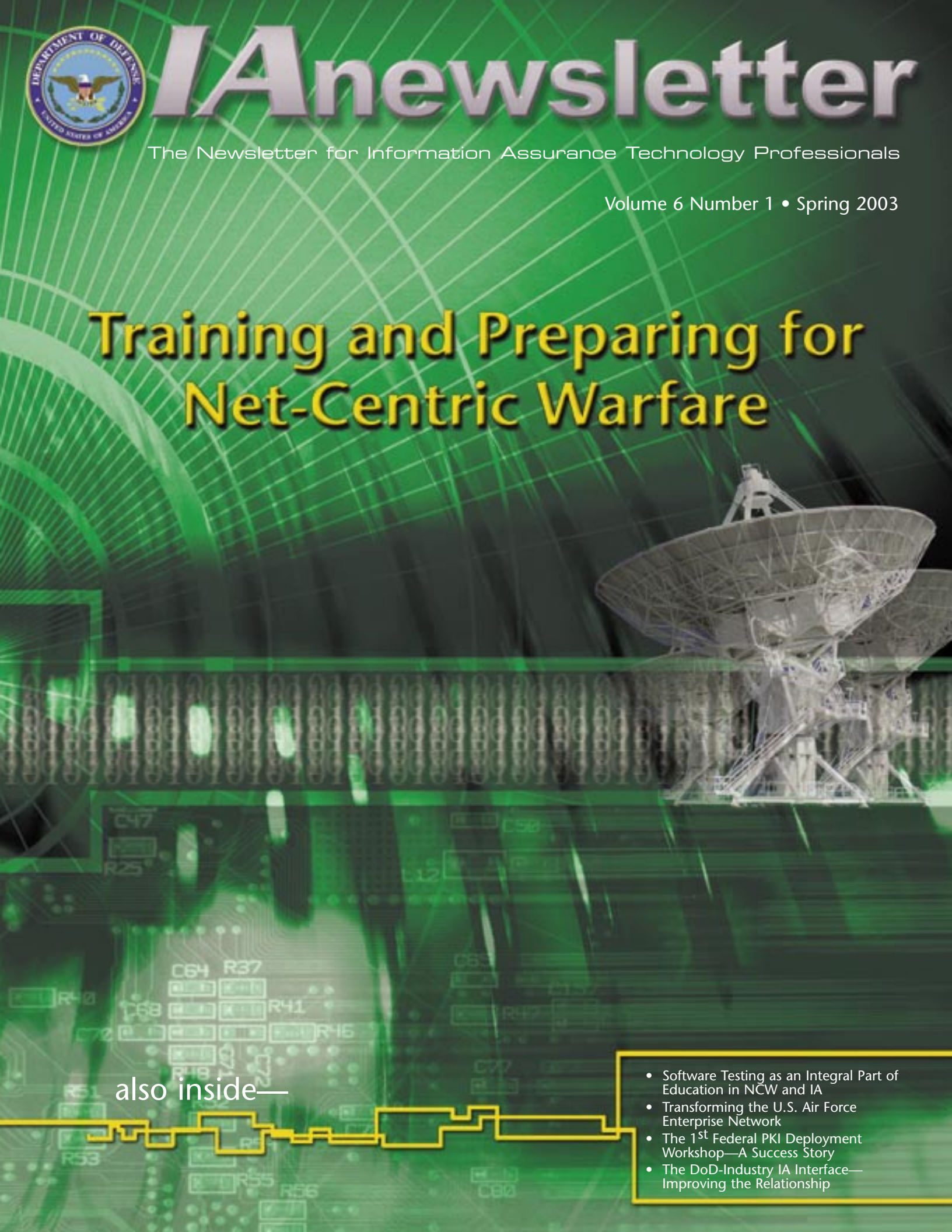
IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 6 Number 1 • Spring 2003

Training and Preparing for Net-Centric Warfare



also inside—

- Software Testing as an Integral Part of Education in NCW and IA
- Transforming the U.S. Air Force Enterprise Network
- The 1st Federal PKI Deployment Workshop—A Success Story
- The DoD-Industry IA Interface—Improving the Relationship

contents

feature

IA initiatives

in every issue

About IATAC & the *IAnewsletter*—

IAnewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA).

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

IATAC Director:	Robert J. Lamb
Deputy Director:	Abraham T. Usher
Inquiry Services:	Peggy O'Connor
Technical Analysts:	April Perera
	Jim Peña
	Brad Soules

IAnewsletter Staff—

Creative Director:	Christina P. McNemar
Art Director:	Ahnie Senft
Designers:	Maria Candelaria
	Holly Shipley
	Trang Dam

IAnewsletter Article Submissions

To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/news_events/author_submission.htm and download an "Author's packet."

IAnewsletter Address Changes/Additions/Deletions

To change, add, or delete your mailing or E-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
3190 Fairview Park Drive
Falls Church, VA 22042

Phone: 703/289-5454
Fax: 703/289-5467

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

Deadlines for future Issues—

Summer 2003	27 June
Cover design:	Holly Shipley
Newsletter design:	Ahnie Senft

IATAC Chat

Robert J. Lamb, IATAC Director

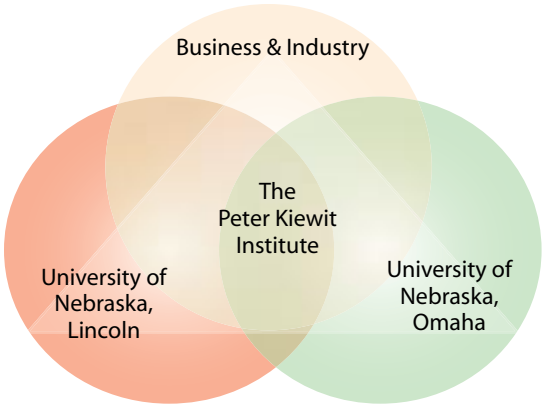
I would like to dedicate this column to the subject of PKI. In this instance, I am not referring to public key infrastructure, but rather the Peter Kiewit Institute…also known as "PKI."

Several weeks ago I had the opportunity to tour and learn about this truly remarkable institution and I would like to take this opportunity to introduce you to the "other PKI." The Executive Director is Ms. Winnie Callahan and I must again thank her for a great visit and thorough tour of their facility.

I would be doing an injustice to simply state that PKI is connected to the University of Nebraska system, and is located in Omaha. It is in fact a state-of-the-art, academic institution, linking top-flight students to outstanding educators, as well as business and industry leaders, through the University of Nebraska—Lincoln's College of Engineering and Technology (E&T) and the University of Nebraska—Omaha's College of Information Science and Technology (IS&T). PKI is a public-private partnership designed from the ground up to be a premier educational experience based upon partnership collaboration between academia and industry. Furthermore, PKI is a National Security Agency (NSA) Center of Excellence and is a key resource for U.S. Strategic Command (USSTRATCOM) in information and network security research and development, as the command assumes an increasing role in this expanding mission area.

There are any number of initial impressions I would share with you from my tour and discussions with students, staff, and faculty. The first relates to the facility itself. It is new…it is modern…and most striking of all…it is one giant, visible, usable science and engineering laboratory with beams, trusses, and power apparatus along with a state-of-the-art, full-spectrum information technology capability, providing students and faculty a first rate learning environment. And if that is not enough, the student living spaces (dorms) have been similarly designed to provide an extension of the academic environment, which supplements and reinforces the Institute's philosophy to provide the very best to its student body and faculty.

My visit was during the Institute's Spring Break and although the hallways were not overflowing with the normal hustle and bustle of a university, I did have an opportunity to speak with several students. In a word…"wow"…talk about an enthusiastic, bright, and focused! Every one of them spoke to a particular area of research in which they were engaged and each was nothing short of impressive as they described with great pride their projects. It



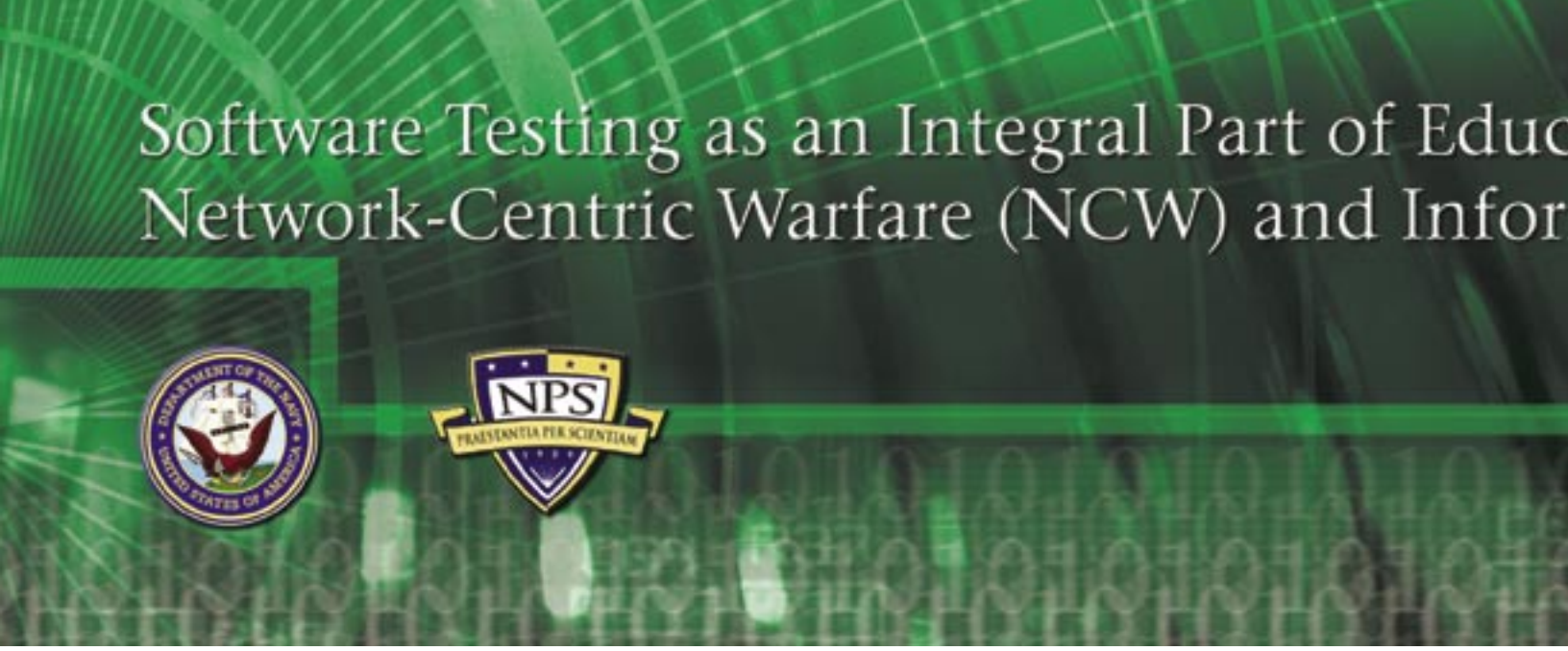
was apparent that both students and faculty thrived in the state-of-the-art facilities and labs designed to stay "cutting edge" through PKI's business and industry partnerships.

PKI has something for everyone. Students (and their parents) should know that, by all counts, PKI is providing an outstanding education. It is highly selective and competitive, on par with the very best schools in the nation. Business and Industry will be engaged in the partnerships upon which PKI is founded, will draw on PKI as a ready source for outstanding interns, and will benefit from the Institute's graduates as they arrive with a terrific combination of education and understanding of the business world. Government and the Department of Defense staff will be interested in the cutting edge research in computer and network security as well as in PKI graduates as an extremely capable source to fill the ranks of the government's work force.

When you visit the "other PKI" Web site at http://www.pki.nebraska.edu there are two quotations from the Institute's founder, Peter Kiewit (1900–1979), which clearly embody his vision and the reality of PKI—

"We don't have to be the biggest, we just have to be the best."
and
"The Institute strives to build not just for today, but for generations to come."

Software Testing as an Integral Part of Educ Network-Centric Warfare (NCW) and Infor



by Dr. J. Bret Michael

As the U.S. Navy moves forward with its goal of achieving information superiority by affixing network-centric warfare (NCW) capabilities at the tip of the United States' spear, Naval officers will become more reliant on software-intensive systems to carry out their missions. These systems will provide advanced warfighting capabilities such as engage on remote (EOR), in which track data from external sensors, in the absence of local sensor data, is passed to the fire control component of a weapon system. The system uses this data to calculate launch parameters, fire the interceptor, and provide in-flight target updates to the interceptor, with the local weapon command center retaining control and responsibility for the engagement.

Systems that provide for cooperative engagement, and other NCW capabilities, will need to be of high quality—meaning that the system will have as few defects as possible. For example, a tactical action officer (TAO) expects an EOR system to be highly dependable, in terms of its availability, reliability, and ability to tolerate faults, in addition to meeting correctness criteria such as the system reaching its desired states given specific events and guard conditions. It is not acceptable for the system to become unavailable, because for instance, security flaws in the shipboard communication software permitted an adversary to modify the behavior of the system. Some software testing must be performed to reveal flaws that can cause the system to behave incorrectly, along with "off-nominal" testing to gauge the effects of inputs from the environment that could affect properties of the system such as its survivability or security; some inputs may result in desired systems behavior, while others may result in undesired or unknown system behavior. [1] The testing results, in addition to actual experience with the operation of the system, form the basis on which the TAO and other stakeholders develop their trust in the system.

There are a numerous reasons that the quality of these systems, in terms of their capabilities and nonfunctional properties (e.g., testability, security), can be difficult to assess. For instance, EOR takes place in a system-of-systems context, for which one must assess the emerging properties of the composite system rather than those of the individual subsystems; this can be especially problematic when the prime contractors and subcontractors working on the same weapon system do not fully exchange information about the subsystems with one another, but rather treat information for each subsystem as being company-proprietary. Another challenge is that DoD relies on capability-based acquisition, in which Government personnel only specify the capabilities of a system, while the contractor provides the customer with a statement of work as to how the capabilities and nonfunctional properties will be achieved and assessed. Another significant challenge is that such systems are largely comprised of software. Software can be complex—such as in terms of its logic, semantics, and dependencies between units of software—making it hard to uncover software defects. Moreover, the software units are often acquired as commercial-off-the-shelf (COTS) products—and, not all vendors provide detailed information about the internal workings or quality of their COTS products.

Among the many efforts underway at the Naval Postgraduate School (NPS) to support NCW initiatives, the faculty of the Department of Computer Science have created specialty courses (e.g., Engineering of Network-Centric Systems) and specialty tracks (e.g., the computer security track with an emphasis on developing EAL7 high-assurance systems), in addition to redesigning some of their existing courses to help prepare Naval officers for the task of acquiring high-quality software-intensive systems. This article, discusses the recent redesign of our course titled "Software Testing" to reinforce the materials the students learn in courses on NCW and related topics such as information assurance (IA).

Overview of the software testing course

This course is offered in the department of computer science curriculum for software engineering. It covers test planning, execution, and analysis. In addition to a thorough treatment of the theoretical underpinnings of software testing, the former is covered in the textbook by Binder on testing object-oriented software, that we rely on the textbook by

Friedman and Voas to introduce the students to software–testing theory. [2, 3] We supplement textbook material with a set of scholarly articles that discuss the latest thinking on how to improve both the quality of software and the effectiveness of software testing—these readings serve as the basis for in-class discussions.

The course is delivered simultaneously to both in-residence and distance-learning students, with the latter participating via interactive video teleconferencing. The lecture material and homework assignments are organized into learning modules that can be accessed via the Web-based Blackboard system—the School standardized on Blackboard for Web-enabled and fully Web-based delivery of courses. Our adoption of the Blackboard system for presenting the course material is in sharp contrast to the approach taken by Ramakrishnan, which involved developing a custom Web-based interactive environment called LIGHTVIEWS for teaching software testing. [4] The course on software testing takes advantage of two of the interactive features of Blackboard that support asynchronous learning—

- Quizzes that automatically provide feedback to students regarding their mastery of key concepts.
- Discussion forums on which the students post their thoughts on topics posed by the instructor and their classmates.

A major component of the existing course is a team-based project in which the students obtain hands-on experience developing a test plan, executing the plan, analyzing the test results, and presenting the results and lessons learned to their classmates. We subscribe to the approach described by Carrington of providing students with an existing software system to test (Carrington found that if students test a system that they have developed, they tend not to be motivated to try to uncover defects in their system). [5] Another advantage of Carrington's approach is that students learn firsthand about challenges such as the need to become knowledgeable about the application domain and contexts in which the software system will be used. Such a project is also important, as pointed out by Braught and Reed for permitting students to experiment—using scientific methods—with different strategies and techniques for testing software systems. [6] In the past, we have supplied the students with the software for a simple discrete-event simulation of the operation of a Carrier-Sense Multiple-Access with Collision Detection (CSMA/CD) local area network, for which the requirements specification, design, and code are given. [7]

Redesign of the course

To better meet the educational needs of the students at NPS, we have redesigned the course on software testing by introducing a case study of a system that exemplifies, to some extent, the concept of NCW and the linkages between software testing and IA—the Ballistic Missile Defense System (BMDS), which is a system-of-systems comprised of Naval assets (e.g., the Aegis and Spy–1 systems) along with those of other services and agencies. The motivation for the case study is to demonstrate to the students the benefits, challenges, and limitations associated with software testing in the context of NCW and IA. Our approach of integrating the subject matter from other courses into the course on software testing is just the inverse of the proposal made by Jones to integrate software testing into other computer science courses. [8]

The case study is now an integral part of the lecture material and discussion topics. For instance, we have created learning modules and discussion forums that cover issues associated with the software testability of system-of-systems. Examples of discussion questions are—

- How does one ensure that laboratory results hold in the operational environment given that a system-of-systems' configurations are dynamic?
- If our test results are only valid for a specific configuration and particular set of variables, then how robust is our testing approach with respect to future system behavior in the operational world?

…continued on page 16

Aggregation and Inference—

Invisible Threats to Information Security

by Tom Ward and Abraham T. Usher

Do you recall the early days of the Information Explosion? 300 baud modems, bulletin board systems (BBSes), telnet prompts and file transfer protocol (FTP)? Over the past 30 years we have leapt into an "Information Age" where information, rather than natural resources or raw materials, is the strategic resource upon which the economy depends and it is being created in ever-greater quantities with constantly increasing speed. According to a study conducted by the School of Information Management and Systems at the University of California at Berkeley, the world's total "yearly production of print, film, optical, and magnetic content would require roughly 1.5 billion gigabytes of storage. This is the equivalent of 250 megabytes per person for each man, woman, and child on earth."

With the establishment of the World Wide Web (WWW) individuals today yield unheard of access to information and communication. A person with internet access can—

- Purchase a huge variety of goods online including books, music, travel tickets, even automobiles
- Research information on every subject known to mankind
- Access an international collection of computer software (much of which is free)
- Communicate in real time with people across the globe

Unfortunately, the proliferation of information is a two-edged sword that has introduced as many problems as benefits. Adversaries of the Department of Defense (DoD) and U.S. government use the Web to gather intelligence on our activities and capabilities. In a message dated 14 January 2003, Secretary of Defense Donald Rumsfeld issued instructions pertaining to Web site Operational Security (OPSEC). According to the message—

> *An Al-Qaeda training manual recovered in Afghanistan states—"Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." At more than 700 gigabytes, the DoD Web-based data makes a vast, readily available source of information on DoD plans, programs, and activities. One must conclude our enemies access DoD Web sites on a regular basis.*

The amount of information on the Web is staggering. If the appropriate policies and controls are absent or inconsistently applied, unclassified military information on the Web can pose a substantial threat to DoD.

The problem

A classic security problem in the realm of relational databases has been *aggregation* and *inference* of information. Although all modern database systems have built in role based access controls that prevent unauthorized disclosure of information, maintaining the confidentiality of data is still a very complicated problem. The challenge stems from the fact that often times restricted information can be gathered *implicitly* from unrestricted data.

- **Aggregation**—the process of gathering pieces of unrestricted information into a logical whole in order to reveal restricted information.
- **Inference**—the process of decomposing public information to imply restricted information.

Aggregation

Aggregation is the process of gathering pieces of unrestricted information into a logical whole in order to reveal restricted information. For a simple example of aggregation, consider a database system where the entire telephone directory of an organization is restricted (because it could provide information about the size and nature of the organization) but the telephone entry of a given individual is not restricted. A clever attacker could exhaustively query the database for every individual record, and then aggregate all of the data into a copy of the organizational telephone directory (see figures 1 & 2).

By aggregating all records, an attacker could determine that this company only has four employees—three of whom are in Virginia (703 area code) and one in Hawaii (808 area code). The attacker could also determine that the company uses Verizon as its Internet Service Provider (ISP), and that it might be a family owned business (run by the Smith family).

John Smith	CEO	703/555–1111	john.smith@verizon.net
Joe Smith	CEO	703/555–2222	joe.smith@verizon.net
Jane Smith	System Admin	703/555–3333	jane.smith@verizon.net
Jack Smith	Network Engineer	808/555–2222	jack.smith@verizon.net

Figure 1. Individual records (unrestricted)

Name	Title	Phone	E-mail
John Smith	CEO	703/555-1111	john.smith@verizon.net
Joe Smith	CEO	703/555-2222	joe.smith@verizon.net
Jane Smith	System Admin	703/555-3333	jane.smith@verizon.net
Jack Smith	Network Engineer	808/555-2222	jack.smith@verizon.net

Figure 2. Aggregated records (restricted)

Inference

Inference is the flip side of aggregation; it relates to the process of decomposing unrestricted information to imply restricted information. Consider a database system where statistical aggregates are not classified, but information related to some specific entities is classified. Consider the following database records that relate to aircraft carriers (see figure 3).

Location	Quantity of Carriers
Persian Gulf	2
Gulf of Mexico	3

Aircraft Carrier ID	Location
A	Gulf of Mexico
B	Gulf of Mexico
C	Gulf of Mexico
D	**SECRET**

Figure 3. Inference example

In this example, the location of aircraft carrier D is classified. However, a clever attacker could easily infer the location of carrier D by combining information from both tables. If three carriers (A, B, and C) are located in the Gulf of Mexico, then carrier D must be in the Persian Gulf (by process of elimination).

Relevance

What is the relevance of these database security issues to DoD? The Web is essentially a very large, unorganized database of publicly available information. Although there is not a structured query language (SQL) for extracting specific pieces of intelligence from the Web, modern search engines can provide capabilities that are similar in nature to relational database management systems.

How serious is the problem?

The problems of aggregation and inference are magnified by the power of Internet applications like Google.com and Altavista.com. Our adversaries can gather vast amounts of information on us almost instantaneously. Search engines have matured to the point of providing very gran-

…continued on page 17

Transforming the U.S. Air Force Enterprise Network

by Captain Carl Grant, (USAF)

All warfare is based on informational advantage with the edge going to the force that collects, analyzes, distributes, and leverages information to meet warfighting objectives faster than its adversary. Information superiority is realized when the force gains and maintains the advantage throughout the full spectrum of military conflict. To achieve information superiority in today's fast-paced combat environment, the U.S. Air Force is transforming how it leverages its communications and information networks supporting the warfighter. The vision of "One Air Force…One Network" forms the foundation of this transformation by treating its loose confederation of base and MAJCOM-level networks as a tiered entity, collectively known as the U.S. Air Force Enterprise Network.

Network operations (NetOps) codifies the processes and controls for assuring the data that enters the U.S. Air Force Enterprise Network is transmitted and delivered to the end user in the same form in which it began and in the defined time to be relevant to the end user's needs. NetOps evolved from a Service level need to view U.S. Air Force communications connectivity as more than just a conglomeration of fiber, switches and computers implemented and operated at the base level. NetOps addresses base-level events (e.g., viruses) that may have a ripple effect on U.S. Air Force/DoD operations by assessing the overall health of the network and responding to anomalies and perturbations from a global perspective.

In concert with NetOps, computer network defense (CND) consists of active measures to protect and defend the enterprise's information and information systems from disruption, denial, degradation, or destruction. CND is primarily a joint responsibility, with Unified Command Plan 2002 designating the Commander, U.S. Strategic Command (USSTRATCOM) as the DoD lead. The Eighth Air Force Vice Commander, as the Commander of Air Force assets to USSTRATCOM's Joint Task Force-Computer Network Operations (JTF–CNO), provides component support and ensures U.S. Air Force assets perform their assigned CND mission.

The basic tenets for NetOps and CND have been in place in the U.S. Air Force for several years. However, what is missing is an integrated and coherent command and control (C2) construct to ensure unity of effort throughout the U.S. Air Force. One challenge with establishing an integrated construct is that NetOps is a Service function and component support to the JTF–CNO's CND mission is a joint function. Additionally, physical reorganization approaches do not work because the two organizations providing NetOps and CND—the Air Force Network Operations Center (AFNOC) and Air Force Computer Emergency Response Team (AFCERT)—suffer if they are removed from their support organizations (Standard Systems Group and Air Force Information Warfare Center) and current locations (Gunter Annex, Alabama and Lackland AFB, Texas).

To address these challenges, Eighth Air Force joined forces with Air Combat Command, Standard Systems Group, Air Force Communications Agency and Air Intelligence Agency to develop a force presentation model using specified command relationships to unify the two mission areas into a single, integrated C2 and execution construct. Based on U.S. Air Force doctrine for Air and Space Expeditionary Task Forces, the construct provides a recognized C2 structure to present NetOps/CND forces and "dual-hat" joint and Service authority under one chain of command. It does not involve large-scale reorganization or physical relocation of forces. The basic premise of the construct is as follows—

- First, to satisfy Service requirements, an accountable commander of commensurate rank will be designated as the Air Force NetOps Commander (8 AF/CC). As part of the designation, the NetOps/CC will have tasking authority over Air Force organizations performing NetOps. The NetOps/CC will delegate day-to-day directive authority to a Director (8 AF/CV). An operations center and staff will assist the NetOps/CC and Director in executing C2.

- Second, to satisfy joint requirements, an operations center and staff will assist the Commander, Air Force Forces (8 AF/CV) in fulfilling his obligations to the JTF–CNO. An operations center and staff is currently missing from the present COMAFFOR–CNO construct.

- Third, to provide an integrated C2 structure for the 8 AF/CV to meet both his Service and joint responsibilities, the NetOps and CND operations center and staff would be dual-hatted. This dual-hat organization will be collectively known as the Air Force Network Operations and Security Center (AFNOSC) and reside at Barksdale AFB, Louisiana.

- Fourth, in addition to the operations center and staff, the AFNOSC will include the duty crews of the AFNOC and AFCERT. The crews remain under the administrative control (ADCON) of their parent organizations, but when on duty, the AFNOSC has operational control (OPCON). This is analogous to how Intercontinental Ballistic Missile wings from Air Force Space Command provide alert forces to USSTRATCOM. Distributed operations keep the duty crews with their support organizations and current locations.

Throughout the latter half of 2002, Eighth Air Force presented the construct to USSTRATCOM staff, the Defense Information Systems Agency (DISA), Headquarters Air Force, the Air Force Chief Information Officer, Air Force Major Commands (MAJCOMs) and the Air Force Doctrine Center—all agreed to the concept in principle. The Air Force Chief of Staff approved the construct in February 2003.

While the AFNOSC provides a single operations-level point of contact for DoD and joint organizations involved in network operations, MAJCOMs will still be responsible for controlling their portions of the network. The intent is for the AFNOSC to exercise centralized control if an outage, intrusion or policy/configuration enforcement issue crosses multiple MAJCOMs or affects the preponderance of the Air Force networks. The AFNOSC will also provide direction if a tasking/corrective action is time-sensitive in nature or comes from the JTF–CNO or higher headquarters. Although the AFNOSC construct does not advocate adding new sensors or system capabilities, it does provide the following value-added benefits—

- An O–9 "sheriff" becomes responsible for operational assessments and policy enforcement across U.S. Air Force networks.

- Improved network situational awareness. With a dedicated C2 and staff structure, the AFNOSC will fuse network status data, intelligence and other sources currently dispersed across the U.S. Air Force to form a complete network situational awareness picture for U.S. Air Force, JFC, and component operations.

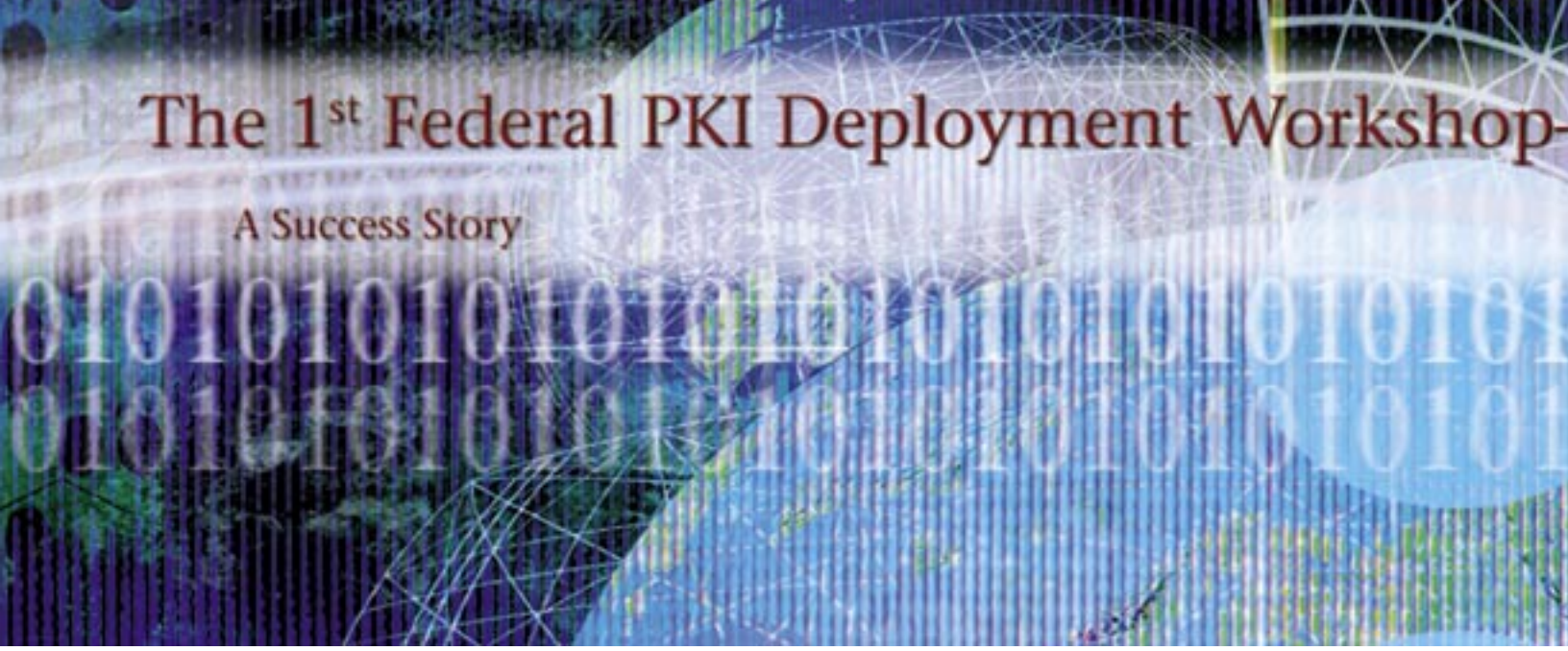
- Better impact analysis in C2 and risk management decision processes.

- Attached and supporting forces remain under their existing support structures and ADCON of host organizations. Squadrons, groups, and wings focus on training and sustaining. Program, policy, resources, and architecture continue within functional channels and the Pentagon and MAJCOMs retain standard weapons system roles.

As the AFNOSC construct comes closer to reality, Eighth Air Force has taken steps to prepare for the new mission. A small cadre of personnel and equipment were taken "out of hide" to start cursory operations. Infrastructure requirements are identified and included into the planned, post-fire renovation of Eighth Air Force Headquarters building. Eighth Air Force, in coordination with Air Combat Command and the Air Force Communications Agency, is preparing official documentation to implement the AFNOSC and outline specific responsibilities.

The AFNOSC addresses Service and Joint requirements through the use of command relationships to unify NetOps and CND operations into a single, integrated C2 construct. The AFNOSC positions the U.S. Air Force for any of the organizational options currently in discussion at the Joint and DoD levels and leaves room for expansion into C2 of Air Force voice, video, and RF communications. Improved C2

…continued on page 17



The 1st Federal PKI Deployment Workshop-

A Success Story

by Mark Lentz and Shelly Patterson

On March 12 and 13, 2003, over two hundred Federal government and vendor personnel gathered at the Hyatt Regency Crystal City in Arlington, Virginia, to hear PKI concepts, lessons learned, and up to the minute federal security objectives from knowledgeable authorities at the first Federal Public Key Infrastructure (PKI) Deployment Workshop. Based on feedback received from attendees, this first workshop was a unanimous success. Here is a sampling of the feedback from the attendees—

- "Very worthwhile"
- "This was great information and a wonderful opportunity to talk to some key people in government and industry with regard to PKI!", and
- "Excellent, must repeat deployment workshop."

The overall objective of this workshop was to provide an overview of the process, practice, and the considerations of a well-deployed PKI, including the benefits of cross certifying with the Federal Bridge Certification Authority (FBCA). Mrs. Michelle Moldenhauer, Director, Department of the Treasury's Information Systems Security and Chair, Federal PKI Policy Authority, hosted this event, kicked off the workshop each day, and served as overall emcee for the workshop. During her kickoff presentation on the first day, Mrs. Moldenhauer provided a brief history of the Federal PKI (FPKI) and described how this workshop would help facilitate information sharing on key topics and issues in the FPKI community.

One of the many insightful presentations during the two-day workshop was delivered by Mr. Tim Polk, National Institute of Standards and Technology (NIST) and Chair, Federal PKI Certificate Policy Working Group (FPKI CPWG). His presentation, "Surviving Policy Mapping," was a tutorial on the concepts, procedures, and expectations associated with the policy mapping process. The FPKI CPWG is the policy workhorse of the FPKI and one of its primary functions is checking the policy compatibility of an applicant PKI Certificate Policy (CP) to the FBCA CP. One of the first critical steps for an applicant PKI on the road to cross certification with the FBCA is to have the FPKI CPWG map the applicant's CP to the FBCA CP, at the assurance level(s) chosen by the applicant. Rudimentary, basic, medium, and high are the assurance levels that applicants may choose from with most of the applicants choosing the medium assurance level. At the end of Mr. Polk's presentation, he directed potential applicants to the FPKIPA Web site at http://www.cio.gov/fpkipa to obtain the mapping matrix template for each of the assurance levels so they know what FBCA CP requirements will be the basis for a policy mapping with their CP.

Two other noteworthy, insightful presentations were delivered by Mrs. Judith Spencer, General Services Administration (GSA) and Chair, Federal Public Key Infrastructure Steering Committee (FPKI SC). In her first presentation, entitled, *The Evolving Role of the Federal PKI—Information Assurance in Cyberspace*, Mrs. Spencer informed the attendees about new developments in Federal government-wide identity management and the emergence of the Common Policy Framework (available at http://www.cio.gov/fpkipa) to establish a new standard for PKI policy for Federal employees, contractors, and their affiliates. In her second presentation later on day one of the workshop, *How to Cross-Certify with the FBCA—5 Steps to Success*, she outline the process and some lessons learned of cross certifying with the FBCA, a process that has been successfully navigated by four PKI entities so far—the National Aeronautics and Space Administration (NASA), the U.S. Department of the Treasury, the U.S. Department of Defense (DoD), and the U.S. Department of Agriculture/ National Finance Center (USDA/NFC).

Other presentations that the attendees indicated on evaluation forms as informative and the most worthwhile were *Legal Issues for Federal PKI* by John Cornell, GSA; *PKI 101* by Bill Burr, NIST; *Certificate Policy (CP) and Certification Practice Statement (CPS)* by Santosh Chokhani, Orion Security; *GAO Sanctioning Process and PKI System Issues* by Chris Martin, GAO; *Assessing the Security of Federal Information Systems—The Development of Standardized Certification and Accreditation Guidelines and Provider Organizations* by Ron Ross, NIST; *Directory Services—The*

Basics by Bob Johnson, Booz Allen Hamilton; *Lessons Learned—NIH – EDUCAUSE PKI Interoperability Project Update* by Peter Alterman, NIH; and *Lesson Learned: NFC's Public Key Infrastructure* by Kathy Sharp, U.S Department of Agriculture/ National Finance Center.

In addition to the 24 presentations during the two days of the workshop, there was an exhibit area where ten organizations promoted their PKI-related products and services, including: VeriSign, Inc., AEP Systems, Inc., RSA Security, nCipher, Inc., U.S. Department of Agriculture/ National Finance Center, Entrust, ACES & FTS Smart Card, Booz Allen Hamilton, and IATAC. Overall, the Federal PKI Deployment Workshop was a good success with a good turnout of attendees, speakers, and exhibitors from the PKI community. Most importantly it was a group of highly qualified people with experience and knowledge to share and a genuine interest to learn. Due to the overwhelming success and positive feedback of the 1st Federal PKI Deployment Workshop, there is a good possibility that the next workshop will be held in the Washington DC/Virginia area in the fall of 2003. For more information about this first workshop or plans for any future workshops, please contact Mark Lentz (410/684–6520, lentz_mark@bah.com) or April Perera (703/289–5699, perera_april@bah.com).

The first working group assembled to plan the Federal PKI met in 1992. The original founding fathers that set the stage for the present Federal PKI included representatives from the Department of Defense (DoD), the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), and the Social Security Agency (SSA). After eight years of ground breaking policy work going on in parallel with testing and prototyping of the FBCA, the Federal CIO Council approved the FBCA Certificate Policy (CP) in June 2000. The FBCA became operational in June 2001. The first PKIs to cross certify with the FBCA; NASA, Department of the Treasury, DoD, and USDA/NFC; were formally recognized in a ceremony at the White House Conference Center on September 18, 2002.

The Federal PKI Deployment Workshop was hosted by the Federal PKI Policy Authority (FPKI PA) and executed by IATAC. Entrust and AEP Systems sponsored and spoke at the catered luncheon on day one following an award ceremony that recognized a dozen deserving people for their hard work and dedication to the Federal PKI effort. RSA Security, Inc., sponsored and spoke on day two and Mr. Steve Duncan, GSA and the Access Certificates for Electronic Services (ACES) Program Manager, provided an informative presentation on the status, challenges, and near-term activities and milestones of the ACES Program. Booz Allen Hamilton and IATAC sponsored the social event in the exhibit area on the first night of the workshop. ■

About the Authors

Mark Lentz

Mr. Lentz earned his B.S. in Computer Engineering, Clemson University 1986. He has 17 years of experience in Information Security/Assurance field as a former National Security Agency (NSA) employee. He currently is a member of IATAC in support of DoD PKI Certificate Policy Management Working Group (CPMWG), Federal PKI Policy Authority, Federal PKI Certificate Policy Working Group, and various PKI training/apprenticeship efforts.

Shelly Patterson

Ms. Patterson, a Booz Allen Hamilton consultant, has seven years experience in the Information Assurance (IA) field. Her areas of expertise include biometrics and PKI. Ms Patterson provides IA support in the way of technology studies and analysis, research and development, and programmatic, technical, and communication support to the FPKI Policy Authority and working groups under the FPKI PA. Previously, she supported the U.S. Government in a variety of program management offices such as the Air Force PKI Systems Program Office, which successfully developed, tested and fielded hardware and software systems to multiple AF Bases throughout the country in support of the PKI deployment effort.

The DoD-Industry IA Interface—

Improving the Relationship

by Vivian Cocca

Innovation and the rate of change in information technology capabilities continue to accelerate. This rate of change outpaces DoD's ability to fully exploit the advantages offered by these new and emerging capabilities given the bureaucratic tendencies of large Government organizations. Furthermore, "network centric warfare" creates heavy demands from DoD consumers for increasingly complex and sophisticated information assurance (IA) capabilities—ones that also must meet the security requirements of the Department as well as its functional and operational needs. As such, the DoD has increasingly reached out to the commercial sector for assistance in coping with the demands of the networked force focusing primarily on meeting functional requirements, with security and interoperability requirements often of second consideration. Concurrently, the commercial industry has also reached out to DoD, and has inundated us with marketing literature that claim each product's unparalleled innovation and excellence in function and security. It is impossible to ascertain from product literature and hour-long discussions with company leadership the viability of a product for use in the DoD environment. Simply put, DoD's traditional approach to handling vendor relations has been overwhelmed by increased supply and demand; and DoD runs the risk of exposure if due diligence in product assessment, testing and evaluation is ignored.

Clearly, this is a complex issue that demands immediate attention. As such, the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I), Information Assurance Directorate and the Defense-Wide Information Assurance Program (DIAP) have taken steps to develop a comprehensive strategy, targeting computer network defense (CND) tools initially—to address the full scope of the problem from the identification of "needs" or requirements to deployment and life-cycle support. Figure 1 details the process and the entities involved in successfully identifying the needs, finding the product or capability that meets those needs, transitioning it to the user, sustaining, and eventually replacing or retiring the capability.

First steps

As a crucial first step, OASD(C3I) IAD/DIAP has partnered with the Defense Information Systems Agency (DISA) and the NSA's Information Assurance Directorate (IAD) Business Affairs Office (BAO) to develop a process to establish a "front door" for vendors of IA and IA enabled products in order to more successfully market their products to the DoD—and at the same time, provide the DoD customer with a baseline of product knowledge relevant to operating in the DoD environment. Creating a single point of access will also enable DoD to identify new and emerging technologies as part of a comprehensive, integrated solutions process (see Figure 1).

Establishing the "Front door"

As stated earlier, many commercial vendors have "reached out" to DoD offering a multitude of IA and IA enabled products and services to assist in solving the many cyber security problems that plague large organizations. This increased interaction has highlighted some significant challenges—

- There are too many commercial IA vendors seeking an audience with senior DoD leadership and not enough time on their calendars. Assuring fairness in competition is a primary concern among senior DoD leaders—they simply cannot advocate or endorse the use of one product over another.

- Information is not available to senior DoD leadership to adequately assess the viability of a particular product to meet a specific DoD need.

- There is not enough time or resources available to evaluate all of the products and services that are being promoted. For example, during just a one year period, the NSA BAO received over 140 requests by vendors to present their products to senior government officials. DISA's Technical Insertion Panel (TIP) received over 100 similar requests during the same time period.

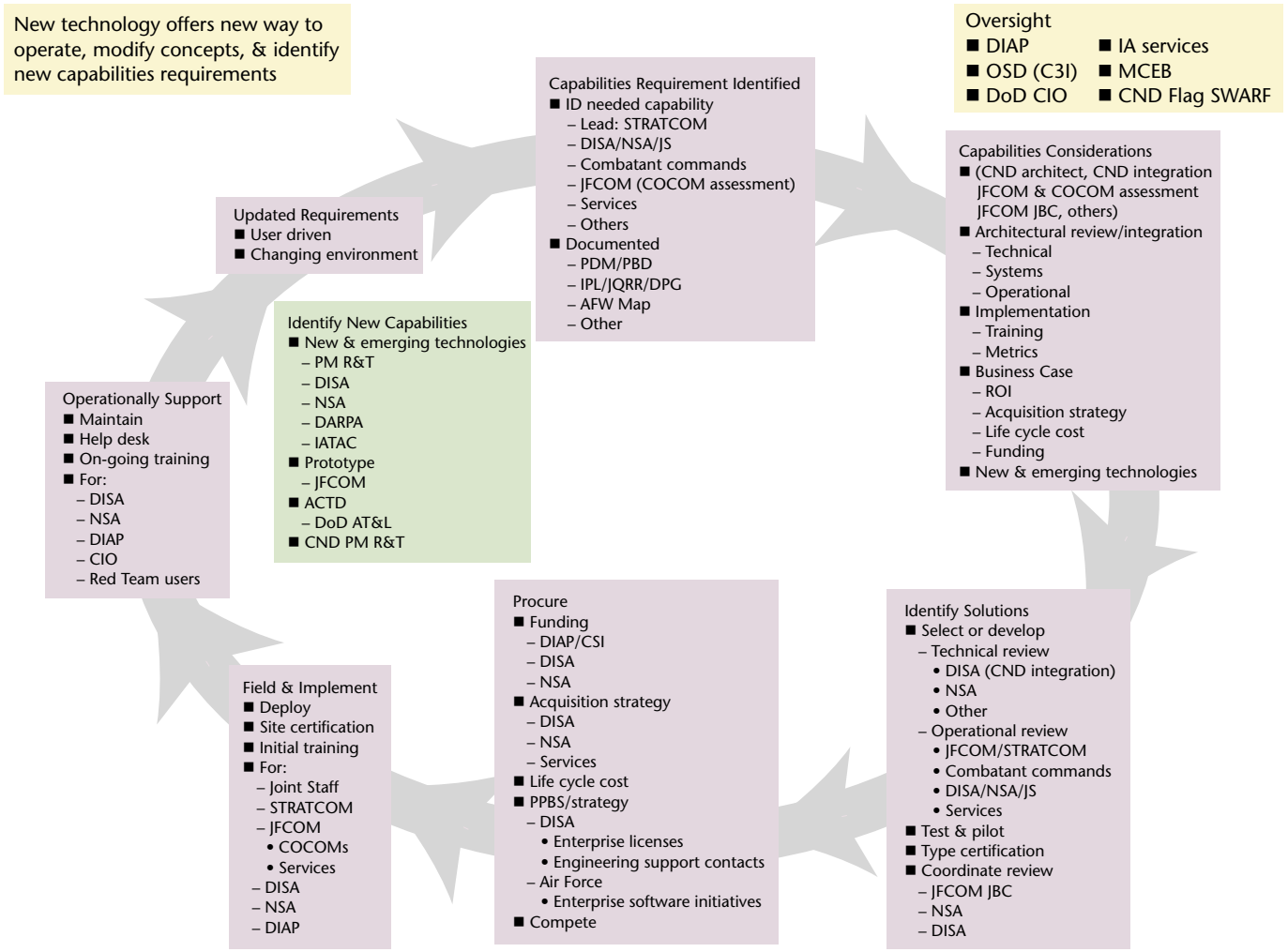


Figure 1: CND integrated solutions process

…continued on page 18

National Security Agency

IA Training Opportunities

by Jeff Seeman

At the 7th Annual IA Workshop in Williamsburg, VA, attendees participated in one of the early bird sessions to learn what other organizations have to offer in terms of information assurance (IA) training. At the National Security Agency (NSA), the National Cryptologic School has an IA training division that offers courses designed for a broad range of skills.

The courses cover job skills from Risk and Key Management, SA, ISSO, ISSM, ISSPM, ISSE, TEMPEST, COMSEC Custodian and Monitoring, OPSEC, to training Classification Officers, and the accreditation process. The method of delivery ranges from platform lecture and exercises to CD–ROM Web based courses. The courses range from entry-level familiarization to intermediate math level skills. Ninety percent of the lecture courses are five days or less in duration. At this time, graduate level courses are not available, but are being considering for the future.

Everyone in the Intelligence Community is welcome to take these courses. The courses are structured around NSA regulations and procedures. However, that should not be a deterent from taking advantage of the course selection. If the current course listing does not meet your needs, a plan can be customized to specifically fit your requirements. Logistical needs can also be met by arranging to have a course brought to your facility.

For information about courses and registration information, log onto the IAD SIPRNET Web page at http://www.IAD.nsa.smil.mil. Look under the library selection for "IA OPSEC Course Catalog." The catalog provides registration information, course descriptions, course classification requirements, student qualifications, and a skill areas map to assist in plotting out a training plan. For further assistance call 410/854–6488, DSN 244–6488.

About the Author

Jeff Seeman

Mr. Seeman has been at the National Cryptologic School for over six years managing and developing the IA curriculum. He can be reached at jaseema@nsa.gov.

OMB Praises Security Assessment Tool

by Marc Stevens

The U.S. Office of Management and Budget (OMB) cited the Automated Security Self-Evaluation Tool (ASSET) as one of its top eight achievements toward improving information security in the Federal government during 2002. IATAC developed the tool with the National Institute of Standards and Technology (NIST). ASSET automates and standardizes the Federal government's annual security self-assessment process for information technology systems.

ASSET, a free utility that meets Section 508 accessibility standards, complements NIST Special Publication 800–26, Security Self-Assessment Guide for Information Technology Systems by automating a system security self-assessment questionnaire and providing report assessment capabilities. The tool was first rolled out in 2002 and continues to add new users.

Many Federal departments use ASSET to develop their annual reports, which are submitted to OMB each fall. NIST and IATAC have met with several departments to identify potential enhancements and will be releasing another version in 2003. For more information on ASSET, visit NIST's Web site, http://csrc.nist.gov/asset/. ■

The development of ASSET was complex in that it had to meet a diverse set of user requirements from very small to extremely large organizations. The true value behind the automated security questionnaire is a series of complex business rules that were previously agreed upon by NIST, OMB, and the General Accounting Office. Those business rules determine how the data collected is used to determine the results of the self assessment. But to a user it's pretty simple—they are just filling out a check-list.

Marc Stevens
ASSET Program Manager

Security Through Cooperation

May 20–23, 2003
Waikiki Beach Marriott Resort, Honolulu, Hawaii.

In the spirit of this year's theme "Security Through Cooperation," USPACOM will bring together Information Assurance (IA) representatives from all the combatant commands and various DoD agencies from outside the USPACOM Theater with IA representatives from within the USPACOM Theater to share information & discuss topics ranging from the latest IA policies, trends, issues, solutions, how organizations are structured, operational lessons learned, and more. Additional activities associated with this year's conference include 2 training courses (held the week of 12 May), an IA/IT Training & Certification workshop (on 19 May), and several fun events. IA professionals interested in this conference can find more information & register at www.iaevents.com. The target audience for this conference includes all IA professionals (both management and technical) & military leaders interested in gaining an increased understanding on a variety of IA-related subjects to include computer network defense, cyber threats & capabilities, and future IA initiatives within DoD.

www.iaevents.com

…continued from page 5

- What guarantees, if any, can be made that the desired system behavior will be maintained in the software as patches and modifications are made after the system is fielded?"

In addition, we have developed team projects around the case study that are to be used to emphasize, for instance, the difference between testing techniques for achieving software quality (e.g., those for module or class testing), those for assessing software quality (e.g., system-level testing), and between feasibility testing (i.e., can the system provide the capability?) and operational capability testing (i.e., can the system provide the capability in an operational context?). The projects also emphasize important tasks associated with testing system-of-systems, such as distinguishing between controllable and uncontrollable system variables, with the aim of minimizing the negative impact on the system of those variables that can be controlled and characterizing the impact of external influences on the system that are outside the engineering-design space. Many of the students who take the software-testing course become software acquisition officers rather than software developers, so we also cover software acquisition topics as they relate to, for instance, testability.

As previously stated, the criticality of BMDS to our nation's security dictates that such safety-critical systems be of high quality. In security courses, the topic of assurance as it pertains to NCW is typically discussed in terms of penetration analysis and formal verification of security kernels. We revised the course on software testing to provide students with lecture material that clearly delineates differences among penetration analysis, formal verification, and software testing. Likewise, we created experiments for the students to conduct. This allows them to discover firsthand some of the pros and cons associated with applying security-specific and off-nominal testing (e.g., fault injection) techniques to reveal security flaws. For example, the fact that fault injection permits the testing of COTS components for which the source code is not available, and the weaknesses of penetration analysis, one of which as pointed out by Du and Mathur is that the tester must either know a priori the types of flaws that exist in BMDS or be able to postulate what those flaws might be. [9] We have also added to the supplementary reading list articles that discuss ways of improving the testing for security flaws, such as the techniques described by Jiwnani and Zelkowitz to direct the application of scarce testing resources based on the distribution and prioritization of security vulnerabilities. [10] In this course, we also discuss such a prioritization of resources from the perspective of safety, reliability, and availability.

Lastly, we plan to invite personnel from combatant commands, Government agencies, and the private sector to give guest lectures. However, often our students have prior experience in conducting network-centric warfare, managing information assurance, or performing software testing—their expertise helps bring to light for their classmates real-world challenges faced by the user, software-systems engineer, and software-acquisition professional.

Technology transfer

We are assisting faculty affiliated with the federally funded National Institute for Systems Test and Productivity (NISTP), located at the University of South Florida, to introduce DoD-specific content into their graduate-level course on software testing. In addition, we are studying the lessons learned reported by others from their experience in teaching software testing to graduate students. For example, we might be able to apply certain aspects of the approach reported by Hoffman, Strooper, and Walsh to improve upon our current design of the learning module on the subject of automated testing. [11] Our efforts are being funded by research grants from the Space and Naval Warfare Systems Command and Missile Defense Agency. ■

About the Author

Dr. J. Bret Michael

Dr. Michael has been an Associate Professor of Computer Science at the Naval Postgraduate School since 1998. His research on information assurance and information operations covers many aspects of distributed computing. Dr. Michael is a member of the IATAC Steering Committee. He may be reached at bmichael@nps.navy.mil.

References

1. Ghosh, A. K. & Voas, J. M., Inoculating software for survivability, *Comm. ACM* 42, 7 (July 1999), pp. 38–44.
2. Binder, R. V., *Testing Object-Oriented Systems: Models, Patterns, and Tools*., Reading, MA: Addison-Wesley, 2000.
3. Friedman, M. A. & Voas, J. M., *Software Assessment: Reliability, Safety, Testability*, New York, NY: John Wiley & Sons, 1995.
4. Ramakrishnan, S. "LIGHTVIEWS—Visual interactive Internet environment for learning OO software testing." In *Proceedings Int. Conf. on Software Eng.*, IEEE (Limerick, Ire., June 2000), pp. 692–695.
5. Carrington, D., "Teaching software testing." In *Proceedings Second Austral. Conf. on Computer Sci. Educ.*, ACM (Melbourne, Aust., July 1996), pp. 59–64.
6. Braught, G. & Reed, D., "Disequilibration for teaching the scientific method in computer science." In *Proceedings Thirty-third SIGCSE Tech. Symposium on Computer Sci. Educ.*, ACM (Covington, KY, 2002), pp. 106–110.
7. Sadiku, M. N. O. & Ilyas, M., *Simulation of Local Area Networks*, Boca Raton, FL: CRC Press, 1994.
8. Jones, E. L., "Software testing in the computer science curriculum—a holistic approach." In *Proceedings Austral. Conf. on Computing Educ.*, ACM (Melbourne, Aust., Dec. 2000), pp. 153–157.
9. Du, W. & Mathur, A. P., "Testing for software vulnerability using environment perturbation." In *Proceedings Int. Conf. on Dependable Systems and Networks*, IEEE (New York, NY, June 2002), pp. 603–612.
10. Jiwnani, K. & Zelkowitz, M., "Maintaining software with a security perspective." In *Proceedings Int. Conf. on Software Maint.*, IEEE (Montreal, Can., Oct. 2002), pp. 194–203.
11. Hoffman, D., Strooper, P., & Walsh, P., "Teaching and testing." In *Proceedings Ninth Conf. on Software Eng. Educ.*, IEEE (Daytona Beach, FL, Apr. 1996), pp. 248–258.

…continued from page 7

"Aggregation and Inference—Invisible Threats to Information Security"

ular search specifications, so that end users can examine particular Web domains (e.g., all .mil sites) and media types (e.g., Microsoft Word documents) with great precision. For example, a Google search for **"CONOPS site:.gov"** will return all of the occurrences of the term 'CONOPS' within the domain of U.S. Government Web sites. Similarly, a search for **"'information security' filetype:doc"** returns a list of over 8,000 publicly available Microsoft Word documents containing the term 'information security.'

In his *Wired News* article, "Google: Net Hacker Tool du Jour" Christopher Null explains several ways that Google and other search engines can be used for nefarious purposes. Rather than searching individual sites for sensitive information, hackers can examine entire domains for a particular piece of information. According to hacker Adrian Lamo, "Google, properly leveraged, has more intrusion potential than any hacking tool."

In fact, search tools like Google can do more than merely facilitating primitive aggregation and inference attacks. Some security risks to networked computers exist due to vulnerabilities in the underlying application servers or database servers. Because many of these application servers and database servers create HTML templates for publishing content to the Web, search engines can be used to locate unpatched servers still configured with default installations. As reported by Christopher Null, "Typing the phrase 'select a database to view'—a phrase from FileMaker Pro database's default Web interface—into Google recently yielded 200 links, almost all of which led to [vulnerable] FileMaker databases accessible online."

Once hackers determine a keyword or phrase that exists on a vulnerable type of system configuration, they can quickly scour the Web for hundreds or thousands of similarly vulnerable systems. For example, a search for the phrase "powered by Movable Type" returns (in less than three seconds) over 175,000 Web sites running the default installation of the popular Web log publishing software.

JWRAC

Both aggregation and inference can pose a substantial threat to the security of DoD's information. Dr. John Hamre, then Deputy Secretary of Defense, understood the seriousness of this threat and directed a government-wide inspection of all Web pages for sensitive information in 1998. In March 1999, Defense Information Systems Agency (DISA) established the Joint Web Risk Assessment Cell (JWRAC). As a component of DoD's layered defense, the JWARC routinely conducts assessments of DoD Web sites, checking to make sure that no sensitive information is available via the public Internet. During its first six months of operation, JWRAC reviewed about 10,000 Web pages and identified hundreds of discrepancies for corrective action.

Conclusion

Aggregation and inference pose an invisible threat to DoD by allowing our adversaries to collect or imply sensitive information from our public Web sites. During World War II, several OPSEC campaigns were launched with slogans like, "Loose Lips Sink Ships." Today, "loose data" poses new risks to the confidentiality of our information and the integrity of our information systems. The protection of DoD's information on the Web is not just the responsibility of JWRAC. Leaders, managers, and administrators at all levels must be very cautious in determining what information they publish to the Web. ■

About the Authors

Tom Ward

Mr. Ward is a member of IATAC and currently supports the Joint Task Force—Computer Netwok Operations (JTF–CNO) Director of Intelligence (J2). He holds a B.A. from DePaul University and an M.S. from Northern Illinois University. Mr. Ward may be reached at wardt@jtfcno.ia.mil.

Abraham T. Usher

Mr. Usher is Deputy Director of the Information Assurance Technology Analysis Center (IATAC). He graduated from the U.S. Military Academy in 1996 with a B.S. double major in Modern Standard Arabic and German language studies and a minor in Computer Science.

Relevant resources—

- DoD Web Site Administration Policy http://www.defenselink.mil/webmasters
- DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release
- DoD Directive 5205.2, DoD Operations Security (OPSEC) Program
- DoD Message "Web Site OPSEC Discrepancies" dated 14 January 2003

…continued from page 9

"Transforming the U.S. Air Force Enterprise Network"

of these capabilities will enable air and space forces to better gain and maintain information superiority with the objective of achieving faster and more effective C2 of assigned forces than the enemy. It will also posture the U.S. Air Force to meet the network-based operations concepts of the future. ■

About the Author

Captain Carl Grant, USAF

Captain Grant received his B.S. in Computer Science and M.S. in Aeronautical Science from Embry-Riddle Aeronautical University. He worked in the Air Force Computer Emergency Response Team for over 2 years and is now part of the team responsible for integrating Information Operations into the Combat Air Forces. He can be reached at cci@barksdale.af.mil.

…continued from page 13

"The DoD-Industry IA Interface—Improving the Relationship"

These issues are not limited to just DoD/OSD senior leadership, but span the entire DoD IA community. The fragmented manner that DoD has performed product consideration evaluation in the past has caused frustration for both commercial vendors as well as members of DoD. In one case, a vendor met with over 44 military entities trying to find a customer for their product. The impact of these problems is threefold—

- It discourages emerging companies with promising technology offerings from doing business with DoD
- It reduces DoD's ability to be opportunistic (too much information, too little time to evaluate it)
- It is not cost effective (multiple tests/buys of the same product)

Targeting vendors: Getting to the "right" place

To minimize the frustration experienced by vendors and DoD decision makers, a process must be implemented to funnel commercial vendors towards a central IA "clearinghouse." This clearinghouse will process vendor requests for evaluation against known needs and then will provide a venue for an assessment prior to committing further resources for testing and evaluation. This clearinghouse will represent the DoD market for IA and IA enabled products and, eventually, technologies. By implementing this process, the DoD IA community hopes to increase visibility into commercial IA capabilities and products, reduce vendor's time and effort finding the appropriate customer for their products, and provide 'value-added' knowledge to products for potential DoD customers.

Targeting the T&E community—Sharing information on product evaluations

Sharing information on products that have already been tested is an easy way to begin to create the needed visibility into a product's capability and understanding its viability of operating in the DoD environment. Not only do Service labs test and evaluate products, but NSA, DISA, DARPA, and other DoD entities also conduct some sort of evaluation prior to experimenting with the product or making a decision to purchase. Often times, these evaluations are done to address the specific needs of the organization, but if shared, this information could assist other organizations in the decision making process and would support a broad range of needs across the community. Therefore, the DIAP has asked IATAC to gather this information and provide a single knowledge base from which to share the information gleaned from the test, evaluation, and assessment process. For more information, see http://iac.dtic.mil/iatac/pdf/dod_tool.htm on the Web (restricted to .mil/.gov domains).

In summary—the way ahead

1. OASD(NI2) will refer all IA products and IA enabled product vendors wishing an audience with NI2 senior leadership to NSA IAD BAO for an initial review against capabilities and security requirements.
2. Expand, leverage, and merge common functions of DISA's TIP process and NSA IAD BAO's process to establish the larger DoD "front door" for IA vendors desiring to have their products considered for use by DoD.
3. Collect and share the IA product evaluations that have already been performed (this is underway at IATAC.
4. Better understand and communicate DoD IA needs and requirements to vendors to improve the "matching" process—to find what we need faster.
5. Establish a CND Tools working group to identify and facilitate enterprise-wide buys in an effort to improve cost sharing.

A note to vendors—

If you are an IA vendor and would like to submit your product to DoD for consideration, contact Carol Cain at crcain@missi.ncsc.mil or dibao@missi.ncsc.mil.

A note to DoD IA professionals—

If you are looking for evaluations related to IA products, please visit the IATAC Web site at http://iac.dtic.mil/iatac/pdf/dod_tool.htm. If you have IA product evaluations that want to share with the rest of DoD please contact Abe Usher at iatac@dtic.mil. ■

About the Author

Vivian Cocca

Ms. Cocca serves in the Information Assurance Directorate of OASD(NI3). She has a bachelor's degree in Geography from the University of California, a Masters in Strategic Intelligence, is CIO Certified from the NDU, and is also a Certified Information Systems Security Professional (CISSP). Ms. Cocca may be reached at vivian.cocca@osd.mil.

product 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 On-line:** http://www.dtic.mil/dtic/regprocess.html.
The *IAnewsletter* is **UNLIMITED DISTRIBUTION** and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ❑ USA ❑ USMC ❑ USN ❑ USAF ❑ DoD
❑ Industry ❑ Academia ❑ Gov't ❑ 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 (3rd ed.) ❑ Intrusion Detection (3rd ed.) ❑ Vulnerability Analysis (2nd ed.)

Critical Review and Technology Assessment (CR/TA) Reports

❑ Biometrics (soft copy only) ❑ Computer Forensics* (soft copy only) ❑ Configuration Management
❑ Defense in Depth (soft copy only) ❑ Data Mining ❑ Exploring Biotechnology
❑ IA Metrics ❑ Network Centric Warfare
❑ Wireless Wide Area Network (WWAN) Security

State-of-the-Art Reports (SOARs)

❑ Data Embedding for IA (soft copy only) ❑ IO/IA Visualization Technologies
❑ Modeling & Simulation for IA ❑ Malicious Code

* You MUST supply your DTIC user code before these reports will be shipped to you.

UNLIMITED DISTRIBUTION

Hardcopy *IAnewsletters* available

Volumes 4		❑ No. 2	❑ No. 3	❑ No. 4
Volumes 5	❑ No. 1	❑ No. 2	❑ No. 3	❑ No. 4
Volumes 6	❑ No. 1			

Softcopy *IAnewsletters* back issues are available for download at http://iac.dtic.mil/iatac/news_events/ia_newsletter.htm

Fax completed form to IATAC at 703/289-5467

June

Protecting America's Infrastructure—
Cyber Defense Homeland Defense Training Conference
June 5, 2003, NRECA Executive Conference Center, Arlington, VA
703/807–2027

Homeland Conference and Expo
"A Federal Partnership for Securing America"
June 4–5, 2003, NIST Conference Center, Gaithersburg, MD
http://www.fbcinc.com/newpromos/HomelandConference_6_4_03.pdf

Federal Information Superiority Conference
June 17–18, 2003, Colorado Springs, CO
http://www.fbcinc.com/fisc/main.php

4th Annual IEEE Information Assurance Workshop
June 18–20, 2003

September–October

InfowarCon 2003
September 30–October 3, 2003, Renaissance Hotel, Washington DC
http://www.infowarcon.com

Workshop on Rapid Malcode (WORM) in conjunction with the 10th AMC Conference on Computer and Communications Security
October 27, 2003, Wyndham City Center, Washington DC
http://pisa.ucsd.edu/worm03/

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church, VA 22042

To change, add, or delete your mailing or E-mail address (soft-copy receipt), please contact us at the address above or call us at 703/289-5454, fax us at: 703/289-5467, or send us a message at: iatac@dtic.mil