, from all sectors are vulnerable to cyber attacks. The survey reports that 90 percent of organizations have had at least one breach in the past 12 months, with nearly two-thirds (59 percent) citing two or more breaches. Sadly, 10 percent did not know if they had been breached. [1] These numbers indicate that it is not a matter of "if" but "when" an organization will be affected by a breach.

While there has been much attention lately on several high-profile incidents in the private sector (*e.g.,* Sony, RSA, *etc.*), the public sector is not exempt from attacks or breaches; in fact, governments are increasingly being targeted by organized groups. LulzSec/Antisec/Anonymous actors have expressed intentions to dedicate significant, ongoing effort to attacks on perceived abusive and corrupt governments. Whether the motivation is driven by the desire to gain mass-media attention or a true belief in their cause, these groups view governments at all levels as prime targets. Attack campaigns will continue to gain popularity, despite attempts to criminalize these acts.

While some attacks are very sophisticated, others are taking advantage of common vulnerabilities. According to the 2011 Verizon Data Breach Investigations Report, of 4 million data breaches in 2010, the majority of them were not highly difficult, and 96 percent were avoidable through relatively inexpensive simple or intermediate controls. [2]

While tremendous progress has been made in raising awareness about the importance of cybersecurity, there is still much work to be done. Many of our behaviors have not changed, and as evidenced by the Verizon Data Breach results, many of the breaches were possible because of a lack in basic controls. [3] While the myriad of obstacles—including current fiscal environment, diminishing experienced workforce, and prevalence of embedded old infrastructure—can make addressing the ever-changing targets and vectors of attack difficult, we must remain vigilant and move forward; the dangers are too great, the risks are too real, and the consequences are too significant. While recognizing that the fiscal, staffing, and infrastructure impediments create additional challenges, there is still a lot that can be done at relatively little cost and effort to minimize the risk of a successful attack.

How Do We Improve Cybersecurity?

One key element that every organization must implement is collaboration. Not one public or private sector organization can do it alone, no matter how big or powerful. Working collectively to address our cybersecurity posture will have a dramatic impact of the overall nation's cyber readiness and defensive capabilities.

Another key element in a successful strategy to make meaningful, long-lasting improvements is to focus attention on the greatest risks and most prevalent vulnerabilities. The fact that we are seeing far too many attacks utilizing SQL-inject, buffer overflow, and other common programming vulnerabilities should not go unheeded.

The MITRE Corporation and SANS Institute—in collaboration with the U.S. Department of Homeland Security (DHS)—recently issued a Top 25 Most Dangerous Software Errors list that contains the most widespread and critical errors that can lead to serious vulnerabilities in software. [4] These vulnerabilities are generally easy for an attacker to find and exploit, potentially allowing a complete takeover of the system, theft of data, or disruption of functionality.

Although not a silver bullet, the Top 25 list gives a great road map to focus those limited resources and dollars to areas where there is a prioritized risk and for which a successful attack would have a major impact on your environment. These standards are an effective tool for state and local governments in mitigating risk.

As we all know, there is no "one-size-fits-all" solution for securing critical infrastructure and the networks

that support them. The most effective strategy builds on layers of security with no one single point of failure. The development of secure applications is a critical component of that layered approach.

Cybersecurity standards are security benchmarks that outline recommendations on how organizations can implement best practice safe security methods and procedures to minimize the number of successful cybersecurity attacks. There are many organizations (*e.g.,* International Standards Organization, National Institute of Standards and Technology, *etc.*) that are widely recognized as providing best practices and acceptable standards (some resources are free and others for sale). Again, there is no "one-size-fits-all" approach; the most important action is to not debate the decision too long but to just select a standard that best suits your organization's needs. Make sure that the standards are implementable—those that read well or profess to be the platinum level of security may be too daunting, too complicated, and too costly. One should set the bar at an acceptable level (minimum requirements versus maximum requirements) initially. Raising the bar periodically as entities demonstrate compliance and as abilities improve to achieve greater controls can yield significant benefits.

Lastly, state and local governments have an untapped leverage through the power of aggregate purchasing that can be maximized to help implement secure solutions. State and local governments represent one of the largest aggregate buying consortiums. By utilizing that collective power, state and local governments can achieve aggressive pricing and favorable terms and conditions that are traditionally only available to federal agencies or large companies. The Multi-State Information Sharing and Analysis Center (MS-ISAC) identifies and negotiates aggregate procurements to assist state and local governments. The concept is simple: how can we make it easy, efficient, and effective for state and local governments to improve their cybersecurity posture? By acting as the aggregator and negotiator, essential cybersecurity services procurement opportunities are presented to the MS-ISAC membership. The MS-ISAC enabled state and local governments to achieve more than $40 million in savings on a joint encryption buy and recently completed an aggregate buy for awareness training, resulting in significant discounts for state and local governments.

By working collaboratively, implementing standards, and maximizing available resources, state and local governments can protect their data and systems in a cost-effective and achievable manner. ■

About the Author

William Pelgrin | is the President and Chief Executive Officer of the Center for Internet Security. He is also the Founder and Chair of the MS-ISAC, the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal governments. He is serving his third term as Chair of the National Council of ISACs and also served as a Commission Member of the Center for Strategic and International Studies Commission on cybersecurity to brief the 44th President of the United States. Government Technology magazine recently named Mr. Pelgrin as one of 2011's Top 25 Dreamers, Doers, and Drivers and one of the Top 10 Government Information Security Leaders for 2011 by GovInfoSecurity. He can be contacted at *iatac@dtic.mil.*

References

1. Perceptions About Network Security: Survey of IT & IT security practitioners in the U.S., Ponemon Institute June 2011. *http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf.*
2. Verizon. 2011 Data Breach Investigations Report. *http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.*
3. *Ibid.*
4. 2011 Top 25 Most Dangerous Software Errors. *http://cwe.mitre.org/top25/.*

Applying and Extending SCAP to Deliver the Trusted Cloud

by W. Wyatt Starnes

The strength of the U.S. economy and our national security are interwoven with our ability to deliver secure and reliable information technology (IT) service delivery. Today, many IT leaders believe that the next wave of IT delivery is cloud computing, which provides dynamic access to pools of computer processing, storage capacity, and network bandwidth. This article suggests that cloud computing will not be fully embraced by government or industry unless it can be trusted.

But what is trust as it relates to the cloud? Conventional thinking tends to focus on cloud security, often with an inference that trust and security are synonymous. Delivering pervasive IT trust, however, is a higher-order expression that requires systems be fully available and able to deliver to *all* security and quality of service expectations. The rapidly evolving cloud landscape represents an opportunity to rethink and redefine our goals, aspirations, and methods for the delivery of this next-generation IT infrastructure.

For the cloud to be fully adopted, it must meet or exceed the cyber challenges we face in today's hostile global environment. In effect, the cloud must not only be cheaper, it must be better. Additionally, new use cases must be explored, and supporting capabilities must be adopted and deployed to improve interoperability, transparency, error recovery, and resiliency from attacks such as advanced persistent threat (APT) and other zero-day risks.

To successfully deploy these technologies and methods, government agencies, private industry, and academia must work together to actively share threat intelligence and vulnerability information, while enabling new levels of automated alerting and remediation. This article will show how the Security Content Automation Protocol (SCAP), pervasive and continuous monitoring, along with software reference integrity methods, are critical to the delivery of a trusted cloud.

Security Is Necessary but Insufficient to Deliver Full Trust

Industry marketing material increasingly refer to trust when discussing cloud computing; however, these discussions are often disappointing as they generally focus primarily on security. While effective security best practices are necessary, they are not enough to ensure a highly-trusted business service delivery. Additional trust enablers include continuous compliance, performance, availability, integrity and supply chain assurance. [1] Essentially, all elements that impact secure and reliable IT service delivery through the entire IT business service delivery life cycle must be addressed. Accomplishing this requires new sensors and assurance methodologies, as well as standardized methods of platform configuration, assurance and validation.

Security Automation—The First Step in Trusted Cloud Delivery

Regardless of the specific cloud deployment model (Public or Private), the shift to the cloud presents a new and deeper level of abstraction for cloud consumers. Outside of transnational and domain issues (not discussed in this article), most consumers should not care where the cloud infrastructure physically resides. The physical abstraction inherent in the cloud IT deployment model, while an important benefit when properly implemented, is also one of key challenges to enterprise adoption. In the cloud, how do I maintain confidence that my data is secure, private, and available when I am not even sure where it is?

Figure 1 illustrates that IT deployment models are shifting rapidly from traditional monolithic models (one software stack on one hardware platform with a single tenant in a known location). The cloud model (n software stacks on n hardware platforms with n tenants) creates significantly more challenging issues for cloud operators and consumers.

Automation methods, including security, are key to providing predictable, reliable, and continuous trust assurance in the cloud

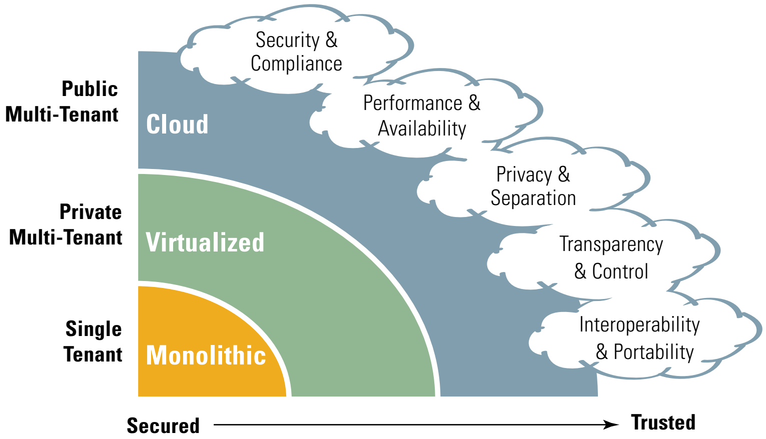


Figure 1 Compute model shifts

environment. These methods should be standardized and largely hardware and software infrastructure agnostic. This allows the cloud provider to choose the best configurations for their specific cloud implementation, while maintaining interoperable assurance frameworks.

SCAP—The Lexicon for Assurance in the Cloud

While its creators and proponents likely did not fully foresee the needs of these emerging IT deployment models, SCAP is an excellent tool to address the needs for standards and automation in the cloud.

The National Institute of Standards and Technology (NIST) SCAP-validated tools. It is important to note that not all of the tools support the full SCAP specification and extensions. [2] The SCAP use cases explored in this article are based on the tools and methods which include two primary components known as the Enterprise Trust Server (ETS) and the Global Trust Repository (GTR). [3]

Continuous Improvement and Business Process Safety

Data center availability has generally been measured by the formula:

$$\text{Availability} = \frac{\text{Mean Time Between Failures (MTBF)}}{\text{(MTBF + Mean Time to Repair (MTTR))}}$$

This is often referred to as the “nines” model. In order to “add nines” to availability providers must simply maximize MTBF (keep it working without interruption) and minimize MTTR (fix it as fast possible). This is an incomplete measurement to enable the trusted cloud. The airline-equivalent measure of safety delivery is much starker. Airlines have had to report and measure passenger fatalities per passenger mile since their commercial inception. While clearly the availability model for IT and the safety model for airlines are not fully comparable, it is interesting to look at the relationship and trends of our key measures.

In 1929, the worst safety year for the airlines on record, the fatality rate per passenger mile was 1 in 1,000,000. [4] When we translate that into the data center nines model, we find a safety (availability) metric of 6 nines (99.9999 percent). Now perhaps that does not sound so bad by IT standards; however, if airline safety metrics remained at 6 nines, the actual passenger fatality rate on current global airline miles delivered would be more than 1,000 deaths per year. While this may be an extreme comparison, it demonstrates the relationship between delivered safety and passenger miles delivered. Clearly, if airline safety were held at 6 nines or less, then the actual number of passenger miles delivered would be far less as the industry would self-limit.

The same condition is true for cloud IT delivery. If we are unable to deliver significantly higher levels of trust, safety, and availability with the cloud IT business process delivery (over traditional data center models), cloud demand will also self-limit.

Currently, the airline industry is delivering passenger miles with a safety record of over 9 nines. This represents over three orders of magnitude of improvement in the last 84 years. [5] The key enablers for these improvements are—

- Better passenger delivery systems designed and operated as "systems" (*i.e.,* airplanes);
- Enhanced best practices and logistics for operating the delivery systems more safely and reliably (standards and methods); and
- Continual and fast feedback loops to improve current operations based on past experience (forensic and root-cause analysis captured and openly shared for the betterment of all operators).

Enabling these same best practices and automation at scale is really what the SCAP innovators had in mind. Implemented and delivered effectively, SCAP has the potential to add several orders of magnitude of improvement for the cloud delivery model, enhancing adoption and maximizing long-term growth.

Moving to an Asymmetrical Assurance Model

A significant challenge for all IT delivery models is the powerful re-emergence of our old zero-day nemesis now commonly called APT. Traditionally we have deployed largely symmetrical defensive models on the (increasingly flawed) assumption that our risks (both benign and malicious) will traverse a specific perimeter and be readily identifiable. [6] Most of the cybersecurity technology, methods, and practices are based on these assumptions. Today, it is clear that the symmetry inherent in most of our current security tools is insufficient to the challenge of trusted IT business service delivery.

Threats, such as APT, represent a significant challenge for all C-level executives and IT professionals dealing with cyber risk. To address these challenges, we must add to our symmetrical defenses, adding awareness of the asymmetrical risk.

These advanced threats (and other changes and disruptions to integrity and configuration) are often hidden in plain sight. As these threats are asymmetrical, often they cannot be readily mitigated with traditional symmetrical tools (perimeter and signature based approaches).

To detect these often crucial changes to the good and/or trusted state of the IT device, it is necessary to understand and/or capture the initial device state, and then enable a means to detect changes to the expected state. This can be accomplished with the reference integrity and positive assurance methods described below.

Reference Integrity and Positive Assurance

The sine waves in Figure 2 represent software cycles executing on a given IT device.

The graph on the left shows the traditional negative detection model. A malicious detection (shown by the red circle) occurs when a pre-identified "bad code" element attempts to load or run. Negative detection methods, in general, seek to identify anomalous change through the identification of that change *via* defined signatures and/or behavioral characteristics.

The positive assurance (plus negative detection) model is shown in the graph on the right side. The positive assurance model works by detecting "out of set" or "out of scope" incursions of code. These code or configuration elements are not in alignment to the established baseline reference models for that device.

This example illustrates a binary load/run exception, which is one aspect of the positive assurance model. In practice, however, every setting that impacts the operational integrity of the device can be monitored. Typically, this would include configuration assertions and permissions in addition to explicit binary attestation. It is also important to note that this method is applicable for all IT devices that run software, including servers, clients, routers, switches, and even mobile endpoints.

To support supply chain integrity and other important advanced assurance use cases, several other trust resources are necessary, including software measurement and harvesting (ideally from trusted sources), which is discussed in further detail below.

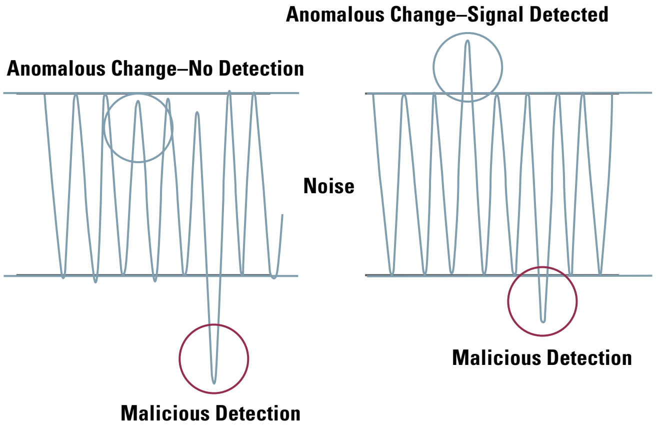

Anomalous Change–Signal Detected
Anomalous Change–No Detection
Noise
Malicious Detection
Malicious Detection

Figure 2 Negative detection versus positive assurance

Trust Resources: Software Measurement and Supply Chain

With an increasingly global supply chain, software for critical IT devices and business applications can be produced anywhere. To assure full supply chain integrity, it is useful, and in some cases crucial, to verify the supply integrity of the software as well as to verify that the integrity established at the supply source can be tracked and verified to the actual usage point. Software measurement and verification (attestation) provides a means to accomplish this.

Software measurement is a method by which larger software objects, as shown in Figure 3. are processed with cryptographic methods to create unique and compact "fingerprints" of the parent objects. One way of capturing these software measurements with an automated process is called "harvesting."

Wherever possible, the process starts at the original supplier/author of the software package. The packages are recursively decomposed to extract fine-grain measurements, including multiple cryptographic digests (hashes) as well as the parent-child relationships of the software elements. Additional data is also captured to form one or many manifests that precisely reflect the intent of the software manufacturer with respect to the installation of that software package.

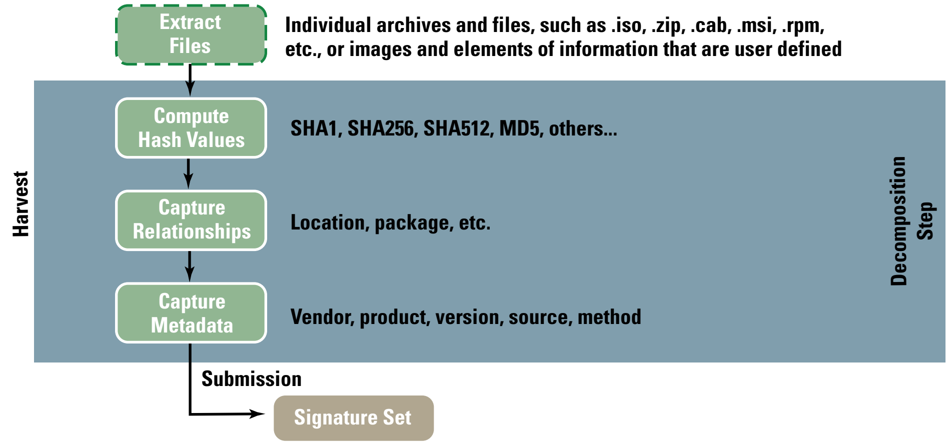

Extract Files
Individual archives and files, such as .iso, .zip, .cab, .msi, .rpm, etc., or images and elements of information that are user defined
Harvest
Compute Hash Values
SHA1, SHA256, SHA512, MD5, others...
Capture Relationships
Location, package, etc.
Capture Metadata
Vendor, product, version, source, method
Decomposition Step
Submission
Signature Set

Figure 3 Software measurement process

Figure 4 shows that it is best to capture the software measurement at the point of supply, allowing a root of trust for the software to be established. As it is not always possible to establish software authenticity to a complete certainty, a field has been created in the data set to establish software source authenticity score (SAS) or software provenance.

The SAS/provenance score represents the confidence level of the measurement provider of the source of origin, or provenance, of the software measurement. The SAS ranking is based on the general guidelines that are depicted in Figure 5. This field is available for interrogation and use at the point of consumption for the software measure(s).

In one implementation, these measurement sets are submitted for inclusion into a much larger database, the Global Trust Repository (GTR), which is depicted in Figure 6. This database is populated with approximately 3 billion rows of software measurements and is expected to double approximately every 10 months. Measurements are available from over 2,000 independent software vendors and

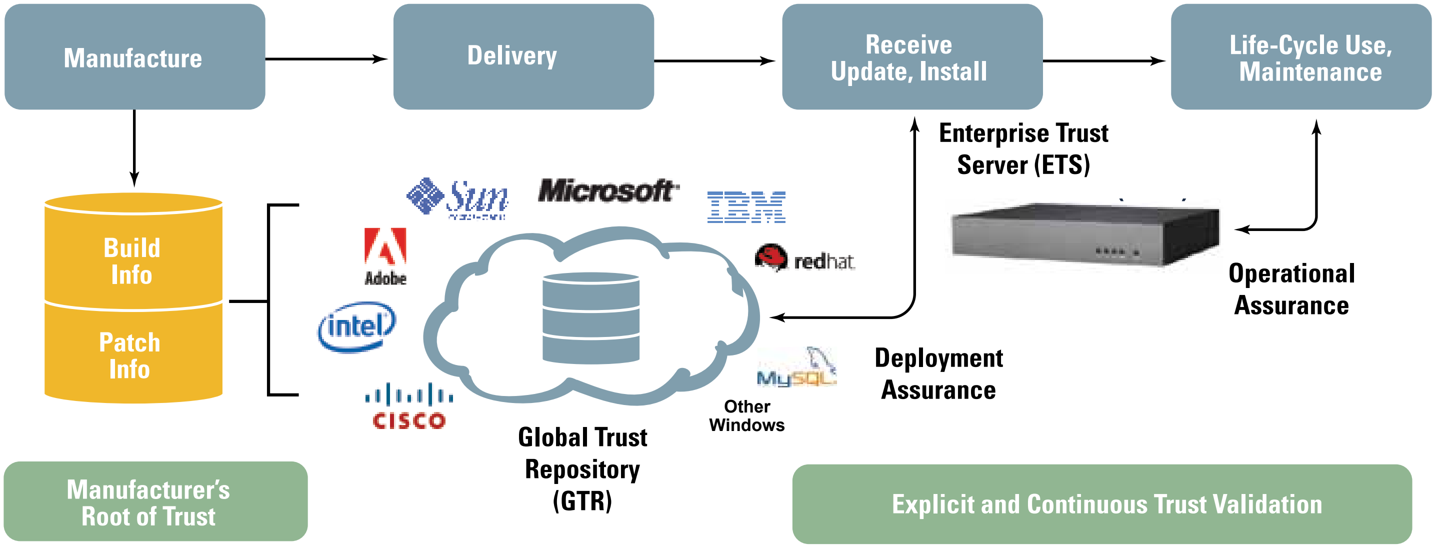


Figure 4 Software supply chain method

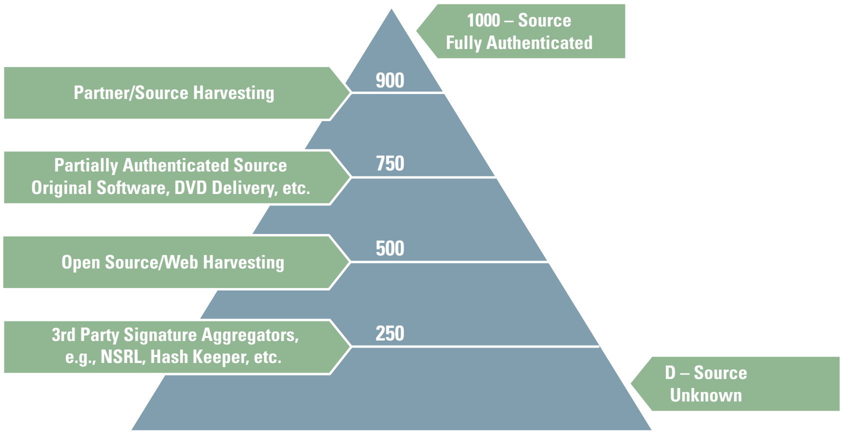

1000 – Source
Fully Authenticated
Partner/Source Harvesting
900
Partially Authenticated Source
Original Software, DVD Delivery, etc.
750
Open Source/Web Harvesting
500
3rd Party Signature Aggregators,
e.g., NSRL, Hash Keeper, etc.
250
D – Source
Unknown

Figure 5 Software source authenticity (provenance)

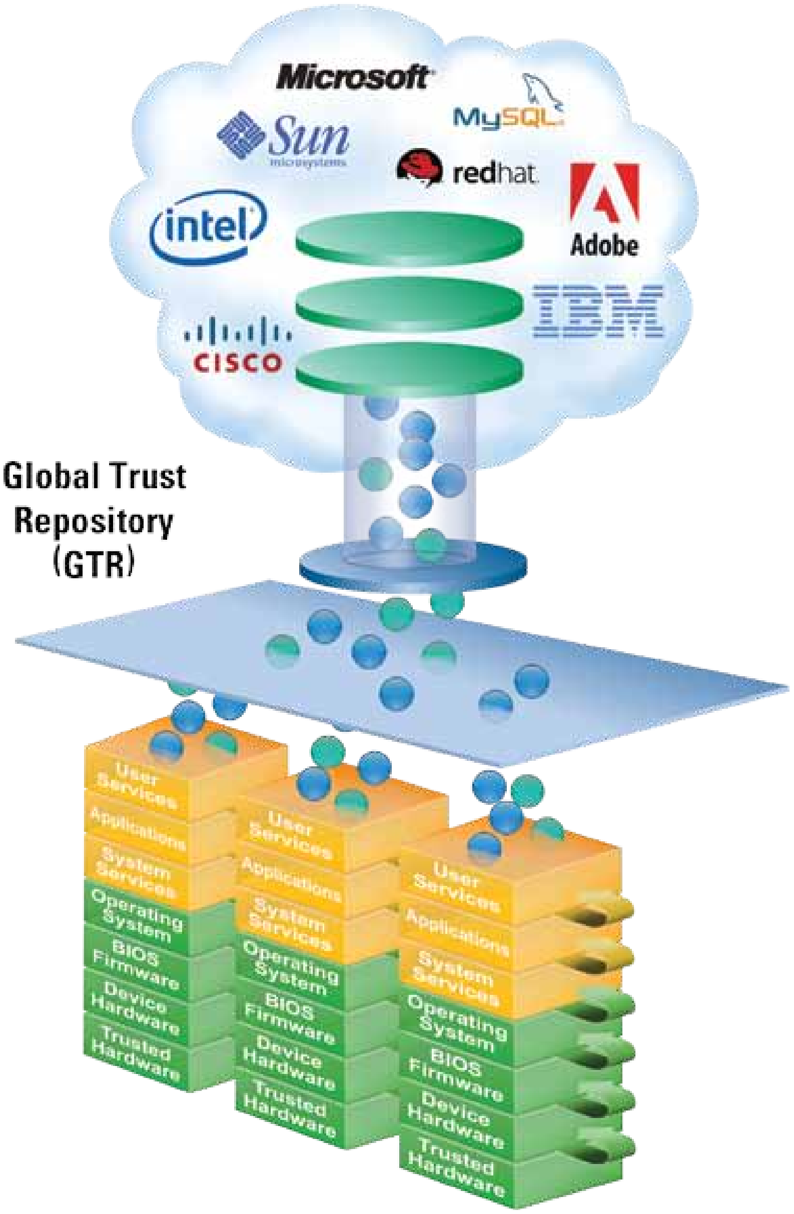


Figure 6 Global trust repository

over 500,000 individual software packages.

The GTR supports many use cases beyond traditional application whitelisting. A full dimensional software capture repository is more than a simple whitelist database as it should support advanced use cases including—

- That a test or assertion can be made to determine if a package install is complete (or incomplete);
- Verification that software patches have been properly (and completely) installed; and
- The degree of confidence that a named application or vendor software element was manufactured by that vendor.

The GTR, which serves as a master library of trusted software measurements, is an important resource for supply chain validation and other forensic methods.

Trust localization is necessary to create and map client and domain-specific reference images to the monitored IT devices. This is accomplished with an appliance (physical or virtual), the Enterprise Trust Server (ETS). One ETS can support hundreds and even thousands of monitored devices. The ETS provides a ready mechanism to extend reference definitions by adding proprietary software (unknown to the GTR) to the local reference library. Additionally, the ETS provides the means to add specific configuration settings to reference images including paths, permissions, registry, and other device-specific information.

Continuous Monitoring and SCAP

Continuous monitoring of platform security, configuration, integrity, and assurance is necessary to deliver the desired compliance outcome. Continuous monitoring methods should include the ability to—

- Check, test, or verify assertions on a regular basis by evidence or experiments;
- Set monitoring periodicity aligned to the risk detection and mitigation profile;
- Verify all elements of an IT device that impact its security, compliance, availability, and performance; and
- Include the ability to attest current integrity, configuration, control settings, and supply chain provenance.

With the cloud model, it is important to deliver active user feedback of the state of all of the devices used to deliver the business services.

Leveraging SCAP Content for Continual Improvement

Another significant benefit of utilizing SCAP for cloud trust assurance is SCAP content aggregation and community sharing. Figure 7 depicts one example to determine a trusted enterprise cloud offering. Automated mechanisms have been created to constantly poll SCAP content sources, such as the National Vulnerability Database, [7] allowing new configuration and vulnerability information to be immediately actionable.

Taking this a step further, you should aggregate many sources of risk and trust resources in the Community Content Cloud (depicted in Figure 8).

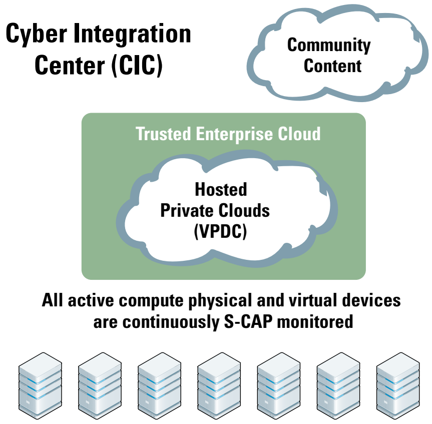

Cyber Integration Center (CIC)
Community Content
Trusted Enterprise Cloud
Hosted Private Clouds (VPDC)
All active compute physical and virtual devices are continuously S-CAP monitored

Figure 7 Clouds and content

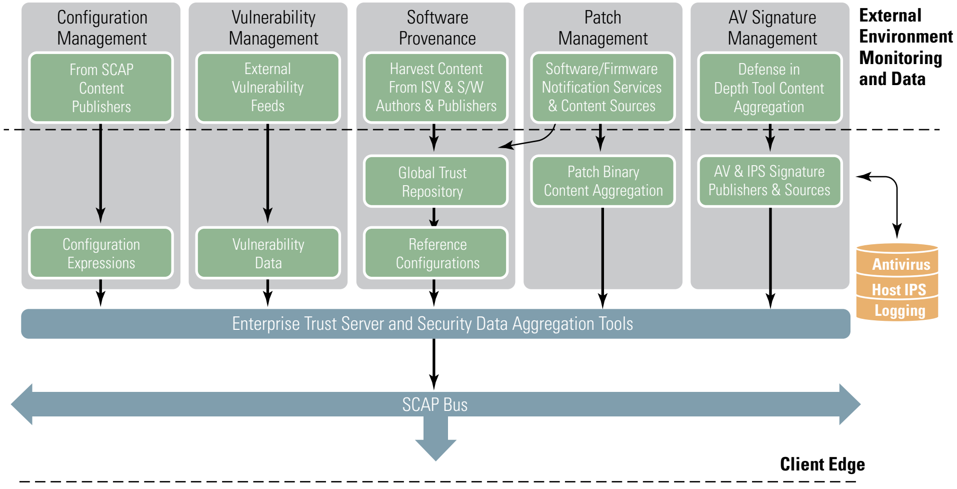

Configuration Management
From SCAP Content Publishers
Configuration Expressions
Vulnerability Management
External Vulnerability Feeds
Vulnerability Data
Software Provenance
Harvest Content From ISV & S/W Authors & Publishers
Global Trust Repository
Reference Configurations
Patch Management
Software/Firmware Notification Services & Content Sources
Patch Binary Content Aggregation
AV Signature Management
Defense in Depth Tool Content Aggregation
AV & IPS Signature Publishers & Sources
External Environment Monitoring and Data
Antivirus
Host IPS
Logging
Enterprise Trust Server and Security Data Aggregation Tools
SCAP Bus
Client Edge

Figure 8 SCAP and community content

Essentially, two pipelines of data are created across the entire trusted cloud framework—

1. Traditional security content, such as antivirus and IDS/IPS signatures; and
2. Trust enablement content including the full GTR as well as aggregated SCAP information from multiple sources.

This information is then used to monitor and maintain the security and trust posture of the entire cloud infrastructure on a continuous basis. Keep in mind that positive assurance methods will allow you to precisely understand and map what system is running where and which version, configuration, and application stack is associated with that system. This provides a powerful mechanism to map prospective vulnerability and system update information to the affected systems.

Additionally, community content information is also available to users and is heavily leveraged to support the trusted enterprise cloud client service level agreement (C-SLA). Subject to the C-SLA risk, vulnerability and configuration information can be made available immediately to clients to enable alerts and or automated remediation processes.

Summary

The IT sector must continue the effort to mature our technology development and delivery with the goal of achieving the trust and safety metrics already achieved by other highly automated consumer-based services. It is crucial to utilize standard methods to enable deeper technical trust based on a common language for measuring, sharing, and enforcing better security and assurance automation.

SCAP, with the reference integrity and positive assurance extensions discussed, creates an indispensable and effective way to manage and assure trusted business service delivery in the cloud. ■

About the Author

W. Wyatt Starnes | is Vice President for Advanced Concepts for Harris Corporation's Cyber Integrated Solutions. He is responsible for the advanced development of the Harris Trusted Enterprise Cloud service portfolio and the Harris Cyber Integration Center. Mr. Starnes has more than 36 years of experience in high technology with eight different startups. He is the founder and

Chief Executive Officer (CEO) of SignaCert, Inc., which was acquired in 2010 by the Harris Corporation, an international communications and IT company serving government and commercial markets in more than 150 countries. Prior to SignaCert, Mr. Starnes founded Tripwire, Inc. and served as its president and CEO for 7 years. Additionally, he is the co-founder of Regional Alliances for Infrastructure and Network Security, a nonprofit public/private alliance formed to accelerate development, deployment, and adoption of innovative technology for homeland security. Mr. Starnes holds four patents on software integrity management methods. In April 2011, Mr. Starnes was selected for the TechAmerica Foundation's CLOUD^2 (Commission on the Leadership Opportunity in U.S. Deployment of the Cloud), which was tasked with providing the Obama administration with recommendations for both government and commercial advancement of the cloud. He can be contacted at *iatac@dtic.mil.*

References

1. *http://www.techamericafoundation.org/content/wp-content/uploads/2011/02/CLOUD2_Report_Cloud_First_Cloud_Fast_Recommendations_for_Innovation_Leadership_and_Job_Creation.pdf*
2. *http://nvd.nist.gov/scapproducts.cfm*
3. *http://www.harris.com/view_pressrelease.asp?act=lookup&pr_id=2989*
4. *http://en.wikipedia.org/wiki/Air_safety*
5. *Ibid.*
6. *http://en.wikipedia.org/wiki/Asymmetric_warfare*
7. *http://nvd.nist.gov/*

▷ *continued from page 13*

SCAPVAL: VALIDATING SPECIFICATION CONFORMANCE

Schematron is much more expressive than an XML schema and allows for more fine gained XML validation. It then runs an SCAP Schematron rule set against the entire bundle. The SCAP Schematron rules check an extensive number of requirements documented in the SP 800-126. Those rules enforce restrictions placed on individual specifications as well as relationships between specifications. For example, SCAP requires that certain XCCDF rules and OVAL definitions identify the CVE, CCE, or CPE for which they are checking. SCAPVal ensures that those identifiers are provided where appropriate, and using the CCE and CPE data feeds from the NVD Web site, it ensures that those identifiers are correct and active. In addition, it enforces how XCCDF and the CPE dictionary reference OVAL and OCIL components and checks that those references are appropriate. The results of each failure are tied back to a specific statement in the SP 800-126 and are reported as XML and hypertext markup language for easy computer and human consumption.

SCAPVal is a critical tool for rapidly ensuring that SCAP content is reasonably well-formed. While SCAPVal cannot automatically check every requirement in the SP 800-126, it provides a level of assurance that content is conformant with the specification. NIST defines multiple tiers of "checklist content" maturity on the NVD Web site, and SCAPVal assists NIST and content authors with producing content that is consistent with a higher level tier. [12]

Currently, there are three versions of the SCAP specification. SP 800-126 and SP 800-126 Rev 1 are final NIST publications that define the first two iterations of SCAP. SP 800-126 Rev 2 is currently a draft. The current release of SCAPVal supports validating content that is consistent with both SP 800-126 and SP 800-126 Rev 1. In addition, SCAPVal can validate result content that is produced by tools compliant with SP 800-126 Rev 1. Result content includes the results of performing an SCAP scan against a target host. SCAPVal can assist tool vendors and the NVD Validation Program in checking that an SCAP-compliant tool produces results consistent with the SCAP specification. [13] Another version of SCAPVal is expected to be released that will support SP 800-126 Rev 2 when that specification is finalized. ■

About the Authors

Adam Halbardier | is a security professional and software engineer working for Booz Allen Hamilton. He supports the NIST Security Automation Program. He developed the SCAP Schematron rules for the SCAPVal, and he now maintains that tool. He can be contacted at *iatac@dtic.mil.*

Angela Orebaugh | is a technologist, researcher, and cybersecurity executive. She leads a team of security experts supporting the NIST Security Automation Program, including the NVD and SCAP projects. She is also the IATAC Director of Research and Academic Integration. Ms. Orebaugh is an international author and invited speaker for technology and security events. Follow her on Twitter @AngelaOrebaugh and connect with her on Google at *http://gplus.to/angelaorebaugh*.

References

1. *http://scap.nist.gov/revision/1.2/index.html*
2. *http://scap.nist.gov/specifications/xccdf/*
3. *http://oval.mitre.org/*
4. *http://scap.nist.gov/specifications/ocil/*
5. *http://cce.mitre.org/*
6. *http://cve.mitre.org/*
7. *http://scap.nist.gov/specifications/cpe/*
8. *http://nvd.nist.gov/fdcc/index.cfm*
9. *http://usgcb.nist.gov/*
10. *http://scap.nist.gov/revision/1.1/index.html#validation*
11. *http://www.schematron.com/*
12. *http://web.nvd.nist.gov/view/ncp/repository/glossary?cid=1#tierDesc*
13. *http://scap.nist.gov/validation/*

Dr.Ehab S. Al-Shaer

by Angela Orebaugh

This article continues our profile series of members of the Information Assurance Technology Analysis Center Subject Matter Expert (SME) program. The SME profiled in this article is Ehab S. Al-Shaer at the University of North Carolina at Charlotte (UNCC). Dr. Al-Shaer is a professor and director of the Cyber Defense and Network Assurability Center in the College of Computing and Informatics.

At UNCC, Dr. Al-Shaer teaches network and information security, information infrastructure protection, and a network security seminar. His primary research areas include network security, security management, fault diagnosis, and network assurability. He has contributed to 10 books and published over 100 referred journal and conference papers in his research areas. Dr. Al-Shaer has been involved with several academic conferences and was—

- General Chair of the 2009 and 2010 Association of Computing Machinery Conference on Computer and Communications Security
- Technical Program Co-Chair for SafeConfig 2011, 4th Symposium on Configuration Analytics and Automation
- Technical Program Co-Chair of Institute of Electrical and Electronics Engineers (IEEE) POLICY
- Technical Program Chair of the IEEE Symposium of Integrated Management.

He is also involved in several IEEE Technical Program Committees including the IEEE International Conference on Communications Security Symposium, IEEE International Conference on Network Protocols, IEEE POLICY, IEEE International Conference on Computer Communications, IEEE/IFIP Network Operations and Management Symposium, and others.

Dr. Al-Shaer has received a number of grants from the National Science Foundation (NSF), Air Force Research Lab, Cisco, Intel, Duke Energy, and Sun Microsystems. Examples of his NSF awarded grants include Global Configuration Verification and Optimization, Investigations of Next-generation Network Reconnaissance Attacks, Automated Testing of Security Configuration Enforcement in Distributed Networks, and Collaborative Problem Diagnosis Using Evidential Reasoning and Adaptive Monitoring.

Dr. Al-Shaer completed his Ph.D. in Computer Science at Old Dominion University, his M.Sc. in Computer Science at Northeastern University, and his B.S. in Computer Engineering at King Fahd University of Petroleum and Minerals. [1] ■

References

1. *http://www.CyberDNA.uncc.edu/~ehab/*

Security Automation from a NIST Perspective

by John Banghart, Stephen Quinn, and Kevin Stine

Security automation can harmonize the vast amounts of information technology (IT) data into coherent, comparable information streams that inform timely and active management of diverse IT systems. Through the creation of internationally recognized, flexible, and open standards, security automation can facilitate IT infrastructure interoperability and broad acceptance and adoption and create opportunities for innovation.

As part of the larger security automation initiative, the Security Content Automation Protocol (SCAP) provides standardized data models and methods for assessing and reporting vulnerability and configuration state of computing systems.

SCAP 1.2

SCAP continues to evolve to meet the needs of expanding use cases, and the security automation community continues to work on refining the capabilities it provides.

Although SCAP has enabled the successful implementation of some limited use cases including the Federal Desktop Core Configuration (FDCC)/ United States Government Configuration Baseline (USGCB) initiative, the significantly greater potential of SCAP is realized with the advent of SCAP 1.2. What is this potential? From a configuration and vulnerability scanning perspective, it means having plentiful SCAP content for commonly used computing operating systems and applications that interoperate seamlessly with validated products that can process and produce correct results and work aggressively to continue wide-scale use and adoption.

SCAP 1.2 Feature Set

SCAP 1.2 builds on previous versions of SCAP by introducing a method for integrating underlying specifications *via* a cohesive data stream model, allowing practitioners to build SCAP content using the primitive specifications in new and innovative ways not defined in the comprising specifications. SCAP 1.2 also introduces digital signing of content to ensure content and result integrity, specifications for asset identification and reporting, and support for new assessment methods using PowerShell. SCAP 1.2 also makes it possible to assess a hybrid of operating system, application, and artifact targets using a single data stream by dynamically determining at runtime the settings and system state rather than be beholden to a static list of settings (as with previous versions of SCAP).

SCAP Validation

To ensure that commercially available security products are able to correctly use SCAP 1.2, the SCAP Validation program was expanded to include new requirements and much more robust testing capabilities. Working closely with National Security Agency (NSA) and Department of Homeland Security (DHS), in the fall of 2011, National Institute of Standards and Technology (NIST) will introduce an updated set of Derived Test Requirements based on SCAP 1.2 along with a publically available test suite that will assist product vendors in the development of their products and provide end user organizations with the ability to conduct their own testing. In keeping with the existing process, accredited third-party laboratories will use these new requirements and significantly expanded test suites to ensure greater product and content interoperability.

SCAP Use Cases

Continuous Monitoring

Information security continuous monitoring enables an organization to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

The process of continuously monitoring the security of systems throughout an enterprise is challenging for several reasons. Most organizations have large heterogeneous computing environments that consist of numerous

operating systems and applications that require secure configuration and patch management. Keeping up with the demands of daily operations while also demonstrating compliance with security requirements expressed in legislation, regulation, and policy is challenging without a proper strategy that involves security automation.

Organization-wide information security continuous monitoring can be difficult using manual processes alone. The use of SCAP checklists and validated products for assembling organization-wide information security information can facilitate efficiencies and improve effectiveness. Recent additions to SCAP 1.2 ensure security automation will expand to still additional use cases within this highly important problem space.

Secure System Configurations

Another supporting use case for continuous monitoring is the USGCB for Windows 7, Internet Explorer 8, and Red Hat Enterprise Linux, representing an evolution from the earlier FDCC for Windows XP, Windows Vista, and Internet Explorer 7. [1] After consulting with the Chief Information Officer (CIO) Council agencies, the Technology Infrastructure Sub-committee (TIS) of the Federal CIO Council took the important lessons from the implementation of the FDCC on federal desktop systems and has put forth a true baseline for Windows 7 and Red Hat Enterprise Linux 5. As with the FDCC, the USGCB checklists use SCAP as the basis for the machine-readable policy. In the future, the TIS will leverage National Checklist Program-hosted checklists at Tier III ranking for inclusion as future USGCB candidates for federal use and adoption. [2]

Health IT

The application of security automation principles and specifications are being extended beyond the federal government to provide value across other sectors and within the context of additional security frameworks.

Security automation is being leveraged to assist healthcare organizations in improving their ability to enable measurement and monitoring of security controls and configurations and to support security compliance management with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 CFR 160, 162, and 164). [3]

By leveraging the FDCC and USGCB initiatives described earlier, NIST is using SCAP specifications to develop HIPAA-specific baseline security configuration checklists for common operating systems that host electronic health record systems, enabling greater automation of the HIPAA Security Rule technical safeguards.

A prototype HIPAA Security Rule self-assessment application, containing nearly 1,000 questions expressed using the Open Checklist Interactive Language, will help HIPAA covered entities and other healthcare organizations to better understand the HIPAA Security Rule standards and safeguards and assist in implementing and assessing those standards and safeguards in their operational environments.

International Standardization

The United States Government (USG) recognizes the benefit of a U.S. public and private partnership to develop, maintain, and implement voluntary consensus standards related to cybersecurity best practices to ensure the interoperability, security, and resiliency of this global infrastructure. This position is supported and guided by U.S. legislation and policy and is illustrated by the USG's promotion and assistance over the past two decades to advance security in commercial off-the-shelf IT products. [4] It has also become widely accepted by the USG and many others that standards only provide value if they are widely used.

Industry has shown great interest in incorporating SCAP into their products but would like to take advantage of economies of scale and ensure that the products they design and produce can be sold globally in multiple markets and validated against one set of standards.

This condition will arise only if SCAP and its supporting components, as well as other specifications in the security automation body of work, are accepted by foreign governments and other major global market players. In turn, many foreign governments and major players are more likely to accept SCAP validated products and not develop their own similar standards if SCAP and its supporting components are accepted and further developed within an acceptable international standards development organization.

Outreach

Broad community involvement and adoption of security automation technologies has always been a hallmark of this multi-year initiative. In addition to open mailing lists and Web sites, several events take place throughout the course of the year to bring experts together to advance the state-of-the-art in security automation. The Security Automation Developer Days is a multi-day event that is the primary face-to-face venue for experts to discuss and approve changes or additions to SCAP and other security automation specifications.

The Software Assurance (SwA) Program of the DHS's National Cyber Security Division co-sponsors SwA Forums semi-annually with organizations in the Department of Defense and NIST. [5] The purpose of the forums is to bring together members of the government, industry, and academia with vested interests in SwA to discuss and promote integrity, security, and reliability in software.

Once a year, NIST, DHS, and NSA sponsor the IT Security Automation Conference to give end users from the government and industry an opportunity to learn about how security automation can assist them in meeting their missions and give them the opportunity to interact directly with experts and hear from senior leaders on where security automation is headed.

These activities ensure that the government and industry are able to coordinate the use cases, resources, and technologies necessary to improve cybersecurity through standards and automation.

Looking Forward

While SCAP has achieved some success and continues to evolve to address new needs, it is not intended to solve all the cybersecurity challenges with which we are faced. To expand the goals of security automation further, NIST and its government and industry partners are conducting research and development into new areas. One such area is network event management, called the Event Management Automation Protocol (EMAP). These specifications bring the successful model of SCAP to the network event space, providing standardized methods for classifying event data and how it is communicated, filtered, correlated, and prioritized. EMAP will provide a level of data and tool interoperability that is required for dealing with the vast numbers of events being generated everyday by desktops, servers, routers, firewalls, *etc.*

Security automation has been and continues to be a broad and active effort that brings together the government and industry to solve real cybersecurity challenges today. Security automation lays the groundwork for solving the cybersecurity challenges of tomorrow through the development of best practices, technical standardization, and international adoption. ■

Disclaimer: Certain commercial equipment, instruments, or materials are identified in this report to adequately specify the experimental procedure. Such identification does not imply recommendation or endorsement by the NIST nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

About the Authors

John Banghart, Stephen Quinn, and Kevin Stine support the NIST Information Technology Laboratory (ITL) Computer Security Division (CSD). The NIST ITL CSD provides standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in Information Technology (IT) systems.

References

1. *http://usgcb.nist.gov*
2. *http://checklists.nist.gov*
3. The HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is created, received, used, or maintained by a covered entity by requiring appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
4. The "National Technology Transfer and Advancement Act" and "Office of Management and Budget (OMB) Circular A-119 Revised: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.
5. *https://buildsecurityin.us-cert.gov/swa/index*

Overcoming the Detail Devil through Open Technology Standards

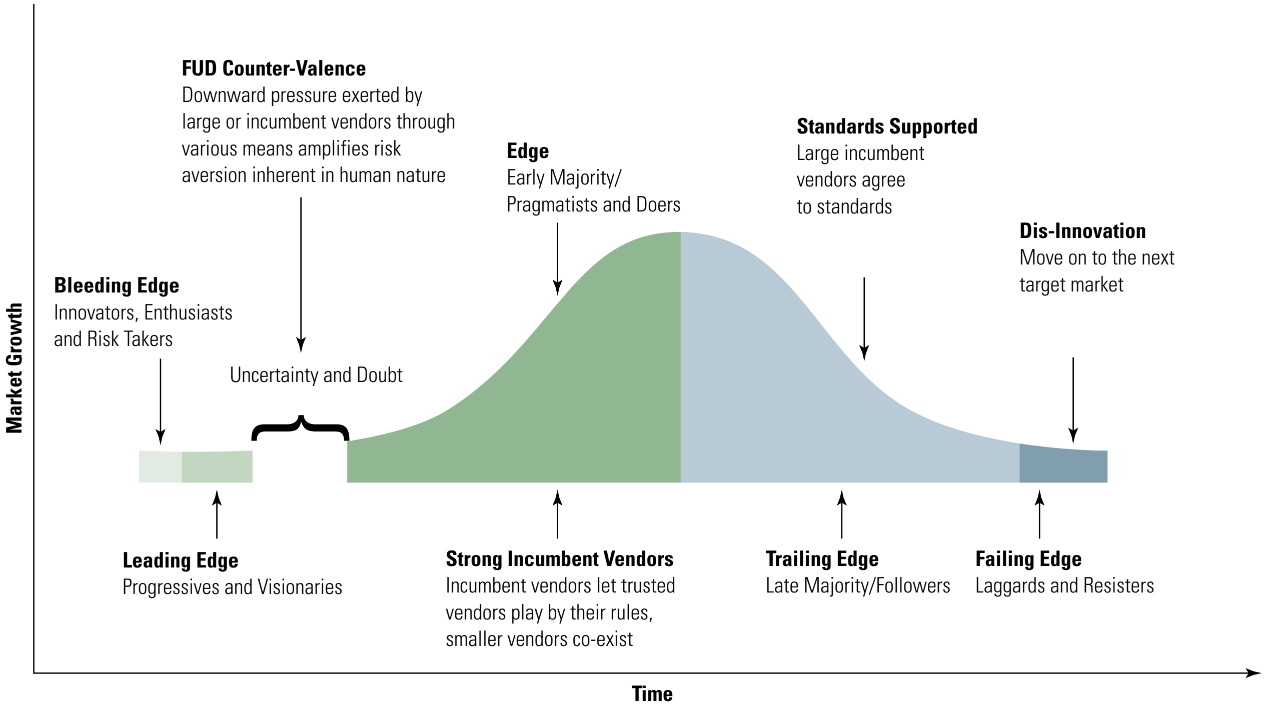
by David O'Berry

It is said that "the Devil is in the details," and this is often the case when key stakeholders broach the concept of standards-based integration for security. Many stakeholders (especially those with significant market interests) either want standards to remain exactly as they are, believe standards slow down innovation, or wonder whether a company may be manipulating a certain standards body for its own benefit. Some argue that developing standards is difficult or that developing standards reduces functionality, which is where many assume that the Detail Devil halts any type of true collaborative, user driven standards attempts.

This article highlights one example of how technology standards enabled a customer to implement a better, cost-effective solution using multiple commercial vendors. It is important, however, to understand the challenges in developing customer- and industry-agreed upon standards to overcome the "Detail Devil."

Standards Development Challenges

Over the last 20 years, customers (not including top federal agencies, the military, or Fortune 500 companies) have not been fully involved in many


Market Growth
Time
FUD Counter-Valence
Downward pressure exerted by large or incumbent vendors through various means amplifies risk aversion inherent in human nature
Edge
Early Majority/ Pragmatists and Doers
Standards Supported
Large incumbent vendors agree to standards
Dis-Innovation
Move on to the next target market
Bleeding Edge
Innovators, Enthusiasts and Risk Takers
Uncertainty and Doubt
Leading Edge
Progressives and Visionaries
Strong Incumbent Vendors
Incumbent vendors let trusted vendors play by their rules, smaller vendors co-exist
Trailing Edge
Late Majority/Followers
Failing Edge
Laggards and Resisters

Original work by David O'Berry with input from Steve Hanna | Adapted from "Crossing the Chasm", Moore, 1991

Figure 1 Technology Dis-Innovation Life-Cycle

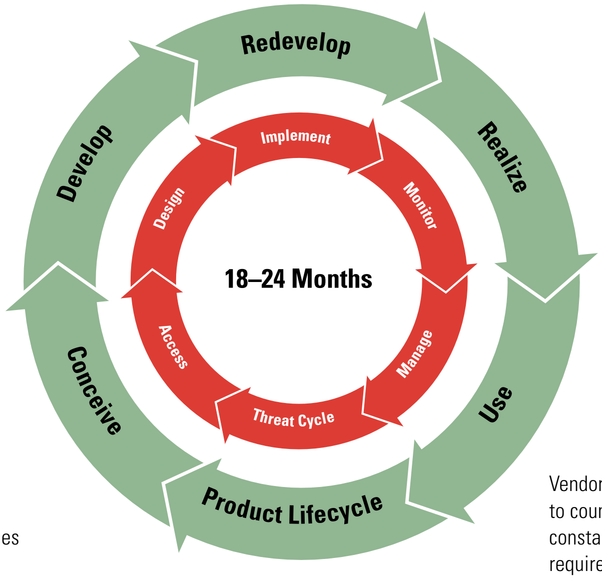
meaningful standards development processes. Overlooking the importance of involving customers has occurred at some of the most forward-looking companies and among standards bodies themselves.

Many individual customers are treated as account numbers within information technology (IT) companies unless they require some type of additional attention whether positive or negative. IT companies need to understand the importance of how much customers can add in developing technology standards.

Historically, the creators/manufacturers of technology and their customers have developed an oddly detached relationship to one another: industry often builds a tool and then convinces customers to purchase it. In many instances, there are limited choices and at times customers fear choosing less well-known solutions. Customers often accept the products and capabilities available. Some companies utilize customer input; however, most companies do not consistently integrate customer input into product development because it does not benefit the company or their shareholders to consider a different model. Companies are also accountable to their owners, which can cause them to overlook the customers or the technology ecosystem.

In the past, larger companies established a market "beachhead," locking customers into relying on certain products and then defending their market share (refer to Figure 1). To some degree, there was nothing wrong with this model in the past; however, we have rapidly moved past that point in time. The interconnected nature of the Digital Industrial Revolution amplifies and extends risks that may have previously been containable by one organization to an incredible number of other enterprises. The potentially devastating ramifications of this new operating model make it absolutely untenable to continue with the old model. Threat cycles are occurring so rapidly that product cycles have no hope of keeping up if businesses and customers continue operating the same way (refer to Figure 2).

Modularity not a main concern: leads to long development lifecycles



Vendor stops and starts with products per internal challenges and market changes

Vendor develops a product to counter a threat; constantly changing threats require new products

Figure 2 Product Cycle vs. Threat Cycle: Modular Frameworks and Standards Required Going Forward

The first step to change requires that key stakeholders join together, work out the details, and develop interoperable standards. Open interoperable standards in the IT industry are viable and fairly simple to implement if there is a mutual effort on both sides of the value chain to do so.

Enabling Customers through Technology Standards

During my role as the Director of Information Technology Systems and Services (ITSS) and then the Director of Strategic Development and Information Technology at the South Carolina Department of Probation, Parole, and Pardon Services (SCDPPPS), my organization adhered to security automation standards whenever possible to give us the agility required to execute our business plan without being forced to rely on companies in the IT industry executing on theirs. The greatest progress that SCDPPPS and the industry made was during a meeting where representatives from the National Security Agency (NSA), National Institute of Standards and Technology (NIST), MITRE, the Trusted Computing Group (TCG), and SCDPPPS sat down and hashed through a pilot project that we thought could make a real impact on the Global Digital Ecosystem as a whole. Tony Sager and Paul Bartock from NSA as well as Steve Hanna from Juniper understood that this time was different and our collaboration would more than likely prove to be a huge turning point for security automation. The meeting demonstrated that while there are huge gaps in our communication and collaboration, living in that state is currently unintentional and certainly undesirable for stakeholders in the future.

The knowledge and ideas put forth from all of the participants of NSA, NIST, TCG, MITRE, and SCDPPPS were impressive. What had been missing and what SCDPPPS was able to contribute as a customer was an outside view of what oftentimes is a fairly closed technology ecosystem within the federal government. Discussions opened up a great deal, and the progress of the planning and completion of the pilot showed what customers, government, and industry can accomplish when working together.

The basic tenet of our success was the integration of NIST'S Security Content Automation Protocol (SCAP) and TCG's Trusted Network Connect (TNC). The most interesting aspect of this integration was how well the two sets of standards fit together and how, in hindsight, this step could have been taken years ago if collaboration had been initiated earlier. Looking back over the past 5+ years, it is discouraging to realize that these two groups and suites of standards were both accomplishing amazing work but were doing so disjointedly. Both SCAP and TNC have strong stories to tell by themselves, but together they open the door for the next version of adaptive and iterative secure configuration management. This collaboration and future work between these groups has the very real possibility of being the foundation for true autonomic security especially if a standardized Network Control Language evolves.

Together SCAP and TNC led to stronger security and more automation than either could have provided by themselves. SCAP's standards for device security management have immense power, and when coupled with TNC's complementary set of network capabilities, SCDPPPS found a rather powerful tool that allowed our enterprise to easily achieve a level of security that was very difficult, expensive, or even impossible to deliver previously: we were able to fully integrate solutions offered by two separate companies. These two companies were incredibly different in size, scope, and mission: one company was extraordinarily small and focused, and the other was incredibly large with a huge breadth of products. They had one thing in common, however, they both supported the standards that SCDPPPS needed and operated together to solve a real world business problem. Although SCDPPPS had been using both companies' products for several years, only after the initial implementation of the pilot were we able to realize our vision of an open, standards-based, fully integrated security automation environment with two companies that barely knew each other before we started.

As the pilot expands and continues to evolve, SCDPPPS expects the integration to not only reduce staff time to deal with increasing compliance management requirements and malware but to also ensure SCDPPPS and other organizations are not required to make exclusive bets on single companies or products. This pilot and the ones that follow should not focus on hard to perform, one-off integration. By approaching this systematically, using the standards and creating the repositories of consumable security data, SCDPPS has a real chance of flipping from 80 percent operations and 20 percent innovation to the exact reverse.

The technology ecosystem needs to commoditize where possible and then use that base foundation to innovate at every juncture, thinking ahead so that we can find proactive solutions. Agility is essential for keeping up with the threat cycle in today's rapidly evolving digital world. The only way one can truly achieve agility is to keep from reinventing the wheel due to thinking our organizations are completely different than others and therefore stove-piped. Industry, government, and customers have to work together and look for the similarities instead of amplifying our differences. Only then will IT evolve in a manner that allows the rest of the world to develop the technological capabilities it needs to function moving forward. The Digital Ecosystem requires this of us and our organizations to survive. Stakeholders can then work out the details by collaboration efforts, helping everyone advance within the technology ecosystem. We, as a profession, must remember and embrace the truism that "a rising tide lifts all boats."

Anytime there are seemingly insurmountable challenges, look around and ask the age-old question: "If not us, who? If not now, when?" You know the answer. Now let us move past the "Detail Devil" and do this together. ■

About the Author

David O'Berry | calls himself a "reformed CIO currently working for 'The Dark Side' as a strategic systems engineer for McAfee." He spent 19 years on the enterprise side as a network manager, director of ITSS, and director of strategic development and IT in the public sector. He is a 2011 ComputerWorld Top 100 IT Leader and has stayed involved in a number of various collaborative organizations in the computing industry like the TCG's Customer Advisory Council, the MS-ISAC Executive Council, and the Open Group. He has been a steadfast advocate for customer involvement in rapidly evolving flexible open standards and speaks at various events on the topic. While he now works for the world's largest dedicated network and computer security company, his thoughts and opinions expressed in this article and anywhere else are his own. He can be contacted at *iatac@dtic.mil.*

Ask the Expert

by Ed Moyle

Information security practitioners—particularly those who have been in the business for a while—likely recognize the importance of personnel screening (*i.e.,* background checks). Any time we provide personnel access to sensitive or critical resources, we are responsible for ensuring that those individuals are trustworthy. This exercise is a staple of information security as a profession. It is one of a select subset of security controls (*e.g.,* firewalls, fire suppression, and ID badges) that are almost universally recognized as a good idea no matter the context, whether you are talking classified versus sensitive but unclassified, public versus private sector, or defense versus civilian agencies.

In the first part of this discussion we provided an overview of employee screening with an eye to some of the general requirements that might drive an organization to adopt this control. This time, we expand to examine some of the complexities in implementation. While background checks may seem simple as compared to some of the more rapidly changing and esoteric technical areas of information security, these security controls can actually be pretty challenging to implement.

> As the amount and intricacy of industry regulations increase, and as technologies like cloud blur the boundaries between organizations, it becomes more important to understand where these areas of complexity are in order to ensure controls are appropriately implemented to safeguard organizational assets.

Beware multiple entry paths

One of the most difficult areas of personnel screening deals with the multitude of types of personnel and the various paths through which they may gain access to the same resources. To illustrate the point, consider the example of a healthcare environment.

In a hospital, how many different ways do you suppose employees are given access to the organizational network? You have medical staff (*e.g.,* physicians), administrative staff, volunteers, contractors/vendors, and patients. Each of these groups has access at varying levels to organizational resources. Is it realistic to conduct the same level of background checks on all staff? What about patients? In practice, what many organizations find is that background checks require specialization. Vendors, in the case of offshoring, may require one type of screening whereas volunteers require another (to keep costs down). As the number of personnel increases, perhaps through greater reliance on service providers or outsourcing, so does the complexity.

It is important to know that the divergence of pre-employment screening—as well as variability in the screening of long-time employees—happens; therefore, it is important for organizations to first understand their internal processes so that onboarding controls make sense. Organizations must also fully examine onboarding procedures at vendors, service providers, and partners when engaging with third parties. Ideally, vetting of coverage (*i.e.,* who gets screened) as well as effectiveness (*i.e.,* how they are screened) is imperative.

Stay within the law

One rule that might not be immediately apparent but makes employee screening more involved is the legal mandates that govern conduct. In the public sector, some of the complexity is offset by long-standing and well-established processes that dictate how they are executed (a Single Scope Background Investigation might take a while, but that is expected); however, outside of that context, there are some tough constraints that rule what information can be asked for and how decisions can be made around ascertaining employment.

Consider the following governing legislation, excepted from the U.S. Equal Employment Opportunity Commission

(EEOC) employment screening fact sheet— [1]

- **Title VII of the Civil Rights Act of 1964**—Prohibits discrimination based on sex, ethnicity, religion, and national origin;
- **Title I of the Americans with Disabilities Act**—Prohibits discrimination based on disability; and
- **Age Discrimination in Employment Act**—Prohibits discrimination based on age.

The EEOC guidance provides background on specific legislative requirements that impact employee pre-screening.

Additionally, some of the EEOC guidance strongly suggests that employers validate candidate credit scores; however, exercise care in this area because the Fair Credit Reporting Act contains provisions for how and why you can use credit information. Notably, you need written authorization before you can do anything. Assuming that you take "adverse action" (*e.g.*, you decide against hiring), you must provide a pre-adverse action disclosure that includes materials mandated by the Federal Trade Commission (FTC), and you must formally notify the employee of the adverse action. Refer to the FTC Web site for useful information on credit validation requirements. [2]

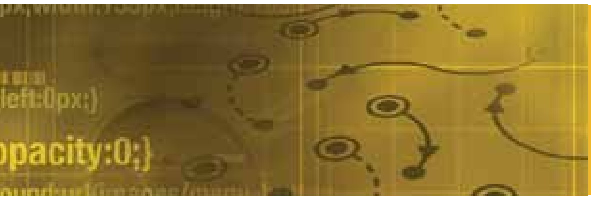
Because of the detailed nature of governing regulation, make sure to carefully vet the processes that you are creating to screen employees. Make sure processes are within the law; involve corporate counsel to ensure that what you are doing is legal and consistent across all personnel. ■

About the Author

Ed Moyle | is a 15+ year veteran of information security as well as an industry-recognized thought leader, advisor, writer, and manager. Mr. Moyle is currently a faculty member at IANS, Senior Security Strategist with Savvis, and a founding partner of SecurityCurve. He can be contacted at *iatac@dtic.mil.*

References

1. *http://www.eeoc.gov/policy/docs/factemployment_procedures.html*
2. *http://business.ftc.gov/documents/bus08-using-consumer-reports-what-employers-need-know*



LandWarNet 2011

LandWarNet 2011 took place August 23-25, 2011 in Tampa, FL. This conference brought together senior leaders from across the U.S. Army, Department of Defense (DoD), the government, and commercial sectors to address "Transforming Cyber While at War."

Attendees had the opportunity to attend one of nine tracks, all of which focused on information assurance related topics and how they impact our combat operations and security. These tracks included—

- Enabling the Joint, Coalition Counter-Insurgency Campaign
- The Year of Action
- Transforming Cyber While at War… We Can't Afford Not To
- See, Know, Do: Network Visibility, Control, and Protection
- The Power to Connect
- Transforming Cyber Capabilities
- Transforming the SIGNAL Regiment
- Tactical
- Army Knowledge Management.

Reputable speakers from across the Army, DoD, and industry participated in this conference. Lieutenant General Susan S. Lawrence, the Chief Information Officer (CIO) for the U.S. Army, delivered the opening remarks. The Honorable Duane Andrews, Chief Executive Officer (CEO) of QinetiQ North America, moderated an industry panel with participants from Booz Allen Hamilton, BlueCoat Systems, Adobe, Harris, and Northrop Grumman.

Other notable speakers included Admiral William H. McRaven, U.S. Navy Commander, U.S. Special Operations Command; Teri Takai, DoD CIO; LTG Carroll F. Pollett, U.S. Army, Director of Defense Information Systems Agency; John T. Chambers, Chairman and CEO of Cisco; and LTG Rhett A. Hernandez, U.S. Army, Commanding General, U.S. Army Cyber Command/2nd Army. [1]

LandWarNet's format will change drastically in the future. Due to budget constraints, this conference will be scaled down into smaller, more focused events. Organizers also plan to leverage social media and various technologies to enhance participation in the future. [2] ■

References

1. *http://www.afcea.org/events/landwarnet/11/intro.asp*
2. Lawrence, Susan, LTG, U.S. Army. LandWarNet, Tampa, FL. 23 August 2011. Opening Remarks.

Evaluating the Benefits of Network Security Systems

by Soumyo D. Moitra

Network security has clearly become a key issue for all organizations in the face of a variety of cyber attacks. An important aspect of network security is the monitoring of network traffic with sensors. In this article, we use the term, *sensor,* to include network security systems that monitor traffic, process the data, and issue alerts if there are any suspicious patterns. These systems often provide security analysts with additional information to help them identify incidents and respond to them; therefore, sensors play a crucial role in network security and information assurance (IA).

Sensors constitute a significant investment, especially if the associated maintenance, monitoring, and training costs are taken into account. Some sensor systems are expensive, and in some cases, an organization may need many sensors. In view of constrained resources, there is a need to justify these expenditures. Decision makers in charge of budgets need to justify expected returns from network sensors—they need to understand the cost-benefits from deploying sensors. In fact, Admiral Mullen has recently noted that we need to optimally apply our resources. [1]

To make the best decisions, it is essential to have metrics by which we can estimate sensor effectiveness. There are many complex issues related to the acquisition and deployment of network sensors. It is important to develop a model that helps with these decisions. There are a number of related decisions: Are expenditures on sensors justified? Are they providing the best value for our money given our security needs? These are decisions that will have to be made on a regular basis since cyber attacks are expected to continue. Given the investments involved, better decisions have a significant effect in improving network security, making it imperative that we have a cost benefit model. In this article, we describe such a model that we have developed in the CERT Network Situational Awareness Group (CERT/NetSA) at the Software Engineering Institute (SEI), Carnegie Mellon University. [2] Although the model was originally developed for sensors, it can be applied to network security decisions generally.

Metrics for Sensor Benefits

The model derives metrics to estimate the value of having a sensor at a particular location. While there have been a number of studies in this area [3] [4] [5] [6], they focus on the private sector and do not address Department of Defense (DoD) concerns. Assumptions made for the private sector may not hold for DoD; the value of sensitive information is of particular concern within DoD. Additionally, while there has been considerable interest in this topic, past studies have not been comprehensive in terms of categories of attacks, kinds of damages that cyber attacks can cause, and realism of the data used. [7] [8] [9] [10] A useful metric in this context should also reflect the uncertainties involved as well as the attack detection and response process. The model described in this article represents a comprehensive methodology that identifies the key dimensions and the critical factors that are involved; it also provides a uniform and consistent method of making these assessments comparable across organizations and over time.

This model represents a balance between complexity and tractability, allowing it to be widely used by decision makers, but difficulty lies in the lack of data to estimate the model and compute the metric. Currently, very little of the relevant data needed is available, and it is difficult to collect. This model, however, precisely identifies the data items needed, which helps in collecting future data. The National Institute of Standards and Technology (NIST) report has recommended such an approach, noting the need to advance the "state-of-the-art" in security metrics. [11] This approach can assist in the data collection and analysis efforts as well as in prioritizing security expenditures.

While various metrics have been suggested to estimate the benefits of information security (*e.g.*, Annualized Loss Expectancy [ALE]), the financial literature generally recommends Net

Present Value (NPV). The metric developed here is equivalent to NPV for one time period, which is the time horizon we consider, which corresponds to the Return on Security Investments (ROSIs) that is often used in the economics of information security literature. [12] [13] [14] [15] If multiple time horizons have to be considered, the standard NPV model can be used with the appropriate discount rate. This decision-making approach could be incorporated into security automation since that will involve making certain decisions automatically through some program or algorithm. A model like this could be embedded in the automation process and could facilitate these decisions and make them more effective by including the relevant tradeoffs.

A Model to Evaluate Benefits

The model applies the economic perspective of cost-benefit analysis. The benefits from having a sensor derive from the reduction in expected losses that we may expect by deploying the sensor. Having the sensor system in place will presumably improve the ability to detect, respond to, and mitigate the impact of cyber attacks; therefore, we estimate the expected losses without the proposed sensor—with the current security infrastructure—and also the expected losses with the sensor in place. The difference is the reduction in expected losses.

Expected losses can be expressed in the simplest form:

Expected loss per event = (probability of an event) × (consequence of that event)

The model takes into account different attack categories (based on the DoD categorization) and different sources of losses (*e.g.*, hardware, software, loss of communications, loss of information, *etc.*). The rates at which the different attacks are experienced are also included in the computation. The model is necessarily probabilistic, given the uncertainties involved and the random nature of attacks. An event tree was constructed that took into account the probabilities of detection, prevention (no loss), and partial protection. Different degrees of mitigation were also considered. The model structure is such that it facilitates sensitivity analysis, allowing decision makers to explore “what-if” questions.

In basic terms, we estimate the expected loss without the proposed sensor as:

$$D- = N(i)*d(i)$$

Where *N(i)* is the number of attacks of category *i* over a unit time period and *d(i)* is the expected loss (or damage) from attack *i*. The event tree allows us to compute *d(i),* taking the various probabilities into account and also different types of damages or sources of loss. Full details can be found in Assessing the Value of Deploying Network Sensor Systems or from the author. [16]

With the proposed sensor in place, we again compute the new expected loss as:

$$D+ = N(i)*d'(i)$$

Where *d’(i)* is the expected loss in this case.

The expected benefit then is:

$$B = [D-] – [D+]$$

which is the difference in the expected losses.

The model is in the form of a template. Users can enter the relevant data for their organization and estimate the effectiveness and benefits from proposed sensors in the planning phase. The results are location specific since the expected losses or damages depend on the characteristics of the location where the sensor is to be deployed. The model can be extended in a variety of ways to include additional attack categories or other damage types. Since many of the parameters are uncertain [17], we have performed a variety of sensitivity analyses. The following section summarizes the results of the model.

Summary of the Results

A particular dollar value for the estimated benefit from a sensor by itself is not meaningful since a number of variables influence it, and these variables will be different from case to case. What is useful is to show how the benefit changes as the variables change; therefore, we present the results of two sets of sensitivity analyses from a larger set of analyses we have conducted. [18] We focus on two key variables: the rate of attacks and the value of information to be protected by the sensor. Figure 1 shows the results of estimating the metric as the total number of attacks increases. These values are for illustration only and should not be construed to represent real cases. The ranges of the values for attack rates, potential damages, and value of information were based on secondary data and expert judgment. [19] The ranges are wide enough to cover most values an organization would encounter. Any organization applying this model, however, would enter values appropriate to itself, estimating the value to itself by placing a sensor at a candidate location on its network.

Three scenarios have been considered and depicted in Figure 1. The straight line (B1) represents the increase in the benefits from a sensor as the attack rate increases. This is as expected since as the rate increases, the greater the expected number of attacks will be detected. As a result of the detection by the new sensor, responses can be taken to mitigate the impact and hence the value of the new sensor will increase with the attack rate; however, this linear relationship may not hold in reality. In reality, as an IA center sees more attacks, it can take a number of precautions and apply other methods of controlling the impact. It may institute additional safeguards such as moving sensitive data to a safer storage location. Additionally, the damage caused by two attacks can sometimes be less than the sum of the damages each would have caused by itself. This effect can be modeled by having benefits increase less than linearly with the attack rate. This is shown by the sloping curve (B2) below the straight line. It is important to recognize this possibility since otherwise the benefits from a sensor may be overstated.

Finally, there can be a scenario with exactly the opposite effect. We particularly consider the case of data exfiltration. One piece of information (extracted by one attack) may not be very valuable by itself. If an adversary obtained multiple pieces of information, through multiple attacks, they might be able to put the pieces of information together and cause severe harm; therefore, the benefits of protecting the information increases more than linearly with the number of attacks. This effect has been modeled in the curve (B3), where the benefits are shown to increase rapidly according to a power term. Again, if such a scenario might hold for an organization, then it is important to recognize and analyze this effect. This scenario assumes that the sensitive data is constantly available at the target. Either of the non-linear cases can hold in reality; therefore, this kind of analysis can give a more accurate insight into potential damages and the benefits from sensors.

To interpret Figure 2 correctly, it is important to keep the following points in mind: 1) These are hypothetical scenarios to illustrate the model and should not be construed as real cases. 2) Higher levels of benefits correspond to cases where there are a large number of attacks and where valuable sensitive information is on the network all the time. This would correspond to a very large network, perhaps most DoD systems, with multiple access points to the Internet or other external networks. 3) Most importantly, the results would hold only if the sensitive information is always available on the network and vulnerable to exfiltration. 4) The model assumes that subsequent data exfiltration exploits cause as much damage as earlier exploits. This linear effect will usually not be true since, if sensitive information is compromised once, most or all of the damage that could be done has been accomplished. In this latter case, the subsequent damages will not be as great as earlier ones; therefore, the value of the sensor, which is there to reduce these possible damages, will be correspondingly lower. The high values for benefits should then be treated as extreme cases. If multiple

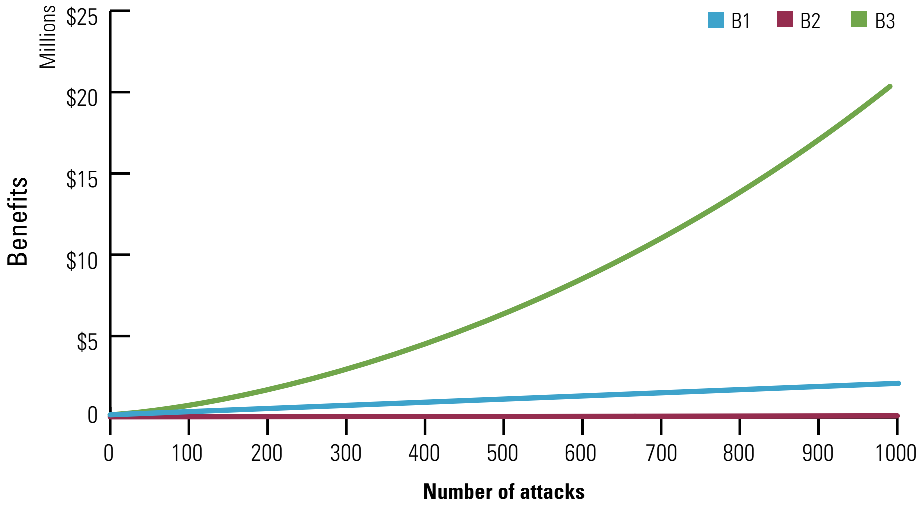


Figure 1 Variation in benefits (B) as attack rate (N) varies

adversaries are involved, it will represent an intermediate case.

Another important concern is the variation in the value of sensitive information (VOSI) from organization to organization. From secondary data and elicitation of expert opinions, the potential damages from the other sources of damage (*e.g.,* hardware or software) tend not to vary that much from any one attack. The potential damage from data exfiltration, however, can vary enormously and can be much greater than damages from just hardware or software; therefore, we have considered a range of values for damages from loss of sensitive information, and Figure 2 shows how benefits (B) vary as attack rate and VOSI vary. The range of values for VOSI are reasonably conservative (up to $300,000) compared to values stated in the media, and we can observe the combined effects of the attack rate and VOSI on the expected benefits from a sensor from Figure 2; however, considerable caution has to be exercised in interpreting the numbers in Figure 2. The model assumes that the damage done increases (linearly) with the number of attacks. For example, twice the number of attacks will cause twice the amount of damage; however, this assumption may not hold in cases where once sensitive information is lost, subsequent attacks may not cause further damage (as most of the damage has already been done). In such cases, the realized benefits may be considerably lower and would correspond to those only for a small number of attacks since later attacks. The model can still be used, but care must be taken when applying the model to ensure that all the assumptions are met. This kind of analysis should help in prioritizing the allocation of limited resources on sensors. Note that the estimated benefit (B) for having a sensor should be viewed as a break-even point. Only if the total cost of acquiring and deploying a sensor is less than B for an organization will it be worthwhile for the organization to have the sensor. The total cost related to having a sensor is actually very complex to calculate because it should include many elements such as hardware, software, installation, configuration, warranties, maintenance, upgrades and patches, monitoring, operational overheads, and the costs of having network security/IA analysts processing the output of the additional sensor. These often add up to a considerable amount, and this total amount needs to be recognized as the full cost of deploying sensors.

These results demonstrate the applicability of this model. In applications, each organization would use the input values appropriate to it. This article has briefly described how the model works and how it can benefit network security decision makers. They can determine the break-even point for acquiring sensors, use the results to justify resources for sensors, and use the model to help them in prioritizing the allocation of sensors when not all needs can be met.

In practice, if the benefits are to be estimated in monetary terms, actual dollar values are needed; however, such data may not be available or difficult to estimate. As an alternative, scaled values or indices can be used to estimate expected damages and the model will provide an estimate of benefits on a scale. In such case, the output is more correctly an effectiveness measure. When used consistently, it can serve some of the same purposes; therefore, the effectiveness can be compared across locations and sensors can be deployed according to a priority.

Such data should be collected because it is vital to effective security management. The use of the model will help identify the data needed for such security decisions. The method can be generalized to consider resource allocations at other levels of decision making as well. In fact, this methodology can help automate the investment decisions with respect to network security. Organizations could develop a database for the model inputs and can implement the model as a template. Managers can then run the model to assess the benefits of proposed security investments and explore "what-if" questions.

Conclusions

The model incorporates a number of advances beyond previous examples:

- A novel model of incident detection and response: managers can get insights into the whole incident handling process in their organization. They can evaluate the effect of different values of the

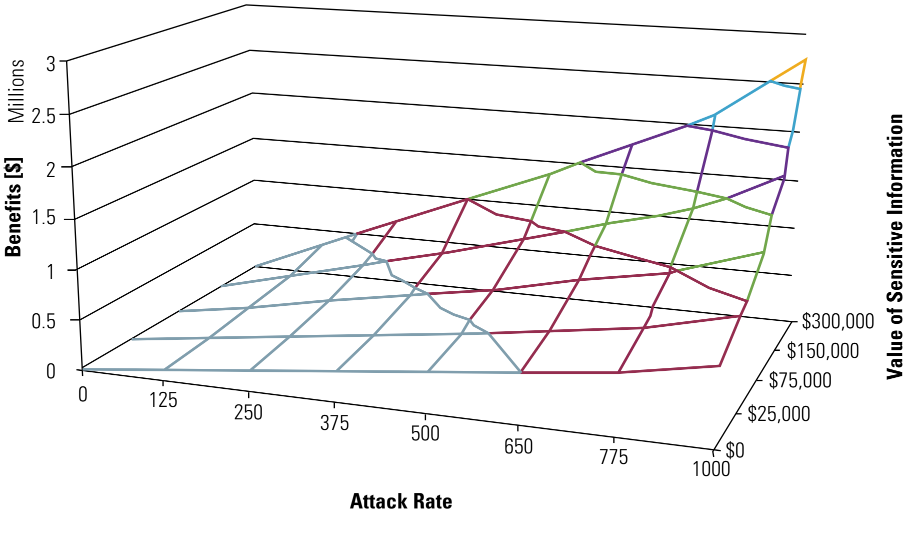


Figure 2 Variation in benefits as total attack rate and VOSI vary

parameters that reflect the effectiveness of incident handling and response. They can also identify ways to increase their effectiveness efficiently.

- A comprehensive set of attack categories and sources of damages from cyber attacks.
- A probabilistic treatment and sensitivity analysis; key parameters can be identified easily as benefits will be more sensitive to their values.
- Care needs to be exercised when applying the model to ensure that its assumptions are satisfied and the results need to be interpreted with caution as explained above.

The benefits of this model include the following—

1. Directly relevant to DoD (*e.g.,* VOSI is considered explicitly);
2. Provides a realistic range of values of the variable of interest (return/benefit from sensors);
3. Makes a significant positive contribution to network security by making decisions more effective;
4. Implications for any sensor strategy, and the results of the model can provide relevant inputs for effective defense-in-depth designs; and
5. Some managerial decisions on expenditures and resource allocation across alternatives might be automated, which expedites decisions that have to be repeatedly.

Challenges

The primary challenge in applying this model is that it is relatively data intensive. It requires an estimation of the different damages that may be caused by different attack types. It requires data on the rate of cyber attacks, and it requires information on the probabilities of detection of the attacks, probabilities of prevention given detection, and probabilities and degrees of mitigation. Most organizations do not collect data at this level today even though this data is necessary for effective security policies. Additionally, there is no standard methodology for collecting this data comprehensively. This data is needed at the organizational level, where security decisions about networks are made. It is hoped that by highlighting the usefulness of this kind of data, there will be a movement to collect it. As security automation evolves, a synergistic relation between it and this methodology may develop where the automation could provide inputs needed for the model. For example, Security Content Automation Protocol, developed by NIST, envisages various security measurements that include some of these inputs. [20]

We also need better ways to assess VOSI. This is of course a particular concern of the DoD, and some research has been done by CERT/NetSA in the SEI at Carnegie Mellon University to develop a standard methodology for this.

Sensitivity analysis is always important given the uncertainties and the dynamic environment in the area of cybersecurity. More such analysis is needed including research on interactions among the variables included (*e.g.,* the number of attacks experienced and the potential damage to sensitive information). In general, the model should be extended to reflect additional complexities of evolving networks and attack techniques.

Finally, there is a need to integrate this approach into security decision making by achieving a consensus among all stakeholders to include these considerations. Intuition often fails us in complex situations, and models like this offer a practical approach to more cost-effective decisions about network security. ■

About the Author

Soumyo Moitra | is a Senior Member of Technical Staff in the CERT Network Situational Awareness Group at the SEI, Carnegie Mellon University. He has applied operations research models in a number of areas including policy analysis, telecommunications, and technology management. He is currently working on various aspects of network sensors, network traffic analysis, and workflow models. He can be contacted at *smoitra@cert.org.*

References

1. Mullen, Admiral M., "Armed with OR," OR/MS Today, August 2010.
2. Moitra, S., "Assessing the Value of Deploying Network Sensor Systems," CERT/NetSA, Software Engineering Institute, Carnegie Mellon University, 2010. (Details available from author).
3. Arora, A., *et al.,* "Measuring the Risk-Based Value of IT Security Solutions," IT Professional, Nov-Dec, 35-42, 2004.
4. Bayuk, J., "Security Metrics: How to Justify Security Dollars and What to Spend Them on," Computer Security Journal, XVII, 1, 2001.
5. Hoo, K. J. S. "How Much Is Enough? A Risk-Management Approach to Computer Security," Working paper, CRISP, 2000.
6. McLean, G. and Brown, J., "Determining the ROI in IT Security," CA Magazine; Apr2003, Vol. 136 Issue 3, pp14-19.
7. Brotby, W. K., Information Security Management Metrics, CRC Press, Boca Raton, 2009.
8. Gordon, L.A. and Loeb, M.P., Managing Cybersecurity Resources, McGraw-Hill, New York, 2006.
9. Herrmann, D. S., Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI, Auerbach, 2007.
10. Jaquith, A., Security Metrics: Replacing Fear, Uncertainty and Doubt, Addison-Wesley, 2007.
11. Jansen, W., "Directions in Security Metrics Research," NISTIR7564-2009, NIST.
12. *Ibid. (see reference 3)*
13. *Ibid. (see reference 7)*
14. *Ibid. (see reference 8)*
15. ANSI, "The Financial Impact of Cyber Risk," ANSI, 2008.
16. *Ibid. (see reference 2)*
17. *Ibid. (see reference 15)*
18. Ryan, J.C.H. and Ryan, D.J., "Expected Benefits of Information Security Investments," Computers & Security 25, 579-588. 2006.
19. Paquet. C. and Saxe, W., The Business Case for Network Security: Advocacy, Governance and ROI. Cisco Press, 2004.
20. *http://scap.nist.gov/*

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 ______________________________

Organization ______________________________

Address ______________________________

____

____

DTIC User Code ______________________________

Ofc. Symbol ______________________________

Phone ______________________________

E-mail ______________________________

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 **□ 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
□ 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)
□ Computer Forensics (soft copy only. DTIC user code MUST be supplied before this report is shipped)

State-of-the-Art Reports (SOARs)

□ Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain (DTIC user code must be supplied before this report is shipped)
□ Measuring Cybersecurity and Information Assurance
□ The Insider Threat to Information Systems (DTIC user code must be supplied before this report will be shipped)
□ A Comprehensive Review of Common Needs and Capability Gaps
□ Software Security Assurance
□ 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

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

Volumes 12	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 13	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 14	□ No. 1	□ No. 2	□ No. 3	□ No. 4

SOFTCOPY DISTRIBUTION

The following are available by e-mail distribution:

□ IADigest
□ Research Update
□ Cyber Events Calendar
□ Technical Inquiries Production Report (TIPR)
□ IA Policy Chart Update

Fax completed form to IATAC at 703/984-0773

IATAC

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

Calendar

November

CSI 2011 Annual Conference
6-11 November 2011
Washington, DC
http://gocsi.com/events

NSA OPS 1
15 November 2011
Fort Meade, MD
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00PCJ2

USSTRATCOM Cyber and Space Symposium
15-17 November 2011
Omaha, NE
http://www.afcea.org/events/stratcom/11/introduction.asp

December

ACSAC 2011
5-9 December 2011
Orlando, FL
http://www.acsac.org

2011 Law Enforcement & Homeland Security Conference and Tech Expo
7-8 December 2011
Chantilly, VA
http://www.ncsi.com/lehs11/index.html

Enterprise Mobility Conference & Expo
8 December 2011
Washington, DC
http://download.1105media.com/gig/Events/Mobile2011/Mobile_LP.html

SANS Cyber Defense Initiative 2011
9-16 December 2011
Washington, DC
http://www.sans.org

January

International Conference on Cyber Security
9-12 January 2012
New York, NY
http://www.iccs.fordham.edu/

SANS North America SCADA 2012
21-30 January 2012
Lake Buena Vista, FL
http://www.sans.org

DoD Cyber Crime Conference 2012
20-27 January 2012
Atlanta, GA
http://www.dodcybercrime.com/12cc/overview.asp

February

NDSS Symposium 2012
5-8 February 2012
San Diego, CA
http://www.isoc.org/isoc/conferences/ndss/12/

CT-RSA 2012
27 February– 2 March 2012
San Francisco, CA
http://ctrsa2012.cs.haifa.ac.il/

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