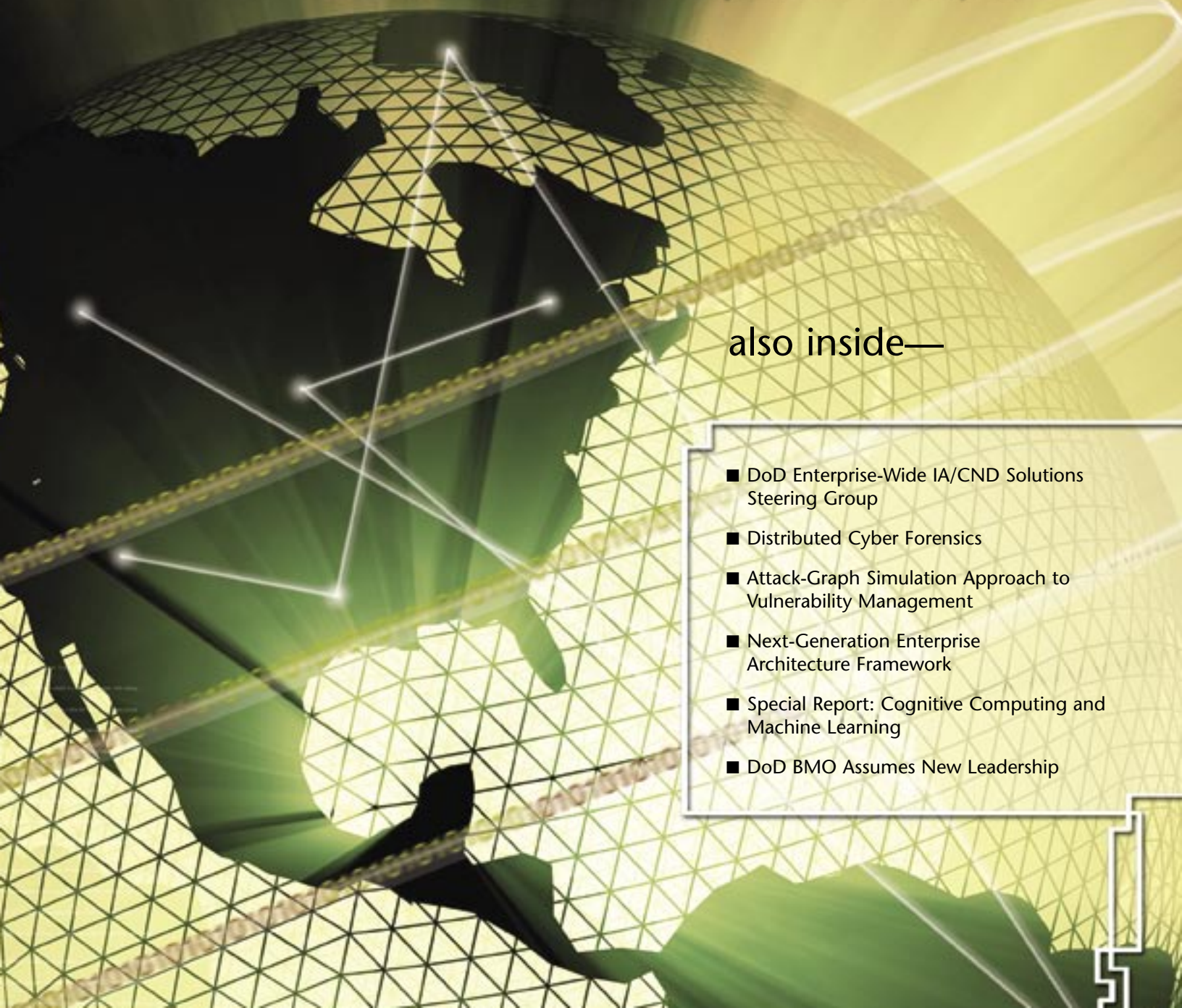
IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 6 Number 4 • Spring 2004

Information Assurance (IA) and Peer-to-Peer File Sharing

—MAJ Michael A. VanPutte, USA



also inside—

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 Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the U.S. Government, DoD, or DISA. The mention of commercial products and/or services does not imply endorsement by the DoD or 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

IAnewsletter Staff—

Creative Director:	Christina P. McNemar
Art Director:	Ahnie Senft
Designer:	Kathy Everett
	Maria Candelaria
Editorial Board:	Abraham T. Usher
	April Perera
	Jim Peña
	Brad Soules

IAnewsletter Article Submissions

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

IAnewsletter Address Changes/Additions/Deletions

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

IATAC
Attn: Peggy O'Connor
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 2004	June 25, 2004
Cover design:	Kathy Everett
	Maria Candelaria
Newsletter design:	Ahnie Senft

IATAC Chat

Robert J. Lamb, IATAC Director

I guess I'm about 30,000 feet up as I write this "chat" session. As I sit here with fingertips resting on the keyboard, I have a couple of things on my mind.

One is preparing my comments for this edition of the IATAC Chat. The other is to prepare a presentation for the DoD Enterprise-Wide IA/CND Solutions Steering Group, which met at the end of March. You will see we have an article in this edition resulting from a recent meeting I had with Chuck Nicholson, author of the article "DoD Enterprise-Wide IA/CND Solutions Steering Group." In that meeting, and in this article, Chuck describes the purpose and mission of this jointly sponsored [USSTRATCOM and ASD(NII)] steering group. Chuck's article provides an overview of the steering group including membership and functions. He also describes the IA/CND Solution Cycle, a two-phased process for selecting and acquiring IA/CND solutions. There are some interesting initiatives coming out of the group with an ambitious agenda, which will have significant impact on the Department.

I ended up finishing that presentation and shipped it off to Omaha. And so I've turned my attentions to this "chat." As I contemplated what I wanted to write about, as those fingertips "danced" across the keyboard, I started to marvel and how much technology I'm packing on this trip…and to reflect on all the security implications it brings, because I know I'm not alone in this thirst for more gadgets, greater computing power, more and more connectivity.

So here I am…I've got my computer of course with its 40-gig hard drive, 14-inch screen, DVD player, and CD writer. Not a bad little notebook. It's got the built in wireless modem, network card, and infrared port. There weren't any "hot spots" in the airport for me to get connected with, but I was able to get my last "fix" of E-mail with my CDMA 1xEvDO card, which gets an amazing 300–500 Kbps in the DC area. I'm not watching a movie right now, but I do have my 20-gig MP3 player playing Norah Jones' newest CD with my noise-cancelling headphones blocking out the ambient aircraft noise. And when I get to the hotel, I can set up some portable speakers and continue to enjoy the "tunes." That MP3 player also serves as a backup hard drive for my important electronic files. Let's see…that's 60 gigs of storage…not to mention the recordable CDs I'm hauling. I brought along some blank recordable and rewritable CDs, not to mention my 512-megabyte memory stick, should I need to transfer my briefing at some point. I've been thinking about a "dummy cord" on that memory stick like Ranger School…would hate to lose that thing.

I'm a little worried about having enough power because the plane's DC power converters aren't working…so I guess that extra half-pound plug-in unit was kind of a waste...but not to worry, I have a spare battery.

I've got my cell phone of course. It's turned off right now, but I could play a few games on it with the built in Palm-based device. If we were allowed to, I could even do E-mail on it, made quite easy with a full-sized, expandable keyboard...just have to squint a little at the screen. It has a memory stick in it as well…can connect to e-mail…and also has an infrared capability.

So you are thinking…that's a heck of a rucksack he's carrying all that gear in and perhaps…what's this have to do with IA? Well perhaps, nothing—I'm just a gadget kinda guy and I'm willing to haul them with me. But in reality—everything—you can't get much more connected on the road than I am—dialup, LAN connectivity, broadband wireless, infrared, and more. Just consider the security implications of that level of connectivity…and don't even think about me losing my briefcase. And, while not everyone is this devoted to their "gadgets," there are plenty who are. Just consider the IA/CND enterprise-wide security implications.

As always, I want to send my warmest regards to all of you, and remember our Service men and women serving in harms way throughout the world. ■

Information Assurance (IA) and Peer-to-Peer File Sharing

by MAJ Michael A. VanPutte, USA

There is increased concern in the Information Assurance (IA) community regarding peer-to-peer (P2P) file sharing. Many IA professionals are concerned about P2P bandwidth consumption and organizational liability in the sharing of copyrighted materials. The IA professional must be aware of other aspects of P2P file sharing, including the compromise of file confidentiality and host and information integrity. This article addresses those issues.

In the past few years system administrators have seen an explosive growth in P2P file sharing technology on networks. The most popular P2P applications like Napster®, GNUtella®, Morpheus®, KaZaA®, Freenet®, Grokster®, and Bearshare® allow users to share digital files easily and freely over the Internet. These applications perform file location and copying for a computer user by locating machines across the Internet running P2P applications with files matching a user's request. Today's P2P applications typically share audio (MP3 music files), graphic (GIF and JPG photos), video (AVI or MPEG movies) formats but may distribute any file type (zip files, disk images, or Microsoft Word, PowerPoint, or Excel documents).

Software developers create P2P applications and share them on the Internet. Computer users download the applications from Internet sites and install the P2P applications on their computers. Next, users decide which files they wish to share with other users on the Internet. When users want files, they request them, the P2P application finds other users on the Internet who have files that match the requests, and the P2P application copies and distributes the files to the requestors.

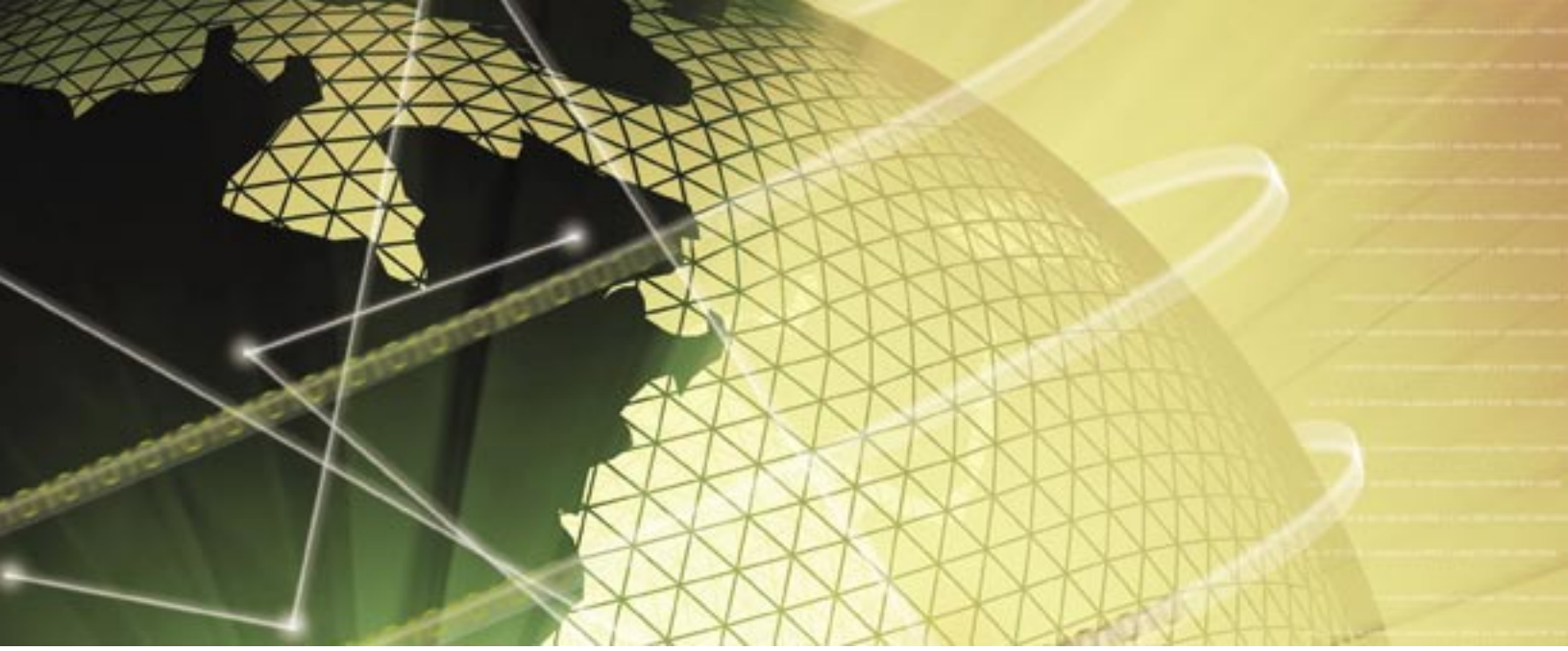
Most system administrators are aware of the performance effects that P2P application use has. There are instances where single users unintentionally deny all other traffic on networks through their use of P2P file sharing—in effect causing an inadvertent self-imposed denial-of-service. When this traffic is aggregated, a few P2P users have the potential to consume an entire network backbone, denying official traffic to entire enclaves.

While many organizations have existing policies that prohibit the use of P2P, the P2P applications have evolved to bypass security countermeasures imposed by system administrators in order for the applications to get out and share files on the Internet. These capabilities include camouflaging P2P traffic by renaming shared files, hopping from blocked network ports, using common network communication ports (53/DNS, 80/HTTP, etc.) and encrypting files. Consequently, preventive measures such as blocking TCP/UDP ports on routers and firewalls are ineffective. When P2P applications detect that they are being blocked, they switch to other ports, until they find one they can communicate through.

Other threats

Many P2P applications rate users by the volume or number of files they share with the P2P community—encouraging users to share all audio or image files. The Kazaa sharing wizard, for example, searches the user's hard drive for audio and image files and shares the content of any folder that contains these file types with the rest of the P2P community. A user who runs this wizard and has a single audio file in the "my documents" folder shares the entire contents of the folder over the Internet. This may result in the inadvertent disclosure of documents on a user's local or network drives without system users knowledge. It is very common to search P2P networks and discover income tax returns, medical records, personal E-mail, and phone rosters being shared with other P2P users around the world. This disclosure is a means for criminals to collect sensitive information in order to perform identity theft, blackmail, or other criminal activities.

When a user downloads and installs a typical P2P application, other software is unknowingly installed on the user's computer. These bundled applications, typically called spyware or adware, record surfing habits, deliver advertisements, collect privacy/configuration information, and modify system settings—and this information is passed back to the developers. P2P developers use these bundled applications as a means to generate income. Not only are these applications annoying and consume additional network bandwidth, they are another means for individuals to collect information on user's private activities and interests.



Like most applications, P2P applications may introduce additional software vulnerabilities into systems. There have been numerous application bugs in the various P2P programs that permit malicious individuals on the Internet to gain complete access to a system, providing a means to access any files, install additional applications including root kits, or damage the system. Additionally P2P users may unknowingly download malicious software, including viruses, Trojan Horses, and worms that are camouflaged as music or image files. For example, the XMS32.EXE backdoor worm, camouflaged as a game or other program file and shared over P2P networks, compromises a computer system, allowing malicious individuals to connect to the compromised systems and do anything to the computer that has been infected. These malicious programs when run unknowingly by a user, permit arbitrary individuals to access a host and cause effects that are limited only by the attackers creativity, and in many cases run invisibly to the user.

The P2P applications, with stealthy port usage and encrypted files, easily drill through the perimeter defense established by security professionals and bypass outer perimeter security, and open up the soft inside to malicious individuals. These applications are installed without system administrator oversight, and permit a covert path not only into the network, but a covert channel to exfiltrate documents out of a network!

While there is no way to prevent P2P file sharing using simple port blocking, P2P file traffic contains digital signatures in the data packets that can be detected. Signatures exist for commercially available intrusion detection systems (IDS) that can report after the fact on users who are using P2P applications, although file names and content may be encrypted preventing the easy identification of the actual files being shared through network traffic analysis. Additionally, commercial intrusion prevention systems (IPS) are available that sit inline with network routers. System administrators can configure these IPSs to throw out all, or some, P2P traffic, denying or severely limiting the use of P2P traffic on local enclaves.

Additionally, network professionals can use rate-limiting technologies to "maintain fairness" of network bandwidth usage. These technologies may limit the amount of bandwidth used by technologies like P2P, permitting other technologies to traverse the network, like E-mail and http. Rate limiting ensures no one user or technology ties up the entire network, and provides for a more stable network for all.

Response to P2P usage is a management issue. First, a decision should be made if this is an administrative (counsel-and-clean) or legal (criminal investigation) response. In the former, a confirmed user of P2P is formally counseled, in writing. The response team as a minimum must ensure the machine used for P2P is cleared of all P2P technologies and patched, and antiviral products updated and run—as well as ensuring that administrative access is removed. In severe cases (and as a deterrent) the machine should be considered compromised by a root-kit and therefore formatted and rebuilt from trusted media. In the latter case, investigative professionals should make a forensic copy of the machine. This forensic copy may reveal P2P usage, search history, and download history.

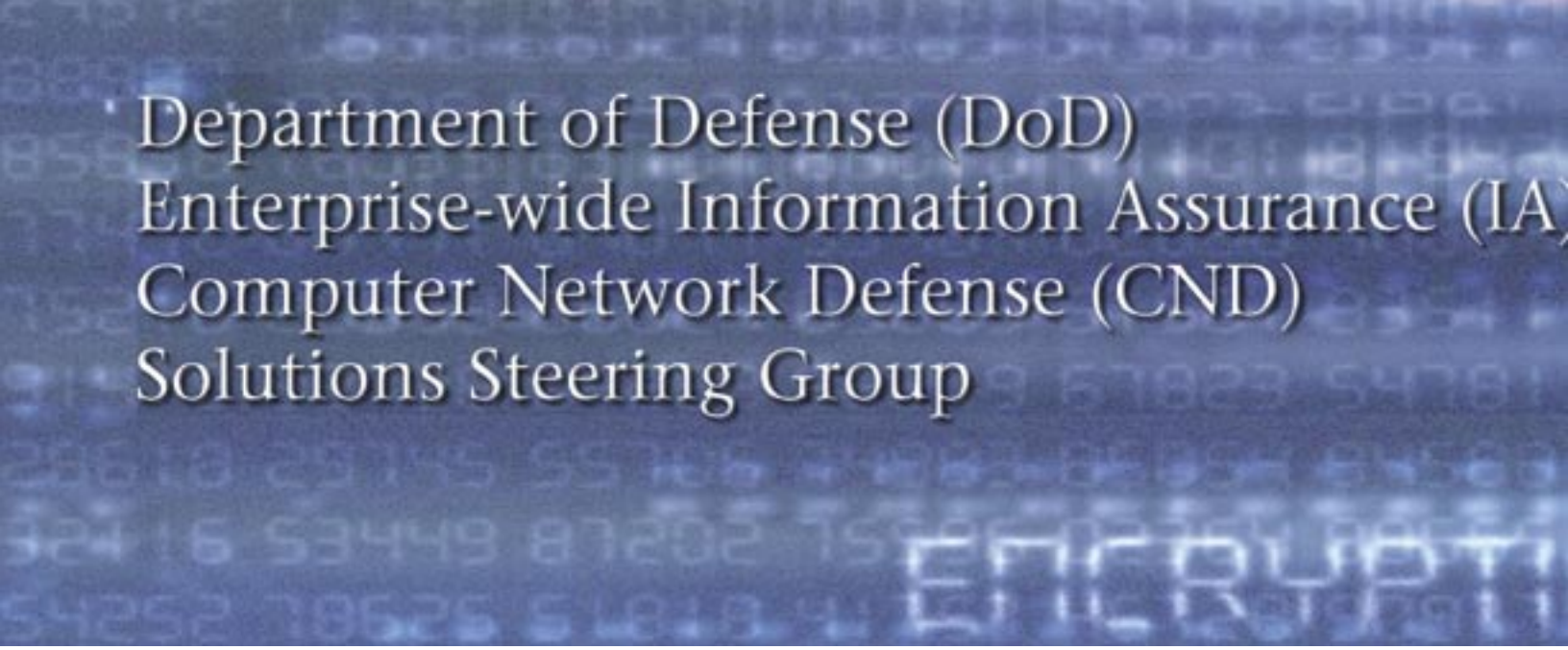
P2P file use is a symptom of other problems. First, a user has shown disregard to the use of the systems for official business only. Second, the user must have administrator/root access to install P2P application. On most systems today users do not, and should not, have the ability to install arbitrary applications on internal machines behind firewalls. Third, managers have failed to train users on the risk that they are placing the system. Management must address these issues before P2P will be eliminated.

Criminal, civil, and administrative results in DoD

Management must be made aware of not only the threat of losing or compromising sensitive information, but that users and organizations may face administrative, criminal, and civil liability as a result of the installation and use of P2P file sharing.

First and foremost, users must be informed that they do not have the authority to install freeware, shareware, and public domain software on official computers. These

continued on page 9…



Department of Defense (DoD) Enterprise-wide Information Assurance (IA) Computer Network Defense (CND) Solutions Steering Group

by Charles Nicholson

The Department of Defense (DoD) is made up of a complex network of multi-dimensional information systems. These systems are often developed, operated and maintained by Combatant Commands, Services, and Agencies (CC/S/As). These systems are jointly referred to as the "Enterprise." The privacy, integrity, and availability of the enterprise may be impacted by each system. It is vital that the DoD put into practice a single integrated method for defending the enterprise across all dimensions. Aware of this fact, the President of the United States changed the Unified Command Plan and assigned United States Strategic Command (USSTRATCOM) as the Computer Network Defense (CND) lead for DoD.

The "DoD Enterprise-wide Information Assurance (IA) and CND Solutions Steering Group" was established to assist USSTRATCOM in its role as the lead for CND. The Steering Group was established and chartered by the Commander USSTRATCOM and the Assistant Secretary of Defense for Networks and Information Integration [ASD(NII)]. This group also ensures inter-CC/S/A cooperation and coordination of IA/CND measures.

The scope of the group's charter extends to all DoD-owned or controlled information systems that receive, process, store, display, or transmit DoD information, regardless of mission assurance category, classification or sensitivity.

Functions

The functions of the Steering Group are to—

- Join together and match solutions for potential implementation to address and resolve shortfalls in the DoD Enterprise
- Advocate adherence to DoD's IA/CND goals
- Establish goals, objectives, and performance measures for IA/CND solutions
- Support a standardized IA/CND architecture and a migration plan of solutions

Membership

The Steering Group cannot be autocratic or narrowly focused. This will ensure viable IA/CND solutions are achieved, keeping pace with current threats and technology. This group must also consider the unique component needs, while focusing on specific Steering Group Charter objectives. To accomplish this, the Steering Group is represented by many organizations supporting many aspects of information security and information technology. The Steering Group is comprised of two categories of membership, voting and non-voting, as well as advisors.

Voting members are normally at the O–6/GS–15 level, but anyone can be given the right to speak for their organization and vote on IA/CND issues. Courses of Action for raised concerns will be decided by a simple majority vote of the voting members. The voting members include—

- USSTRATCOM
- United States Joint Forces Command (USJFCOM)
- Office of the Joint Chiefs of Staff, J6
- Defense Information Systems Agency (DISA)
- National Security Agency (NSA)
- Defense-wide Information Assurance Program (DIAP) Office
- Defense Intelligence Agency (DIA)
- U.S. Army
- U.S. Navy
- U.S. Air Force
- U.S. Marine Corps

Non-voting members include those not identified as voting members in the Steering Group charter. Any person or group may present information of interest to the Steering Group. This is pre-coordinated and done by invitation. Non-voting members and observers may attend meetings and participate in working group activities, however, they will not have voting privileges. Advisors include—

- DoD CND Architect (ASD(NII))
- DoD CND Systems Integrator (DISA)
- Joint Task Force-Computer Network Operations (JTF–CNO)
- Those providing technical or functional support to the Steering Group or its member.

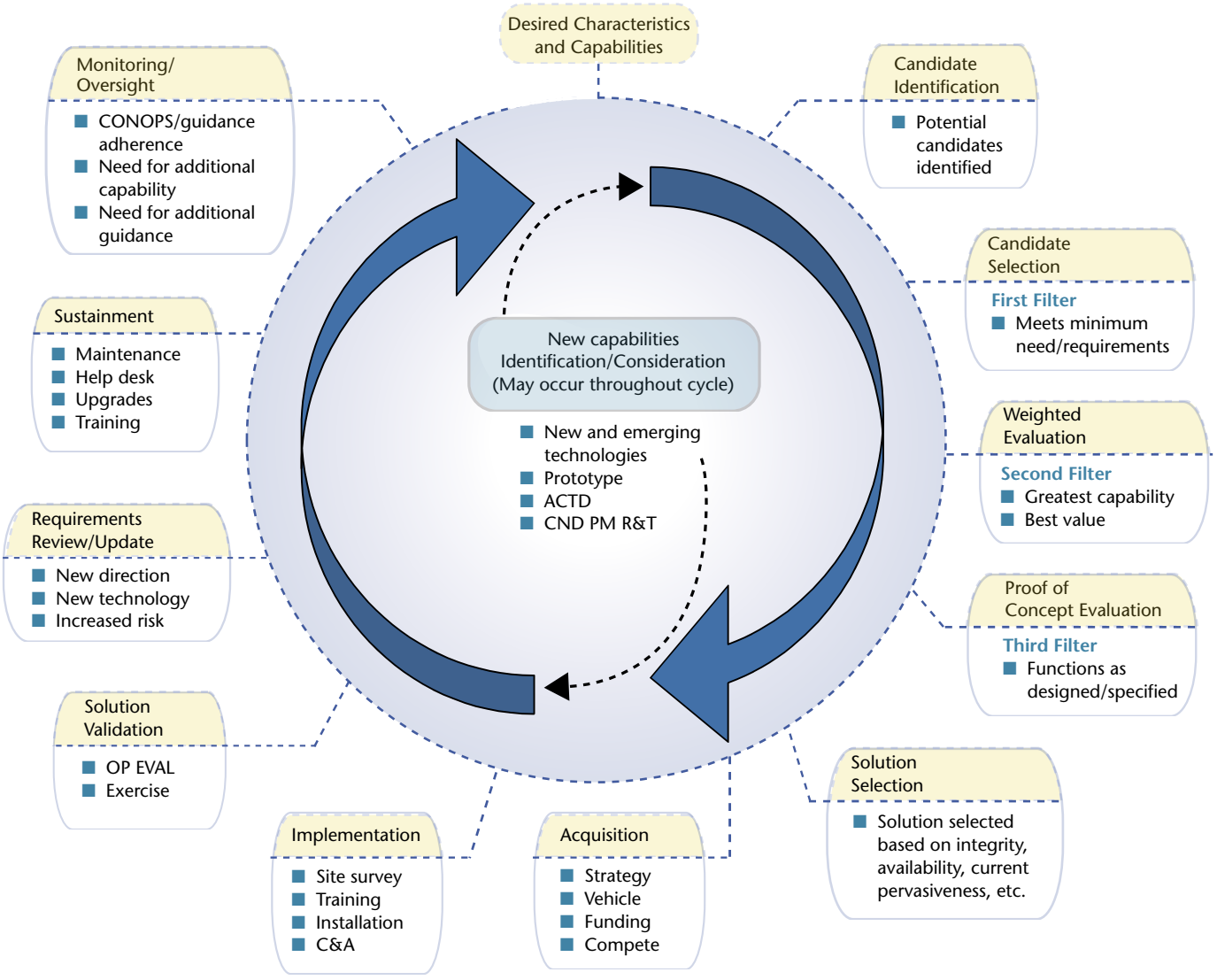


Figure 1. IA/CND solution cycle

Working Sub-Groups

To assist the Steering Group in achieving its chartered goals and activities, two working groups have been created—the Technical Advisory sub-Group (TAG) and the Acquisition Working sub-Group (AWG).

Technical Advisory Sub-Group (TAG)

The TAG is in its formative stage, and is envisioned to provide the primary research for potential solutions from the government, commercial and academic sectors. This group relays gathered information and deployed products within the enterprise to the AWG. The TAG also assists with the creation of a Request for Information (RFI) by providing technical and expert support. After the consolidated solutions' listing is received from the AWG, the TAG will oversee the testing and evaluation. Once this is complete, the TAG will recommend a solution for acquisition to the Steering Group. The core membership of the TAG will be—

- JTF–CNO
  - Technical Director
  - Applied Technology Unit (ATU)
- USJFCOM Joint C4ISR Battle Center (JBC)
- NSA
  - Business Affairs Office (BAO)
  - Resource and Testing (R&T)
- DISA
  - Field Security Operations
  - Joint Interoperability Test Command (JITC)
  - Technology Integration Panel (TIP)
- Service/Agency Labs

The core membership of the TAG is relatively static, while the advisors and membership at large is dynamic. This is to ensure the requisite expertise is available to achieve the goals and tasks of the group.

Acquisition Working Sub-Group (AWG)

The AWG is the main interface with the commercial industry for RFIs and Request for Proposals (RFPs). The AWG will combine commercial industry's answers to RFIs and any known solutions for an identified shortfall and provide this to the TAG. The focus of this combined solutions listing centers on maturity and ease of acquisition. Once the Steering Group has reached an acquisition decision, the AWG will begin developing the needed documents and acquisition strategy. Key members of the AWG include—

- DISA Chief Information Assurance Executive (CIAE) (Chair)
- DIAP
- DISA Field Security Operations (FSO)
- JFCOM JBC
- USAF Enterprise Software Initiative (ESI)

Similar to the TAG, key membership of the AWG is static. The structure of the AWG can vary to fulfill assigned tasks.

IA/CND Solution Cycle

The IA/CND Solutions Cycle is a two-phased process, focusing on selecting and acquiring IA/CND solutions. The first phase includes activities such as listing requirements, selecting candidates and assessing technologies using weighted factors. The second phase includes acquiring, implementing, sustaining, monitoring, and oversight.

The IA/CND Solutions Cycle model is not a sequential process, where one step must be done before moving to the next. This model represents a very active process, where multiple steps are being worked at the same time. The IA/CND Solution Cycle model is shown in Figure 1 (see next page). ■

About the Authors

Charles Nicholson

Chuck Nicholson is the Senior Information Assurance Specialist in the IA Division at USSTRATCOM and a retired U.S. Naval Officer. He received a M.S. in Computer and Electrical Engineering from the Naval Postgraduate School and is a Certified Information Systems Security Professional (CISSP). Mr. Nicholson is the current holder of the NSA's Frank B. Rowlett Trophy for Individual Achievement in the field of information systems security for his work at USSTRATCOM. He may be reached at nicholsc@stratcom.mil or 402/232-5948.

Alan Hensley

Alan Hensley is a retired Naval Cryptologic Officer. He received a B.S. in Health Care Management from Park College in 1982, B.S. in Computer Management Information Systems (CMIS) from the University of Maryland University, College Park, in 1989, and a M.S. in Criminal Justice from Troy State University in 1995. He may be reached at hensleya@stratcom.mil or 402/232-6640.

Robert Ferguson

Bob Ferguson is a retired US Air Force Senior Non-Commissioned Officer. He received a BS in Computer Information Systems Management from Colorado Christian University in 2000. Mr. Ferguson can be reached at fergusor@stratcom.mil or 402/232-6343.

continued from page 5…

"Information Assurance (IA) and Peer-to-Peer File Sharing"

systems are not an employee's personal property. [1] While some might say that P2P applications may be used for "morale purposes," P2P introduces too significant a risk to DoD, and has a detrimental effect to DoD systems. [2] All four DoD services have policies prohibiting the use of P2P, and a soon-to-be released DoD policy, signed by the DoD Chief Information Officer, makes it very clear that local authorities should not authorize P2P use without compelling operational reasons and not for sharing copyrighted materials.

Users who use P2P applications on DoD computers or networks may have inadvertently violated a lawful order/directive and be subject to administrative and punitive actions. Even without a signed user agreement, Service policies make the use of P2P applications punishable under Uniform Code of Military Justice (UCMJ) or through civilian disciplinary action.

Government employees who duplicate and share copyrighted materials may violate numerous directives, regulations, and federal laws. Contractors and government employees face both administrative and disciplinary actions. Employees or contractors whose use of P2P applications threaten, damage, or potentially harm the information or information systems, or who perform unauthorized activities, may be banned from network usage by local authorities as specified in DoD policy (CJCSM 6510.01), which may deny an employee or contractor from being able to perform their duties and result in their termination. [3]

Additionally, the act of duplicating and distributing copyrighted materials may be in violation of Federal law, Pursuant to 17 United States Code 512(c)(2) (Digital Millennium Copyright Act of 1998). Criminal and civil prosecution may result in fines in the tens to hundreds of thousands of dollars, for which the user may be personally responsible. The embarrassment and costs to an individual or command could be tremendous.

P2P is not permitted on DoD computers or networks

As IA professionals we cannot, through indifference, permit users to place themselves and the organization at risk. If users want digital files they need to look for reputable ways to obtain files. There are commercial sites that allow free listening to music and other sites to purchase music files.

It is up to you to use P2P applications on your personal computer on your own time. However, you should realize that, like many other aspects of the Internet you place yourself at risk. If you have questions on the use of P2P applications, contact your Staff Judge Advocate, Chief Information Officer, or Commander. ■

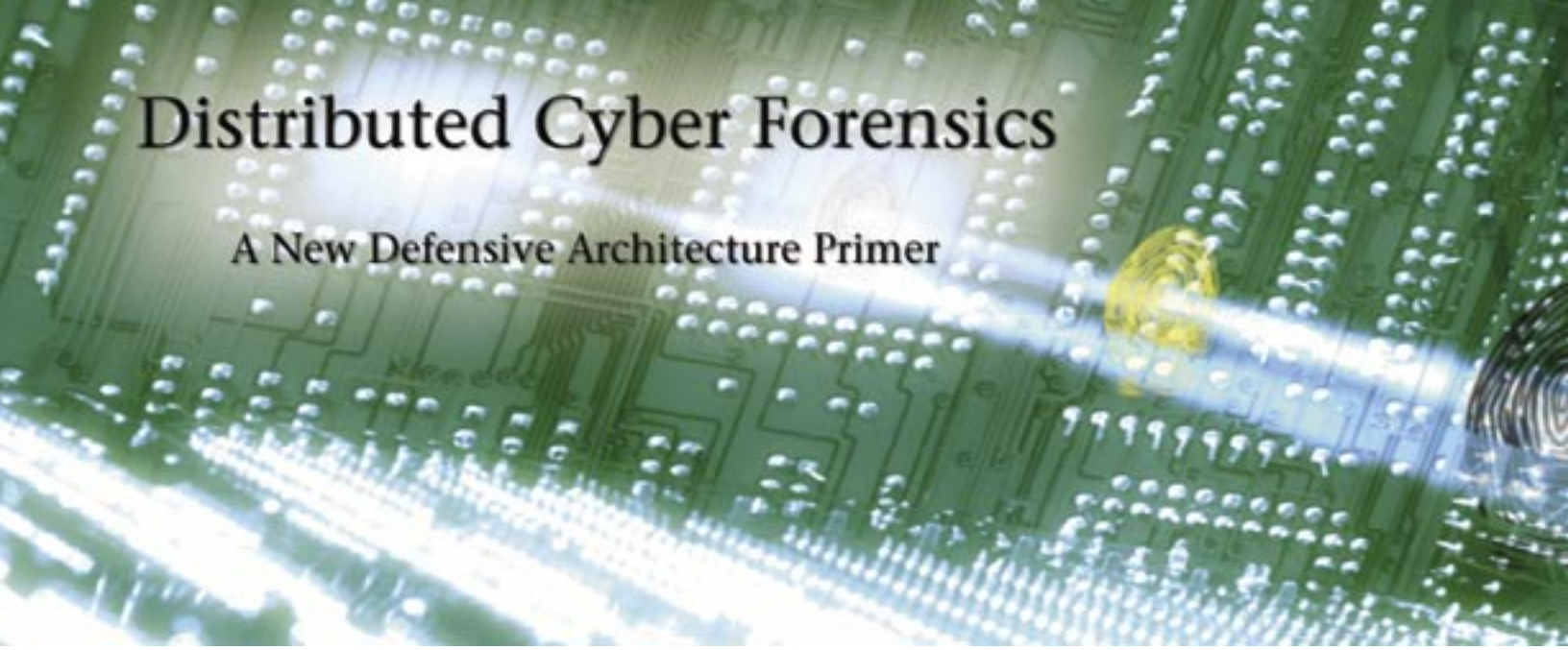
About the Author

MAJ Michael A. VanPutte, USA

MAJ Michael A. VanPutte is the Branch Chief , Network Defense Operations for the Joint Task Force for Computer Network Operations (JTF–CNO), U.S. Strategic Command (USSTRATCOM). He received a Bachelor's degree from the Ohio State University, a Master's Degree from the University of Missouri-Columbia, and a Ph.D. from the Naval Postgraduate School. He may be reached at michael.vanputte@us.army.mil.

References

1. "Public domain software products (freeware) may be used in DoD systems if an official requirement is established, the product is assessed for IA impacts and is approved for use by the responsible [DAA]." CJCSI 6510.01C subj: IA and CND, Encl A, para 2.l., dated 1 May 01.
2. "All DoD military, civilians, and contractors will…use DoD information systems only for official use and authorized purposes IAW DODI O–8530.2." CJCSM 6510.01, dtd 25 Mar 03, App A to Encl A, para 7.b.(5). Additionally, Joint Ethics Regulation Subsection 2–301.a(2) states that "Authorized use also includes personal communications from the employee's usual work place that are reasonably made while at work when the Agency Designee permits such categories of communication, determining that the use: (1) does not adversely affect the performance of official duties by the employee or the employee's organization; (4) does not reflect adversely upon DoD or the Agency (such as uses involving pornography,…violations of statute or regulation;…and other uses that are incompatible with public service); and (5) does not overburden the communication system…, creates no significant costs to DoD…"
3. "CC/S/As will suspend network access for users who knowingly threaten, damage, or harm DoD information systems, networks, or communications security…or perform unauthorized use of the network" CJCSM 6510.01, dtd 25 Mar 03, App A to Encl A, para 8.



Distributed Cyber Forensics

A New Defensive Architecture Primer

by Peter M. Tran

The Information Assurance Technology Analysis Center (IATAC) published a critical review and technology assessment (CR/TA) entitled "Computer Forensics: Tools and Methodology" in May of 1999, discussing emerging computer investigative techniques and methodologies. Since its release there have been significant changes, not only in the worldwide information technology (IT) landscape, but also in how global enterprises such as the U.S. Department of Defense (DoD) utilizes cyber forensics to safeguard critical information resources.

Research conducted by International Data Corp (IDC), predicts the IT market worldwide is poised to experience growth resurgence in 2004, more specifically in a shift away from proprietary architectures, with a trend towards business continuity innovation, open platforms and IT standardization. [1] To remain agile in this dynamic IT environment and to continue facilitating collaborative efforts between the public and private sectors, the DoD must continue to embrace a New Defensive IT Architecture (NDA). Whereas DoD IT architectures in the past have been monolithic and slow moving, NDA has provided the DoD with the tools necessary for operational agility by refocusing on a new "value web" comprised of innovative technologies, multi-agency partnerships, shared intelligence, uniform information assurance practices and real time global collaboration through standardized common information portals. [2] A most critical component within the NDA value web is the role in which cyber forensics plays in enabling the DoD IT agility. A detailed examination of all cyber forensic resources is beyond the scope of this article; however, a summary of pertinent resources is provided in Table 1.

As NDA becomes increasingly prolific within the DoD, cyber attack methodologies and techniques (Intrusion Vectors) will adapt to changing IT environments. In a four-year period from 1999 to 2002, total reported cyber incidences increased from 454 to 489,890. [3] In a nine-month period in 2003, the Department of Homeland Security (DHS) reported an increase from 3,505 total cyber related incidents in January to 204,756 in September (see Figures 1 and 2 on page 12).

Table 1. Related Cyber Forensic Resources

Resources
Introduction to Cyber Forensic Analysis (Power Point) http://www.blackhat.com/presentations/bh-usa-99/PeterStevens/inet-investigation-short4.ppt
Computer Emergency Response Team (CERT) Coordination Center http://www.cert.org
Sys Admin Audit Network Security (SANS) Institute http://www.sans.org
Computer and Internet Crime FAQ http://www.forensic-science.com/faq_computer.html
Complete List of Computer Forensic Tools and Vendors http://www.forensics.nl/tools
High Technology Crime Investigation Association http://htcia.org/linksframe.htm

Cyber attacks of the past were comprised of one-dimensional intrusion vectors with a single scope (i.e., denial-of-service, root compromise, Web site defacement). To date, cyber attacks have evolved into complex, multiple-layer, multistage mechanisms (blended intrusion vectors) designed to intelligently exploit IT systems in waves (see Figure 3 on page 12). According to Paul Schmehl of Avien, a non-profit organization of information security professionals, the dividing line between different types of cyber attacks such as malicious code (Malware) and network intrusions has begun to blur to a point that one attack is indistinguishable from the other. [4]

Table 2. Related U.S. Legislation

Legislation	Overview
Sarbanes-Oxley Act of 2002	Requirement for self-policing and internal investigation. Severe liability for destruction of electronic records; Up to $25 million fines, 20 year prison terms. http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
Patriot Act of 2001	Must monitor financial activities as they may be related to terrorism; 25K per day fines. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf
NASD Rule of Conduct 3110	Broker/Dealers Must Retain all Communications With Customers. http://www.nasdr.com/conrule_3110.htm
FTC Safeguards Rule	Requires covered entities to maintain Infosec program that includes "Detecting, Preventing and Responding to Attacks, Intrusions, or Other Systems Failures." (16 CFR Part 314.4(b)(3). http://www.namb.org/government_affairs/front/FTC_Standards_for_Safeguarding_Customer_Info.pdf
Gramm-Leach-Bliley Act of 1999, Title V	Must ensure the privacy of financial information. Must have comprehensive security plan in place. http://www.senate.gov/~banking/conf/confrpt.htm
HIPAA Act of 1996	Must keep patient records confidential, fines to 250K and 20 years; Must have comprehensive information security plan in place. http://aspe.hhs.gov/admnsimp/pl104191.htm

Government and law enforcement officials rely on proven scientific forensic disciplines, such as cyber forensics to provide vital evidence utilized in apprehending cyber criminals and preventing future attack incidents. Continual changes in IT environments, increased opportunities for cyber crime coupled with robust U.S. legislation necessitate advances in government, law enforcement and forensic computing technical areas (see Table 2).

Traditional cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and/or computer peripherals that allow investigators and other information security officers to respond and prevent cyber crimes. Reminiscent of a post-mortem examination, cyber forensics looks for evidence after the commission of a crime (Figure 4 on next page).

Two distinct components exist in the field of cyber forensics. The first component is a static examination that deals with gathering evidence from computer media seized at a cyber incident scene by—imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for

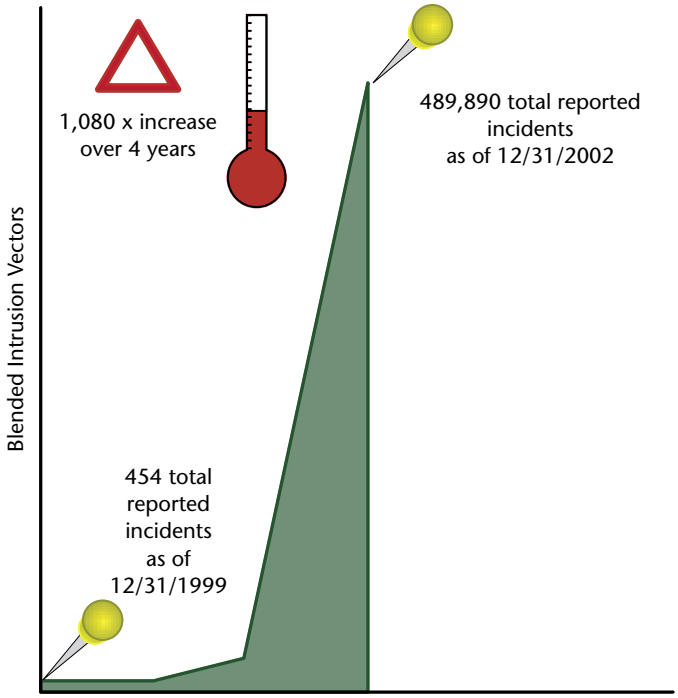


Figure 1. January 1, 1999 through December 31, 2002 annual totals of incidents reported by the Department of Homeland Security Federal Computer Incident Response Center (FedCIRC).

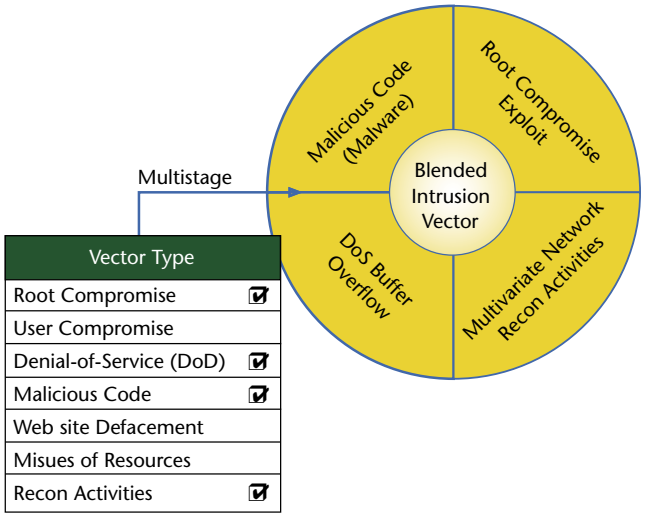


Figure 3. Cyber attacks have evolved into complex, multi-layer, multi-stage mechanisms (blended intrusion vectors).

Figure 4. Reminiscent of a post- mortem examination, cyber forensics looks for evidence after the commission of a crime.

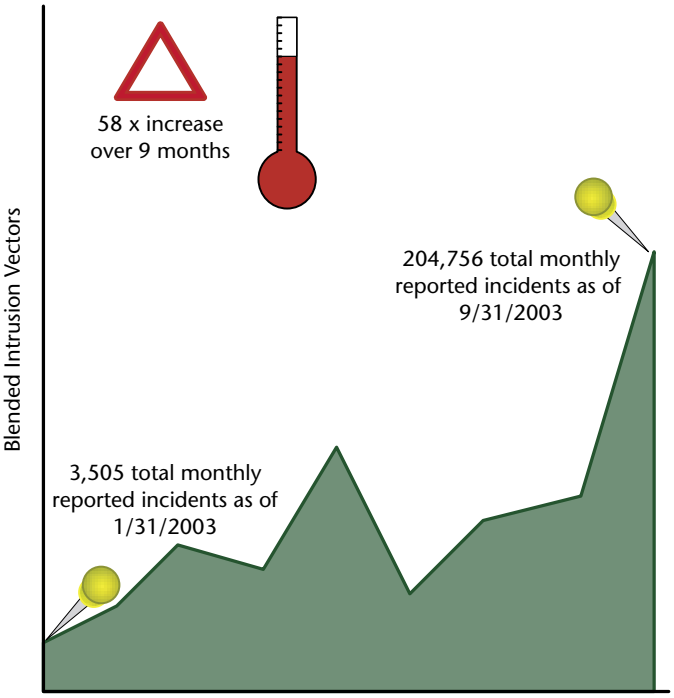


Figure 2. Nine Month Period (1/1/2003 through 9/31/2003) of incidents reported by the Department of Homeland Security Federal Computer Incident Response Center (FedCIRC).

investigative purposes. The second component, dynamic examination, is a more technically challenging aspect of cyber forensics that entails gathering digital evidence that is distributed across large, complex networks. This evidence is most frequently transient in nature and not preserved within persistant storage media. Dynamic or Distributed Cyber Forensics (DCF) focuses on real-time, online evidence gathering rather than the traditional offline "static" computer disk forensic technology. Promulgated by the DoD NDA focus for rapid response and prevention, DCF systems are increasingly being evaluated for operational implementations given inadequacies in current commercial intrusion and forensic analysis tools. In order to contain and mitigate operational interruptions and data destruction, it is imperative to perform "forensic-esque" examinations of victim and non-victim information systems on a continuous basis, in addition to traditional postmortem forensic analysis. This is essential to continued availability of critical information systems and infrastructures. In the battle against malicious hackers, investigators must perform cyber forensic functions in support of various objectives, to include timely cyber attack containment, suspected attacker identification and location, damage mitigation and business continuity/disaster recovery initiation in the case of a crippled network (see Figure 5).

Figure 5. In the battle against malicious hackers, investigators must perform cyber forensic functions in support of various objectives.

A comprehensive forensic Defense-in-Depth (DiD) methodology includes layered examination of many sources of data evidence (intrusion detection system (NIDS) logs, firewall logs, audit trails, and network management information (see Figure 6 on page 13). DCF adds inspection of transient and frequently overlooked elements such as contents and state of memory, registers, basic input/output system (BIOS), input/output buffers, serial receive buffers, L2 cache, front side and back side system caches, and other various system buffers such as video, audio and drive buffers.

DCF is increasingly becoming an integral component of the information assurance (IA) value web by intelligently combining forensic techniques and technologies in a balance between cost, performance, protection capability, and operational considerations, which are often barriers to a DiD security architecture. As we head into new territories of information warfare, we must continue to turn our information assurance infrastructures "inside out" with a New Defensive Architecture to address the availability, integrity, and confidentiality of our critical information resources. ■

About the Author

Peter M. Tran

Peter M. Tran supports the Defense Information Systems Agency (DISA) Joint Task Force Computer Network Operations (JTF–CNO) Law Enforcement Counter Intelligence Center (LE/CI). His main area of expertise, encompasses the DISA information assurance program in designing and deploying proactive information system protections, cyber attack detection, and performing information assurance (IA) threat analysis and operations. Mr. Tran served as a Special Agent in the Computer Investigations Division of the U.S. Naval Criminal Investigative Service (NCIS) Washington Field Office. He principally handled investigative and technical matter relating to network intrusions, computer forensic analysis and research technology protection (RTP). Mr. Tran holds numerous software patents in the field of biometric data authentication over TCP/IP and possesses a broad research background in automated comparative forensic analysis of genomes over networks from the Harvard University where he was a research fellow in 1995. Mr. Tran holds a Master of Forensic Sciences from the George Washington University, a Bachelor of Arts from the University of California at Santa Barbara and is an MBA candidate at the Johns Hopkins University.

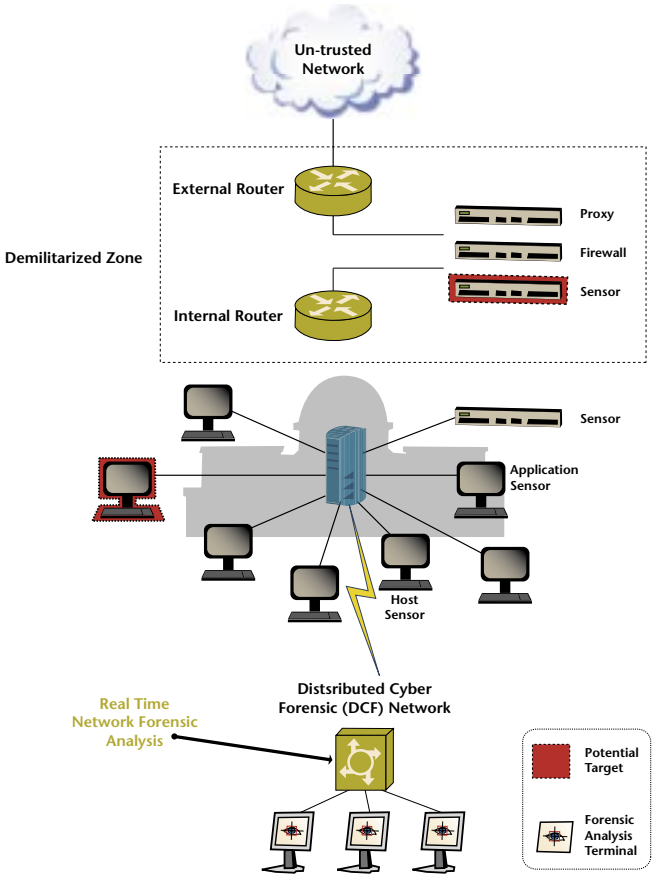


Figure 6. DCF adds inspection of transient and other frequently overlooked elements.

References

1. Singh, Piyush, et. al., Asia/Pacific Predictions 2004, Doc#AP383100K, International Data Corp, December 2003.
2. Schulman, Jeff, Comport, Jeff, Enterprise Architecture Special Report, COM–17–3617, Gartner Research Group, August 13, 2002.
3. Incident Related Statistics, Federal Computer Incident Response Center (FedCIRC), Department of Homeland Security, http://www.fedcirc.gov/index.html.
4. Schmehl, Paul, New Infection Vectors for Malware, Security Focus Group, August 6, 2002, http://www.securityfocus.com/infocus/1615.

Attack-Graph Simulation Approach to Vulnerability Management

by Alper Caglayan, Paul Thompson, and Sergey Bratus

With increasing levels of vulnerabilities, exploits, worms, viruses, and hacker activity, security teams struggle to keep their infrastructure and mission critical digital assets protected. Implementing and maintaining effective information security against symmetric, asymmetric, and malicious insider threats is a critical mission for the Department of Defense (DoD) components. Managing it is complex and expensive, and competes for scarce budget dollars with the weapons systems that it supports. The claims of a rapidly increasing number of security solution providers, with promises to stem the tide of intrusions and threats, add to the problem. As articulated in (Usher, 2003), [1] identifying vulnerabilities on a system or network is only half of the challenge—the other half is actually fixing the problems found through patching, updating, or reconfiguring. The remediation process is beset by the false positives introduced by security tools, growing number of vulnerabilities, labor intensive manual auditing and the open exposure window between discovery and remediation. Research at Dartmouth Institute of Security Technology Studies (ISTS) underlines the significance of the "vulnerability exposure window," which states that four to six months after a system audit "the probabilities are very high (66 percent to 99 percent) that an attacker can conduct a full consequence compromise." [2]

Pro-active continuous non-invasive vulnerability assessment

Given the security risk management challenges, DoD security managers need vulnerability management solutions that will enable the evolution of methodologies and policies from reactive response to proactive control, from periodic assessment to continuous assessment, and from limited penetration testing to exhaustive non-invasive testing. We believe that an attack-graph, simulation-based approach can provide such a security assessment methodology.

Attack-graphs create a graphical structured model to describe the ways in which a system may be compromised. By using network topology based attack-graph simulations that are synched with a vulnerability dictionary, security teams can understand the ways in which they will be attacked, determine the likelihood and impact of these attacks, and decide what action to take where the risks are unacceptable.

The attack-graph simulation approach to network vulnerability assessment follows the guidelines set forth by the National Institute of Standards and Technology (NIST) [3] and is consistent with research on information system survivability simulation modeling. [4] As illustrated in Figure 1, the attack-graph simulation approach consists of the iterative application of four processes—

- **Step 1**—Build the security model that captures the network model and threat contexts
- **Step 2**—Simulate attack scenarios that find real exposures
- **Step 3**—Calculate mission risks based on the impact of potential exploit of vulnerabilities
- **Step 4**—Plan the remediation for critical vulnerabilities while optimizing cost-benefit

Executed on a daily basis, this process provides an up-to-date view of the organization's security status, the impact of recent changes to the enterprise network, and the impact of new vulnerabilities and threats. The process model for this research effort also supports a key provision of NIST's "Operations/Maintenance" recommendations—Continuous Security Control Monitoring (e.g., "verifying the continued effectiveness of those controls over time").

Attack-graph simulation history

The paths of a graph represent all possible sequences of exploits, where any given exploit can take advantage of the penetration achieved by prior exploits in its chain, and the final exploit in the chain achieves the attacker's goal. Typically, attack-graphs are produced manually by Red Teams. Since construction by hand is error-prone and impractical for networks larger than a hundred nodes, researchers have proposed automated techniques for gen-

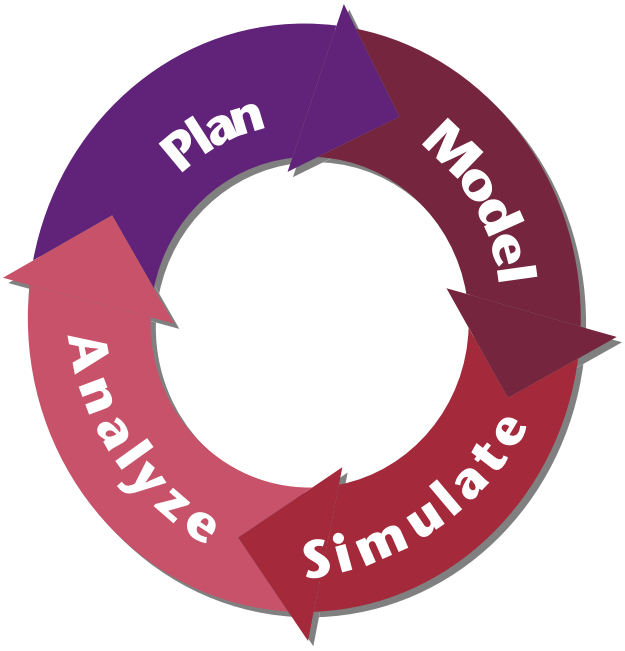


Figure 1. Attack-graph simulation risk management process

erating and analyzing attack-graphs. An early application is the attack-graph simulation tool developed by Swiler and colleagues at Sandia National Laboratory (Phillipps and Swiler, 1998), [5] (Swiler et. al., 2001). [6] The Sandia tool, one of the first tools that considered the physical topology of the network in analyzing threats, constructs attack-graphs by forward exploration starting from initial state. The Sandia tool has been applied to small networks due to the scalability of the graph and decomposition and aggregation of nodes. Sheyner proposes symbolic model checking algorithm based on NuSMV, which works backward from the goal state to produce the attack graph. [7] A major advantage of this approach is that the backward algorithm never explores the vulnerabilities that are not related to the goal of the intruder. The major disadvantage of the NuSMV symbolic checker is the computational time complexity, which is exponential.

Ammann proposed a more compact and scalable representation that relies on an explicit assumption of monotonicity, which, states that the precondition of a given exploit is never invalidated by the successful application of another exploit. [8] The assumption of the attacker never needing to backtrack reduces the complexity of the analysis problem from exponential to polynomial, thereby bringing even very large networks within reach of analysis. Jha at Carnegie Mellon University (CMU) developed a minimization technique that allows analysts to decide which minimal set of security measures would guarantee the safety of the system. [9] The CMU approach is based on a greedy algorithm with provable polynomial bounds and a reliability technique that allows analysts to perform a simple cost-benefit analysis depending on the likelihoods of attacks. The importance of the CMU approach is that attack graphs produced are exhaustive, covering all possible attacks, and succinct, containing only relevant states and transitions.

Bilar's recent thesis at Dartmouth is perhaps the most extensive treatment of risk computation in an attack-graph simulation environment. In particular, Bilar introduces the notion of extended risk where one program—usually a service—is used as a stepping stone to exploit the vulnerability in another program—usually an application. In this approach, risk assessment is obtained after assigning cost to each consequence of a basic service shown in Table 1 (see next page).

Operational deployment

The recently released commercial tool, Skybox View is an example of the deployment of an attack-graph simulation based vulnerability assessment in an operational environment. [10] Skybox View has computational time complexity similar to the CMU tool and demonstrated scalability to networks with 10,000's of nodes. Similar to Bilar's formal quantitative research on extended risk, this tool enables users to specify application dependencies in addition to discovering dependency among applications based on services.

Table 1. Quantitative risk assessment

Type	Consequence	Example
Availability	Some software or data is unavailable	Denial of service
Confidentiality	Unauthorized read access	Reading a password file
Integrity	Unauthorized write access	Remote access of a service with an integrity privilege compromise
Process	User access or software or data	Remote access of a service with a process breach
Full	Full access over software or data on a device	Root access

Network information

The network information includes network topology, routers, firewalls, servers, and other hosts. For each gateway, namely routers and firewalls, routing information and filtering rules are collected for the analysis of possible network access. For each server or host, a list of network services is collected. For instance, the following network information is automatically collected using various methods—

- Retrieving data from infrastructure management systems
- Connecting to infrastructure nodes such as firewalls and routers
- Using built-in discovery techniques to scan and retrieve network information

Figure 2 shows the hierarchical attack graph map for a sample application in Skybox View.

Vulnerabilities data

Skybox View imports vulnerabilities from existing vulnerability scanners. Using a constantly updated Vulnerability Dictionary and dynamically collected network information, this attack-graph simulation tool further distills the list of vulnerabilities by filtering false-positives.

Business logic

Business logic specifies properties for both the sources of security breaches, namely threat origins, and the targets for attack, such as business applications. Skybox View manages any number of threats, both internal and external. Threats can be defined in a variety of ways, including a human-based attacker and malicious code. Possible starting points, skills, and likelihood to attack are used to model threats. Skybox View comes with an initial set of predefined, common threats including Internet Hacker and Malicious Insider.

In Skybox View, the user can calculate risk factors both on a detailed level, for every attack scenario and vulnerability, and on an aggregated level, for business applications

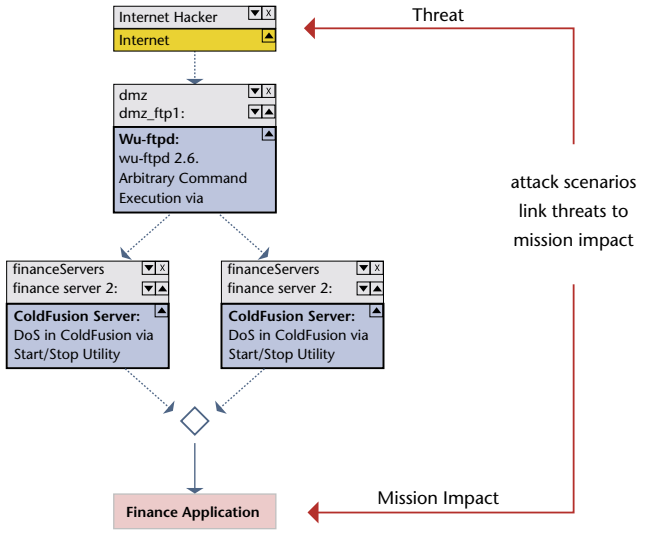


Figure 2. Attack simulation map

and threats. The risk is calculated by the multiplication of attack likelihood and the business impact (i.e., damage).

Business Risk = Attack Likelihood x Business Impact

…where the business impact is typically the economic loss associated with losing a specific business application, and attack likelihood is the probability of the business application being exploited. For DoD applications, one can use—

Business Risk = Attack Likelihood x Mission Impact

…where mission impact signifies the loss of an application on the mission success. In this approach, one needs model only for high-level output applications (e.g., weapon targeting, target tracking, and the like). The dependency of these applications on intermediate applications (e.g., domain name server) is modeled in the graph simulation.

The likelihood of an attack scenario is calculated using many factors, such as the threat likelihood and skills, difficulty to perform the attack and the specific properties of vulnerabilities along the attack path. The threat properties are derived from business logic which is contained within the Integrated Security Model. Figure 3 shows the rankings of vulnerabilities according to risk classified as direct (vulnerabilities that can be directly exploited by a threat), indirect (vulnerabilities that can be exploited only after exploiting a directly exposed vulnerability), or mitigated (vulnerabilities that cannot be exploited because of the remedies taken) vulnerabilities.

As illustrated in Figure 4, the simulation of attack graphs helps reduce the vulnerability exposure window from weeks/months to hours. Commercial tools supporting the simulation of attack graphs are scalable to large networks as, in contrast to intrusion detection systems operating on millions of temporal events, these attack-graph simulations propagate only vulnerability states along exploitable paths. Hence, a comprehensive model of the network environment is a necessary prerequisite to access analysis, which is the enabler for attack simulation. Attack simulation represents a magnitude level improvement over current vulnerability management methods that rank or categorize vulnerabilities based on gross categories—yielding sometimes misleading and incomplete listings of so-

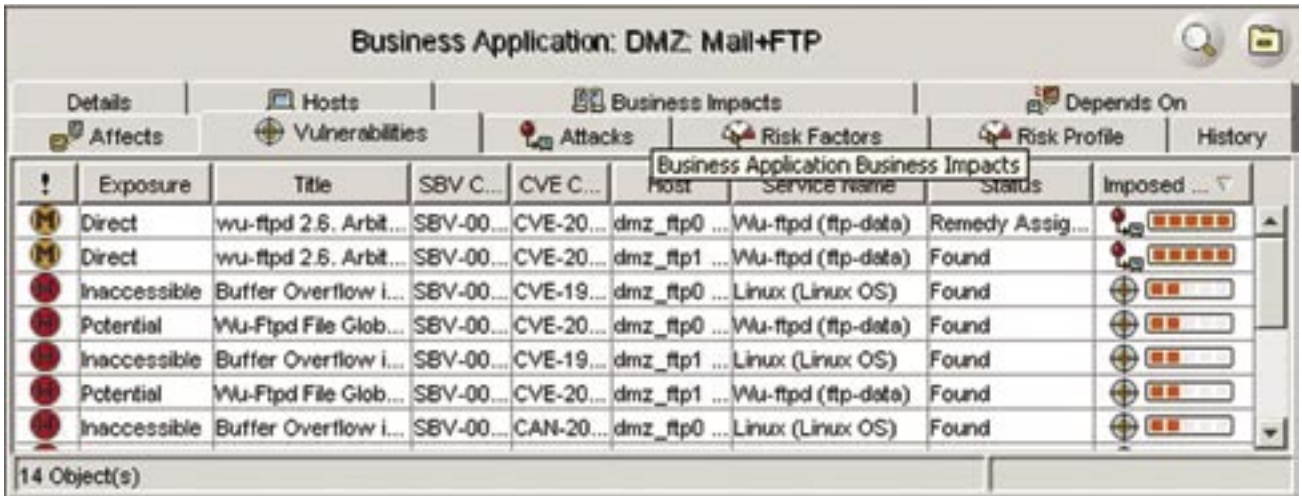


Figure 3. Ranking of vulnerabilities based on mission impact

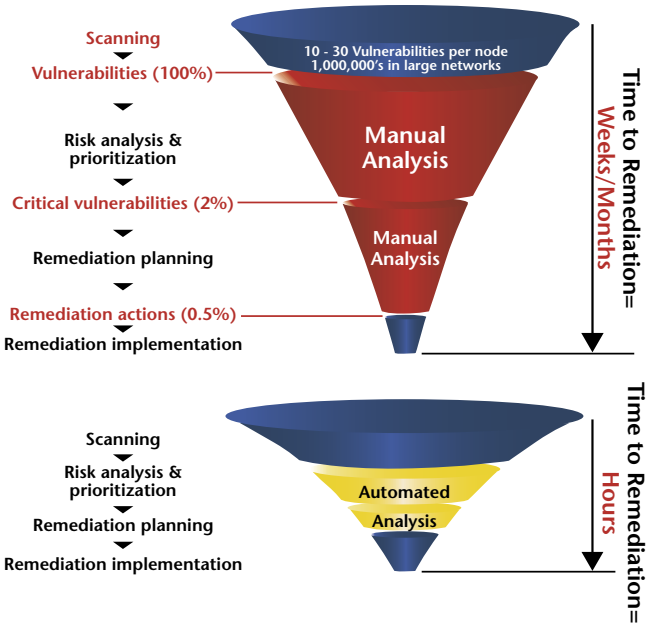


Figure 4. Closing the window of exposure

called critical vulnerabilities, and is in fact the only way to get at a provable set of critical vulnerabilities that lie along the attack path.

Summary

Attack-graph simulation tools, while automating the vulnerability assessment process, still leave the human as the ultimate decision maker to review, accept or reject the recommended remediation. Moreover, the expertise of the security expert can still be brought to bear on the insider and external threat modeling. Following the lead of US Army's mantra "all but war is simulation," [11] attack-graph simulations are now ready as an active network defense tool for integration into a 'defense in depth' information security architecture. [12] Attack-graph simulations can provide a zero-latency, proactive approach to vulnerability management that filters out the spurious vulnerabilities and closes the exposure window by providing continuous attack simulation. ■

About the Authors

Dr. Alper Caglayan

Dr. Alper Caglayan is a Principal Scientist at Milcord, LLC and held Senior Scientist positions at NASA and BBN, and senior executive positions at Open Sesame and Bowne. His research focus is in reasoning under uncertainty, machine learning, and software agents, and he is the co-author of "Agent Sourcebook." Dr Caglayan received his Ph.D. in Electrical Engineering from Virginia Tech.

Dr. Paul Thompson

Dr. Paul Thompson is a Senior Research Engineer at the Dartmouth College Thayer School of Engineering's Institute for Security Technology Studies (ISTS). His research focus includes semantic hacking, information security, machine learning, and information retrieval. Previously, Paul was a Principal Scientist at PRC, Inc. (now part of Northrop Grumman). Paul earned his Ph.D. in Library and Information Studies from the University of California, Berkeley.

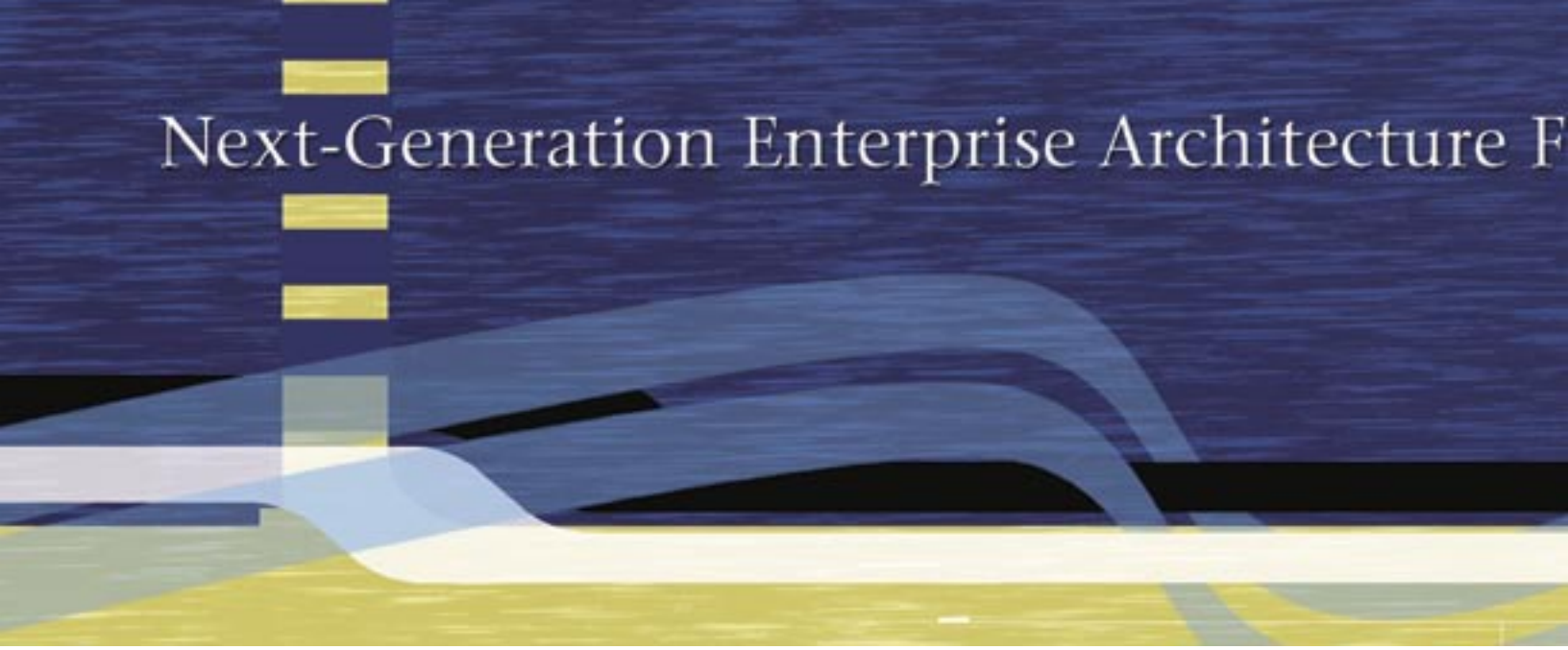
Dr. Sergey Bratus

Dr. Sergey Bratus is a Postdoctoral Research Associate at the Computer Science Department at Dartmouth College. His current research focuses on applications of machine learning and AI techniques to intrusion analysis, Unix security, and NLP and P2P networking applications for Semantic Web. Previously, Sergey worked on text understanding projects at BBN Technologies. Sergey received his Ph.D. in Mathematics and Computer Science from Northeastern University.

References

1. Usher, A. T. "Vulnerability Assessment." IAnewsletter, Volume 6, Number 2, Summer 2003.
2. Bilar, D., "Quantitative Risk Analysis of Computer Networks." Ph.D. Thesis, Dartmouth College, Hanover, NH June 2003.
3. Stoneburner, G., Goguen, A. and Feringa, A. "Risk Management Guide for Information Technology Systems." NIST Special Publication 800–30, Washington, DC, 2001.

continued on page 24…



Next-Generation Enterprise Architecture F

by Wilfredo Alvarez

The next-generation enterprise architecture (NGEA) framework for the Federal Government (FedGov) (see Figure 1) combines the use of enterprise portals—also called secure federated environments, public key infrastructures (PKI), biometrics, role-based access control (RBAC), single sign-on (SSO), intelligent identity-management, Web services, and global directory services to provide a secured, trusted, and ubiquitous enterprise environment. Although not all applications can benefit from this type of architecture, most enterprise applications will need to comply with some aspect of the DoD's Business Management Modernization Program (BMMP).

Enterprise portals

A portal (including secure federated environments) requiring authentication and authorization via a username and password or a digital certificate—the latter being preferred—limits collaboration, interchange, and access to applications and content to authorized and trusted enterprise users: a person, process, or agent. A federated environment, virtual and physical, protects intercommunication between middle-tier core services and back-end systems.

Although portals are effective for hosting Web-based applications and content, they require considerable software engineering effort to transition from fat-client-based legacy applications.

Portal solutions come in several forms—government-off-the-shelf (GOTS), commercial-off-the-shelf (COTS), or open source. The choice of an appropriate solution depends on the policy involved, the network and software, and budget constraints.

Authentication

PKI and biometric solutions can provide an authentication mechanism into a portaled environment. They also can be leveraged as an authoritative data source for user identity-management systems or services, since they contain validated and trustworthy user information—for example, a user's name, social security number, service, or unit.

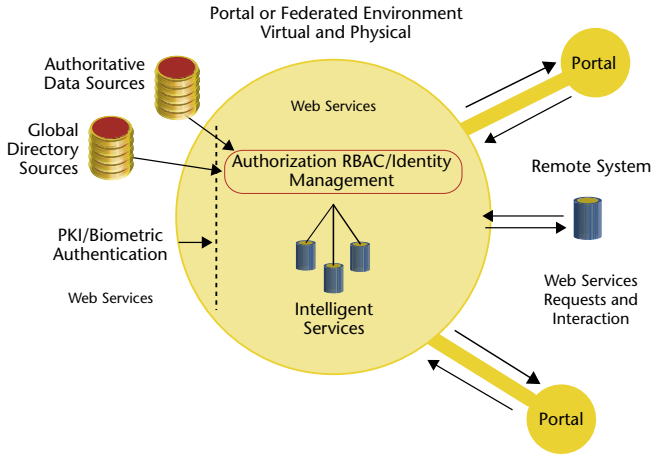


Figure 1. Next-generation enterprise architecture framework

A two- to three-factor authentication mechanism should be required for access to any DoD enterprise portal system, since systems that only require a username and password pose no real challenge for a foreign intelligence agent or malicious hacker. Unfortunately, at the time of writing several DoD portal systems exist that only require a username and password, without a clipping level or password timeout setting.

Access control

RBAC is the only authorization model that can effectively address the issues inherent within federated enterprise applications and their organizational identity-management requirements. These issues include the overburdening of application administrators with increased user account-management responsibility with no additional funding, effective, and ubiquitous identity management, enterprise-system orphan accounts, and the enforcement of application-level Information Assurance Information Conditions (INFOCONS).

Managers and developers should be familiar with the RBAC standard from the National Institute of Standards

and Technology (NIST). The standard provides a framework for incorporating various access-control models synergistically with RBAC. It includes a taxonomy and ontology for understanding and developing RBAC-controlled environments, both physical and virtual. But RBAC by itself is only a partial solution which should be leveraged with an effective authentication and identity-management component.

Single sign-on (SSO)

The term SSO describes the process of integrating a single login mechanism to one that can authenticate a user to more than one application or system, thereby not requiring further logins by the user. Such SSO solutions are already in use within DoD, and could serve as a benchmark for new software engineering efforts or COTS requirements.

SSO can be viewed as a management decision, in that a single sign-on mechanism is not necessarily required to gain access to an application or system, but would certainly ease the burden on a user who must log on to more than one application in order to accomplish his or her duties. Web services can also leverage the single sign-on component by taking advantage of it to ease the remote authentication and authorization service requirements.

Intelligent identity management

Intelligent identity management comprises a framework to create and manage a user's digital identity for use within a system or application. Intelligent denotes the fact that artificial intelligence (AI) techniques, such as rule-based expert systems, neurofuzzy nets, and intelligent agents, are an optimal and effective approach to the overall management of the mapping of users to processes and roles within a given system, and to control autonomously the type of information contained within a user's profile. Portal-to-portal communication and credential passing is the key to a true enterprise system.

Autonomous agents that act as a trusted delegate for an authorized user can benefit from an intelligent identity-management component and RBAC, especially in the extension of digital dashboard Web services, similar to stock tickers.

An intelligent RBAC component provides a resource owner the ability to control access to the resource by specifying the conditions and requirements for access to their application, as well as the ability to dynamically enforce INFOCONS. Information assurance (IA) oversight is essential for the overall success of security- and trust-based systems and processes. By providing an IA component for INFOCON management at the application level, unauthorized users can be prevented from gaining access to an application or service.

Web services

Web services are instrumental in the development and functionality of federated and Web-portal-based applications, specifically the Simple Object Access Protocol (SOAP), Security Assertions Markup Language (SAML), eXtensible Access Control Markup Language (XACML), and the WS-Security extensions to SAML developed by IBM and Microsoft. By leveraging WS-Security and SAML, a user's digital certificate could accompany a request for information from another organization's exposed service, while providing the resource administrator from that organization assurance of session confidentiality and integrity within transport and a non-repudiatable request. This would eliminate the problem of multiple users requesting information based on a single server certificate.

The decision point as to where to deploy SOAP, SAML, or WS-Security within the NGEA is based on the standard and on the type of the request. As a guide, any request going outside the system that requires extensive security should use the WS-Security extensions to SAML, while requests that remain within a secured system could simply use SOAP. Although standards development and research in Web services are on-going, current successful enterprise applications can serve as an industry best practice and provide benchmarks for future DoD Web service-based development efforts and decision-making.

continued on page 25…

Cognitive Computing and Machine Learning

by Angela Orebaugh

IAnewsletter Volume 6 Number 4 • Spring 2004 http://iac.dtic.mil/iatac

Editor's Note: *This report is the first in a series that examines new technologies that will likely have impact across DoD with implications for security professionals. It describes two subareas of artificial intelligence: cognitive computing and machine learning. Over the past five years, technology and hardware processing has drastically improved to allow these emerging technologies to develop into usable, real life products. This report will discuss some of the current focus areas and initiatives for cognitive computing and machine learning. It will also address cognitive computing and machine learning leaders in academia, R&D, government and commercial industry. Examples of existing implementations are highlighted and security initiatives, which are currently underway, are also demonstrated.*

Overview

The term "artificial intelligence" often conjures up memories of HAL, the *2001: A Space Odyssey* computer, or the more recent Steven Spielberg film, *AI*, where machines have the ability to think, act, and react like humans. Although we are still far from either of these scenarios, various subareas of artificial intelligence are under development today, led by cognitive computing and machine learning, which are appearing in both cutting edge scientific research projects and, increasingly in readily-available consumer products. Much of the advancement in the research for cognitive systems and technologies comes from the Defense Advanced Research Projects Agency (DARPA), as well as commercial computing companies such as IBM with their Autonomic Computing initiative.

Cognitive computing incorporates models of computation inspired by biological systems. DARPA defines a cognitive system as one that—

- can reason, using substantial amounts of appropriately represented knowledge
- can learn from its experience and improve its performance over time
- can explain itself and take naturally expressed direction from humans
- is self-aware and can reflect on its own behavior
- can respond robustly to surprises in a very general way

Cognitive systems can accomplish the following—

- Reflect on what goes wrong when an anomaly occurs and anticipate its occurrence in the future
- Assist in their own debugging
- Reconfigure themselves in response to environmental changes

- Respond to naturally expressed user directives to change behavior or increase functionality
- Be configured and maintained by non-experts
- Thwart adversarial systems that do not know what they are doing;
- Last much longer than current systems [1]

Note: *These are also characteristics of autonomic computing systems, for which cognitive computing is an enabling technology.*

Machine learning is the use of computer algorithms to simulate the process of learning. The goal is to understand the computational mechanisms by which experience can lead to improved performance. Learning is based on observations and data, such as examples, direct experience, or instruction.

For instance, a user may be interested in learning to complete a task, make accurate predictions, or make intelligent decisions. The emphasis of machine learning is on automatic methods to achieve these objectives.

The goal is to devise learning algorithms that do the learning automatically without human intervention or assistance. A cognitive system could not be considered truly intelligent if it were incapable of learning, since learning is at the core of intelligence. Machine learning interacts with many other technical disciplines including statistics, cognitive psychology, information theory, logic, complexity theory, operations research, mathematics, physics, and theoretical computer science.

Technology leaders

In 2003, DARPA released a strategic plan that included its top eight research areas, one of which is cognitive computing. The DARPA Information Processing Technology Office (IPTO) is leading the research in cognitive computing. Its mission is to create a new generation of computational and information systems that possess capabilities far beyond those of current systems. According to Dan Caterinicchia in "DARPA Releases Strategic Plan" (Federal Computer Week, 10 February 2003), IPTO is focusing on five core research areas—

1. Computational perception
2. Representation and reasoning
3. Learning, communications, and interaction
4. Dynamic coordinated teams of cognitive systems
5. Robust software and hardware infrastructure for cognitive systems

IPTO's goal is to develop computing systems that think and are self-monitoring and self-healing. As documented by Tony Tether of DARPA in a news item published by the agency in April 2002, IPTO is currently funding

development of software, networks, components, and full systems that are self-aware.

Current and future technologies

There are many examples of cognitive computing tasks that use machine learning; the following list includes some real life examples—

- **Optical character recognition**—Categorize images of handwritten characters by the letters represented. This technology is currently used in Personal Digital Assistants (PDAs).
- **Face detection**—Find faces in images, or detect if a face is present. This is currently used in biometric authentication.
- **Spam filtering**—Identify E-mail messages as spam or non-spam based on Bayesian mathematics.
- **Topic spotting**—Categorize news articles as to whether they are about politics, sports, entertainment, etc.
- **Spoken language understanding**—Within the context of a limited domain, determine the meaning of something uttered by a speaker to the extent that it can be classified into one of a fixed set of categories.
- **Semantic Web**—Uses intelligent agents to analyze Web sites and databases to perform more thorough and exhaustive information searches.
- **Medical diagnosis**—Diagnose a patient as a sufferer or a non-sufferer of a disease. Biomedical research also uses Semantic Web to automatically generate its own hypothesis and check the validity of it using intelligent agents.
- **Customer segmentation**—Predict which customers will respond to a particular promotion.
- **Fraud detection**—Identify credit card transactions which may be fraudulent in nature.
- **Weather prediction**—Predict if and how much it will rain tomorrow. [2]

These examples are currently being used in products and research. Several commercially available tools already exist to build expert systems such as LISP, Jess, and Smalltalk.

Standards efforts

As noted earlier, cognitive computing still lies very much in the realm of research and development. Thus, no standards have been proposed governing the implementation of machine learning and cognitive computing-based applications.

Security implications

In the areas of cognitive computing and machine learning, the primary vulnerabilities exist in the learning algorithm, data, and conclusions of the task. These vulnerabilities can include—

- Improper, inadequate, or flawed learning data
- Inadequate computational methods for performing learning
- Inadequate or improper results and decisions derived from the learned data

In cognitive computing, there is general agreement that representational issues are central to learning. In fact, the field is often divided into paradigms that are organized around representational formalisms, such as decision trees, logical rules, neural networks, case libraries, and probabilistic notations. Early debate revolved around which formalism provided the best support for machine learning, but the advent of experimental comparisons around 1990 showed that, in general, no formalism led to better learning than any other. However, as noted by Tom Dietterich and Pat Langley [3] the specific features or representational encodings selected mattered greatly, and careful feature engineering remains a hallmark of successful applications of machine learning technology.

The performance of learning systems that produce classifiers is, at present, typically evaluated in terms of the accuracy of the classifier that is learned. This evaluation method is inadequate if one of the classes is much more prevalent than the others, or if the cost of misclassifying an example from one class is different than the cost of misclassifying examples from other classes. A method of performance evaluation that is superior to accuracy in all circumstances is receiver-operating-characteristic (ROC) analysis, which is well-known in medical and signal detection fields, but has only recently been introduced to the machine learning community. While it offers a definite improvement in accuracy, ROC analysis is inadequate for the routine needs of experimental machine learning research. Learning a classifier is difficult when the training set given to the learning algorithm is imbalanced (i.e., it has many more examples of one class than the others). This problem has received considerable attention in the past few years and, as noted by the Alberta Ingenuity Centre for Machine Learning—there now exist several different ways of coping with imbalance.

Security initiatives

Throughout 2003, DARPA awarded several contracts in support of its cognitive computing initiative. The controversial project, Lifelog, has become the largest and most widely publicized. Lifelog is composed of digital assistants that digitally capture and record a person's experiences. By capturing experiences, DARPA claims that LifeLog could help develop more realistic computerized training programs and robotic assistants for battlefield commanders. The data gathering device for Lifelog is a small, sophisticated, wireless, and wearable device called a Perceptive Assistant that Learns (PAL). The PAL has sensors that collect and store the data from its users' experiences. The data collected is then transmitted to the centralized Lifelog database and cognitive computer system.

The DARPA IPTO manages the PAL program, as well as its two main research contributors—Carnegie Mellon University's School of Computer Science and SRI International. Carnegie Mellon University's effort under PAL is called Reflective Agents with Distributed Adaptive Reasoning (RADAR). The system will help busy managers to cope with time-consuming tasks such as organizing their E-mail, planning meetings, allocating scarce resources such as office space, maintaining a Web site, and writing quarterly reports. Like any good assistant, RADAR must learn by interacting with its human master and by accepting explicit advice and instruction. The RADAR project draws on Carnegie Mellon's expertise in artificial intelligence, machine learning, natural-language understanding, and human-computer interaction.

SRI's project is called Cognitive Agent that Learns and Observes (CALO). The name was inspired by the

Latin word "calonis," which means "soldier's assistant." The CALO software, which will learn by working with and being advised by its users, will handle a broad range of interrelated decision-making tasks that have in the past been resistant to automation. It will have the capability to engage in and carry out routine tasks, and to assist when the unexpected happens. Researchers for both project teams will themselves use the PAL software during its development to ensure that it satisfies all fundamental information assurance requirements, including privacy, security, and trust. As described by Jan Walker [4] in a news item published by the agency in July 2003, technical progress will be assessed each year through a series of experiments and structured evaluations.

Another DARPA funded cognitive computing initiative is taking place at the Department of Energy's Sandia National Laboratories. Over the past five years a team led by Sandia cognitive psychologist Chris Forsythe, has been developing cognitive machines that accurately infer user intent, remember experiences with users, and allow users to call upon simulated experts to help them analyze situations and make decisions. Work on cognitive machines took off in 2002 with funding from DARPA to develop a real-time machine that can infer an operator's cognitive processes. This capability provides the potential for systems that augment the cognitive capacities of an operator through "Discrepancy Detection." In Discrepancy Detection, the machine uses an operator's cognitive model to monitor its own state and when there is evidence of a discrepancy between the actual state of the machine and the operator's perceptions or behavior, a discrepancy may be signaled. Early this year work began on Sandia's Next Generation Intelligent Systems Grand Challenge project.

Commercial companies are also supporting research in cognitive computing, including Intel, with its release of the Open Source Software for Machine Learning library (OpenML), described in its whitepaper "Microprocessors: Intel's Open-Source Probabilistic Networks Library (PNL)." This software is open source under a BSD license and is free for academic and commercial use. OpenML is based on "Bayesian" mathematical principles, which essentially are the idea that the probability of future events can be calculated by studying their prior frequency. Because Bayesian models are based on data collected from experience, the more data obtained the better the predictions, and if the data changes, the results correct themselves. OpenML's libraries include the Open Source Computer Vision Library (OpenCV), Audio-Visual Speech Recognition, and Probabilistic Network Library (OpenPNL).

IBM's Autonomic Computing initiative is working towards building computing systems that are self-managing, resilient, responsive, efficient, and secure. Researchers at the Georgia Institute of Technology are working with IBM-donated equipment to develop self-healing systems for corporate settings. They are exploring how systems can respond to outages and other events more quickly than they can today, according to Karsten Schwan, director of the university's Center for Experimental Research in Computer Systems. One area of the research will be to find ways, perhaps through "network-aware middleware," to have systems self-heal across network layers, from Layer 1, the physical layer, to Layer 7, the application layer, Schwan further noted. For example, TCP today slows the sending of packets at lower network layers, especially when they include rich multimedia content. Schwan observed: "But this may not be in the interest of the servers running atop TCP. With appropriate middleware, the application server could decide to take steps to affect the transmission, such as compressing the multimedia content more or marshaling more CPU resources, or maybe even sending a thumbnail of an image instead of the full picture."

DARPA is evaluating proposals to support research and testing for its Self-Regenerative Systems program. As reported by Matt Hamblen [5], DARPA's solicitation for bids stated that "Network-centric warfare demands robust systems that can respond auto-

...The goal of this Grand Challenge is to significantly improve the human capability to understand and solve national security problems, given the exponential growth of information and very complex environment. We are integrating extraordinary perceptive techniques with cognitive systems to augment the capacity of analysts, engineers, war fighters, critical decision makers, scientists, and others in crucial jobs to detect and interpret meaningful patterns based on large volumes of data derived from diverse sources.

Larry Ellis, Sandia's Principal Investigator
Excerpt from the August 2003 Press Release
"Sandia Team Develops Cognitive Machine"
Written by Chris Burroughs, Sandia

matically and dynamically to both accidental and deliberate faults."

Cognitive computing and machine learning could be the driving force behind the next computing revolution. This will require a radical shift in the way information technology professionals conceive and develop computing systems today, thus launching a whole new area of study. Machine learning is a sea of change in the development of applications, as it allows computers to be more proactive and predictive. Many products currently exist that are using machine learning and cognitive computing including anti-spam technology and intrusion prevention systems. In February 2004 Technology Review magazine listed machine learning as one of the "10 Emerging Technologies that Will Change Your World" [6]

Maybe HAL isn't that far from becoming a reality. ■

About the Author

Angela Orebaugh

Angela Orebaugh (CISSP, GCIA, GCFW, GCIH, GSEC, CCNA) has worked in information technology for 10 years. Her focus is on perimeter defense, secure architecture design, vulnerability assessments, penetration testing, and intrusion detection. Angela is the author of the recently published Syngress best seller, *Ethereal Packet Sniffing*.

References

1. As noted by Ron Brachman in "A DARPA Information Processing Technology Renaissance: Developing Cognitive Systems."
2. An application cited by Rob Schapire of Princeton University in his February 2003 class COS 511: Foundations of Machine Learning.
3. "Machine Learning for Cognitive Networks: Technology Assessment and Research Challenges" (May 2003).
4. DARPA awards contracts for pioneering R&D in cognitive systems.
5. "System Cure Thyself: Self-healing software and hardware are on the way" in the January 2004 issue of Computer World.
6. Daphne Koller in the February 2004 issue of Technology Review.

Related Resources

Alberta Ingenuity Centre for Machine Learning. http://www.aicml.cs.ualberta.ca/Projects/fundamental.htm

Brachman, Ron: A DARPA Information Processing Technology Renaissance: Developing Cognitive Systems. http://www.darpa.mil/ipto/briefings/IPTO-Overview.pdf

Burroughs, Chris, Sandia National Laboratory: "Sandia team develops cognitive machines" (August 2003 press release). http://www.sandia.gov/news-center/news-releases/2003/comp-soft-math/cognitive.html

Caterinicchia, Dan: DARPA Releases Strategic Plan (Federal Computer Week, Feb. 2003). http://www.fcw.com/fcw/articles/2003/0210/web-darpa-02-10-03.asp

DARPA IPTO. http://www.darpa.mil/ipto/

Dietterich, Tom and Pat Langley: Machine Learning for Cognitive Networks: Technology Assessment and Research Challenges (May 2003). http://web.engr.oregonstate.edu/~tgd/kp/dl-report.pdf

Hamblen, Matt: "System Cure Thyself: Self-healing software and hardware are on the way" (Computer World, January 2004). http://www.computerworld.com/softwaretopics/software/story/0,10801,88872,00.html

Koller, Daphne: "10 Emerging Technologies that Will Change Your World" (Technology Review, February 2004). http://www.technologyreview.com/articles/emerging0204.asp?p=5

Microprocessors: Intel's Open-Source Probabilistic Networks Library (PNL). http://www.intel.com/research/mrl/pnl

Schapire, Rob: COS 511: Foundations of Machine Learning (Feb. 2003). http://www.cs.princeton.edu/courses/archive/spring03/cs511/scribe_notes/0204.pdf

Tether, Tony: DARPA News Items, April 2002. http://www.darpa.mil/body/NewsItems/pdf/DARPAtestim.pdf

Walker, Jan: "DARPA awards contracts for pioneering R&D in cognitive systems" (DARPA News Items, July 2003). http://www.darpa.mil/body/NewsItems/pdf/pal.pdf

continued from page 17…

"Attack-Graph Simulation

4. NIST, "Guideline for Identifying an Information System as a National Security System" http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf; "Security Considerations in the Information System Development Life Cycle" http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf.
5. Moitra, S. D. and Konda, S.L., "A Simulation Model for Managing Survivability of Networked.
6. "Information Systems" Technical Report, CMU/SEI–2000–TR–020 ESC–TR–2000, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 2000.
7. Phillips, C. and Swiler, L. "A graph-based system for network-vulnerability analysis." Proceedings of the 1998 workshop on New security paradigms, p. 71–79, September 22–26, 1998, Charlottesville, VA.
8. Swiler, L., C. Phillips, D. Ellis, and S. Chakerian. Computer-attack graph generation tool. In Proceedings DISCEX '01: DARPA Information Survivability Conference & Exposition II, pgs. 307–321, June 2001.
9. Sheyner, O., J. Haines, S. Jha, R. Lippmann, and J. Wing. Automated generation and analysis of attack graphs. In proceedings of the 2002 IEEE Symposium on Security and Privacy, Oakland, CA, May 2002.
10. Ammann, P., Wijesekera, D., Kaushik, S. "Scalable Graph-based Network Vulnerability Analysis" Proceedings of the 9th ACM Conference on Computers and Communications Security, Washington, DC, 2002.
11. Jha, S., Sheyner, O., and Wing, J. M., "Minimization and Reliability of Attack Graphs" Technical Report, CMU–CS–02–109, Carnegie Mellon University, Pittsburgh, PA, 2002.
12. Skybox View User Manual, Version 1.1, Skybox Security, Inc. Menlo Park, CA, Oct. 2003.
13. Welch, D., Conti, G., Marin, J., "A Framework for Information Warfare Simulation" Proceedings of IEEE Workshop on Information Assurance and Security, West Point, NY, June 2002.

continued from page 19…

Next-generation enterprise architecture

From an IA perspective, the NGEA framework provides a secure and trusted Web-based collaboration, content delivery, and application-hosting environment with systems, applications, and services benefiting from a centralized authentication and authorization service provider. The availability of authoritative user information to an intelligent digital-identity manager could also alleviate the requirements for each resource owner to manually manage application-specific access control lists (ACLs), user accounts, and INFOCON requests.

It is imperative that IA play a central role in enterprise Web-service development, especially in light of the high risk of data-aggregation from multiple Web services—for example, users could develop Web services that aggregate too much unclassified information thereby making it classified.

PKI and biometrics can minimize or prevent the exploitation by unauthorized users of systems residing within the NGEA. Therefore, applications hosted by the framework should eliminate backdoors into their applications.

The dangers of orphan accounts can be minimized once an application or service is placed within the framework, since the management of user accounts and the authentication and authorization component is centralized.

Information regarding the internal architecture and the Web services that are exposed should be minimized, preferably out of the general public's view, since malicious hackers and foreign intelligence services could exploit such open-source intelligence for unlawful activities. Web services provide easy access to information, but imagine, for example, the damage that could be caused by exposing Federal Government Supervisory Control and Data Acquisition (SCADA) type information to anyone with access to the Web service. IA managers and senior leadership should develop policies to address enterprise Web services within any enterprise architecture, including NGEA.

The NGEA is based on the use of enterprise portals, a PKI, biometrics, RBAC, SSO, and intelligent identity-management-leveraging Web services to provide a secured, trusted, and ubiquitous enterprise environment for users within the DoD community. By combining the NGEA with effective IA policies and oversight, the risks of exploitation can be minimized. This architecture is just one of the many approaches to effectively designing enterprise applications and services, but it's certainly not the only one. ■

About the Author

Wilfredo Alvarez

Wilfredo Alvarez is an Associate with Booz Allen Hamilton, a U.S. Army Reserve Intelligence Officer, and a Ph.D. CIS Candidate (with a concentration in Applied Artificial Intelligence for InfoSec and CyberWarefare) at Nova Southeastern University, Florida. He currently supports Federal, and Allied Military organizations with IA, InfoSec, and Technology Transition Strategies and Services. He can be reached at alvarez_wilfredo@bah.com or 703/377-0433.

References

1. "Task Force Web," Retrieved from the Web, January 10, 2004. http://www2.clf.navy.mil/tfw/tfw.nsf
2. "Secure Enterprise Access Transition Portal (SEAT)," COMPACFLT, Retrieved from the Web, January 10, 2004. https://seat1.cpf.navy.mil
3. "Army Knowledge Online," Retrieved from the Web, January 10, 2004. http://www.us.army.mil
4. "Navy Knowledge Online," Retrieved from the Web, January 10, 2004. http://www.nko.navy.mil
5. "Information Assurance Support Environment: Public Key Infrastructure," Retrieved from the Web, January 9, 2004. http://iase.disa.mil/pki/index.html
6. Weilminster, R., "Navy PKI Implementation Update," CAC PMR, 2003, Retrieved from the Web, January 8, 2004. http://www.don-ebusiness.navsup.navy.mil/pls/portal30/docs/FOLDER/SMART_CARD_CAC/SMART_CARD_HOMEPAGE_FOLDERS/COPY_OF_SC_PMR/PMR_03/TOPIC+5A+-+PKI+POLICY+AND+IMPLE.+UPDATE+-+CAC+AFLOAT+UPDATE.PPT
7. Buda, G. & M. King, "Biometrics: Fingerprint Identification System," Critical Review & Technology Assessment Report, Information Assurance Technology Analysis Center (IATAC), Falls Church, VA, 1999.
8. Department of Defense Biometrics Office. Retrieved from the Web, January 11, 2004. http://www.dod.mil/nii/biometrics/
9. Alvarez, W., "Role-Based Access Control Overview Brief," 2003, Retrieved from the Web January 13, 2004. http://csrc.nist.gov/rbac/alvarez.ppt
10. Hutchinson, A., "Navy Enterprise Single Sign-On (NESSO)," 2003, Retrieved from the Web, January 10, 2004. https://www.metnet.navy.mil/~hutchina/nesso/
11. W. Alvarez, R. Fernandez, R. Kanno, J. Hironaga, T. Huynh, W. Fukumae, & D. Torres, "Secure Enterprise Access Control - Role Based Access Control Prototype," COMPACFLT, Pearl Harbor, HI, 2004.
12. "Department of Defense Business Management Modernization Program," Retrieved from the Web, January 12, 2004. http://www.defenselink.mil/comptroller/bmmp/pages/overview.html
13. "Role Based Access Control," American National Standard for Information Technology, 2003, Retrieved from the Web, January 13, 2004. http://csrc.nist.gov/rbac/rbac-std-ncits.pdf
14. Hutchinson, A., "Navy Enterprise Single Sign-On (NESSO)," 2003, Retrieved from the Web, January 10, 2004. https://www.metnet.navy.mil/~hutchina/nesso/
15. "OASIS," 2004, Retrieved from the Web, January 13, 2004. http://www.oasis-open.org/home/index.php
16. "National Infrastructure Protection Highlight", 2004, Retrieved from the Web, http://www.nipc.gov/publications/highlights/2002/highlight02-03.pdf

by Dennis Fringeli

Acting on behalf of the Secretary of the Army, Executive Agent for the Department of Defense (DoD) biometrics, LTG Steven W. Boutelle, the Army Chief Information Officer (CIO–G/6) appointed John D. Woodward, Jr. to succeed Dr. Linda S. Dean as Director of the DoD Biometrics Management Office (BMO) upon her recent retirement. In addition, Samuel J. Cava has been appointed Director of the Biometrics Fusion Center (BFC), which is the West Virginia-based technical and operational support center for the BMO.

Since its inception in 2000, the BMO has been promoting the development, adoption, and use of biometric technologies across DoD. Deputy Secretary of Defense Paul Wolfowitz underscored the BMO mission stating in his 25 Aug 03 Department of Defense Biometrics Enterprise Vision memorandum—

> *By 2010, biometrics will be used to an optimal extent in both classified and unclassified environments to improve security for logical and physical access control.*

Woodward comes to DoD from the RAND Corporation, a public policy research organization. His broad experience working on policy issues for the national security and intelligence communities will help propel current and future efforts of DoD biometrics in ways that will ensure interoperability and standardization. To accomplish this goal, he is expected to establish stronger ties with other DoD organizations and Federal Agencies. Woodward has testified about biometrics before Congress, the Commission on Online Child Protection, and the Virginia State Crime Commission. He is the primary author of "Biometrics: Identity Assurance in the Information Age" (McGraw-Hill, 2003). He also served as an Operations Officer for the Central Intelligence Agency (CIA) for 12 years.

Cava is responsible for enhancing the BFC's technical capabilities, particularly with respect to testing and evaluation of biometric technologies. He comes to the BFC from West Virginia University, where he was the Director of Forensic and Biometric Development. Cava previously served on active duty with the U.S. Air Force, working in several high-level intelligence-related assignments.

Cava fills a senior-level civil service position, as part of the DoD plan to continue migrating core Biometrics Office functions to the BFC. Woodward comes to the BMO via the Intergovernmental Personnel Act Mobility Program (5 USC Section 3371–3375), which permits movement of personnel between qualified organizations.

Current DoD Biometrics Management Office initiatives

The BMO leads, consolidates, and coordinates the development, adoption, and use of biometric technologies for Combatant Commands, Services, and Agencies to support the warfighter and enhance Joint interoperability. Current BMO priorities include biometric standards development, particularly as related to biometric collection, data storage, and system interoperability. Other initiatives include upgrading legacy identification systems and supporting the use of biometrics on the Common Access Card. Interagency cooperation is crucial to leveraging the multiple U.S. Government biometric initiatives currently underway. To that end, the BMO and BFC are supporting the work of the National Science Technology Council Biometrics Research and Development Interagency Working Group, which includes membership from the Department of Homeland Security, Department of Justice, National Science Foundation, National Institute of Standards and Technology, and other U.S. Government biometric stakeholders.

The BMO is continuing its educational partnership with West Virginia University. The programs currently in place are designed to equip government and IT personnel with the knowledge necessary to succeed in the biometrics and information assurance fields.

More information about the DoD BMO and BFC can be found at http://www.dod.mil/nii/biometrics. ■

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 ❑ Intrusion Detection ❑ Vulnerability Analysis

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 (soft copy only) ❑ 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	❑ No. 2	❑ No. 3	❑ No. 4

Softcopy *IAnewsletters* back issues are available for download at http://iac.dtic.mil/iatac/IA_newsletter.html

Fax completed form to IATAC at 703/289-5467

May

DoDIIS Worldwide 2004
May 3–6, 2004
Hyatt Regency, San Francisco, CA
http://www.federalevents.com/dodiis/

IAD Industry Days "Net-Centric Operations: Conquering the Dynamic Information Assurance Challenges"
May 11–13, 2004
Baltimore North Hotel, Baltimore, MD
https://www.iaevents.com/ID04/newinfo.cfm

AusCERT Asia Pacific Information Technology Security Conference
May 23–27, 2004
Royal Pines Resort, Gold Coast, Australia
http://conference.auscert.org.au/conf2004/

Heartland TechNet 2004
May 25–27, 2004
Offutt AFB Club, Omaha, Nebraska.
http://www.afcea-omaha.org/

Federal Information Security Conference (FISC) 2004
May 16–17, 2004
Antler`s Hotel, Colorado Springs, CO
http://www.fbcinc.com/event.asp?eventid=Q6UJ9A0078BN

Technet International 2004
May 11–13, 2004
Washington DC Convention Center
http://www.technet2004.org/default.htm

2004 Pacific Command Information Assurance (IA) Conference "Operationalizing Information Assurance."
May 25–28, 2004
Honolulu, HI
http://www.iaevents.com

June

10th Annual Gartner IT Security Summit
June 7–9, 2004
Marriott Wardman Park Hotel, Washington DC
http://www3.gartner.com/2_events/conferences/sec10.jsp

National OPSEC Conference and Exhibition
June 7–11, 2004
Baltimore Marriott Waterfront Hotel, Baltimore, MD
http://www.iaevents.com

Army IT Conference
June 8–10, 2004
Hershey Lodge & Convention Center, PA
https://ascp.monmouth.army.mil/scp/aitc/generalinfo.jsp

Annual IEEE IA Workshop
June 10–11, 2004
U.S. Military Academy, West Point, NY
http://www.itoc.usma.edu/workshop/2004/index.html

TechNet 2004
June 11–13, 2004
Washington DC Convention Center
http://www.technet2004.org/generalinfo_faq.htm

NetSec 2004
June 14–16, 2004
Hyatt Regency Embarcadero, San Francisco, CA
http://www.gocsi.com/events/netsec.jhtml

3rd Annual Government Symposium on Information Sharing & Homeland Security
June 28–30, 2004
Royal Pacific Resort at Universal Studios, Orlando, FL
http://federalevents.com/ishs/September

September

Gartner IT Security Summit 2004
September 20–24, 2004
Landmark Hotel, London
gg@delegate.com

Attend InfowarCon 2003
September 30–October 3, 2004
Renaissance Washington DC Hotel, Washington, DC
http://www.infowarcon.com/app/homepage.cfm?appname=100206&moduleid=451&campaignid=338&iUserCampaignID=718381

(There are no events for July-August)

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