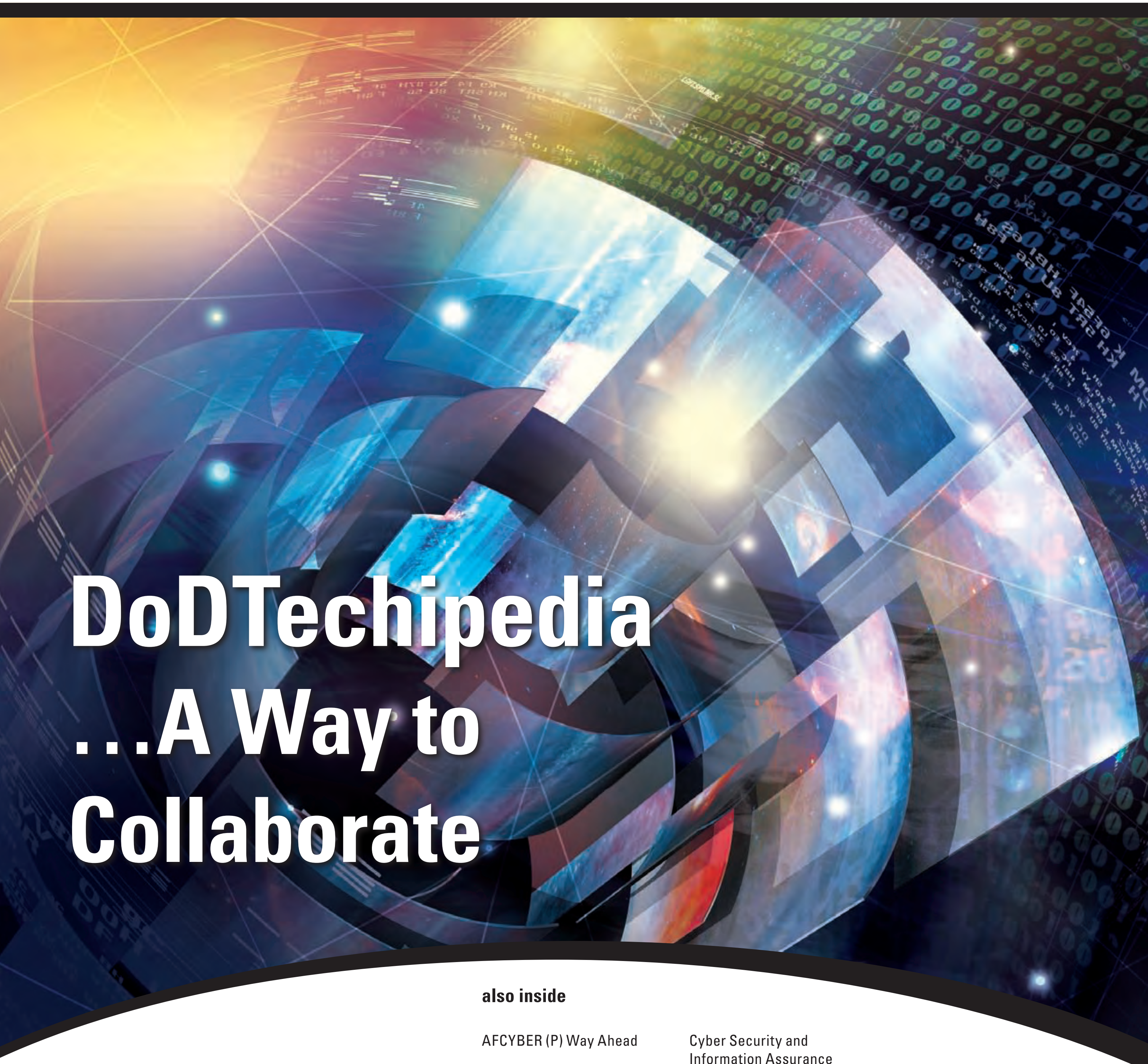
12/2

Volume 12 Number 2 • **Summer 2009**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



DoDTechipedia ...A Way to Collaborate

also inside

IATAC

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

DEFENSE TECHNICAL INFORMATION CENTER

contents

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

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

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

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

***IAnewsletter* Staff**

Promotional & Creative Director:	Christina P. McNemar
Art Director:	Don Rowe
Copy Editors:	Christina McNemar Lindsay Marti
Designers:	Don Rowe Ricardo Real Azadeh Pajouhesh
Editorial Board:	Dr. Ronald Ritchey Angela Orebaugh Dennis Storey 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

Spring 2010	September 4th, 2009
Cover design:	Azadeh Pajouhesh
Newsletter design:	Donald Rowe

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

in every issue

IATAC Chat

Gene Tyler, IATAC Director

Since the last time we had a chance to "chat," much has happened in the information assurance (IA) community. I want to take this time to talk about two big topics—the annual Department of Defense (DoD) Information Assurance Symposium (IAS) held in Dallas, TX, the first week in February this year and the DoD IA Strategic Goals. Either of these could be a full article, or even make up the foundation of an entire edition, but I thought I should take this opportunity to say a few words on each.

As with every IAS, this one was bigger and better with over 1,000 attendees, 85 vendor demonstrations/displays, interesting and timely talks by DoD's senior IA leadership, and group discussions in the various tracks. The IAS structure included an Early Bird Session with five snapshot topics—For Official Use Only (FOUO) Guidance for Identifying, Marking, and Safeguarding FOUO; The Web and Its Danger to the Department of Defense; Comprehensive National Cybersecurity Initiative (CNCI) Initiative 7; Workforce Improvement Process Office of Primary Responsibility (OPR) POC Meeting; and DIACAP Training. A series of large group sessions were held each morning where seniors talked on important IA topics. The core of the symposium was the grouping of four tracks to work important issues. IAS Tracks were—

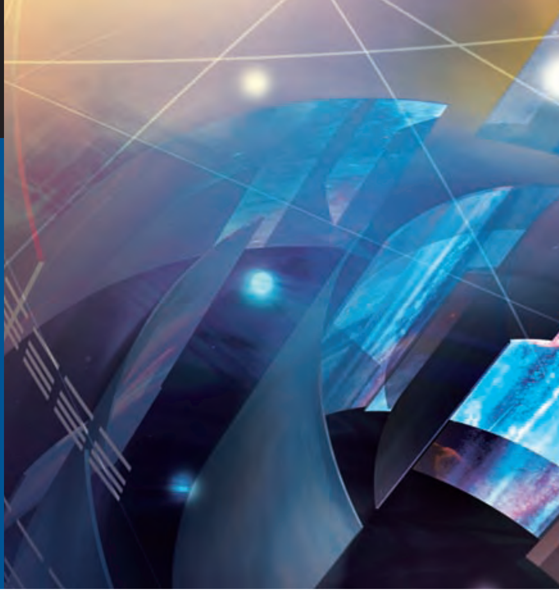
- Track One–Protect Data and Networks–Critical Weapons in Today's Modern Warfare. This track aligned with DoD IA Strategic Goal 2–Anticipate and prevent successful attacks on data and networks.
- Track Two–Respond to Attack/Events–The Cyber Arms Race. This track aligned to Goal 3–Maintain mission operations despite cyber attack or degradation.
- Track Three–Secure Information Exchange–Signed, Sealed, Delivered–Secure! This track aligned to Goal 1–Secure the flow of information across dynamic mission environments.
- Track Four–Information Assurance Enablers–Don't Trust Anyone Without Them. Track four aligned with Goal 4–Guide, govern, and partner for a battle-worthy environment; and Goal 5–Develop and sustain the cyber workforce.

Although this IAS is over, its topics are enduring points where work and resolution are ongoing. Please provide related input to your service, agency, or combatant command leads for these topics. Another annual IA symposium will take place February 2010. When we know the exact date, location, and topics, I will provide information in the *IAnewsletter*, IA Digest, IA/IO Events Scheduler, our website, and other means. With over 1,000 attendees, the organizers of the symposium and the track leads will need your focused help—to ensure the right persons are attending and to ensure they bring the requisite knowledge to move these (and new) topics forward. I hope to see you all at the next IAS—they are exciting and worth your time.

The second major point I wanted to talk about is the DoD IA Strategy. You can see from the IAS that this year's focus revolved around the current DoD IA Strategy. It has been around for a number of years and since requirements evolve over time, the IA leadership of DoD wants to ensure the strategy is flexible enough to accommodate evolving requirements; after over five years, it is time for a strategic review. With that in mind, senior DoD IA leaders are looking at updating the strategy. I do not know what it will look like, but I assure you it will be comprehensive. IATAC and the *IAnewsletter* produced an entire edition focused on the DoD IA Strategy (Volume 8, Number 1, Summer 2005)—we will work with DoD's IA leadership to present any changes. Stay tuned to IATAC and the *IAnewsletter* for updates and information on this and other topics.

Again, you will find many articles of interest—our intent is to cover as much of the IA waterfront as possible. We are featuring Duke's IA program and a subject matter expert from Duke, a very good article on DoD's wiki, DoDTechipedia—I encourage you to make this your IA wiki (*https://www.dodtechipedia.mil/dodwiki*). Finally, we have two articles that should pique your interests—an article that describes our next State-of-the-Art Report (SOAR) for IA Metrics and a revealing article about an IA wargame. I look forward to hearing from you in the future. ■

Gene Tyler



DoDTechipedia…A Way to Collaborate

by Tzeyoung Max Wu

The heavy convoy grinds through the dusty path along the southern outskirts of Baghdad, wheels of the personnel carriers send dust wafting towards the horizon. Date palm trees along the row of yellow houses make it almost seem like Florida. But it's definitely not tourist season here. Windows are covered, and aboard the humvees, with noses glistening with sweat, US Marines sit poised, ready to communicate back to command center in a moment's notice using radio over Internet Protocol (IP) routed network (RIPRNET) equipment. RIPRNET is a revolutionary wireless IP-based communications system that reliably extends communication ranges for convoys from the traditional line-of-sight radio range of 10 miles to over 1,000 miles, all without the need for multiple manned relay points, thereby minimizing costs and, more importantly, saving lives.

On the other side of the world at Cape Canaveral, men in bright blue uniforms scurry along the main launch tower. Storage tanks pump a Delta II rocket with enough cryogenic fuel to rip the rocket out of Earth's unrelenting grasp, delivering a new Navstar satellite safely into orbit. Equipped with reprogrammable processors and anti-jamming devices, the brand new satellite will join ranks with Global Positioning System (GPS) constellations, transmitting detailed imagery and pinpoint positioning to terrestrial receivers.

In a university laboratory in New York City, forensic engineers pore through piles of statistical reports generated *via* ForNET, a pioneering forensics data-monitoring and analysis system uncommonly useful in detecting botnets, stealthy attacks, and exfilteration detection incidents. A new tool in the arsenal, ForNET represents the next step in the ongoing race between malicious attackers and defensive administrators.

This is just a sampling of article topics found in DoDTechipedia. DoDTechipedia is a wiki, designed by the Department of Defense (DoD), that facilitates increased communication and collaboration among DoD scientists, engineers, program managers, acquisition professionals, and operational warfighters. In October 2008, at the direction of the Honorable John J. Young, Jr., Under Secretary of Defense for Acquisition, Technology and Logistics, the Director of Defense Research and Engineering (DDR&E), and the Defense Technical Information Center (DTIC) officially announced the launch of DoDTechipedia. This is where you can find information on topics such as RIPRNET, satellite programs, and ForNET.

Indeed, from military bases to research labs to battlefields, exciting ground-breaking work is being done in technology, every single day and all around the world to support our country's national, political, technological, and military objectives. Each year, DoD invests more than $10 billion in science and technology research and development. Universities channel the world's best and brightest minds toward innovation, and in the spirit of entrepreneurship, private firms compete toe-to-toe in sponsoring research and bringing new products to market. Even as technology shrinks our world, technology itself becomes ever more complex.

> DoDTechipedia is a wiki, designed by the Department of Defense (DoD), that facilitates increased communication and collaboration among DoD scientists, engineers, program managers, acquisition professionals, and operational warfighters.

Amidst accelerating changes, it becomes critical for those in DoD to stay abreast of ongoing and even past developments and research. With foreign militaries developing their own net-centric systems and enhancing technical capabilities, it becomes all the more challenging to maintain our own edge—staying ahead of the curve. Essentially, the key is to foster a creative and innovative environment with researchers and technical managers collectively collaborating and brainstorming fresh ideas. Dangers manifest especially when researchers become myopic. Our nation's security is at stake. In the words of Mr. Young, "Where our adversaries don't labor under all the traditional ideas, processes and behaviors that we have in the system, they are capable of adapting new methods and technology in days, hours, in some cases, and certainly weeks. Our processes don't measure themselves in those time lines." Mr. Young also added that "The real power is to ensure we share technical information and lessons on best practices in design, testing, manufacturing and maintenance."

Capabilities

Mr. Paul Ryan, DTIC Administrator, said, "DoDTechipedia is an opportunity for the Department of Defense to take advantage of wiki technology to share science and technology knowledge more efficiently."

More specifically, the following goals have been identified for DoDTechipedia—

- Increase communication and collaboration among DoD scientists, engineers, acquisition professionals, and warfighters to bring capabilities to the warfighters more rapidly
- Identify solutions to technological challenges that enable the DoD enterprise to provide greater capabilities to the warfighter
- Provide an opportunity for US Government employees and their contractors to network with the DoD science and technology community

DoDTechipedia enables DoD personnel to collaborate on technology solutions, reduce costs, add capability more rapidly, and avoid duplication of research and effort. To support the site, every working day of the week, site administrators and content managers actively review content and article formatting for accuracy and consistency. DoDTechipedia boasts the following features—

- Sandbox for wiki users to practice editing
- Quick registration for users with a Common Access Card (CAC)
- Acronyms/terminology pages
- Technology area pages
- Country pages
- Personal, technology area, and country blogs
- Organization pages
- Interest area pages
- Ability to upload attachments including documents, spreadsheets, images, and video
- Ability of all registered users to make direct changes and add new pages on the subject matter of their choice
- Ability to propose new topics/subject areas

Indeed, the demand for this wiki site was apparent on the very week of its launch when over 1,500 users connected to DoDTechipedia.

Of course, the final applicability of DoDTechipedia and achieving Mr. Young's goals depend on the efforts of all of us. Still at its infancy, there is much room for DoDTechipedia to grow.

So go ahead! Share your knowledge, assist a colleague, ask a question, post an event, blog, and be part of the cutting-edge development of the DoD's premier knowledge network. To ensure the most advanced technologies get to the warfighter tomorrow, collaborate on DoDTechipedia today. After all, when it comes to our national security, we need all the resources we can get.

Logging in

Users may access DoDTechipedia *via https://www.DoDTechipedia.mil.* The site is open to all DoD employees, DoD contractors, federal employees, and federal contractors. DoD personnel with a CAC may click through a self-registration process. Registered DTIC users have already been pre-registered to access DoDTechipedia. If you are not registered with DTIC and do not have a CAC, begin the process at *https://register.dtic.mil/DTIC*.

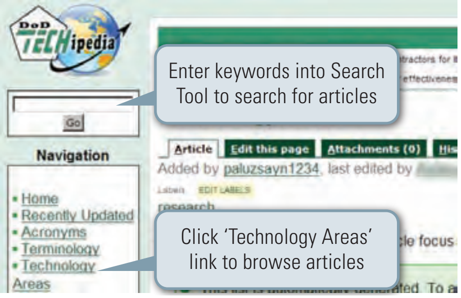
To log in, insert your CAC, or alternatively, enter your DTIC user ID and password. New users may sign up for access by following instructions in the 'registration' link.

Once logged in, users have access to the interactive encyclopedia, blogs, and much more. Most features in the wiki site may be accessed *via* the Navigation Panel on the left-hand side.

After surveying trends across industries, administrators for DoDTechipedia have identified 23 major technology areas for the categorization of articles. New pages can be created as sub-pages within each. By no means comprehensive, new technology areas have also been added over time.

Original Technology Areas

- Advanced Electronics
- Armor Technology
- Augmented Reality
- Biometrics
- Combating WMD
- Data Mining
- Directed Energy Technology
- Electro-Optical Infrared Sensors
- Energetic Materials
- Energy and Power
- Foundational Sciences
- Human Performance and Cognitive Enhancements
- Information Assurance
- Information Warfare
- Manufacturing Science and Technology
- Metamaterials
- Monitoring Marine Environments
- Networking Technology
- Networking Unmanned Vehicles
- Radar
- Robotics
- Sensor and Data Fusion
- Specialty Materials for Airships


Enter keywords into Search Tool to search for articles

Click 'Technology Areas' link to browse articles

Figure 3 Finding Articles

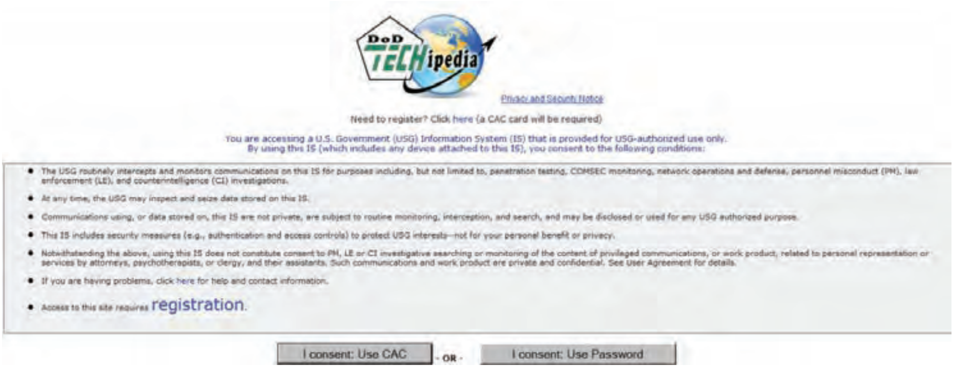
Users may add additional technology areas by clicking "Add a page" at the top of the main "Technology Areas" page.

All articles may be perused *via* browsing, but users can also search for specific articles by entering keywords into the search tool.

Information Assurance, Information Warfare, and Networking Technology

The year 2008 saw the creation of the classified National Cyber Security Center under the Department of Homeland Security. In that same year, a major computer virus shut down operations in two major hospitals in London, malware activity sharply increased globally, attacks continued on federal systems, and additional federal policies and mandates for information assurance (IA) and resilience were issued. Amidst rapidly evolving IA trends and developments in the ongoing race between security attacks and defenses, information security professionals can gain an edge over potential threats by sharing information over DoDTechipedia.

Among the 23 original technology areas in DoDTechipedia, of particular interest to the IA community are IA, information warfare, and networking technology. Within these three technology areas, DoDTechipedia's

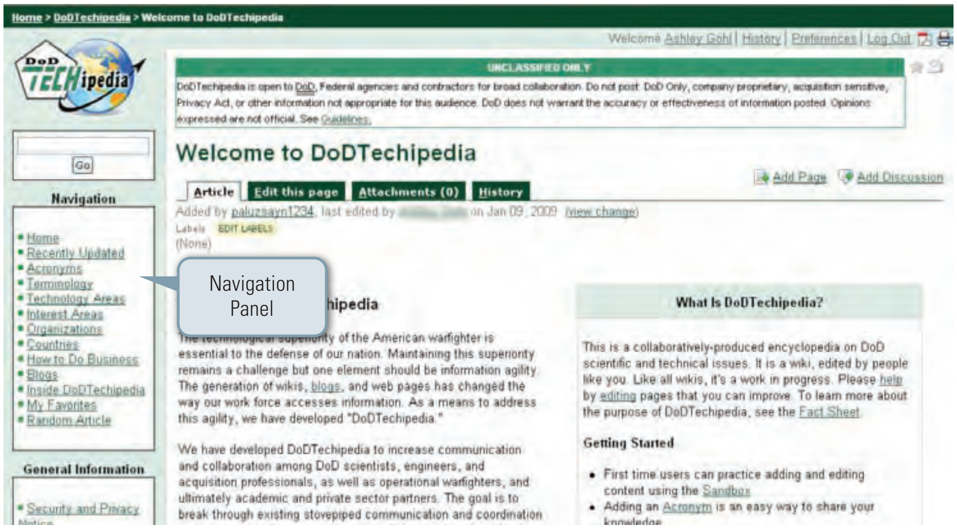

Privacy and Security Notice

Need to register? Click here (a CAC card will be required)

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.
- If you are having problems, click here for help and contact information.
- Access to this site requires registration.

Figure 1 DoDTechipedia Login Page


Home > DoDTechipedia > Welcome to DoDTechipedia

Welcome Ashley Gohl | History | Preferences | Log Out

UNCLASSIFIED ONLY

DoDTechipedia is open to DoD, Federal agencies and contractors for broad collaboration. Do not post DoD Only, company proprietary, acquisition sensitive, Privacy Act, or other information not appropriate for this audience. DoD does not warrant the accuracy or effectiveness of information posted. Opinions expressed are not official. See Guidelines.

Welcome to DoDTechipedia

Added by paluzsayn1234, last edited by [redacted] on Jan 09, 2009 (view change)

Labels: EDIT LABELS
(None)

Navigation Panel

hipedia

The technological superiority of the American warfighter is essential to the defense of our nation. Maintaining this superiority remains a challenge but one element should be information agility. The generation of wikis, blogs, and web pages has changed the way our work force accesses information. As a means to address this agility, we have developed "DoDTechipedia."

We have developed DoDTechipedia to increase communication and collaboration among DoD scientists, engineers, and acquisition professionals, as well as operational warfighters, and ultimately academic and private sector partners. The goal is to break through existing stovepiped communication and coordination

What Is DoDTechipedia?

This is a collaboratively-produced encyclopedia on DoD scientific and technical issues. It is a wiki, edited by people like you. Like all wikis, it's a work in progress. Please help by editing pages that you can improve. To learn more about the purpose of DoDTechipedia, see the Fact Sheet.

Getting Started

- First time users can practice adding and editing content using the Sandbox
- Adding an Acronym is an easy way to share your knowledge

Figure 2 Navigation Panel

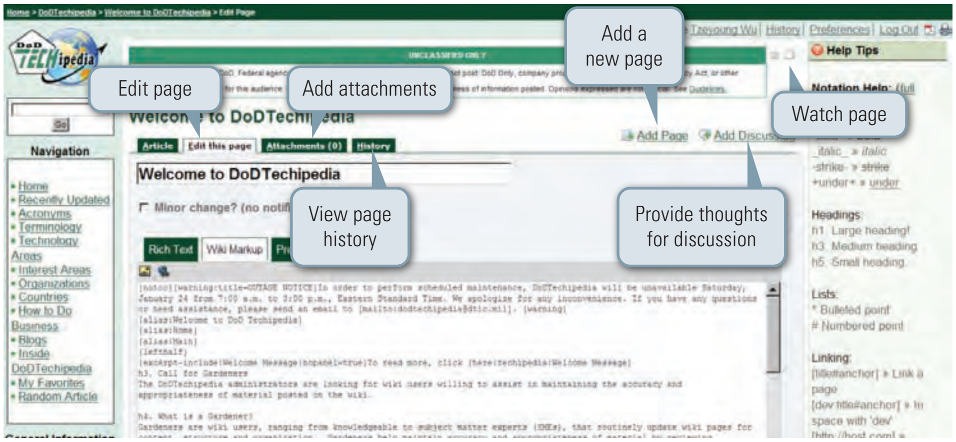
growing body of articles cover federal policies such as the Federal Information Security Management Act (FISMA) and DoD Information Assurance Certification and Accreditation Process (DIACAP); describe information repositories such as the National Vulnerability Database; and highlight industry practices and methodologies for penetration testing and risk assessments. For the latest news on IA developments, check the regularly updated blog postings. Blogs can be referenced for related current events, information about conferences, and more.

For example, a security professional perusing news about events might reference the November 25, 2008, Information Warfare blog post on the new Internet attack vector using script fragmentation, and then read articles on the Non-Secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) as examples of secure federal networks. Concerned over security standards, the user may obtain guidance on industry IA standards by reviewing information on the Common Criteria article, which also contains references to external information sources for further research. The same user may read up on the Defense Research and Engineering Network (DREN) article to find out about available research-oriented systems maintained by federal agencies.

Articles

The meat of DoDTechipedia lies in the encyclopedia of interactive articles that all users may access and upon which they can collaborate. Editing pages, adding attachments, creating sub-pages, posting discussion boxes, and viewing the change history of the page are only a sampling of the many ways users may interact with an article. Remember, with the ongoing evolution of technologies and projects, updates are very important.

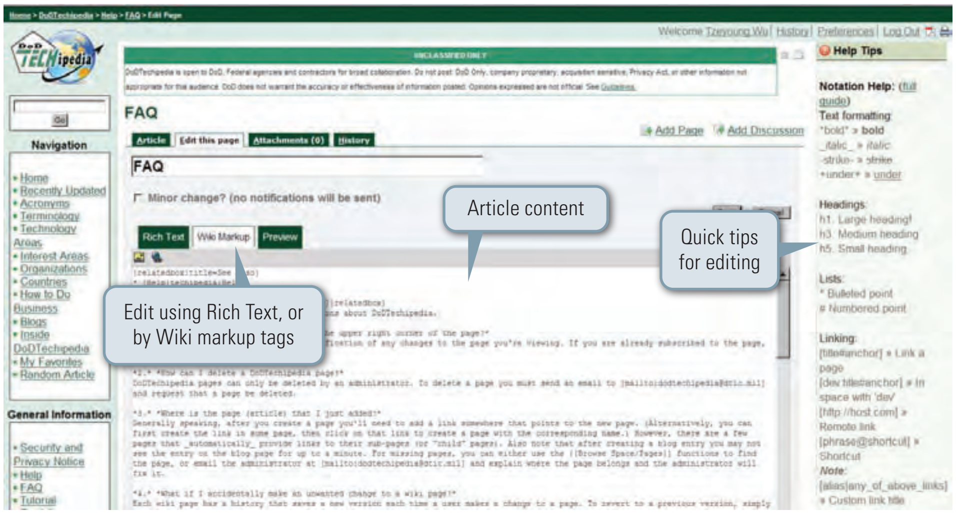
Users can even start discussions on the page itself by adding discussion boxes at the end of the article. Within the discussion boxes on the page, all users may respond to one another's thoughts and post feedback. This is a great way to share ideas and news about topics and to suggest improvements to article material.



```
[notoc][warning:title=OUTAGE NOTICE]In order to perform scheduled maintenance, DoDTechipedia will be unavailable Saturday,
January 24 from 7:00 a.m. to 3:00 p.m., Eastern Standard Time. We apologize for any inconvenience. If you have any questions
or need assistance, please send an email to [mailto:dodtechipedia@dtic.mil]. [warning]
[alias:Welcome to DoD Techipedia]
[alias:Home]
[alias:Main]
[lefthalf]
[excerpt-include:Welcome Message|nopanel=true]To read more, click [here|techipedia:Welcome Message]
h3. Call for Gardeners
The DoDTechipedia administrators are looking for wiki users willing to assist in maintaining the accuracy and
appropriateness of material posted on the wiki.

h4. What is a Gardener?
Gardeners are wiki users, ranging from knowledgeable to subject matter experts (SMEs), that routinely update wiki pages for
```

Figure 4 Interacting with an Article



DoDTechipedia is open to DoD, Federal agencies and contractors for broad collaboration. Do not post DoD Only, company proprietary, acquisition sensitive, Privacy Act, or other information not appropriate for the audience. DoD does not warrant the accuracy or effectiveness of information posted. Opinions expressed are not official. See Guidelines.

```
[relatedbox:title=See      so]
]|relatedbox]
ns about DoDTechipedia.
he upper right corner of the page?*
fication of any changes to the page you're viewing. If you are already subscribed to the page,

*2.* *How can I delete a DoDTechipedia page?*
DoDTechipedia pages can only be deleted by an administrator. To delete a page you must send an email to [mailto:dodtechipedia@dtic.mil]
and request that a page be deleted.

*3.* *Where is the page (article) that I just added?*
Generally speaking, after you create a page you'll need to add a link somewhere that points to the new page. (Alternatively, you can
first create the link in some page, then click on that link to create a page with the corresponding name.) However, there are a few
pages that _automatically_ provide links to their sub-pages (or "child" pages). Also note that after creating a blog entry you may not
see the entry on the blog page for up to a minute. For missing pages, you can either use the {{Browse Space/Pages}} functions to find
the page, or email the administrator at [mailto:dodtechipedia@dtic.mil] and explain where the page belongs and the administrator will
fix it.

*4.* *What if I accidentally make an unwanted change to a wiki page?*
Each wiki page has a history that saves a new version each time a user makes a change to a page. To revert to a previous version, simply
```

Figure 5 Editing an Article

Adding a new page or sub-page is as easy as clicking on the "Add Page" link. Any user may then continue by providing an article title and entering text. Users are also encouraged to add information to existing pages. You can do this by clicking the "Edit This Page" tab. Users may edit using rich text or using plain text with wiki markup. Of course, others may further revise your own changes. But by clicking on the "Watch Page" envelope icon on the upper right-hand side of the screen, you will be notified *via* email whenever users make edits to the page.

Acronyms and Terminology

Any user working in or with the US Government should be familiar with its affinity for using acronyms. While acronyms can streamline communication between personnel within the same program, the abundance of acronyms in regular use by various agencies and programs may overwhelm the uninitiated. Moreover, acronyms may hold different meanings according to the user.

Fortunately, DoDTechipedia hosts a living list of acronyms along with definitions and, when available, links to related articles. Now any user may look up acronyms on this page. If none are found, anyone can add to the list by clicking the "Edit This Page" tab. Similarly, DoDTechipedia also contains a page that lists terminology.

Blogs

To promote a collaborative culture, DoDTechipedia supports blogging, with threads categorized under each of the original technology areas. Users also can request blogs be created for additional technology areas by contacting site administrators. Blogs are intended to be the center for collaboration and informal information-sharing between users. Not only can users share thoughts, but they can also meet others with similar interests. This will facilitate networking within the community. DoDTechipedia blogs are controlled by blog owners who provide regular postings. While any user can comment on a blog entry, only the blog owner can post an entry. DoDTechipedia is always looking for additional blog owners. Threads notify the community about current events, technology developments, and upcoming conferences.

DoDTechipedia provides technology blogs maintained by technology area content managers. A user can create a personal page that showcases articles highlighting personal research and interests, as well as maintain a personal blog open to all registered users.

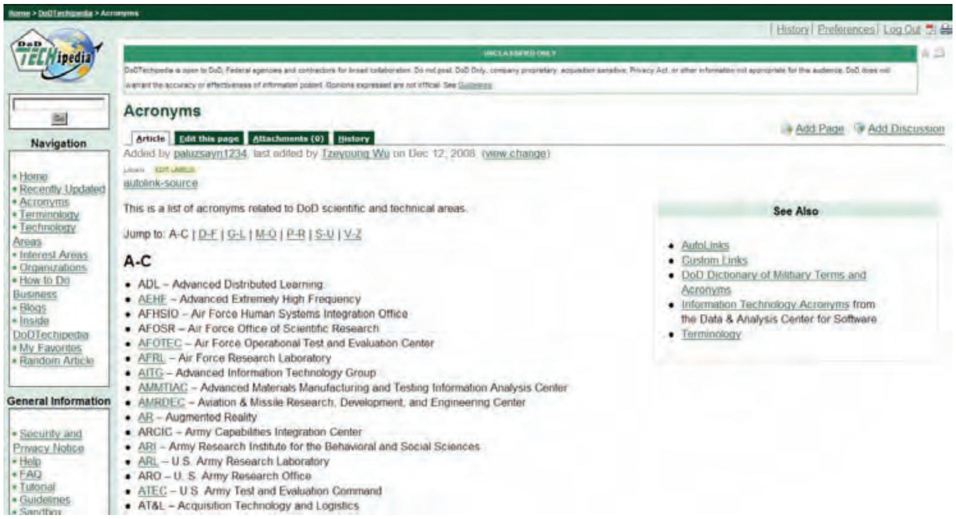
You are invited to start a blog, comment on threads, and add material to the "Inside DoDTechipedia" community blog. On the blogs main page, announcements from administrators are listed on the right. The main page lists the most recent blog updates. Users can initiate their own thoughts and respond to others. Similar to articles, users can edit the page, view change history, and add attachments.

Some Guidelines

First and foremost, remember that all information posted on DoDTechipedia must be unclassified information.

For the sake of consistency, users should follow common formatting when creating and editing articles. Users should cite references and credit information sources. DoDTechipedia

▷▷ *continued on page 10*



DoDTechipedia is open to DoD, Federal agencies and contractors for broad collaboration. Do not post DoD Only, company proprietary, acquisition sensitive, Privacy Act, or other information not appropriate for the audience. DoD does not warrant the accuracy or effectiveness of information posted. Opinions expressed are not official. See Guidelines.

Acronyms

Added by paluzsayn1234, last edited by Tzeyoung Wu on Dec 12, 2008 (view change)

Labels: autolink-source

This is a list of acronyms related to DoD scientific and technical areas.

Jump to: A-C | D-F | G-L | M-O | P-R | S-U | V-Z

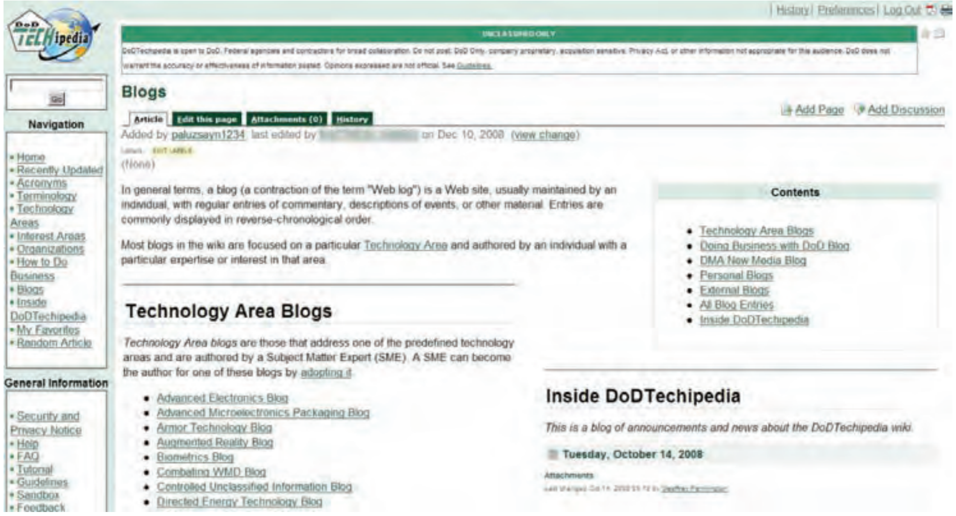
A-C

- ADL – Advanced Distributed Learning
- AEHF – Advanced Extremely High Frequency
- AFHSIO – Air Force Human Systems Integration Office
- AFOSR – Air Force Office of Scientific Research
- AFOTEC – Air Force Operational Test and Evaluation Center
- AFRL – Air Force Research Laboratory
- AITG – Advanced Information Technology Group
- AMMTIAC – Advanced Materials Manufacturing and Testing Information Analysis Center
- AMRDEC – Aviation & Missile Research, Development, and Engineering Center
- AR – Augmented Reality
- ARCIC – Army Capabilities Integration Center
- ARI – Army Research Institute for the Behavioral and Social Sciences
- ARL – U.S. Army Research Laboratory
- ARO – U.S. Army Research Office
- ATEC – U.S. Army Test and Evaluation Command
- AT&L – Acquisition Technology and Logistics

See Also

- AutoLinks
- Custom Links
- DoD Dictionary of Military Terms and Acronyms
- Information Technology Acronyms from the Data & Analysis Center for Software
- Terminology

Figure 6 Acronyms Page



DoDTechipedia is open to DoD, Federal agencies and contractors for broad collaboration. Do not post DoD Only, company proprietary, acquisition sensitive, Privacy Act, or other information not appropriate for the audience. DoD does not warrant the accuracy or effectiveness of information posted. Opinions expressed are not official. See Guidelines.

Blogs

Added by paluzsayn1234, last edited by [redacted] on Dec 10, 2008 (view change)

Labels: (None)

In general terms, a blog (a contraction of the term "Web log") is a Web site, usually maintained by an individual, with regular entries of commentary, descriptions of events, or other material. Entries are commonly displayed in reverse-chronological order.

Most blogs in the wiki are focused on a particular Technology Area and authored by an individual with a particular expertise or interest in that area.

Contents

- Technology Area Blogs
- Doing Business with DoD Blog
- DMA New Media Blog
- Personal Blogs
- External Blogs
- All Blog Entries
- Inside DoDTechipedia

Technology Area Blogs

Technology Area blogs are those that address one of the predefined technology areas and are authored by a Subject Matter Expert (SME). A SME can become the author for one of these blogs by adopting it.

- Advanced Electronics Blog
- Advanced Microelectronics Packaging Blog
- Armor Technology Blog
- Augmented Reality Blog
- Biometrics Blog
- Combating WMD Blog
- Controlled Unclassified Information Blog
- Directed Energy Technology Blog

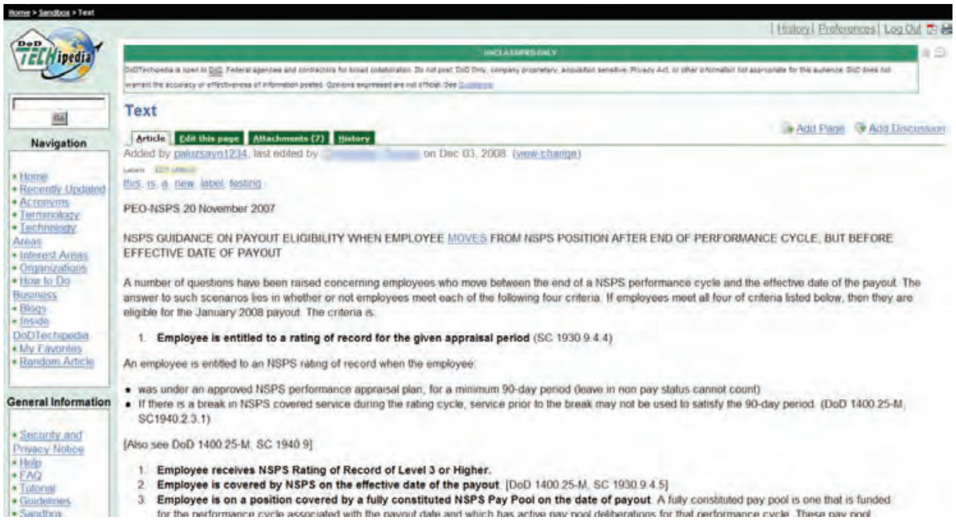
Inside DoDTechipedia

This is a blog of announcements and news about the DoDTechipedia wiki.

Tuesday, October 14, 2008

Attachments

Figure 7 Blogs Page



DoDTechipedia is open to DoD, Federal agencies and contractors for broad collaboration. Do not post DoD Only, company proprietary, acquisition sensitive, Privacy Act, or other information not appropriate for the audience. DoD does not warrant the accuracy or effectiveness of information posted. Opinions expressed are not official. See Guidelines.

Text

Added by paluzsayn1234, last edited by [redacted] on Dec 03, 2008 (view change)

Labels: this, is, a, new, label, testing

PEO-NSPS 20 November 2007

NSPS GUIDANCE ON PAYOUT ELIGIBILITY WHEN EMPLOYEE MOVES FROM NSPS POSITION AFTER END OF PERFORMANCE CYCLE, BUT BEFORE EFFECTIVE DATE OF PAYOUT

A number of questions have been raised concerning employees who move between the end of a NSPS performance cycle and the effective date of the payout. The answer to such scenarios lies in whether or not employees meet each of the following four criteria. If employees meet all four of criteria listed below, then they are eligible for the January 2008 payout. The criteria is:

1. **Employee is entitled to a rating of record for the given appraisal period** (SC 1930.9.4.4)

An employee is entitled to an NSPS rating of record when the employee:

- was under an approved NSPS performance appraisal plan, for a minimum 90-day period (leave in non pay status cannot count)
- If there is a break in NSPS covered service during the rating cycle, service prior to the break may not be used to satisfy the 90-day period. (DoD 1400.25-M, SC1940.2.3.1)

[Also see DoD 1400.25-M, SC 1940.9]

1. **Employee receives NSPS Rating of Record of Level 3 or Higher.**
2. **Employee is covered by NSPS on the effective date of the payout.** [DoD 1400.25-M, SC 1930.9.4.5]
3. **Employee is on a position covered by a fully constituted NSPS Pay Pool on the date of payout.** A fully constituted pay pool is one that is funded for the performance cycle associated with the payout date and which has active pay pool deliberations for that performance cycle. These pay pool

Figure 8 Sandbox

AFCYBER (P) Way Ahead

by Carla Pampe

For more than a year, a small Barksdale Air Force Base team has been working toward the goal of establishing a command within the United States Air Force that would integrate systems and capabilities and establish a command and control structure for cyber warfighting forces.

In October, the service's new leadership—Secretary Michael B. Donley and Chief of Staff Gen Norton A. Schwartz—decided that the best organizational construct for the Air Force's cyber capability would be a Component Numbered Air Force (C-NAF). The new C-NAF, to be designated 24th Air Force, will fall under Air Force Space Command, which is a natural fit, according to Maj Gen William T. Lord, Commander of Air Force Cyberspace Command (Provisional) (AFCYBER [P]).

"I think there are great synergies between the cyber domain and the space domain," he said. "They require similar skills—it's combat capability provided by the non-kinetic world, so, most importantly, it's about cross-domain synergies. We can become more effective by working together. Air plus space plus cyber is greater than the sum of each of those, in our opinion." [1]

General Lord said that while the team has had to shift gears from planning for the standup of a major command to the standup of a numbered air force, almost all of their work easily will carry over. In fact, the AFCYBER (P) team already has completed a tremendous amount of planning, dialogue, and coordination over the past year to establish a successful cyber organization.

"It's not like we have to start from scratch," General Lord said. "The doctrine is the same, the budget is the same, the training is the same, the changes to the curriculum at the schoolhouses are all the same, so it's not a lot of rework.

"This whole dialogue over the past year has shown the importance of the Air Force's dependence on cyber," General Lord said. "There has been recognition of a new domain of warfare, and as a result of that, we now have Air Force doctrine on how you fly, fight and win in Cyberspace."

One of the biggest accomplishments of the team this year was identifying resources in terms of both people and money required to maintain the right cyber capabilities.

"This has led to successful decisions on how we ought to organize cyber forces—what capabilities fall into our organizational constructs," General Lord said. "We have identified what's required to have a capability to defend the Air Force portion of the cyber domain, and if necessary, deny an enemy's portion of the cyber domain."

In addition, the team has also worked over the past year to improve cyber education both inside and outside the Air Force.

"We have made significant strides in identifying and codifying education and training opportunities for the cyber force," said General Lord. "In fact, the Air Force now offers a Master's degree in cyber operations, and many US academic institutions are beginning to incorporate cyber-related curriculum to produce students with cyber expertise."

As a result of the work done on the education and training plans, the Air Force now has a career field roadmap that outlines the transition from today's cyber career forces to tomorrow's cyber career forces for both officers and enlisted members. According to General Lord, this plan includes a variety of skills and describes how the transition will occur.

The AFCYBER (P) team also worked to strengthen organizational ties with other government agencies such as the Department of Justice, the Department of Homeland Security and the Office of the Director of National Intelligence (ODNI).

"This will make us much more effective nationally, because we have government organizations that are exchanging data and talking to one another," General Lord said.

AFCYBER (P)'s work also helped to shape a growing cyber-related industrial base.

"It has led to a US industrial base that is thinking about bringing, and inventing, new capabilities in the cyber arena, some of which not only have military applications, but commercial applications as well, because the US is so dependent on the cyber domain for our economy."

Now that a majority of the planning and coordination has been done to establish the cyber mission as a C-NAF, the team is shifting gears to work on finalizing the program action directive that outlines the specifics of exactly how the 24th Air Force will be set up.

To do that, they have been working very closely with their counterparts at Air Force Space Command.

"The Air Force Space Command personnel folks are already heavily involved—the plans directorate is heavily involved, and the operations directorate is helping us think through force presentation issues," General Lord said. "So, we have this instant support of a major command staff, where we were going to have to build one from scratch—it's like walking into an organization that's partially built, and they were very, very gracious in accepting this new mission."

One of the challenges General Lord foresees for the future of cyber is a cultural change in the Air Force with regard to cyberspace as a domain.

"We're talking about a domain that the Air Force has been involved with for 25 years, but considering this as a warfighting domain…it's a cultural change," he said. "We have to be prepared to fight with an enemy inside the network, we have to protect the Air Force's ability to command and control our forces so they are available for the Joint fight.

"This is an exciting new era for our Air Force," General Lord added. "We are all looking forward to seeing all the hard work done on behalf of the Air Force over the past year come together with the standup of the 24th Air Force. We are making history in and for a new warfighting domain, with our Joint partners." ■

Reference

1. "Air Force leaders work to develop cyberspace roadmap." Air Force Link, October 24, 2008, *http://www.af.mil/news/story.asp?id=123121153.*

About the Author

Carla Pampe | has more than 15 years of experience in journalism and public affairs. Previously, she served more than seven years as a public affairs officer in the United States Air Force. She received an MS in professional media management from Southern Illinois University and a BS in journalism from Louisiana Tech University. Her research includes the military's use of the new media to communicate messages to members of the media and public audiences. She may be reached at *iatac@dtic.mil.*

▷ *continued from page 8*

DODTECHIPEDIA

offers pre-formatted section headings and page titles. The first sentence of each article should start with the article topic as the subject, and a definition should follow. All language should be professional and unbiased. Further guidelines can be obtained on the site under "Editorial Guidelines" and "Behavioral Guidelines." A link to this page can be found on the main "Guidelines" page, located in the "General Information" panel on the left.

For assistance, help, tutorial, and frequently asked questions pages are available, and users may contact site administrators at *DoDTechipedia@dtic.mil*.

For practice, DoDTechipedia offers a sandbox accessible by clicking on the appropriate link on the "General Information" panel on the left.

Conclusion

According to Mr. Young, DoDTechipedia "is the enterprise tool to lead a paradigm shift for the Department." With your support, this wiki will ensure greater transparency and communication among DoD scientists, engineers, program managers, and warfighters.

Certainly, collaboration on DoDTechipedia today will ensure the most advanced technologies get to the warfighter tomorrow. ■

About the Author

Mr. Tzeyoung Max Wu | as a DoDTechipedia content manager, creates and edits material in the IA, information warfare, and networking technology areas. He also manages blogs in all three areas. His experiences in information technology security have included administering and configuring servers and network devices within organizations; designing secure architecture for enterprise systems; and configuring access control lists, profiles, and border controls for network applications.

Currently, Mr. Wu is completing his MBA at the University of Chicago Booth School of Business with concentrations in economics, entrepreneurship, and strategic management. Mr. Wu received his BA degree in computer science from New York University, where he also studied journalism and biology. He also received a Master in IT from Virginia Tech.

For more DoDTechipedia general information, you may request a briefing by contacting Ms. Jessica Jones at 703/767-8216. Please contact Mr. Rogelio Raymond or Mr. Max Wu by email at *iatac@dtic.mil* for DoDTechipedia information related to IA, information warfare, or networks.

Expectations for 2009

by Allan Carey

This coming year will be one of the most challenging in decades for information assurance professionals. Instead of information security teams getting more resources, budgets are likely to be cut as security is expected to "do more with less." In addition, in many organizations, the IANS is observing a trend where information security may not be a freestanding group in the future. There may be fewer chief information security officer (CISO) roles as security becomes a part of a broader risk management function.

Yet, the threat landscape is getting more targeted, sophisticated, and nefarious at the same time that new technologies, including virtualization, cloud computing models, and smartphones, are proceeding with security as an afterthought; remember the introduction of wireless access points? The pace of innovation may be slowing; however, organizations are looking for every opportunity to drive efficiencies, rationalize what they have, and illustrate their value to the business.

Conversations with IANS clients throughout the Fortune 1000, US Government, and academia have surfaced some trends in the areas of buyer behavior, organizational structures, information technology (IT) security vendors, and technology advances.

Buyer behavior

Companies will be very reluctant to purchase new software as capital expenditure budgets will be slashed, pressuring organizations to do more with less. Buyers will pursue solutions that may be perceived as weaker, but where certain items are bundled in, such as free antivirus software from Microsoft. Buyers also will go after maintenance contracts, demanding lower prices and considering non-renewal. Despite any talk of innovation, the focus will be on "optimizing" what already exists in the near-term.

Organizational structures

The economic downturn will put pressure on security teams, and in some instances, will lead to a dissolving of the security team. The trend will continue to be more advisory and less operationally hands-on, which will be a difficult transition for some security professionals.

Our observations indicate that we might be at the beginning of the CISO phase-out. At a time when security is more important than ever, dedicated security functions are being driven into operational IT. For example, anti-virus desktop defense is part of the desktop team; firewalls and intrusion detection systems (IDS) and intrusion prevention systems (IPS) are part of the networking team; and application security assessments are part of the quality assurance (QA) team.

In addition, while there is talk of security's role in terms of risk management, this role is way down the ladder. IT security risk is a subset of IT risk. IT risk is a subset of operational risk, and operational risk is a subset of enterprise risk. So, while organizations are thinking more in terms of risk, security risk is just one component of it. There is an increase in companies organizing around the "information lifecycle" with a transition in CISO positions.

IT security vendors

During the last year and a half, spending on software has been strong, growing by more than 10%. However, as the economy has declined, so has software spending, which right now is flat versus a year ago. It will only get worse before it gets better.

Vendors will slash marketing budgets, relying more on revenues from maintenance than on new sales. Many of them will downsize by 10% to 20% (or even more), with layoffs in areas such as sales and support. Layoffs in support give buyers even more ammunition to negotiate for lower maintenance fees. Some companies will also cut research and development, and smaller, venture-backed private companies will seek acquirers.

Seed money for new IT security companies is evaporating, which could likely inhibit innovation. In the next 12 to 18 months, it is unlikely that there will be much, if any, funding for new IT security firms. There are two reasons—
1) Venture capitalist firms will be focused on their current investments, not new ones; and 2) many venture capitalists do not see compelling new ideas in the IT security space.

Technology advances

The large vendors will continue to acquire smaller players, resulting in security industry Darwinism. Since many of these bloated suites will not

▷▷ *continued on page 17*

There and Back Again

Centralizing Security by Migrating to a Thin Client Architecture

by Brennon Thomas, Lt Col Jeffrey Humphries, and Dr. Robert Mills

Disclaimer

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

Introduction

It is no surprise that almost every employee of the Department of Defense (DoD) has a computer. The computer is a tool that cuts communication time, organizes data and information, and increases job efficiency. The operation of the tool should be like any other utility in that the end user should be able to use the tool without having to know much about the underlying technology. Whether the electricity coming to the power outlet came from a nuclear plant, hydroelectric dam, or wind power is immaterial, and the end user really does not need to know or care. Likewise, the way in which email flows through the network, how websites transfer information, and how and where data is stored should all be transparent to the average user. Users should not need to be concerned about whether the latest encryption protocols are being used or if the newest operating system patches have been installed. They should be able to use their computers in much the same way they use other standard tools and appliances. Requiring or assuming that the common user be competent in computer technology is unwarranted.

Unfortunately, too much of our current security approach relies on the vigilance and security consciousness of these same end-users. Constant warnings of phishing emails, malicious links, and information operation conditions (INFOCON) require that users understand these issues. In addition to performing their real jobs, users are expected to conscientiously and consistently defend computers from attack. This is counterproductive and presents a massive overhead to administrators who have to provide user training, push timely patch rollouts, lock down user rights, and perform general troubleshooting.

One solution is to transfer the responsibility of defending the desktop and insecure software from the user to a centrally managed server using a thin client architecture. The thin client architecture is a hardware solution to implement and promote secure software on large-scale networks. Thin clients are attractive because they are centrally managed and easier to secure. By moving applications and data from the desktop to a secure, centrally managed server, many of the vulnerabilities and weaknesses network administrators deal with either go away or become much more manageable. The thin client architecture provides a viable solution to securing large-scale networks because it offers numerous benefits with limited disadvantages.

Background

The concept of a thin client architecture dates back to the days of mainframe computing. In the early days of computing, scientists, engineers, and accountants used mainframes for computation-intensive applications. At the time, the physical size of these mainframes required large rooms and support systems, and individuals used "dumb terminals" to access the system. With the advent of the personal computer and the explosion of processor technology and capabilities, these big mainframe computers were slowly supplanted with inexpensive and increasingly capable desktop computers. Hewlett-Packard embodied this movement with their slogan, "The computer is personal again." Over time, we have seen many new capabilities, such as email, Web browsing, distributed file-sharing, and the pervasive use of removable media devices. There is a dark side to this pervasive computing ability, however, as DoD struggles to manage the onslaught of phishing attacks, pharming ploys, viruses, Trojan horse programs, worms, and other malicious software threats. The issue is how to manage these systems since network administrators are overwhelmed with the daily wave of network security reconfigurations, operating system patches, and various other application updates.

A few years ago, the US Air Force (USAF) decided to address some of these

issues by adopting the Standard Desktop Configuration (SDC) to provide a consistent and secure computing environment. The purpose of the SDC was to add another layer of security and standardization to the user's desktop. [1] Looming in the future is an even broader and wider security implementation for government computers known as the Federal Desktop Core Configuration (FDCC). The FDCC is a National Institute of Standards and Technology (NIST) initiative to provide a secure desktop standard for all federal computers. [2] It is the SDC on steroids. Current computer systems and technology within DoD and the US Government will have to adopt this new security standard. This immense undertaking adds yet another element of complexity in securing our systems, and, we believe, is a move in the wrong direction. If DoD is serious about running secure software on its systems, we should instead consider the adage, "The computer is NOT personal again." A thin client architecture can provide a solid base to distribute and supply secure software by moving away from the use of personal computers for every user.

Thin Client Solution

A thin client architecture follows the client/server model for communication. The clients are stripped-down computers usually consisting of a small chassis with a monitor, mouse, and keyboard. Thin clients generally lack a hard disk drive and on-board processing capabilities. Instead of running applications and processes on local machines, thin clients connect to a central server that provides an operating system, applications, and storage space to each client. Figure 1 illustrates the basic concept.

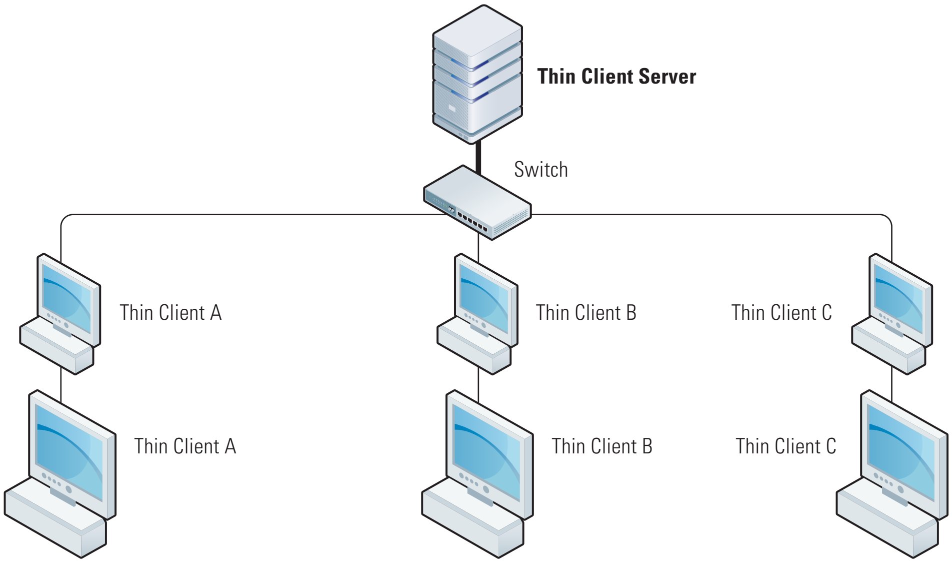


Figure 1 Simplified Thin Client Architecture

The thin client concept was once considered to be the future of computing. Larry Ellison, the chief executive officer of Oracle, quipped in the mid-1990s that, "the era of the PC is almost over, and the era of the thin client is about to begin." [3] Ellison's prediction did not bear itself out, but there is renewed interest in thin clients in the information technology (IT) industry. DoD (and other large enterprises) should aggressively investigate thin client architectures for its major enterprise networks because of the security benefits they bring.

Central Operating System Image

A common approach in enterprise network management is to use an approved enterprise system, such as Microsoft's Systems Management Server (SMS), to monitor desktops for operating system patch compliance. In essence, a server checks to make sure a desktop computer has the latest patches. If the desktop computer is non-compliant, the SMS server forces the computer to download and install these updates. There are two main problems with this approach. The first is that the computer must always be active and on the network in order to communicate with the SMS server to check for updates. The second, and much more serious, problem is the window of opportunity between when a vulnerability is discovered and when a patch is actually pushed to fix that vulnerability. Any window of time could allow an attacker to take advantage of a system. Thin clients offer the ability to present the most updated operating system to every user. Each thin client pulls the operating system image from the server (assuming the administrators have provided updates) and thus executes with the latest, patched software.

Bastion for Applications

Thin clients not only provide a secure operating system to users, but also provide secure software in the form of patched applications. In addition to operating system updates, DoD computer systems must be compliant with a host of other application updates. Some of these include the entire Microsoft Office suite, QuickTime, Internet Explorer, Adobe, Java, structured query language (SQL), Cisco virtual private network (VPN) clients, *etc*. This bundle of diverse software, in addition to the operating system updates, quickly compounds the challenge of maintaining and securing software on computers resulting in a "never ending battle" to keep up. [4] In a sense, there really is no such thing as an IT baseline anymore, because there are too many variables. Thin clients offer a solution equivalent to the operating system-update problem. Instead of hopelessly managing the deluge of updates for applications, DoD should consider a shift to a thin client architecture, which can provide one updated and secure software application platform for all its users at once.

Data Control and Security

A network may be secure against external threats, but it is still vulnerable to the insider threat. For example, users still employ Universal Serial Bus (USB) drives for file transfers between home and work computers. Problems arise when users sneakernet files between systems. This meshing of software domains and exposure does not reinforce the concept of secure computing on DoD networks. Exposing a DoD computer to a virus from a home computer carried by a USB drive is possible. Efforts have been made to extend anti-virus and anti-spyware software to members of DoD and US Government employees, but these free software licenses are only a remedy and not a cure to protect information-moving between private home and DoD networks. [5]

The threat of USB drives came to fruition in November 2008 when the commander of United States Strategic Command (USSTRATCOM) "suspended the use of thumb drives, compact discs (CD), flash media cards, and all other removable data storage devices." [6] This would have been unnecessary if networks used thin clients since users do not have any external device inputs or ports to introduce, download, or modify data residing on the computer (because data resides on the servers). To accommodate personnel on business trips and telecommuters, administrators can still provide VPN and remote access solutions.

Thin Client Hardware

Thin clients offer a reliable, sturdy hardware architecture and are less prone to failure and malfunction because of their limited moving parts. The hardware configuration is modest and only contains the necessary elements to function correctly. One of the leaders in thin client technology is Wyse Technologies. Table 1 lists the hardware included in the Wyse S10 model, the introductory model in the Wyse line of thin clients. [7] The design is simple and small. This hardware configuration, including the other variations, allows administrators to provide economy of mechanism as well as adhere to the principle of least privilege. It should also be noted that many thin clients also have smart card readers permitting the use of Common Access Cards (CAC). The CAC infrastructure can work in concert with a thin client architecture to provide a secure working environment.

Hardware	Description
Processor	AMD Geode GX 366 MHz
Memory	Flash/128MD RAM
I/O Peripherals	VGA, keyboard, mouse, serial, USB
Networking	10/100 Base-T Fast Ethernet
Display	VESA monitor support
Audio	1/8-inch mini input and output

Table 1 WYSE S10 Thin Client Hardware

Environmental Considerations

In February 2008, the Environmental Protection Agency announced that the USAF was "the largest purchaser of green power in government and the third-largest purchaser among public and private sector employers nationwide." [8] It is apparent that DoD is leading the government, defense, and industry in striving for reduced energy costs and promoting clean power in the world. Since the majority of processing and work is done at the servers, this reduces the energy demands from desktop computers. Some thin client devices have been shown to consume a mere five watts of power in operation, [9] which could result in a smaller electrical demand on IT infrastructures. Another environmental reason to migrate to thin clients is that the amount of plastic and metal needed to produce one unit is less than that of most personal computers. This also helps when recycling expired thin clients that are at the end of their lifecycle. Thin clients provide another opportunity to promote DoD's environmental leader image and sustain the ranking as a proponent of green technology.

System Administration

Besides offering secure software, better data security, and environmental advantages, the most important benefit of a thin client architecture is that administration becomes more centralized and streamlined. System administrators are able to focus on long-term projects and security improvements instead of juggling temporary IT problems. IT departments can focus on maintaining a group of central servers instead of spending time and resources fixing, upgrading, and replacing personal computers. As a result, IT departments can trim budgets, staff, and man-hours required to support the current personal computer architecture. Furthermore, if a massive federal standardization of computers, networks, and software comes to reality, such as the FDCC, compliance can be ensured in hours or days instead of months. This is because IT departments can provide the latest secure operating system image as soon as it is available. The thin client architecture facilitates accelerated patch compliance for all federal entities and promotes a uniform security front.

Shortfalls

There are some disadvantages to thin client architectures. The first is that the entire thin client architecture relies on a network connection. If the network connection malfunctions, work comes to a standstill since thin clients rely on near-constant communication with its servers. In reality though, network downtime is a rarity these days. Furthermore, the activities that most people commonly perform—collaborating on documents, using email, and Web browsing—are all dependent on the network. When the network is down, there are few things that can be accomplished on the computer—especially if the system requires the network to even log the user on!

Naysayers also cite the lack of network bandwidth and increased demand for memory and processor-intensive applications as another shortcoming. Fortunately, advances in decreased network transmission times and increased bandwidth are keeping pace (*e.g.,* Gigabit Ethernet). Thin clients can be configured to transmit only the minimal amounts of information needed to operate. [10] An increased transmission throughput combined with a thin client's decreased network load enables a near frictionless user experience.

Another limitation of these architectures pertains to engineering, scientific, and high-end graphic applications. Currently, thin clients simply cannot provide the resources and demands necessary to complete these intensive tasks. There is a distinction, however, between the everyday computer user and those requiring the computing power of a desktop (*e.g.,* engineers, scientists, *etc.*). Possible solutions include providing a separate network for these special needs or creating a separate internal VPN connection for Internet and email access.

Good Beginnings

DoD already has begun to field thin client solutions, but on a small scale. The Defense Intelligence Agency (DIA) teamed up with Trusted Computer Solutions to create the Department of Defense Intelligence Information Systems (DoDIIS) Trusted Workstation (DTW). The solution is used to "access multiple levels of classified data and then disseminate actionable information" in addition to providing "enhanced security, enhanced functionality, enhanced audit management, simplified installation and administration, reduced support costs and ease of certification and accreditation." [11] The solution also drastically reduces the hardware footprint on intelligence analysts' desks by providing a single thin client chassis and monitor. Previously, multiple computers and monitors were required for each classification level. In addition to the reduction in computer hardware, the network infrastructure also is reduced to a single network. Separate network devices, cables, and administrators were also needed to manage the different classified networks. Now, the entire thin client architecture rides over a single network. Finally, thin clients have been configured to employ a technique called "hot desking," which allows users to sit down at any workstation, insert their smart ID card, and pull up previous documents and sessions. [12]

A second case of DoD utilizing a thin client architecture and reducing hardware comes from the USAF. In 2002, the Communications Squadron at Hill Air Force Base successfully implemented a hybrid concept of thin client technology, called ClearCubes, in a hospital annex. Results were a reduction in manpower and a $250,000 savings in system maintenance costs. [13]

Lastly, in 2005, the USAF experimented with deployable thin clients (DETHINC) at a forward operating location supporting Operations Iraqi Freedom and Enduring Freedom. The project was designed by the Air Warfare Battlelab with a goal of deploying 50 DETHINCs to a remote and environmentally difficult region. They also aimed to reduce purchase costs and decrease the number of hours required to support them. [14] Thin clients fit appropriately with DoD's global missions by providing a durable computing platform. In addition to having superior hardware durability, thin clients were also more conducive to working in austere environments. Those environments include many of DoD's global and deployable locations around the world. Thin clients have the benefit of low-power consumption and reliable fanless operation. [15] The prevalent dust, sand, and dirt in many deployed regions do not readily affect their hardware performance.

The previous case studies demonstrate the hardware capability and reduction potential within DoD. Thin clients can help achieve a security nirvana while also providing an acceptable hardware solution for DoD computer-users to complete missions.

Conclusion

The concept of thin clients is not new, and in many ways it reminds us of the mainframe era, one that was much simpler and less expensive from a security and maintenance perspective. The time has come to confront and solve the problem of insecure software on DoD networks by employing an older technology. It is a proven approach to solving a software problem with a hardware solution. While DoD has implemented some of these architectures on a smaller scale, it may be time to consider an enterprise-wide implementation. If DoD has any hope of securing its systems against current and future threats, it should consider migrating to a thin client architecture. The concept of providing one secure operating system image, with supported applications, is the closest DoD can get to the ideal of secure software. Tighter data control and security, reliable hardware, environmental independence, energy savings, and easier management are just a few more reasons for DoD to consider adopting an enterprise thin client architecture. Threats and vulnerabilities continue to assail DoD systems. The current process, which uses inefficient update distribution and patch management, is ineffective. Leadership must be convinced and policies reassessed before an event jeopardizes the network and national security. A thin client architecture is an essential step toward promoting and implementing a DoD-wide secure computing network. ■

References

1. Lopez, K. "Standard Desktop Configuration keeps AFMC ahead of 'bad guys'." May 16, 2006. *http://www.afmc.af.mil/news/story.asp?id=123020383*
2. "Federal Desktop Core Configuration." February 27, 2008. *http://nvd.nist.gov/fdcc/fdcc_faqs_20070731.cfm*
3. Callow, B. and Turner, R. "Back to the Future: Virtualization Pushes Thin Client Computing Into the Enterprise Mainstream." VXL Instruments Ltd. Whitepaper, 2007, pp. 1-8.
4. Church, R. and Mauersberger, G. Air Force Institute of Technology Communications and Information Directorate (AFIT/SCB), Interview, November 20, 2008.
5. Knight, C. "Anti-virus Software Available for Home Use." January 11, 2007. *http://www.travis.af.mil/story.asp?id=123037389*
6. Shachtman, N. "Under Worm Assault, Military Bans Disks, USB Drives." November 19, 2008. *http://blog.wired.com/defense/2008/11/army-bans-usb-d.html#more*
7. Wyse Technologies. "Wyse S10." *http://www.wyse.com/products/hardware/thinclients/S10/index.asp*
8. Kauffman, T. "Air Force is Biggest User of Green Power." February 25, 2008. *http://www.federaltimes.com/index.php?S=3387087*
9. Fraunhofer Institute for Environmental, Safety and Energy Technology UMSICHT, "Environmental Comparison of the Relevance of PC and Thin Client Desktop Equipment for the Climate, 2008." 2008, pp. 87, *http://it.umsicht.fraunhofer.de/TCecology/docs/TCecology2008_en.pdf*
10. Rouzaud-Cornabas, J. and Viot, N. "Secured Architecture for Remote Virtual Desktops." International Symposium on Collaborative Technologies and Systems, 2007, pp. 80.
11. Trusted Computer Solutions, "JEDI PMO To Manage Rollout of the DoDIIS Trusted Workstation (DTW)." *http://www.trustedcomputersolutions.com/documents/JEDICaseStudy.pdf*
12. Kenyon, H. "Desktop System Streamlines Analysis Work." October 2004. *http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=427&zoneid=31*
13. Thornberry, S. "Air Force Base CIO Finds an Alternative to PCs and Thin Clients." Tech Republic, September 17, 2002. *http://articles.techrepublic.com.com/5100-10878_11-1059667.html*
14. Tarantino, J. "DETHINC Initiative." Intercom, May 2005, Volume 46, Number 5, pp. 28. *http://public.afca.af.mil/shared/media/document/AFD-070129-205.pdf*
15. Krikke, J. "Thin Clients Get Second Chance in Emerging Markets." Pervasive Computing, IEEE, Volume 3, Issue 4, pp. 6-10, October–December 2004.

About the Authors

Brennon Thomas | currently is pursuing a Master's degree in cyber operations at the Air Force Institute of Technology (AFIT) at Wright-Patterson Air Force Base. He previously spent three years on active duty as a communications officer at the Air Force Communications Agency, performing network defense and network security auditing. He also received a BS degree in electrical engineering from Rensselaer Polytechnic Institute.

Lt Col Jeffrey Humphries | is an assistant professor of computer science in the electrical and computer engineering department at AFIT. Lt Col Humphries received a BS in computer science from the US Air Force Academy, an MS degree in computer science from Georgia Institute of Technology, and a PhD in computer science from Texas A&M University. His research interests include cryptography, computer/network security, information assurance, cyber operations, and software protection.

Dr. Robert Mills | is an assistant professor of electrical engineering in the electrical and computer engineering department at AFIT. Dr. Mills received a BS degree in electrical engineering with highest honors from Montana State University, an MS degree in electrical engineering from AFIT, and a PhD in electrical engineering from the University of Kansas. His research interests include digital and spread spectrum communications; low-probability-of-intercept and anti-jam communications and networks; signal detection and exploitation; and mobile communication networks and security.

Dr. Gershon Kedem

by Angela Orebaugh

This article continues our profile series of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) Program. The SME profiled in this article is Dr. Gershon Kedem, associate professor in the department of computer science at Duke University. Dr. Kedem's research interests are in computer-aided design (CAD), very large scale integration (VLSI) design, computer architecture, applied combinatorial algorithms, secure collaborative computing, and computer security.

Dr. Kedem received his BS degree from the Hebrew University, Israel, in 1972 and MS and PhD degrees from the University of Wisconsin in 1975 and 1978. Before joining Duke as an associate professor in 1984, he was an assistant professor of computer science at the University of Rochester, Rochester, NY. Dr. Kedem has been teaching and researching computer security topics for over 10 years. He currently teaches a computer and network security course that is focused on very practical skills involving computer attacks and defense and related security tools. One early research effort that Dr. Kedem led is the CipherFlow Project, which used parallel machines for brute force cryptanalysis. Other research papers by Dr. Kedem include—

- "Brute Force Attack on UNIX Passwords with SIMD Computer"
- "Categorizing Attacks on Cryptographic Protocols Based on Intruders' Objectives and Roles"
- "New Procedure for Cryptographic Protocol Analysis"
- "New Attacks on Some Cryptographic Protocols"
- "SADDLE: An Adaptive Auditing Architecture"
- "NOSCAM : Sequential System Snapshot Service"
- "RheoStat : Real-time Risk Management"
- "Real-time Access Control Reconfiguration"
- "Paranoid: A Global Secure File Access Control System"
- "Augmenting Storage with an Intrusion Response Primitive to Ensure the Security of Critical Data"

You can find more information on Dr. Kedem and his research and publications at *http://kedem.cs.duke.edu.* ■

References

Kedem, G., and Ishihara, Y. The CipherFlow Project. *http://kedem.cs.duke.edu/CipherFlow/index.html.*

▷ *continued from page 11*

work well, there will be opportunities for good point solutions. In this consolidation, some previously freestanding product categories will become features within suites, such as data loss prevention (DLP) or network access control (NAC).

Signature-based technology continues to fail us, so new options are required. Some people have thought that signature-based antivirus solutions can address 80% of viruses. New research shows that the real number is actually closer to 40%. Vulnerability scanners face the same coverage problems. Alternative options, such as whitelisting or blended coverage models, are worthwhile solutions to explore.

We expect to see more compartmentalized access and mass centralization of process with the use of more thin clients. In addition, organizations are finding utility models compelling and will do more things through the cloud that they previously would not have considered. ■

Using Technology to Combat Data Loss—What It Can Do, What It Can't

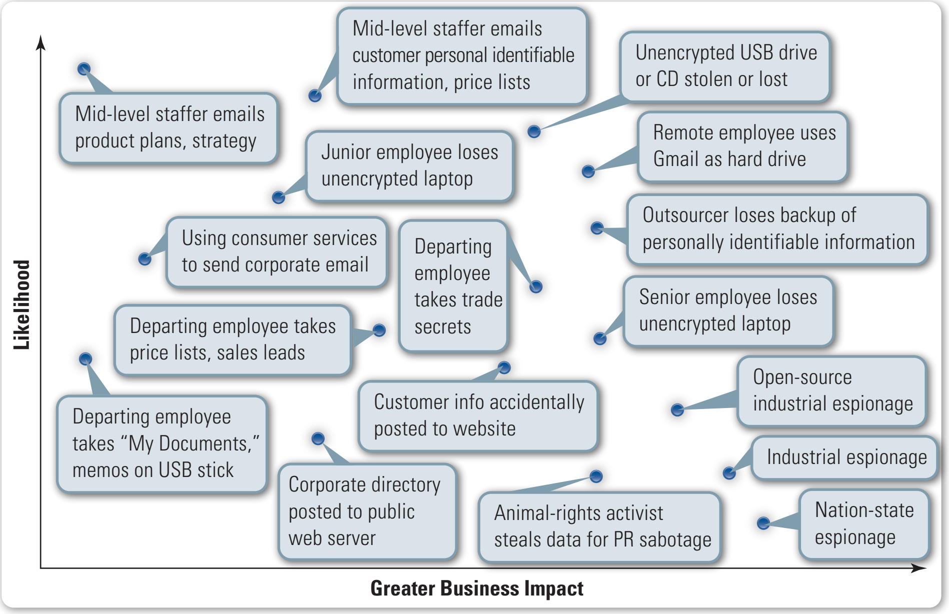
by Nick Selby and Aaron Turner

For the past three years, data loss prevention (DLP) has been one of the hottest sub-sectors of the information security industry, generating breathless hype and confusing marketing statements about how it offers the "solution" to the problem of lost data in the enterprise. DLP is itself not the solution to data leakage any more than the firewall-solved network security, but when used effectively, DLP technologies can comprise part of an overall initiative to control how an organization creates and consumes data internally and externally. DLP products are a key part of a program to understand and inventory data, place actionable metrics around data creation and movement, and then create policies to control the creation, dissemination, storage, use, and ultimate retirement of confidential information.

Data leakage—the inadvertent dissemination of proprietary information—accounts for the overwhelming volume of proprietary and classified or secret information that leaves private and government organizations each year. Whether it's a laptop that's been stolen from a car or left in a taxi, or someone sending out files she shouldn't, data leakage is the most common—and the most preventable—type of data loss.

Data theft, ranging from an employee taking his My Documents files on a USB stick to open source, to commercial and public relations espionage, to nation-state espionage is more challenging to define. It can occur in varying degrees of severity, and is spurred on by a wide range of motives. One thing that is clear is that reducing inadvertent loss allows you to concentrate on the less common, but far more damaging, issues surrounding data theft.

While data theft is as old as recorded data (there's a good case that, before his journey west in 1492, Christopher Columbus and his brother Bartolomeo engaged in some old-fashioned cartographic espionage-for-profit), the nature of digital networks means that by volume, most data losses are inadvertent (see Figure 1).

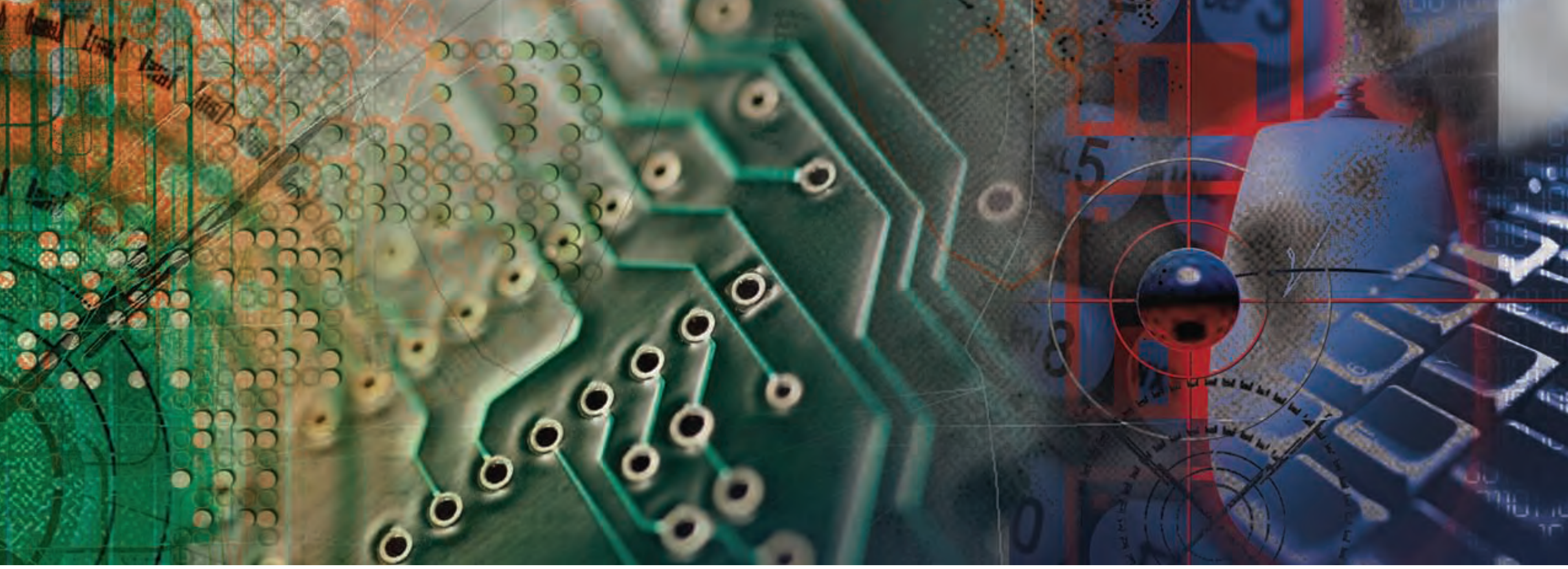


Source The 451 Group

Figure 1

In Figure 1, we see that data loss scenarios like departing employees making off with sales leads or documents are most common, and have a modest impact on the business. It is an understandable human emotion to feel a desire to benefit twice from the same work, and to a certain extent, this kind of behavior is expected. In some industries, it is not such a big deal.

But in others, leaked information can lead to millions in lost revenues, or in the case of nation-state secrets, can literally mean the difference between life and death. In most industries, the



impact of data loss lies somewhere in the middle of those two extremes.

Regardless of industry or government entity, data loss is a symptom of mismanagement of the data supply chain. One reason that this is harder to control in the private sector than in the public is obvious: in the public sector, disciplinary action includes things like forcing people to break big rocks into little rocks—an option not typically available to a private corporation. Whether in a private or public sector organization, management leaders can work with information technology (IT) professionals to build sensible, enforceable policies and procedures to control data loss. It won't solve the problem, but it can reduce it dramatically. And while it may seem as if data is 'leaking out everywhere' you can do some groundwork on your own to get a sense of where it is flowing, where it is leaking, and why.

Implementing a truly effective strategy requires the creation and maintenance of a culture of integrity throughout your organization. Plan ahead for the worst-case scenario, but don't create it: you don't want to be stuck in a situation where you know you have leaking data and under law, such knowledge requires you to take specific action—but you are unable to take any specific action because you have not yet created a process to comply with the law. Put another way, you don't want to be in a position of having to create a process under duress after discovering the data that necessitates it.

Rather, create the process to deal with data loss before you know that it is being lost. This might sound like a Catch-22, but it isn't—begin to build a process around your discovery of data that is (a) sensitive to your business, but (b) does not have a legal or ethical requirement of immediate reaction on your part. Building the process will allow you to handle different types of losses. Once an effective loss process is in place, your organization will be in the position to, for example, discover that it has allowed personally identifiable information to be leaked or lost, and immediately deal with the loss through an established process, which would include notification of law enforcement, notification of the affected customers, isolation of the root cause of the loss, *etc*.

Ask some basic questions

You can get help in this from your IT department and then from the DLP vendors themselves, provided you are clear to them about what you want (and don't want) to find. Start with the basics: where does your data live? Where does your data come from? How does it get from its source to its resting place? Who touches it once it is 'home'? How long does it live? Where does it go when it dies? Does it die? And most important, are you sure?

Understanding your data lifecycle—where your data comes from, how it is used and for how long, then how or if it dies—can unlock untold riches. To the Six Sigma practitioner, the answers to those questions could contain keys to unlocking more efficient processes. To the legal and human resources department, they could mean more sleep at night. And to your chief executive officer (CEO) and chief financial officer (CFO), the bottom line can only be helped by a more complete understanding of how you really do business. Senior management buy-in to this process is essential from the start, and we would recommend having the CEO introduce the company to the project of quantifying your data risk. A senior IT manager and senior business manager should be entrusted with the process, using business and not IT terminology to drive the discovery process.

Determine the expected

How do you expect business will create traffic flows between and within departments? As a first exercise, consider using a large whiteboard in a room full of business and IT folks. Draw dots on the board to represent different departments, and business process by business process, think about which departments communicate with which departments. Before long, there will be a lot of lines between the dots.

As an aid to getting this done, think about typical transactions, and follow the process—from the salesperson getting the lead to following up; bringing in more people to fill in blanks and answer questions; bringing in Legal to make contracts; negotiating a price, outsourcing and contractors, dealing with provisioning that customer once the deal is done; then getting the product made, inspected, packed, inventory-controlled, and shipped, *etc.* Keep going through all the transaction types you can think of until you're ready to kill every other person in the room.

Now look at the whiteboard—there are a bunch of dots and lines between them. The dot with the most lines coming to and from it? That's the department where you start digging. To dig deeper into business processes, IT and business leaders should consider ways of looking at each phase of each business process, asking questions beginning with 'Why do we do this?' While the exact 'hows' of the discovery process are clearly a matter outside the scope of this report, we would suggest some basic principles and a framework. To dig deeper into a single department, replicate this process with your focus solely on communications within that single department to identify expected data flows.

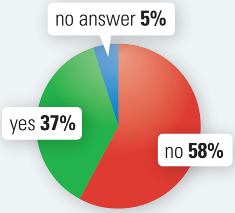
The point of this is to quantify your expectation of traffic and get a sense of expected information flow. Dedicated vendors of DLP products will be able to provide highly customizable and

The Antidata Sidebar

To begin painting a picture of what is happening within end-user organizations, The 451 Group and its partner, ChangeWave, surveyed 381 information technology professionals in a variety of industries. It received responses to a series of questions designed to determine the work that organizations were doing to understand the nature and sensitivity of data traversing their networks.

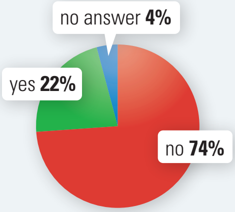
Q: Has your organization done any work to determine where data lives within its network (*e.g.,* scripts, processes or content management systems)?

Nearly 60% of organizations have done nothing to understand the location of data within their networks (or, more specifically, the scripts, processes and content management tools that create and manipulate data). Over the past several years, data sources have proliferated at an exponential rate, and management response or awareness of this has lagged.



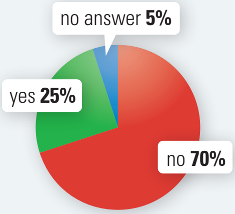
Q: Has your organization done any analysis of interdepartmental communication to determine which departments communicate most frequently with others within the organization?

If organizations are doing a poor job of understanding where their data lives, they are doing an even poorer job of determining where their data goes, especially if the data is moving in that increasingly quaint concept known as 'inside the firewall.' Due to factors including the way companies deal with partners and outsourcers, increased use of smartphones and the emergence of a new social class of work-at-home telecommuters, this concept of the 'big red circle' is nearly meaningless today. Yet at least 74% of companies surveyed state that they have done nothing to determine where data is moving on corporate managed laptops among (presumably) their own employees.



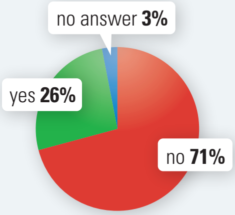
Q: Has your organization done any analysis of external communication to determine which departments communicate most frequently with business partners, outsourcers or unknown third parties?

Organizations are only doing slightly better at making determinations about who their employees are communicating with 'outside the firewall' – that is, either with business partners, outsourcers or even unknown third parties. From a standpoint of information protection, these answers lead us to the clear conclusion that an understanding of where an organization's data is, and how it is being communicated between internal and external parties, is a necessary first step before any attempt is made at classification of data.



Q: Does your organization have a data-classification plan in place? For example, do you classify data as 'public,' 'partner/NDA,' 'regulated,' or 'proprietary'?

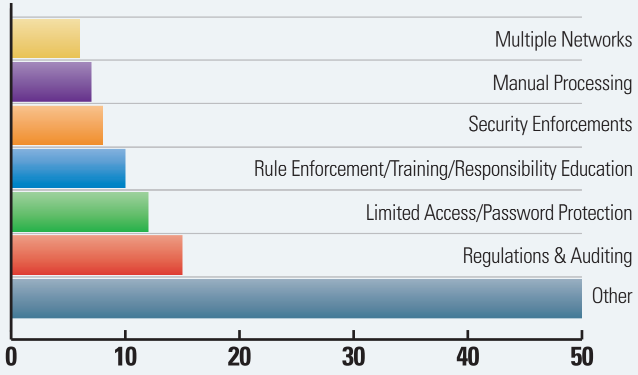
We asked whether organizations are classifying their data, and many – about a quarter – thought they were. However, based on conversations with large numbers of end users about this very subject, we suspect that the actual number of organizations with classification policies in place is lower – substantially – than that. Or at the very least, if, as our survey indicates, about a quarter of companies have programs in place to classify data, as many that were in the Blair Administration might tell you, the difference between a 'program to classify data' and the actual, enforceable classification of data are two vastly different things.



Q: If you do have a data classification plan in place, how is it enforced?

Unsurprisingly, when we delved further into the case, we found that of the people who had said they had data classification in place in their organizations, fully half were unable to state a plausible method by which they enforced such classification. Of the remaining half, we detected a reliance on highly vague statements, which we infer to mean, 'I don't actually know but felt I should say something.' For example, 'regulations and auditing' seems an unlikely practical enforcement mechanism for anything but the smallest of enterprises. A total of 22% of organizations claiming that data-classification programs were in place answered with plausible enforcement capabilities, which jibes with both survey responses to the other questions we asked and with anecdotal evidence in conversations with hundreds of end users. The 451 Group feels it is safe to say that at least 70% of organizations have no effective and enforceable data-classification policy in place.

If yes, how is this policy enforced? (60 responses)



powerful tools once you get to the point of calling one in. The tools you use to confirm whether actual information flow matches expected information flow at first should be free, and should for the most part be something that your existing IT staff can operate.

Start with the lowest-hanging fruit. The Pareto Rule applies here. You're not seeking every single email, but trying to get a grip on the most commonly engaged-in business communication and data transfer. The scope and volume of the problem is the unknown factor that you are trying to understand. Don't try to exceed this goal.

Two tools your IT team will find extremely valuable include the following—

- Netflow analysis tools—Analysis of netflow is probably the best way to start this examination. Make a list of top talkers and ask yourself in each case, 'What business purpose is served by this communication?' Once you get a sense of 'normal,' you can delve into the traffic itself.
- Application firewalls, intrusion detection systems (IDS), ngrep—These are not DLP, but can be used to seek specific strings in traffic and write them to a log file that can be searched; IT staff can then make reports. Be careful not to search for regulated or sensitive data that would require action on your part. A good way to start is to find a clued-in line-of-business manager and ask, 'What non-regulated but business-critical phrase or string would you not want people to email or instant message (IM) out of the building?'—and then search for communications that contain it. At the end of the month, your IT people can make a report showing how many times the string appeared in plain-text emails, documents, or IMs.

Once you have a sense of the problem's scale, an idea of how you expect data to flow and how it actually does and the beginnings of some processes to deal with data loss, you're ready to bring in some DLP vendors to talk about the ways they can be helpful.

Back to the DLP Industry

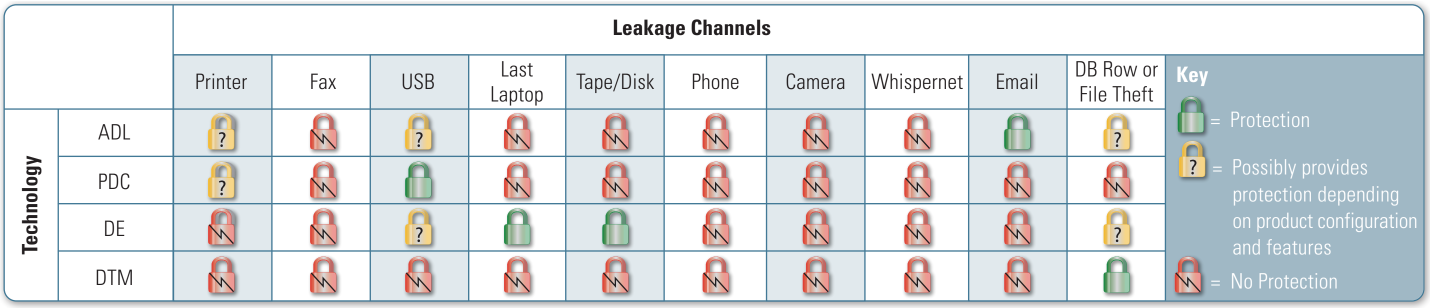
To add some breadth to those breathless marketing claims, let's look briefly at the channels used to disseminate data, and more to the point, the channels that DLP technologies try to cover. We categorize DLP as comprising anti-data leakage, port and device control, disk and file encryption, and database transaction monitoring technologies (services that track down digital assets once they've been exfiltrated are related but outside the scope of this article). Even the combination of all these approaches—a combination we might add is rarely offered by any single vendor—would be powerless against a slew of data loss channels, from telephones to camera phones to whispered conversations.

The basic concept of data leakage detection products is simple: 'If we can see the data as it moves, rests or is used, we can search it for information that is 'sensitive'—as defined either by regulations or by the organization—and if so, do…something.' The 'something' could be as simple as creating a log of the event, emailing a data guardian for review, or blocking its transmission.

But where to 'look' at the data? A religious debate arose among IT professionals as to whether the best place to look for data was 'in-flight' (as it traversed the network) or 'at-rest' (on the actual computers used by workers—a classification tool operating very much like anti-virus programs or rootkits: at the kernel level of the operating system—this allows too for examination of the data as it is used). Or, both: monitor traffic as it moves across the network and install software agents on each machine?

Generally speaking, both network- and agent-based monitors faced serious challenges. On the network side, capturing enough data fast enough to be useful, then interpreting the various document formats (Word, Excel, email, Zipped files, *etc.*), searching through those documents to find keywords that match pre-determined words, phrases, or signatures and then attempting to take action was processor-intensive.

Building filters to crack open the document formats in all their versions was research and development-intensive (and quite possibly illegal, as it required 'reverse engineering' of copyrighted, binary code in products like Microsoft Office and WordPerfect). Even if they could do it, the processes were resource-intensive and slow. Many DLP vendors licensed document decoders from specialist firms like Oracle (Stellant) or Autonomy to do that part. Those



		Leakage Channels									
		Printer	Fax	USB	Last Laptop	Tape/Disk	Phone	Camera	Whispernet	Email	DB Row or File Theft
Technology	ADL	?	✗	?	✗	✗	✗	✗	✗	✓	?
	PDC	?	✗	✓	✗	✗	✗	✗	✗	✗	✗
	DE	✗	✗	?	✓	✓	✗	✗	✗	✗	?
	DTM	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓

Key
✓ = Protection
? = Possibly provides protection depending on product configuration and features
✗ = No Protection

Source: The 451 Group

Figure 2 DLP technologies make it harder to steal, and much harder to inadvertently leak, data.

Anti Data Leakage	Port and Device Control	Disk/File Encryption	Database Transaction Monitoring
Symantec (Vontu)	Safend	Check Point (Pointsec)	Guardium
McAfee (Reconnex)	Check Point (Pointsec)	Sophos (Utimaco)	Imperva
Fidelis	Trend Mirco (Provilla)	PGP	Sentrigo
Websense (Port Authority)	GuardianEdge	McAfee (SafeBoot)	Secerno
Verdasys	Verdasys	WinMagic	Application Security, Inc
Vericept	Credant	GuardianEdge	

Figure 3 Selected DLP Vendors by Product Category (not complete; not a ranking)

familiar with IDS will immediately see the similarity of approach, challenges, and ultimate efficacy.

Operating at the kernel level, as a file-filter—essentially standing between the operating system and any attempt to write to disk—does grant great visibility into everything that a user is doing. It was a small step, for example, to get hold of data in system memory or the Windows Clipboard to prevent people from simply taking and then printing screenshots of what they were viewing. This could mean catching a leak before it happened—preventing pasting of sensitive data from one document into another, for example.

But while building an agent is relatively easy, building a good one is really hard. Microsoft Windows is a complex and rapidly changing beast, and rootkits tend to cause crashes, lead to the infamous 'Blue Screen Of Death' (when the entire Windows environment crashes, forcing a restart and the loss of all unsaved data) or at the very least, to interfere with the functionality of other Windows programs, processes, or anti-malware and anti rootkit agents.

Another problem became clear very quickly: most of the data these products sought to examine was unstructured, meaning that an on-the-fly examination and audit was less practical than classification of extant data in addition to classification of data as it is created. Indexing, or making structured tables of extant data to tie words and objects to documents is the classic method of searching—all search products at some point use an index to speed up the process of search. In addition to the document opening and search, many of these products began to look to ways to pre-index documents resident on the hard drive.

The approach eventually taken has varied slightly from vendor to vendor, but essentially it involves examination of each file it sees on the wire, on a file server, or on a hard drive; opening it, removing articles, stemming words (removing the '–ing' and '–ly'); and then creating an index. To speed up searches, document data objects are hashed then 'registered' with the agent or box. Again, the analogy to IDS is tempting, though we would say that DLP signatures are more flexible and encompassing in DLP since it seeks concurrently document, word, phrase, and regular expression matching.

Of course, it can get more complex: statistical analysis, complex subsets of overlapping hashes, behavioral analytics, and other methods have been introduced. Most DLP products offer the ability to set a search 'window', so for example, one can say that if we detect a document with several words within a certain proximity of one another, it can say it has discovered a partial match to a document. This is helpful when trying to detect data loss in which someone copies a block of text from a Word document and pastes it into a differently-named text file or into the body of an email.

But hashing documents requires finding documents—knowing where to look—and in a large organization, that is its own enormous problem. Getting the documents indexed and hashed takes time, so it's a bit like painting a bridge—by the time it has completed its index, the file server is filled with new documents (the side you started on has begun to rust), so one needs to go back and index the files (paint the bridge) again.

For technology to have a chance at success in reducing data loss—and note we say 'reduce', not 'prevent' or, dare we say it, 'solve'—it must take a credible shot at addressing competently the issues laid out above plus have enterprise-class centralized management, reporting, and audit features. It also must be deployed as part of an enterprise-wide initiative to develop processes that leverage technology to help people understand where their data is coming from, what kind of data it is, where it resides, where it travels, where it rests, and where and how it dies. Without the integrity of those processes, no technology stands a chance at stanching the flow of data from your organization.

That is not by any means to say that technology, particularly the technologies that are being marketed as DLP, cannot play a useful, or indeed a key role, in helping to prevent data loss. It does mean that they cannot do them alone.

About the Authors

Nick Selby | is Vice President and Research Director of the Enterprise Security Practice at The 451 Group, and CEO and co-founder of Cambridge Infosec Associates, Inc., a consultancy. He and **Aaron Turner** are at work on a book on strategies to control enterprise data loss. Portions of this article appeared as part of The 451 Group's "Mind The Data Gap," available at *http://the451group.com.* Mr. Turner is CEO of rFinity and has served the Idaho National Laboratory as Cybersecurity Strategist for the National & Homeland Security division, and was Security Readiness Manager for Microsoft, where he led the development of the information security curriculum.

Cyber Security and Information Assurance Metrics State-of-the-Art Report

by Nadya Bartol

The IA Metrics SOAR will include a broad set of subjects from current CSIA metrics-development methodologies and the multitude of definitions of CSIA metrics to research attack-based measures and software assurance measurement.

The Information Assurance Technology Analysis Center (IATAC) is developing an information assurance (IA) Metrics state-of-the-art report (SOAR) to describe a broad picture of the current state of cybersecurity and IA (CSIA) and the summary of progress made over the last eight years since IATAC published the "Critical Review and Technology Assessment (CR/TA) Report" in 2000. The SOAR and supporting research will support the Office of the Director, Defense Research & Engineering goal of understanding and improving cybersecurity and information assurance metrics. The intended audience of the IA Metrics SOAR is the Department of Defense (DoD) and US Government research and development community, senior DoD officials, as well as government and industry IA practitioners.

Metrics mean many things to many people, and the IA community has not yet agreed upon a single definition of metrics nor on a single set of terms for describing activities that quantify the state of IA. The IA Metrics SOAR will include a broad set of subjects from current CSIA metrics-development methodologies and the multitude of definitions of CSIA metrics to research attack-based measures and software assurance measurement. The report will list currently used terms and definitions that describe CSIA metrics-like activities, including IA metrics, CSIA metrics, and information security metrics. It will also address the fact that the terms "metrics" and "measures" are used interchangeably and that the majority of standards bodies are moving towards standardizing the term "measures." To demonstrate the variability in the meaning of metrics, the SOAR will list definitions found in national and international standards and best practices documents. The SOAR also will summarize existing standards, guidelines, and best practices for development and implementation of CSIA metrics, including those by the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Department of Homeland Security (DHS) Software Assurance (SwA) Measurement Working Group (WG), Open Web Application Security Project (OWASP), Securitymetrics.org, and others.

The report will tackle a challenge of describing a variety of CSIA activities that provide measurable data and statistics on IA that are sometimes referred to as metrics, such as blue team/red team evaluations, computer network defense (CND) assessments, static and dynamic code reviews, vulnerability and network management, Federal Information Security Management Act (FISMA) evaluations, certification and accreditation, and potentially other activities. The report also will describe current efforts to make security more measurable through a variety of protocols and enumerations and those activities that leverage these protocols and enumerations, including the National Vulnerabilities Database (NVD), Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), Common Configurations Enumeration (CCE), Common Vulnerabilities Common Scoring System (CVSS), Common Configurations Scoring System (CCSS), and Secure Content Automation Protocol (SCAP) Program. The SOAR will provide pointers and links to publicly available CSIA metrics lists, including those

▷▷ continued on page 28

The Evolving Domain of Cyber Warfare: An Update

by Dondi West

Disclaimer

The views expressed in this article are those of the author alone and do not reflect the official policy or position of the Department of Defense, United States Strategic Command, or any other entity of the US Government.

Introduction

In 2003, the White House published the "National Strategy to Secure Cyberspace," (National Strategy) a document that presented cybersecurity as a subset of homeland security by outlining three strategic objectives: to prevent cyber attacks against America's critical infrastructures; to reduce national vulnerability to cyber attacks; and to minimize damage and recovery time from cyber attacks that do occur. [1] The National Strategy was just the start. President Barack Obama, within his first 100 days, commissioned a 60-day study on cyber and began planning a Pentagon Cyber Command to coordinate both cyber security and offensive cyber warfare. [2]

To realize the importance of such an initiative, one needs to look no further than two events that caused the world to witness cyber warfare on an international scale. First, in April 2007, a series of cyber attacks swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers, and broadcasters amid Estonia's row with Russia about the relocation of the Bronze Soldier of Tallinn, a Soviet-era memorial to fallen soldiers, as well as war graves in Tallinn. [3] Second, during the Russia-Georgia conflict in August 2008, a multi-faceted cyber attack was conducted against the Georgian infrastructure and key government websites. The attack modalities included defacing websites (hacktivism); web-based psychological operations (PSYOPS); a fierce propaganda campaign; and distributed denial-of-service attacks (DDoS). [4]

These two events were noteworthy to US cybersecurity professionals who were concerned that attacks of those magnitudes would one day end up on US "virtual soil." Ironically, and a little closer to home, in November 2008, the Pentagon suffered a cyber attack so alarming that it took the unprecedented step of banning the use of external hardware devices such as flash drives and DVDs. [5] In April 2009, the Wall Street Journal (WSJ) reported that the US electrical grid has been penetrated by cyber spies. Days later on the front page, the WSJ reported that cyber hackers have breached the Pentagon's $300 billion Joint Strike Fighter project. Will it take a "Cyber 9/11" in order to fully appreciate how cyberspace is truly a domain of warfare; or has the US Government finally gotten the message?

Currently, a significant part of the cyber mission falls under the United States Strategic Command (USSTRATCOM)'s Joint Task Force-Global Network Operations (JTF-GNO) and Joint Functional Component Command-Network Warfare (JFCC-NW). Because Cyber Command is expected to be a part of USSTRATCOM, creating Cyber Command will likely cause a substantial amount (or all) of JTF-GNO and JFCC-NW's missions to merge. While efforts to protect the DoD Global Information Grid (GIG) enjoy high visibility, it is necessary to recognize DoD's offensive cyber warfare efforts that empower warfighters and deter attacks against the GIG. To completely understand cyber, we must consider it within the context of the three domains of computer network operations (CNO). The creation of Cyber Command shows that there is a major effort to overhaul cyber security.

Securing Cyberspace Appears to be a major National Security Priority as the Obama Administration is in the process of Creating a New Pentagon Cyber Command

Even in the midst of a dire economic crisis, the Obama administration appears to be committed to securing cyberspace. President Obama, America's most tech-savvy president, is likely to dedicate significant resources on cyber. In fact, analysts estimate he will spend up to $1 billion on biometrics alone. [6] During White House Budget Director Peter Orszag's confirmation hearing, cybersecurity was touted as a major priority of the Obama administration. [7]

Prior to President Obama taking office, the Center for Strategic & International Studies (CSIS) released an informative report, "Securing Cyberspace for the 44th Presidency," to highlight the importance of cybersecurity, cyber-terrorism, and other threats that exist within cyberspace. In this report, the CSIS Commission on Cybersecurity for the 44th Presidency found that—

- Cybersecurity is now one of the major national security problems facing the United States.
- Decisions and actions must respect American values related to privacy and civil liberties.
- Only a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will improve the situation. [8]

Upon taking office, President Obama commissioned a 60-day study to review the plans, programs, and activities related to cyber security. As of the date of this publication, the details concerning the results of this study are being finalized. But, according to a draft memo by Defense Secretary Robert Gates, a new Cyber Command will be created in order to coordinate cyber security and warfare. Cyber Command will reportedly be collocated with the National Security Agency (NSA) at Fort Meade, MD, and be directed by Lieutenant General Keith Alexander, who is both the director of the NSA and Commander of JFCC-NW. Cyber Command is expected to be a part of USSTRATCOM. [9] Creating Cyber Command, therefore, will likely cause a substantial amount (if not all) of JTF-GNO and JFCC-NW's missions to be combined. Nevertheless, analysts tout President's Obama's move to create Cyber Command as a major step toward securing and dominating cyberspace. A look into the missions of JTF-GNO and JFCC-NW, along with the three domains of Computer Network Operations, may give a glimpse into the new Cyber Command.

JTF-GNO—Securing the DoD Global Information Grid

Even prior to the publication of the National Strategy, by statute, the Secretary of Defense was given the responsibility to "protect and defend DoD information, information systems, and information networks that are critical to the Department and the armed forces during day to day operations and operations in times of crisis." [10] Thus, on a day-to-day basis, each service, agency, and combatant command has the responsibility to protect and defend its computer data and networks that are interconnected with the DoD GIG. With the director of the Defense Information Systems Agency (DISA) as its commander, the JTF-GNO, a subordinate command of USSTRATCOM, directs the operation and defense of the GIG to assure timely and secure net-centric capabilities across strategic, operational, and tactical boundaries in support of DoD's full spectrum of war fighting, intelligence, and business missions. [11]

The Three Pillars of Computer Network Operations—Computer Network Attack, Exploitation, and Defense

According to Joint Publication 3-13, the full-spectrum of CNO encompasses three domains: computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND). Within the military domain, CNO is considered one of five core capabilities under Information Operations (IO). The other capabilities include PSYOPS, military deception (MILDEC), operations security (OPSEC), and electronic warfare (EW). The Joint Publication also defines each of the three domains of CNO—

- CNA includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within enemy computers and computer networks.
- CNE includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.
- CND includes actions taken via computer networks to protect, monitor, analyze, detect, and

respond to network attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple defense information systems and networks.

The term "cyber" can sometimes be abused. It is therefore necessary to understand it within the context of which of the three CNO domains are being referenced. For example, for the most part, JTF-GNO, as described above, is concerned with CND.

Offensive Cyber Warfare (CNA) and JFCC-NW

Although closely related to the mission of JTF-GNO, offensive cyber warfare mainly falls under the domain of CNA. In fact, the terms offensive cyber warfare and CNA are oftentimes used interchangeably. The 2006 National Military Strategy for Cyberspace Operations states that, "As a warfighting domain…cyberspace favors the offense." As such, offensive capabilities in cyberspace offer both the US and our adversaries an opportunity to gain and maintain the initiative. According to the USSTRATCOM website, JFCC-NW was established in order to coordinate offensive cyber warfare. The commander of JFCC-NW is also the director of the NSA. Offensive cyber warfare has the dual benefit of achieving strategic objectives for military commanders while deterring attacks against the DoD GIG. Many aspects of DoD's CNA mission are highly classified, but considering the net-centric nature of today's society and recent events, one can imagine how important it is for the DoD to maintain readily-deployable CNA capabilities. [12]

Draft Legislation worth Tracking

In addition to the creation of Cyber Command, pending legislation reflects the high priority of overhauling cyber security. In April 2009, two cyber security bills (S. 773 and S. 778) were introduced in the 111th Congress by Sen. John D. Rockefeller IV (D-W.Va.), Sen. Olympia Snowe (R-Maine) and Sen. Bill Nelson (D-Fla.). Some of the provisions of these bills come from CSIS's "Securing Cyberspace for the 44th Presidency" report. Other provisions have received mixed reviews, such as S. 773's controversial provisions giving the President broad power to declare a "cybersecurity emergency" and shut down government networks and possibly parts of the public Internet. [13]

- **S. 773: Cyber Security Act of 2009.** A bill to ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes. Draft Bill available at *http://tiny.cc/Rqvw4*.
- **S. 778: Untitled.** A bill to establish, within the Executive Office of the President, the Office of National Cybersecurity Advisor. Draft Bill available at *http://tiny.cc/HpMpG*.

Conclusion

The need to defend the DoD GIG and maintain the ability to conduct offensive cyber warfare will only increase. The "National Strategy to Secure Cyberspace" was just the start of the US Government's commitment to secure and dominate cyberspace. President Obama, within his first 100 days, has shown that securing cyberspace is and will remain a priority in his administration. The term "cyber" is broad, making it necessary to understand it within the context of the three pillars of CNO. USSTRATCOM's JTF-GNO and JFCC-NW remain substantial players within the realm of cybersecurity and warfare, although the creation of Cyber Command under USSTRATCOM will likely cause their missions to merge.

References

1. The National Strategy to Secure Cyberspace. February 2003. *http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.*
2. Gorman, S. "Gates to Nominate NSA Chief to Head New Cyber Command." The Wall Street Journal, April 24, 2009.
3. Traynor, I. "Russia accused of unleashing cyberwar to disable Estonia." The Guardian, May 17, 2007.
4. Coleman, K. "Cyber War 2.0 – Russia v. Georgia." Defense Tech, August 13, 2008. *http://www.defensetech.org/archives/004363.html.*
5. Lohrmann, D. "Cyber Attack Leads Pentagon to Ban Removable Drives." Securing GovSpace, November 23, 2008. *http://www.govtechblogs.com/securing_govspace/2008/11/cyber-attack-leads-pentagon-to.php.*
6. Lipowicz, A. "Analyst: Obama may spend a billion on biometrics." Federal Computer Week, January 7, 2009. *http://fcw.com/articles/2009/01/07/analyst-obama-may-spend-a-billion-on-biometrics.aspx.*
7. "Orszag Promises More Oversight and Transparency." The Washington Post, January 14, 2009. *http://voices.washingtonpost.com/federal-eye/2009/01/orzsags_testimony.html?hpid=topnews.*
8. Securing Cyberspace for the 44th Presidency. CSIS Publications, December 8, 2008. *http://www.csis.org/component/option,com_csis_pubs/task,view/id,5157/.*
9. Gorman, S. "Gates to Nominate NSA Chief to Head New Cyber Command." The Wall Street Journal, April 24, 2009.
10. US Code Title 10 U.S.C. § 2224, "Defense Information Assurance Program." January 3, 2007.
11. USSTRATCOM [Online] *http://www.stratcom.mil/.*
12. Lasker, J. "U.S. Military's Elite Hacker Crew." Wired.com, April 18, 2005. *http://www.wired.com/politics/security/news/2005/04/67223.*
13. Bradner, S. "Yet Another Government Attempt at Cybersecurity." Computerworld, April 6, 2009.

About the Author

Dondi West | currently supports DoD clients as a senior cyber intelligence analyst. In addition, Mr. West is the lead author of *The Cyber and Business Law Commentary* blog at *http://cyberblc.blogspot.com.* He received a BS degree in mathematics, an MS degree in applied information technology, and is currently a 2010 Juris Doctor candidate at the University of Maryland School of Law, where he also is a staff member on *The Maryland Law Review.*

Duke University Department of Computer Science

by Angela Orebaugh

Duke University, founded by James B. Duke in 1924, is located on 9,000 acres in Durham, NC. It is home to over 13,000 students, roughly a 50/50 split between undergraduate and graduate students. Duke's nine schools and colleges consist of arts and sciences, law, divinity, graduate, medicine, nursing, environment and earth sciences, engineering, and business. The Trinity College of Arts and Sciences houses Duke's department of computer science.

The department of computer science at Duke University offers a combination of teaching and research programs that engages with the broader community at Duke, Research Triangle Park, and beyond to advance the state of the art in computing and information technology. The department of computer science offers PhD, MS, BS, and BA degrees. The department also offers a cooperative double major with the department of Electrical and Computer Engineering (ECE). It offers a wide range of programs, including geometric computing, Internet systems, networking, security, biological computing, memory systems and massive data management, learning, and modeling. Research initiatives also exist in computer graphics and visualization, sensor networks, numerical analysis, software engineering, complexity theory, and robotics. Many of these research areas overlap with other disciplines such as biology, engineering, nanotechnology, and environmental sciences.

A unique characteristic of Duke's computer science department is the symbiosis that exists between education and research faculty. This synergy is critical in continuously reforming and strengthening the curriculum and integrating research and education. The department uses a dual approach to combine research and education by bringing research into the curriculum to train students about emerging technologies. One such example is the integration of information, network, and computer security into various curriculums such as parallel computing and distributed systems. Several computer science department faculty integrate security teaching and research into their curriculums as it relates to their disciplines. They encourage students at both the undergraduate and graduate levels to pursue independent study topics in areas they find intriguing and challenging, many of which include information security-related topics. ■

The department of computer science at Duke University offers a combination of teaching and research programs that engages with the broader community at Duke, Research Triangle Park, and beyond to advance the state of the art in computing and information technology.

Reference

Duke University Department of Computer Science. [Online]. *http://www.cs.duke.edu.*

About the Author

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

▷ continued from page 23

available from NIST Special Publication (SP) 800-55 Revision 1, DHS SwA Measurement WG, and others.

Measurement is a broad discipline that encompasses quantitative and qualitative activities such as ratings and rankings. The SOAR presents quantitative and qualitative metrics, such as maturity model rankings and other ratings methods. It will summarize existing research within and outside DoD and the US Government on the subject of CSIA measurement and will identify gaps in the research. The report also will summarize current views and existing approaches to quantifying economic value of security, such as return on investment and other economic indicators, and will identify linkages with CSIA measurement activities required to support creation of these economic indicators.

Finally, the SOAR will also discuss the reasons why so many CSIA metrics efforts fall short of the expectations that the stakeholders place on these efforts and will describe characteristics of successful efforts. The SOAR will identify existing gaps between expectations and the state-of-the-art and provide recommendations for filling the identified gaps where appropriate. IATAC will publish the IA Metrics SOAR in May 2009. ■

About the Author

Nadya Bartol | has worked with multiple government and industry organizations to develop and implement information security measurement programs. She co-authored NIST guidelines on security measurement and is one of the primary experts working on ISO/IEC 27004, Information Security Management Measurement. Nadya is serving as the Co-Chair of Department of Homeland Security (DHS) Software Assurance Measurement Working Group and was the primary author of Practical Measurement Framework for Software Assurance and Information Security. She is an active member of the ISO standards community developing information security and privacy standards.

Letter to the Editor

Q ***Can you please tell me how to get a copy of the latest Information Assurance Technology Analysis Center (IATAC) State-of-the-Art Report (SOAR), The Insider Threat?***

A The Insider Threat SOAR is marked For Official Use Only (FOUO) and distribution code "C" (US Government agencies and their contractors). If you have a .mil or .gov email address, you may request a copy by sending an email to *iatac@dtic.mil.* If you do not have a .mil or .gov email address, you may obtain a copy through the Total Electronic Migration System (TEMS). To access TEMS, you must have a valid Common Access Card (CAC) or be a Defense Technical Information Center (DTIC) registered user. (See registration instructions at *http://www.dtic.mil/dtic/registration/*.)

Q ***I am a government contractor working at a government client site. I do not possess a Common Access Card (CAC) or a government assigned email address but would like to have DoDTechipedia access. Is this possible?***

A The answer is YES. You can acquire access to DoDTechipedia even without a CAC or a government assigned email address. With the permission of the Contracting Officer Representative (COR) and their agreement to sponsor you, you can register for a Defense Technical Information Center (DTIC) account at *http://www.dtic.mil/dtic/registration*. Once you are approved and registered, you may use your DTIC credentials to register with DoDTechipedia at *https://www.dodtechipedia.mil/dodwiki.*

Paranoid: A Global Secure File Access Control System

by Dr. Gershon Kedem

As the ability to share information has increased, so has the desire to protect information. When information security measures make it too difficult to share information, however, people generally choose to assume the risks involved with making their information available. The Paranoid file system helps solve this problem. It allows users to share information easily while also maintaining appropriate levels of information security.

The Paranoid file system [1] is a "proof of concept" encrypted file system. It implements an encrypted, secure, global file system with user managed access control. The system provides efficient peer-to-peer, application-transparent file sharing, while allowing users to grant safe, selective, UNIX-like, file access to peer groups, regardless of administrative boundaries. Group members similar to web users can be anywhere; they need not have local accounts, nor do they need direct access to local files. Files are kept encrypted and access control translates into key management. The system uses a novel transformation key scheme and access control that enables access revocation. Paranoid also works seamlessly with existing applications through the use of interposition agents. A layer of indirection makes it possible to access remote files and use encryption/decryption without OS-kernel modifications. Performance evaluations show that encryption and remote file-access overheads are small, demonstrating that the Paranoid system is practical.

Paranoid uses a hybrid encryption scheme. Symmetric keys are encrypted with the owner's public key, and each file is encrypted with a different random symmetric key. The encrypted key, along with the file's digital signatures, a version number, and a time-stamp are stored in the header part of the encrypted file.

In addition to its hybrid encryption scheme, the Paranoid system uses a novel scheme for group sharing. When a group owner creates a new file-access group, he creates a new public and private key pair for the group using the RSA public key cipher. [2] He publishes the group public key. All group members use the same modulus N, but each group member is given a different private key. Associated with each group member's private key is a transform key known only to the group owner.

When a group member requests access to a file, the group owner applies a member-specific transform key to the file's group-encrypted symmetric key. The transformation changes the symmetric key's encryption from an encryption with the group public key to an encryption that corresponds to the member's unique private key. Both the file and the transformed symmetric key are sent to the member. The member uses her private key to decrypt the symmetric key and uses the symmetric key to decrypt the file.

It is important to note that explicit authentication is not used. The system relies on the fact that only the designated group member holds the member-specific private key, and therefore only she can access the file content. Others that do not possess the private key can't access the file's content. To revoke group member access rights, the group owner deletes the member's transform key.

In order to implement a global encrypted file system, we use the Bypass system, [3] which allows us to augment the I/O system by replacing a selected set of system calls with code that we supply. The Bypass system traps system calls and executes users' supplied code in user space. By modifying selected system calls, we extend the UNIX file system to include a global encrypted file system. Since the extension is done at the system-calls level, the extended file system is totally transparent to existing applications. For example, the UNIX text editor vi was used, unchanged, to access and modify encrypted remote files.

To share files globally, a file server agent running on the group owner's machine provides secure global file sharing. This process authenticates access requests on behalf of the owner, performs key transformations, sends requested files to group members and writes files on behalf of group members. Modifying group access rights is done by adding,

▷▷ continued on page 34

Information Assurance Risk Assessment (IARA)

by Dr. Larry Johnson and Deborah Williams

Information Assurance Risk Assessment Process for Military Systems

Challenge

The emergence and implementation of the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) and the associated information assurance (IA) controls have infused greater rigor and repeatability into the practices of assessing information assurance postures of government DoD systems. [1] By using these controls as the objective benchmarks, a system's security can be measured against consistent and well-defined criteria. While these controls offer a solid way to measure compliance with applicable standards, they fall short with regard to risk assessments. From a risk perspective, not all controls are created equal. That is, compliance with some controls affords a greater risk reduction than compliance with other controls. Similarly, the costs and time associated with achieving compliance with unique controls vary significantly depending upon conditions inherent in the system and the operational profile of the system. Given these system- and environment-driven constraints, information security analysts need a well-defined, documented, repeatable process to assess the risks accruing from non-compliance with the DoD 8500.2 controls.

Purpose and Applicability

IARA provides step-by-step guidance to information systems security professionals across DoD in their efforts to make meaningful risk assessments based on a documented, defendable, and repeatable process. IA professionals can apply this process to assessments of US military systems, and meet the new risk management requirements specified in CJCSM 6510.02. While this paper provides only a summary level IARA description, the full step-by-step IARA process can be found at *http://www.sentar.com/informationassurance.htm#assessments*.

The processes described in this paper facilitate discrete risk assessments for specific IA control non-compliances and IA issues that are found within a system. [2] The objective of IARA is to provide a consistent, methodology that—

- Is appropriate for the multitude of information technology (IT) systems within the military regardless of criticality, scope, and mission
- Is benchmarked against accepted DoD/civilian agency/international/industry standards
- Facilitates a risk-ordered ranking across multiple non-compliance issues within the same system
- Supports the development of risk-based plans of action and milestones (POA&M) for issue mitigation
- Supports certification determinations
- Includes system stakeholders as part of the overall process

While the IARA is designed to produce well-documented, defendable, and repeatable risk assessments, there are some caveats that the user should keep in mind. Solid risk assessments are an outcome of a well-defined process being used by knowledgeable analysts. Best results will come from analysts who have a clear understanding of the following—

- Mission, function, and operation of the system being assessed
- Information system architecture
- Information systems security architecture

A solid grasp of these three critical and inter-related aspects of the system being assessed is critical for a well-founded risk assessment.

The Information Assurance Risk Assessment Process Flow

The overall IARA process flow is shown in Figure 1. It may be used to determine the operational risks associated with IA vulnerabilities identified during certification and accreditation (C&A) testing, and any other risk assessment based upon identified non-compliance with an IA control or other requirement. The IARA process flow begins with an *understanding of the threat* that characterizes the information system (IS) and its operational environment. This

understanding provides the necessary insight into the threat motive, means, and opportunity that is essential for application of the IARA process itself to determine true IA to the operational mission of the system stemming from an identified vulnerability. The actual IA risk assessment process flow consists of five sequential steps as indicated in Figure 2.

Selection of the Appropriate Risk Rating Criteria and Evaluation Matrix

IA vulnerabilities may arise within two considerably different domain contexts. Many IA vulnerabilities stem directly from conditions that are purely in the realm of computer security (CS) concerns (*e.g.*, weak patch profiles,

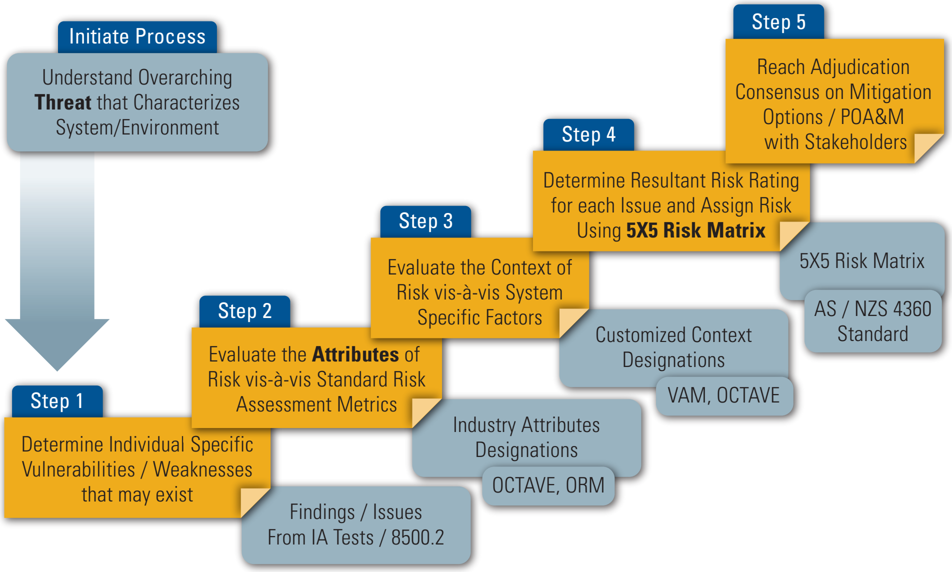

Initiate Process
Understand Overarching **Threat** that Characterizes System/Environment
Step 1
Determine Individual Specific Vulnerabilities / Weaknesses that may exist
Findings / Issues From IA Tests / 8500.2
Step 2
Evaluate the **Attributes** of Risk vis-à-vis Standard Risk Assessment Metrics
Industry Attributes Designations
OCTAVE, ORM
Step 3
Evaluate the Context of Risk vis-à-vis System Specific Factors
Customized Context Designations
VAM, OCTAVE
Step 4
Determine Resultant Risk Rating for each Issue and Assign Risk Using **5X5 Risk Matrix**
5X5 Risk Matrix
AS / NZS 4360 Standard
Step 5
Reach Adjudication Consensus on Mitigation Options / POA&M with Stakeholders

Figure 1 IARA Process Flow

Step	Process	Expanded Description of Process
1	Determine the individual, specific IA vulnerabilities that may exist within the system, component or sub-system	An IA analyst, who will document the analysis results as part of the IARA process, makes vulnerability determination. Specific vulnerabilities may stem from C&A testing, other IA Vulnerability testing, or from IAVAs.
2&3	Identify the appropriate "Likelihood" and "Consequence" risk factors associated with each vulnerability and failed IA Control, and then determine the resultant overall risk posed by the vulnerability.	Risk determination is made by an IA analyst, who will document the rationale for "Likelihood," "Consequence," and "Risk" determination as part of the IARA process. Section X contains the detailed assessment process for "Likelihood," "Consequence," and "Risk" evaluation.
4	Assign an Initial Risk Rating and mitigation approach for each failed IA Control or identified vulnerability, based on the results from Step 2 and Step 3 above, and adjudicate with system stakeholders (developers, system-security engineers, Program Managers and others as appropriate)	The Initial Risk Rating is based on the analyzed risk associated with each failed IA control or other identified IA vulnerability. The analyst assigns an initial risk rating and mitigation approach to each failed control. The risk rating and mitigation approach is finalized when stakeholder adjudication is complete.
5	Develop POA&M, make Certification Determination, and staff with all stakeholders. Results of interactions with stakeholders may introduce new information causing the analyst to adjust the initial risk rating.	Based on the final risk rating reflecting any adjustments reached through adjudication efforts with stakeholders, the IA analyst assigns the final risk rating.

Figure 2 Detailed Steps in the IARA Process Flow

Control Family Heritage	Control Family	Recommended IARA Allocation
DoDI 8500.2	Security Design and Configuration (DC)	PEPA
	Identification and Authentication (IA)	CS
	Enclave and Computing Environment (EC)	CS
	Enclave Boundary Defense (EB) CS	CS
	Physical and Environmental (PE)	PEPA
	Personnel (PR)	PEPA
	Continuity (CO)	PEPA
	Vulnerability and Incident Management (VI)	PEPA

Figure 3 Recommended Allocation of Controls to CS and PEPA Grading Matrices

incorrect privilege settings, poor passwords, *etc.*). Alternatively, vulnerabilities may stem from factors that relate to the overall operational environment in which the IS operates, and could affect the overall IA posture, but are not directly correlated to CS vulnerabilities. Vulnerabilities that may not be attributed directly to CS may include shortcomings in the programmatic (*e.g.,* policies, component documentation, design, *etc.*), environmental, physical, and/or administrative security posture of an IS. This recognition suggests that the analyst must know the proper domain context of each IA control before conducting a risk assessment of a vulnerability associated with that control. The analyst must correctly discern between operational risk stemming from vulnerabilities that are sufficient in and of themselves to have a high probability of resulting in a *direct* CS IA exploit with potential operational consequences, and operational risk stemming from vulnerabilities that create an environment in which an IA weakness could *indirectly* lead to adverse mission consequences.

For the purposes of IARA, the analyst may consider that CS vulnerabilities are limited to those with a direct IA impact, and the programmatic, environmental, and/or physical/administrative security (PEPA) vulnerabilities may be considered as having an indirect impact. As such, the likelihood and consequence determination scales for CS- and PEPA-based vulnerabilities are different. Each control as contained within DoD Instruction 8500.2 may be allocated to either the CS or the PEPA grading scale. While the allocation of specific controls may differ for various systems, a general allocation of controls may be based upon the family designator of the controls. Figure 3 presents a recommended allocation for DoD Instruction 8500.2 controls.

Conclusions

While the IARA process may be extended to IA risks within systems existing within other public and private sector concerns, the construction of the matrix tables and associated weightings have been developed with a particular focus to IA risk assessments for US military arenas. Similarly, the IARA process as described here-in has been limited to the discussion of determining risks stemming from individual instances of IA control non-compliance and IA issues. Complementary processes are available that facilitate the aggregation of risks to larger systems and systems-of-system architectures. It is the authors' intent that this IARA process might be used as presented, or tailored to better fit the specific needs of the organization that chooses to apply it to their IA risk processes. ■

References

1. DoD Instruction 8500.2, "Information Assurance (IA) Implementation." February 6, 2003.
2. DoD Instruction 8510.01, " DoD Information Assurance Certification and Accreditation Process (DIACAP)." November 28, 2007.

About the Authors

Dr. Larry Johnson | holds dual PhD degrees from Vanderbilt University in Chemistry and Physics. Recent career interests have included developing and implementing effective and efficient Information Assurance policies and practices for DoD customers. Dr. Johnson is a leading industry advocate on the convergence of Information Assurance and Anti-Tamper in today's network-centric military systems. He is the author of numerous DoD policies and technical studies.

Deborah Williams CISSP | holds a Masters degree in Public Administration / Public Policy from the University of Alabama at Birmingham. Her research interests include development and implementation of meaningful cybersecurity metrics, and information security risk assessments for systems-of-systems constructs. For DoD and other Government customers, Ms. Williams provides lifecycle engineering based approaches for effective Information Security policies and practices.

Defense in Breadth

by Robert Baldi

Information security professionals around the globe work to defend their network infrastructures with a variety of hardware and software mechanisms to prevent unauthorized access. A variety of enterprise security devices are employed to establish a defense-in-depth environment, where multiple layers of firewalls, intrusion detection systems, software patches, and antivirus solutions protect enterprise users from malicious attacks. "Defense-in-depth" has been the latest buzz term until recently, when the corporate enterprises, and more importantly the Department of Defense (DoD), adapted a defense-in-breadth strategy to strengthen their overall security posture. DoD Chief Information Officer John G. Grimes recently told DoD, "A defense-in-breadth approach is required to assure that our information capabilities and information critical components are trusted throughout their lifespan to achieve Decision/Mission Superiority." [1] With the recent shift in focus, the question many information security professionals are asking is, "What is defense-in-breadth?"

The principles of defense-in-breadth are closely related to the principle of defense-in-depth. [2] A defense that uses only a single type of countermeasure can be considered deep if it uses multiple instances of the countermeasure. For example, a defense consisting of multiple firewalls could be considered deep. If an organization establishes defense-in-depth by placing multiple Vendor A firewalls throughout the infrastructure, an attacker would just need one exploit to bypass the multiple firewall layers; thus, [3] if you employ a defense-in-breadth environment by using multiple firewalls in series from different manufacturers, an attacker requires a breadth of knowledge to exploit your layers of protection. The idea is that two products from different manufacturers are less likely to be exploited than two products from the same manufacturer.

Security professionals must [4] think of applying "breadth" as plugging the holes across a single wall. Each hole represents a different way in or different type of vulnerability. Breadth is used because a single type of control rarely eliminates all vulnerabilities. For example, suppose one needs to control access to a small one-story warehouse. The facility has a front door, a rear door, a large garage door, and fixed windows that do not open. Locks on the doors control one type of pathway to the inside, but offer no protection for the breakable windows. Thus, bars would be/could be an additional control to provide complete coverage.

The challenge many organizations face is how to harness the synergy from their geographically dispersed network security departments. Each location tends to focus on their users and their network. Defense-in-breadth is not just about the implementation of a variety of tools, but rather the process of managing the enterprise threats in the most effective manner possible. [5] Robert Lentz, Deputy Assistant Secretary of Defense for Information and Identity Assurance said, "IA [Information Assurance] within the DoD previously relied on a defense-in-depth approach to assuring information based largely upon firewalls and software patches; the focus was on attempting to keep intruders out and data safe. As approaches to IA have evolved, the DoD is moving towards a defense-in-breadth approach, integrating capabilities of people, operations, and technology to establish a multi-layer, multi-dimensional protection."

A determined adversary will invoke a variety of attacks to circumvent an organization's security mechanisms. Once the perimeter defenses have been neutralized, they will use phishing, viruses, malware, data-fuzzing, and a variety of techniques to bypass antivirus, anti-malware, and software security. Network defenders fortify their networks in a reactive manner by blocking attackers once detected, updating software to combat known vulnerabilities after they have been exploited, and removing malware and viruses once they have been infected. The defenders are always in a reactive role.

In the next *IAnewsletter*, I will examine defense-in-breadth on a deeper level and demonstrate how every organization can proactively

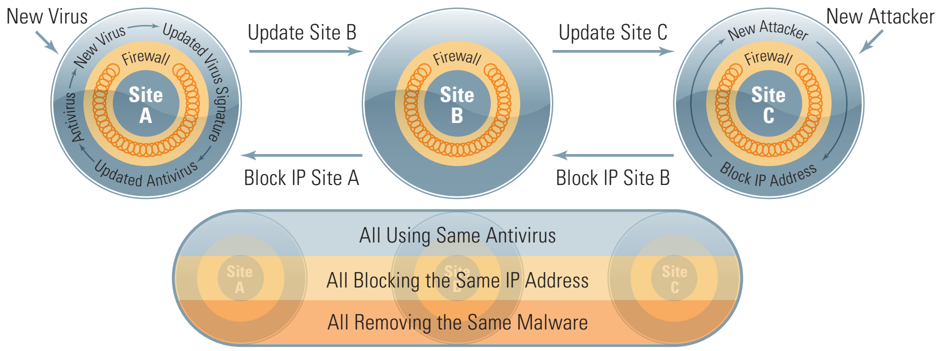


Figure 1

implement a defense-in-breadth security posture in their environment to increase their incident-response reaction time, collaboration capabilities, and overall effectiveness. ■

References

1. The Department of Defense Interim Information Assurance Strategic Plan. March 2008. *http://www.defenselink.mil/cio-nii/docs/DoD_IA_Strategic_Plan.pdf.*
2. McCarty, B. Red Hat Linux Firewalls. Wiley, 2002. p. 73.
3. Ruth, A., and Hudson, K. Security+ Certification Training Kit (CompTIA Exam SY0-101). Microsoft Press, 2003.
4. Tipton, H.F., and Krause, M. Information Security Management Handbook, Sixth Edition. Auerbach, 2007, p. 1328.
5. Lentz, R. "An Introduction to the Deputy Assistant Secretary of Defense for Information and Identity Assurance." July 2008. *http://www.stsc.hill.af.mil/crosstalk/2008/07/0807Lentz.html.*

About the Author

Robert Baldi MBA, CISSP, CEH | is a contractor supporting the United States Strategic Command (USSTRATCOM) and the National Security Agency (NSA). Mr. Baldi is also an adjunct instructor at ITT Technical Institute in Omaha, Nebraska, focusing on the NSA Committee on National Security Systems (CNSS) information security program. He may be reached at *iatac@dtic.mil.*

▷ *continued from page 29*

PARANOID

removing or modifying a member's entry in the group definition file. Symmetric keys of files that a revoked user has already accessed are lazily re-encrypted. Note that only the group owner can perform these operations.

In contrast, when a client application opens a file, an interposition agent traps the system-call. If the file is a Paranoid file, the interposition agent invokes a Paranoid client agent. The client agent connects to the remote Paranoid file-server which manages the communication, verification, key management, and all needed encrypt/decrypt operations. To the running application, the file appears as a local UNIX file.

A modified RSA cipher for group access

Let **P** and **Q** be large prime numbers. Let **N** = **P*Q** and ϕ =(**P-1**)*(**Q-1**). Find **e** relatively prime to ϕ and **r** such that **r*e** = **1** mod ϕ. The pair **<e, N>** is the public key for the group. The pair **<r, N>** is the private key for the group. To generate a private key for a group member, get a number t relatively prime to ϕ and a number s such that **s*t** = **1** mod ϕ. The pair **<s, N>** is the private key of the group member. Compute the member specific transform τ = **r*t** mod ϕ. Now, the key **K** is encrypted with the group public key: $C = K^e \bmod N$.
To transform the encrypted key **C** for the group member, compute $U = C^\tau \bmod N$. The group member recovers the key by computing $K = U^s \bmod N$.

The Paranoid file system is an innovative approach to file encryption. It allows users to share information while also implementing information security measures in a manner transparent to others. Paranoid's hybrid encryption scheme and novel approach to group sharing, as well as its use of the Bypass system and a file server agent allow its users the ability to share their information globally, securely, and easily. ■

References

1. Zaffar, F., Kedem, G., and Gehani, A. "Paranoid: A Global Secure File Access Control System." ACSAC 2005, December 2005, pp. 293-301.
2. Rivest, R., Shamir, A., and Adleman, L. "A method for obtaining digital signature and public-key cryptosystems." Communications of ACM, Volume 21, 1978.
3. Thain, D., and Livny. M. "Multiple bypass: Interposition agents for distributed computing." Journal of Cluster Computing, 2001.

About the Author

Dr. Gershon Kedem | received a BS Degree from the Hebrew University in 1972, an MS Degree in 1975 and PhD Degree in 1978 both from the University of Wisconsin. He was an Assistant Professor of Computer Science and Electrical Engineering at the University of Rochester from 1978 to 1984. Since 1984, he has been an Associate Professor of Computer Science at Duke University. His interests include: VLSI Design, Computer Aided Design of Digital Systems, Computer Architecture, and Computer Security.

FREE Products

Order Form

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

Name ____________________ DTIC User Code ____________________

Organization ____________________ Ofc. Symbol ____________________

Address ____________________ Phone ____________________

____________________ Email ____________________

____________________ Fax ____________________

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

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

____

LIMITED DISTRIBUTION

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

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

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

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		

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

July

22nd IEEE Computer Security Foundations Symposium
8–10 July 2009
Port Jefferson, NY
http://www.cs.sunysb.edu/csf09/

Black Hat USA 2009 Briefings and Trainings
25–30 July 2009
Las Vegas, NV
https://www.blackhat.com/

August

Workshop on Foundations of Computer Security (FCS '09)
9–10 August 2009
Los Angeles, CA
http://www.disa.loria.fr/~cortier/FCS09/

LandWarNet 2009
18–20 August 2009
Ft. Lauderdale, FL
http://events.jspargo.com/lwn09/public/MainHall.aspx

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

2009 IEEE International Conference on Information Privacy, Security Risk and Trust
29–31 August 2009
Vancouver, Canada
http://cse.stfx.ca/~passat09/

September

SecureComm 2009
14–18 September 2009
Athens, Greece
http://www.securecomm.org/

Symposium on Reliable Distributed Systems (SRDS 2009)
27–30 September 2009
Niagara Falls, NY
http://www.cse.buffalo.edu/srds2009/

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