IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 3 Number 3

WARFIGHTER Support in a Coalition Environment

JFCOM's Coalition Interoperability Solution

EUCOM's Information Assurance Conference

also inside

on the cover

ia initiatives

in each issue

IAnewsletter

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

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

Robert P. Thompson
Director, IATAC
703.289.5454

We welcome your input! To submit your related articles, photos, notices, feature programs or ideas for future issues, please contact:

IATAC
ATTN: Christina P. McNemar
3190 Fairview Park Drive
Falls Church, VA 22042
Phone 703.289.5454
Fax 703.289.5467
STU-III 703.289.5462

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

Cover and newsletter designed by Christina P. McNemar

THE HEXAGON

A U.S. Joint Forces Command Solution to Coalition Interoperability

"Successful completion of the CMHP project will require careful transition from risk avoidance to risk management in the way classified information is managed and safeguarded."

Admiral Harold Geham
Commander in Chief,
United States Joint Forces Command

Mr. Craig Vroom
Mr. Allan H. McClure

Support to coalition operations in the future is an information assurance challenge today. Since 1994, little has changed in the methods and mechanisms we use to provide information to our allied partners. As each coalition operation (Haiti, Somalia, Bosnia, Kosovo) comes and goes, the lessons learned statements always cry for improved interoperability within the coalition. The requirements are well documented throughout the Department of Defense (DoD). Even Joint Vision 2010, the DoD road map for the future, states, "It is not enough to be joint when conducting future operations. We must find the most effective methods for integrating and improving interoperability with allied and coalition partners." True interoperability with our allied partners will come only after we have an information exchange system designed from the ground up for use by coalition forces.

Colonel Dennis Treece's article in the Spring 1999 *IAnewsletter* was right on target in describing the shortcomings and challenges of releasing and disseminating classified military information to our multinational partners in a coalition environment. As Colonel Treece says, the "really hard part, the 'Achilles heel' of coalition information sharing, is the mechanism by which any nation transfers information outside its own system." Because of valid security policy restrictions, we are not allowed to connect our Defense networks to multinational networks, thus creating the need for "sneaker nets"—literally, running the releasable information from the U.S. side, across an air gap, to the multinational side. Anyone who has experienced the pain of this method knows its difficulties and limitations. (In 1994, those of us in U.S. Atlantic Command had our turn when we provided information support to the 29 countries involved in Haiti peace operations.)

U.S. Joint Forces Command (USJFCOM, formerly, U.S. Atlantic Command) is responsible within DoD for joint task force (JTF) interoperability. At Joint Forces Command, we have embarked on building a system for secure information exchange. It is called the Coalition Multilevel Security (MLS) Hexagon Prototype or CMHP. The CMHP is composed of six functions that will allow us to exchange information with our allies in a secure, flexible manner.

Side 1 of the Hexagon (Figure 1 on page 4), Marking Standards, uses the classification and control marking standards adopted by the U.S. intelligence community. These standards were coordinated by the Controlled Access Program Coordinating Office (CAPCO) and continue to be fine-tuned by CAPCO as required.

Side 2 of the Hexagon is called Document Marking, which is designed to implement human-readable markings. Basically, this software

continued on page 4

continued from page 3

enables the information originator to mark Microsoft Word, PowerPoint, and Excel documents in accordance with the CAPCO and Executive Order 12958 standards. The marking is a simple operation, done with the point and click of a mouse and made still easier by pull-down menus that provide choices for basic classification, caveats, and "release to" options for countries, coalitions, operations, organizations, and exercises. Once the document is marked, it is then transformed into a "computer-readable" label, side 3 of the Hexagon. A digital signature attaches the label to the document, which is then encrypted and sent to the "Coalition Server," an Oracle 8 relational database management system.

Figure 1. Coalition MLS Hexagon Prototype

Hexagon's side 4, Personal Authentication, is the linchpin of CMHP. A personal token called a Hexcard allows us to identify the user and all of his or her security attributes. Much as an automated teller machine (ATM) card does, the Hexcard will store a user's fingerprint template and a credential set based on his or her clearance levels, citizenship, and need-to-know roles. Hexcards will be inserted into workstation smart-card readers to identify the user to the system.

Side 5 of the Hexagon is the hardware, including NT workstations, fingerprint scanners, and smart-card readers, required for the CMHP.

Hexagon's side 6 is Security Management. A special staff security officer must be assigned to coordinate system security requirements, issue Hexcards to CMHP participants, understand the information assurance requirements, and monitor the system for improper attempts to access data.

The Hexagon concept provides the flexibility required in coalition-supported joint task force operations by encrypting and protecting the object, rather than the network. This is the key difference between CMHP and other multilevel security (MLS) solutions. Using object protection, we can compare the attributes of an individual with the objects that reside in the server. If there is a match, the coalition participant can retrieve and decrypt the document.

The CMHP will be tested and demonstrated at the Joint Battle Center (JBC) in Suffolk, Virginia, in May 2000. The objective of the demonstration will be to bring existing technologies together to allow users with different clearance levels from different countries to use the same local area network and gain access only to information they are authorized to see. After the concept is demonstrated, the Joint Battle Center will provide an independent assessment of the system's military utility.

The ultimate goal of the Hexagon is to provide the joint task force commander a tool that increases the effectiveness of communications with allied or interagency forces.

Figure 2. CMHP HexCard

Mr. Craig Vroom is the International Programs Branch Chief at U.S. Joint Forces Command, located in Norfolk, Virginia. He has an undergraduate degree in Computer Science from San Diego State University and is currently participating in DoD's Defense Leadership and Management Program (DLAMP). You may reach him via E-mail at vroom@jfic.jfcom.mil.

Mr. Allan McClure is a Lead Engineer supporting the US Joint Forces Command Director for Intelligence. During the last seven years, he has helped in the implementation of Intelink and developed a collaborative architecture for the Non-Proliferation Center, a Director for Central Intelligence (DCI) controlled activity. He may be reached at amcclure @mitre.org.

USEUCOM
U.S. European Command

Information Assurance Conference

Brigadier General Charles E. Croom, director, United States European Command (USEUCOM)/J6, hosted USEUCOM's first Information Assurance Conference, 30 November–2 December 1999, at the Abrams Center in Garmisch-Partenkirchen, Germany. The conference had three purposes:

- To present pressing information assurance (IA) issues and review associated IA products
- To foster teamwork and synergy among key IA players in the theater
- To provide the latest IA informational updates for theater IA personnel.

Framework

The conference attracted a total of 162 people, representing Headquarters (HQ) USEUCOM, U.S. Army Europe (USAREUR), U.S. Air Forces Europe (USAFE), US Naval Forces Europe (USNAVEUR), Marine Forces Europe (MARFOREUR), Special Operations Command Europe (SOCEUR), the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and other commands, such as U.S. Special Operations Command (USSOCOM), U.S. Pacific Command (USPACOM), and U.S. Central Command (USCENTCOM), as well as several other DoD agencies involved in USEUCOM IA.

Brigadier General Charles E. Croom.

By design, all levels of IA professionals, from enlisted to general officer grades, participated in the sessions. This arrangement ensured expression of various viewpoints at the forum and enabled individuals with hands-on working experience to interact directly with policy makers at the highest levels.

Each morning's general session started with a senior-level keynote address. The speakers were Brigadier General Gary Salisbury, DISA/D6; Mr. Richard Schaeffer, Office of the Secretary of Defense (OSD), Command, Control, Communications, and Intelligence (C3I); and Mr. Orville Lewis, NSA/DDI Chief of Staff. All addresses were followed by extended question-and-answer sessions that immediately indicated a very high level of interest in the rapidly developing IA field.

Mr. Kent Waller

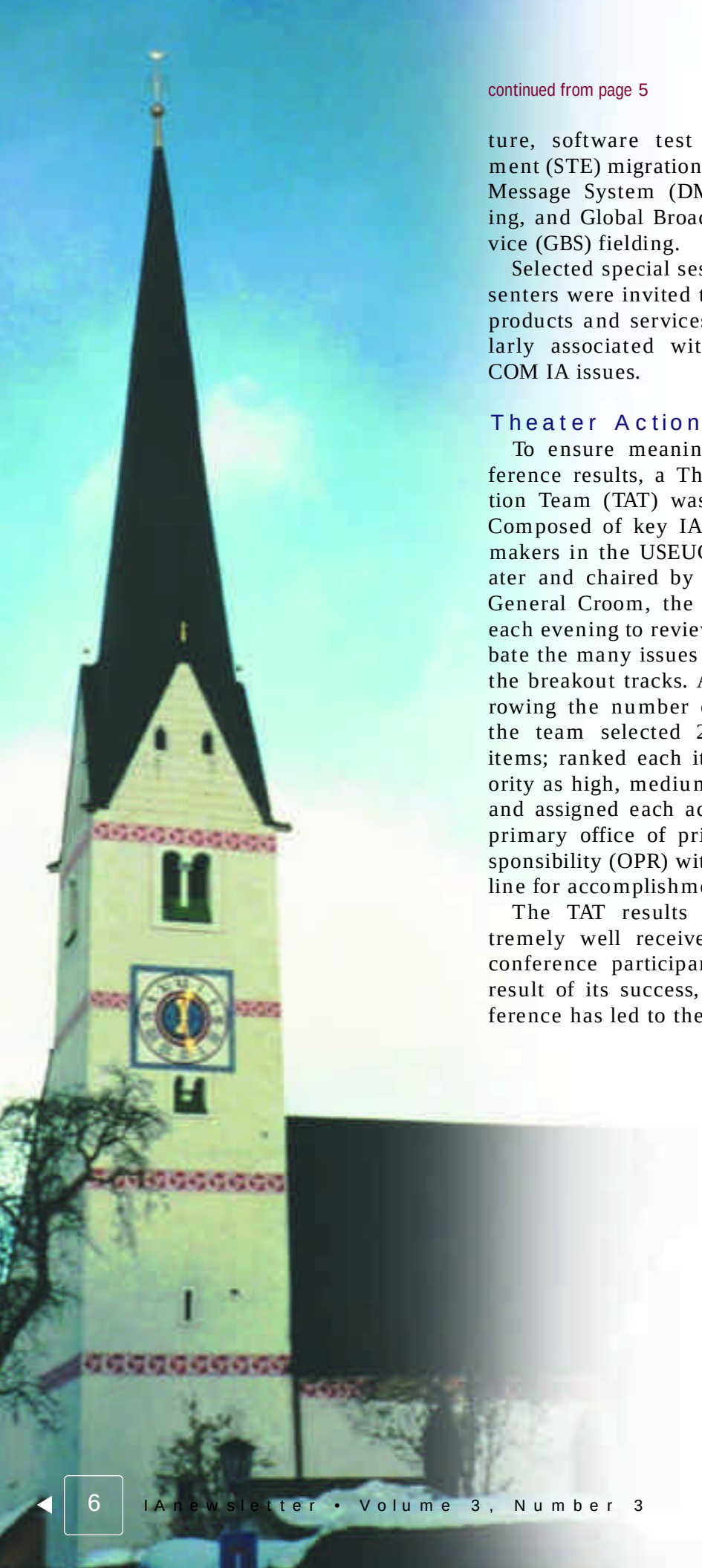
Immediately following the keynote addresses were general session presentations from theater-specific IA leaders. A total of six speakers (two per day) from USNAVEUR, HQ USEUCOM, USAREUR, USAFE, and the North Atlantic Treaty Organization (NATO) presented issues and fielded questions.

The afternoons were divided into three in-depth breakout tracks in the areas of operations, computer security (COMPUSEC), and communications security (COMSEC). These sessions were smaller in number of participants, more technical, and more discussion oriented than the general sessions.

Operations discussions focused primarily on lessons learned from Kosovo operations and plans for future support. COMPUSEC participants dealt with information assurance vulnerability alerts (IAVA) issues and discussed the technical details of dealing with theater-specific threats.

The COMSEC sessions, which were often filled to capacity, explored the areas of key management infrastruc-

continued on page 6



continued from page 5

ture, software test environment (STE) migration, Defense Message System (DMS) fielding, and Global Broadcast Service (GBS) fielding.

Selected special session presenters were invited to display products and services particularly associated with USEUCOM IA issues.

Theater Action Team

To ensure meaningful conference results, a Theater Action Team (TAT) was formed. Composed of key IA decision makers in the USEUCOM theater and chaired by Brigadier General Croom, the TAT met each evening to review and debate the many issues raised by the breakout tracks. After narrowing the number of issues, the team selected 20 action items; ranked each item's priority as high, medium, or low; and assigned each action to a primary office of primary responsibility (OPR) with a deadline for accomplishment.

The TAT results were extremely well received by all conference participants. As a result of its success, the conference has led to the development of a new European Information Assurance Steering Council composed of senior IA leaders and aimed at providing continuing, unified guidance to theater IA personnel.

Additional Information

All conference materials, including the TAT action items, attendee lists, and briefings are available for download from the HQ USEUCOM SIPRNET Web site.

The office with primary responsibility for the conference was the HQ USEUCOM C3I Directorate's Defensive Information Warfare Division directed by Col LaForrest Williams, U.S. Air Force (USAF). On behalf of Brigadier General Croom, this group extends appreciation to all the speakers who made the conference a success.

Mr. Kent Waller is an Information Assurance Program Manager for HQ United States European Command. He earned his B.S. in Engineering from the University of Oklahoma in 1986 and his Master of Public Administration from the University of Oklahoma in 1990. He may be reached at wallerkl@eucom.mil.

JTF-CND
Intelligence Support

CDR Robert D. Gourley, USN

The Joint Task Force for Computer Network Defense (JTF-CND) is a new organization with a new mission: to direct the defense of all Department of Defense (DoD) computers and networks and the information that moves in them from any threat, foreign or domestic. Our intelligence (J2) role on this team resembles any other JTF-level intelligence effort. That mission is to provide the commander, the JTF-CND staff, and assigned components with all-source, fused, predictive intelligence on enemy locations, capabilities, and intentions. The JTF-CND J2 must understand the enemy in cyberspace, and must provide decision-makers with the actionable intelligence required to support defensive operations.

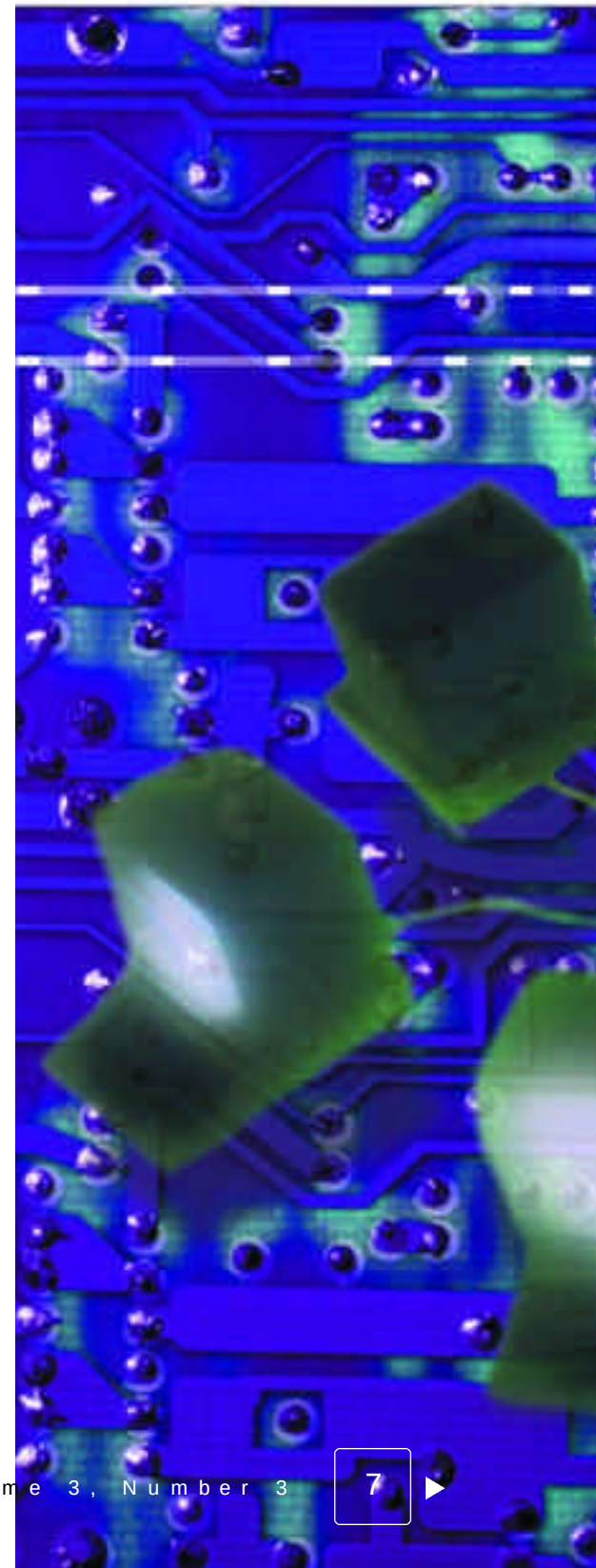
That task is easier said than done. Those who choose to attack or exploit our information systems operate with great anonymity in globally interconnected networks. Additionally, our adversaries are armed with software tools that strike at the speed of light, and use tactics that are hard to detect in the noise of the net.

Finding the enemy in cyberspace is also complicated by the nature of this new terrain. There are few useful charts by which to orient us and little agreement on what the concept of "cyberspace" means. Perhaps the most useful definition remains William Gibson's original explanation of the term: Cyberspace is "a consensual hallucination experienced daily by billions... [an] unthinkable complexity." Try visualizing enemy locations in that!

The adversary may be a terrorist attempting to attack Department of Defense (DoD) networks to draw attention to a cause or to slow our response to an act of physical terror. Threats also come from espionage agents seeking to acquire sensitive but unclassified information for use by a foreign state or criminal organization. We may soon face nation state adversaries in cyberspace who seek military advantage, possibly by attacking our combat support infrastructure or, in perhaps the most insidious attack, by attempting to manipulate the perceptions of senior DoD decision makers.

Although the computer network defense intelligence problem is complex and relatively new, developing JTF-CND intelligence tactics, techniques, and procedures (TTP) has been simple and straightforward. We have based most of our TTPs on the existing playbook for JTF intelligence support, the Joint Staff's Joint Doctrine for Intelligence Support to Operations (Joint Pub 2-0). Using intelligence doctrine as the bedrock for JTF-CND intelligence TTPs have already paid off. Following doctrine has increased the intelligence community focus on and support of the CND mission.

continued on page 8



continued from page 7

Joint Pub 2-0 also directly assisted in planning for the U.S. Space Command (SPACECOM) assumption of the DoD CND mission, which occurred 1 October 1999. Intelligence staffs at and JTF-CND quickly realized the importance of adhering to joint doctrine wherever possible. Using joint doctrine allowed us to clarify important aspects of the new relationship, including the most efficient means of handling intelligence collection and production requirements and appropriate division of labor between CINC and JTF intelligence personnel.

The central principle: Know the adversary. Perhaps Joint Pub 2-0's most critical contribution is a clear articulation of the general functions that must be conducted by a JTF J2. It also provides guidance on how these functions should be carried out. The following points show JTF-CND J2 application of these principles.

The fundamental responsibility of the JTF-CND J2 is to provide JTF-CND decision makers with the fullest possible understanding of the cyber threat. This understanding must include knowledge of the adversary's goals, objectives, strategy, intentions, capabilities, methods of operation, vulnerabilities, and sense of value and loss. To provide this understanding, the JTF-CND J2 and intelligence staff must develop and continuously refine an ability to think like the cyber threat.

Intelligence support is critical to operational success. JTF J2 staff must understand the adversary in order to support operations. Intelligence must be made actionable by tailoring it into a useful form and then getting it into the hands of the commander, the operations division (J3), and other JTF decision makers. Operations support also requires J2 assessment of J3 intentions from the adversary's perspective to determine probable adversary responses.

Intelligence support requires the integration of intelligence efforts at strategic, operational, and tactical levels. Strategic intelligence is used to formulate defensive strategies and operations at national and theater levels, making both SPACECOM and JTF-CND key consumers of intelligence produced on the cyber threat to our Nation. Operational intelligence is used by SPACECOM and JTF-CND to determine defensive objectives and to support the planning and conduct of CND operations. Tactical intelligence required for CND is a new discipline that is still in an initial stage. When fully developed, tactical intelligence procedures and processes will support rapid reaction to tactical threats by JTF-CND components.

Strategic, operational, and tactical intelligence must be employed in a way that reduces our chances of being deceived or surprised. Deception and surprise are inherent factors in cyberspace, however, and will probably always be concerns.

Intelligence sources are the means or systems used to observe, sense and record, or convey information. JTF-CND J2 staff must understand the strengths and weaknesses of all intelligence sources relevant to this mission area. The seven primary intelligence sources are imagery intelligence, human intelligence, signals intelligence, measurement and signature intelligence, open source intelligence, technical intelligence, and counterintelligence. Unity of effort is maintained by tasking these disciplines in accordance with joint doctrine. All results are fused to provide the best possible assessments. Integration also helps reduce deception and surprise.

Intelligence supports all aspects of JTF-CND operations. JTF-CND J2 will participate in planning from the outset of any operation. Early involvement in JTF-CND planning will allow the J2 to articulate intelligence collection and production requirements to the intelligence community and to formulate, at an early stage, intelligence guidance for JTF-CND components. It will also allow the J2 to provide intelligence at every stage of the decision-making process.

Providing understanding of the enemy to support counterintelligence and operational security measures. Concurrent with JTF-CND planning and operating process, the J2 will provide the commander with an understanding of the adversary's command and control processes and adversary intelligence collection capabilities, so appropriate operational security

and counterintelligence operations can be implemented.

Evaluating the effects of defensive operations. The JTF-CND J2 will assist the JTF commander and J3 in evaluating operational results and determining when objectives have been attained, so forces may be reoriented or operations terminated. Some defensive measures that may have to be taken on DoD networks to thwart a sophisticated adversary could affect millions of DoD computer users, making intelligence support for exit strategies of paramount importance.

Intelligence systems will be interoperable, usable, scalable, reliable, and user-friendly. Joint Pub 2-0 provides overarching guidance on establishment of a joint intelligence architecture for support to a JTF. Much of this architecture already exists in the military intelligence community infrastructure. CND intelligence architecture is based on the Joint Worldwide Intelligence Communications System (JWICS) and the Joint Deployable Intelligence Support System (JDISS). By tailoring JWICS and JDISS to the JTF-CND mission, JTF-CND joins a network linking the entire intelligence community.

New threat databases are being established to support this mission, and many new intelligence fusion, collaboration, and visualization tools are being developed to support CND intelligence analysts. As they are developed, strict adherence to joint doctrine and joint standards (where they exist) will help ensure interoperability and proper mission focus.

Intelligence TTPs must be understood by all players. A key reason for having joint doctrine is to know how the rest of the team will play. Intelligence TTPs spell these plays out in detail, describing agreed-upon ways that organizations interact. For example, JTF-CND components will follow joint doctrine in stating intelligence collection and production requirements to JTF-CND for further validation, prioritization, and tasking. When operations require, JTF-CND will issue statements of intelligence intentions to components, clarifying additional support procedures tailored to the particular mission. Component commanders will also provide feedback to the JTF on Service-related issues affecting the joint command, and will plan and develop implementing instructions for wartime intelligence support, including augmentation of joint forces.

Many aspects of this new mission area have yet to be covered by joint doctrine. That is to be expected in any modern military operation. But by starting with a foundation in joint doctrine, areas that have yet to be resolved are being discovered quickly and dialog is already underway to address them.

A Final Note

Operational units in the field or fleet who have a need for intelligence on cyberthreats can also rely on joint doctrine for intelligence. It is the basis for J2 procedures in every CINC area of responsibility, and is worth a good read by all uniformed professionals.

Commander Gourley is the Director of Intelligence, Joint Task Force-Computer Network Defense (J2, JTF-CND). He received a B.S. in Chemistry from Middle Tennessee State University in 1981, an M.S. in National Security Affairs from the Naval Postgraduate School in 1985, and an M.S. in Military Science from the Marine Corps University in 1996. He may be reached at gourleyr @jtfcnd.ia.mil.

Endnotes

Gibson, William. *Neuromancer*, Berkley Publishing Group, New York, NY, July 1984.

Joint Pub 2-0 *Joint Doctrine for Intelligence Support to Operations*, Pentagon, Washington, D.C., 5 May, 1995.

Joint Pub 2-0, III-4.

Joint Pub 2-0, vii.

Joint Pub 2-0, xi.

Joint Pub 2-0, x.

MAJ Gerald Burton, USA
Mr. Richard Phares

On 13 and 14 October 1999, IATAC conducted an exercise on information operations (IO) for computer network defense (CND) for the Joint Task Force for CND (JTF-CND). This tabletop exercise, Zenith Star 99-1, was designed to look both at a CND scenario similar to that used for Eligible Receiver 97-1, and at the interagency working-level coordination necessary to react to such a scenario. Zenith Star 99-1 also exercised the JTF-CND Tactics, Techniques, and Procedures (TTPs) and assessed progress made since the JTF-CND stand-up in December 1998. Although the exercise used the Eligible Receiver 97-1 scenario as a base, it did not replay that exercise completely. Instead, it focused primarily on CND-related events to determine how new DoD organizations and processes built since Eligible Receiver 97-1 affect the CND community's response to a similar crisis.

More than 55 participants attended the exercise, including players from U.S. Space Command (SPACECOM), the National Infrastructure Protection Center (NIPC), the National Security Agency (NSA); the Defense Intelligence Agency (DIA), the Central Intelligence Agency (CIA), the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I), the Joint Staff, and JTF-CND and its component commands. Several observers from U.S. Pacific Command (PACOM), U.S. Special Operations Command (SOCOM), U.S. Joint Forces Command (JFCOM), the National Communications System (NCS), and others also attended. Facilitators included personnel from both IATAC and JTF-CND.

Zenith Star 99-1's goal was to foster understanding of the process and products required in interagency coordination and the resulting impacts on the CND community's ability to perform its mission. The exercise achieved this goal by helping participants accomplish four specific objectives:

- Understanding the roles of new CND organizations in responding to a contingency similar to Eligible Receiver 97-1 in scope and complexity
- Understanding interagency coordination requirements
- Examining processes and procedures for JTF-CND coordination with other supporting agencies (e.g., NIPC, Intel)
- Understanding needs for improvement highlighted by several communities—intelligence, law enforcement and counterintelligence, and operations.

The exercise structure included information briefings and "hot washes." Zenith Star 99-1 emphasized team play, so information briefings were kept to the bare minimum required. The exercise clock began while participants received their "situation briefing"—exercise time and real time were one and the same. Participants were divided into functional teams as follows:

- Operations team (SPACECOM, JTF-CND and its components)
- Intelligence team (CIA, DIA, NSA)
- Law enforcement/counterintelligence team (Defense Criminal Investigative Organizations, NIPC)
- Other team (Joint Staff, Office of the Secretary of Defense [OSD])

Participants within teams were allowed to communicate freely with each other. Communications among teams, however, were strictly regulated. Participants used either real communications (the secure telephone units, third generation [STU-III] available in each team room or face-to-face meetings arranged through the facilitators) or simulated communications (fax and E-mail). Additionally, the Control Cell brought participants together in a forum that allowed them to share information, and work together on their responses.

Team play was driven by "Red Force" actions: teams received injects describing specif-

continued on page 14

Distributed Denial of Service Tools

1Lt Brian Dunphy, USAF

It was a dark and stormy night...With nothing else to do, you search for "places that don't rain" using your favorite Web search engine only to get an ominous "Error 404." It is quite possible that the search engine's Web site is under attack from hundreds of systems at once, just as Yahoo's page was in mid-February for 3+ hours. Could such a coordinated attack occur in reality? Unfortunately, a single individual could, with relative ease and little chance of repercussion, stage such an attack using a new breed of tools referred to as Distributed Denial of Service (DDoS) tools.

Reality #1

The number of poorly configured systems connected to the Internet is rapidly increasing. This is partially the result of well-connected university dormitories and high-speed connections to the home, (cable-modems and DSL connections).

Reality #2

Based on the observed rate of network-wide probes and publicly available hacker tools, intruders are more interested in the number of compromised hosts rather than specific targets.

The reality is that, using publicly available tools, a determined intruder can compromise 100+ systems Internet-wide in a matter of days. Sadly, the number of vulnerable systems riding the Internet has outpaced a typical intruder's ability to do something useful with the compromised systems. Distributed intruder tools have matured in this environment and now enable an intruder to use a large number of compromised systems in a coordinated and collective manner. The first widely used example of distributed intruder tools is denial of service tools, though others are expected to follow shortly. With the current generation of tools and little effort, an intruder can flood a target with a massive amount of traffic from hosts around the world. These DDoS tools are called names such as Trin00, Tribe Flood Network (TFN) and Stacheldraht and are available on UNIX and Windows systems. It is believed that variants of these tools were used to successfully launch large-scale attacks against such popular Web sites such as Yahoo, E-bay, CNN and others. Many of the victims have been very well connected sites with over a gigabit per second of sustained bandwidth.

The current generation of DDOS tools requires an intruder to install a "daemon" on each of the compromised systems. At least one "master" system keeps track of the daemon systems and directs the attack. When prompted by an intruder the master contacts each of the daemons and specifies the tar-

continued on page 12

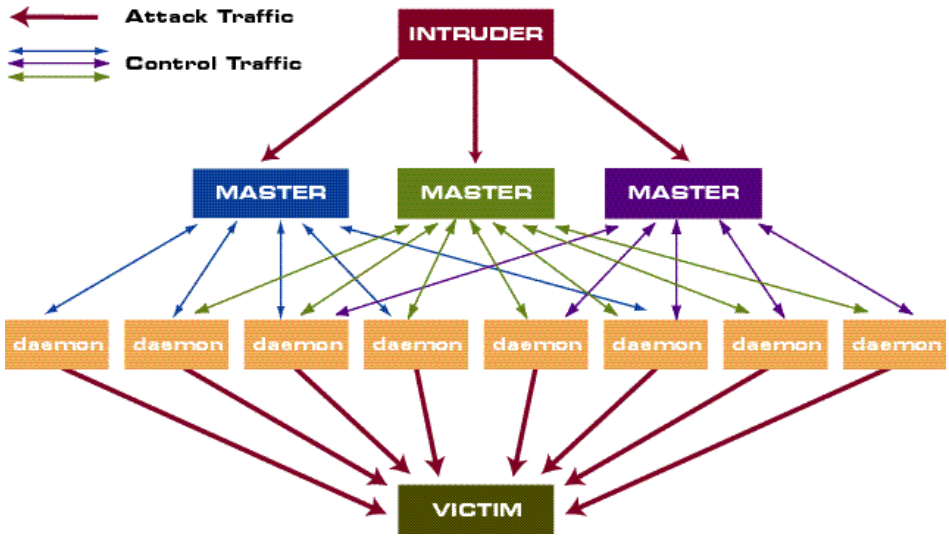


Figure 1. Example DDoS network

continued from page 11

get and method of attack. From the victim's perspective, they appear to be under attack from hundreds of systems from around the world all at once.

There are two primary computer network defense goals with relation to the recent distributed attacks:

1 Don't be a participant in an attack.

The Internet community is already struggling with the scale of these attacks. Vulnerable DoD systems can be unwitting participants in a DDoS network serving only to increase the scale and complexity.

The current set of DDoS tools are installed after a system is compromised by an intruder and does not exploit any specific vulnerability. Based on past incidents, most DoD compromises are the direct result of unpatched vulnerabilities that DoD's Information Assurance Vulnerability Alert (IAVA) Process has documented (http://www.cert.mil/iava). Sites are encouraged to routinely check their systems for IAVA compliance. Sites are also advised to do the following:

- **Periodically run DDoS scanning tools.** Sites are encouraged to use either vendor or government developed tools to detect known instances of DDoS tools.

  —The National Infrastructure Protection Center (NIPC) has produced a host based scanning tool to detect known DDoS tools. The tool only runs on Solaris and Linux at the time of this article. The tool is available on the DoD-CERT's homepage (http://www.cert.mil/resources/security_tools.htm).

  —The current DoD contracted antivirus vendors, Symantec and McAfee, have developed signatures to detect the Windows' variants of the DDoS tools.

- **Sites are encouraged to pressure their vendors** (antivirus, intrusion detection, etc) to update their detection signatures if they have not already done so.

- **Enable anti-spoofing rules at enclave perimeter.** Sites should configure their perimeter firewall and router to only allow out traffic with valid source IP addresses. Many of the tools spoof their source IP address to make the attack look like it is originating from somewhere else.

- Disable directed broadcast at enclave perimeter. Sites should configure their router and firewall to disallow network traffic destined for their broadcast address.

2 Don't be a victim of a DDoS attack.

While it has not happened to date, it is possible that DoD systems will (or could) be targeted in the future by such attacks.

From a potential victim's perspective, the best advice is to **be prepared** to be a victim. The current denial of service attacks only rely on a site's ability to receive network traffic through a finite network connection. These attacks take advantage of the large number of vulnerable systems connected to the Internet, so there is no simple "fix" for these attacks. Once a site has been targeted, there are a number of things that can be done to restore service in a timely manner. Systems owners are advised to be prepared in the following manner:

- **Identify mission-essential systems** that must be available to users from the Internet. If a denial of ser-

continued on page 34

Air Force Materiel Command's Information Defense

Cyberterrorism, Internet attacks, malicious intrusions, and hacker activity are on the rise. Credit card data for thousands of people is offered for sale over the net.

Col Kevin J. Kirsch, USAF

Air Force systems and networks are targets. Protection of our systems and data is the new challenge, and Air Force Materiel Command (AFMC) is structuring itself to meet that challenge with a dedicated effort addressing all aspects of information assurance (IA).

Efforts to attack, sabotage, and corrupt government and industrial systems and data, sometimes in "sport" and sometimes as a conspiracy, have become a widespread problem plaguing everyone from the smallest businesses to the biggest government organizations. Network defenses and vigilance have been the two most common responses, but waiting for the next hacker is an insufficient approach to network protection. In AFMC we have taken a proactive approach to protecting our systems.

In an aggressive effort beginning in late 1998, AFMC developed and deployed a team of network security and operational experts under the banner of **Operation Palisade.** The team's continuing mission is to seek out network security weaknesses before they can be exploited and to remove them through the implementation of security network practices and technologies. The effort is focused on the single goal of protecting the mission-critical information contained on AFMC networks throughout the United States and the world. The challenge is particularly daunting because AFMC's relationships with various research centers and contractors mean that our networks have a larger-than-expected number of potentially open components.

The primary foundation on which Operation Palisade builds is the full application of the Air Force's Barrier Reef process. This proven methodology is designed to create boundary protection for all AFMC base intranet networks, protect those networks at their entry points to the Internet, provide specific network security training to base network managers, and increase AFMC network monitoring and auditing as soon as security weaknesses are identified. We feel that our Operation Palisade efforts, combined with the mandated actions laid out in applicable Air Force regulations and instructions, have positioned us not only to respond to problems, but to prepare our subordinate bases and organizations to position themselves proactively for the threats that surely lie just around the corner.

Are we where we want to be or need to be in our defensive posture? The answer is clearly "no." We need to move beyond Barrier Reef and Operation Palisade. We need to address all the capabilities of the Air Force's Defensive Counter-information (DCI) Operations program, including not only information assurance, but also operations security, electronic protection, counterintelligence, and other capabilities, as spelled out in Air Force Policy Directive 10-20. In the process of moving forward, AFMC has put the IA lead in charge of the overall command DCI program and given me the responsibility to coordinate all of the efforts in the realm of Defensive Information Operations.

By consolidating IA and DCI Operations leadership, we have put ourselves on a path for continuous improvement—and created a self-initiated challenge to succeed. There is much to do. AFMC is a target-rich environment for both the

continued on page 14

Air Force Material Command

continued from page 13

recreational hacker and the industrial spy. On the other hand, our challenges are no different from those faced by industry, other Air Force Major Commands (MAJCOM), or our sister services.

We are proud to be part of the large team, working hard with the other MAJCOMs, the Services and in industry to stay one step ahead of the next incident. We feel we have a positive story to tell, but recognize that others do also. For every good idea we have, we seek multiple opportunities to gather the best practices of others and to explore, in the field or in the lab environment, the best use of current capabilities and information on products under development.

Colonel Kirsch is the Chief, Mission Support, Network Operations & Security Division, HQ Air Force Material Command, Wright-Patterson AFB, OH. He was commissioned as a 2nd Lieutenant following completion of the ROTC program and graduation from Duquesne University in Pittsburgh PA. He has held a variety of base level and tactical positions to include four command positions, ranging from a detachment in Iceland to Installation Commander of RAF Croughton, England. In his current position he is responsible for assessment of the operational effectiveness and efficiency of information, security, applications and systems for customers throughout Air Force Materiel Command, and is the overall lead for the command Defensive Counter Information program.

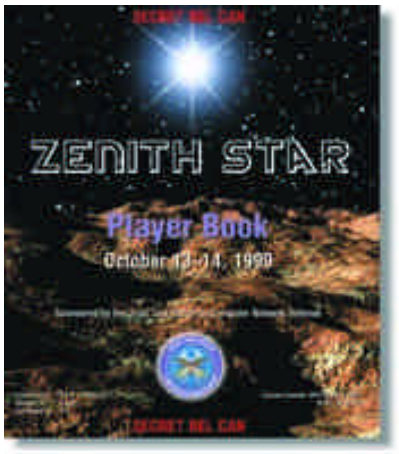
Zenith Star

continued from page 10

ic events from the facilitators at predetermined times. The participants were expected to evaluate the events in real time and formulate a response. While this sounds relatively simple, the intent of Zenith Star 99-1 was to examine interagency coordination—thus the teams had to present a coordinated response to the Control Cell for a specific event. If the participants recommended an appropriate action within a reasonable amount of time, long duration events would be stopped prematurely by the Control Cell. Otherwise, events continued until terminated as determined by the scenario.

Coordination between teams was conducted using the communications available to the participants. All coordination activities, such as phone calls, simulated E-mails, and faxes were recorded on templates provided to the participants. Facilitators were also present at any face-to-face meetings. Using the exercise scenario as ground truth, facilitators were therefore able to assess situational awareness within and across teams, and determine the overall state of the exercise at the end of each day. These assessments helped facilitators identify lessons learned and issues for future consideration.

Participants generally found the exercise to be beneficial. Zenith Star 99-1 showed that the CND community is making significant progress toward developing an effective CND process. Specifically, the ongoing efforts to increase CND coordination between operators, intelligence, and law enforcement are paying dividends. Continued planning initiatives and exercises will help to refine processes further, and prove valuable to the CND community as a whole.



The *Zenith Star 99-1 After Action Report* (AAR) is available on the JTF-CND SIPRNET Web site. Questions and comments are welcomed and encouraged.

Major Gerald Burton, USA, is a Defensive IO Planner in the JTF–CND J5/7 Section. He is an Information Operations Functional Area Officer, and holds an M.S. from Central Michigan University. He may be reached at burtong@jtfcnd.ia.mil.

Mr. Richard Phares is a member of the IATAC, and designs, develops, and executes Information Operations wargames for various clients. He holds an M.S. from the Naval Postgraduate School, Monterey, CA.He may be reached at iatac@dtic.mil.

Information Assurance

The Army Prepares for the Next Generation of Warfare

MAJ Robert Turk, USA
CPT Shawn Hollingsworth, USA

As the Army prepares to digitize the force, a new threat is developing—one that is unlike any the Army has seen before. Rather than spending billions of dollars on materiel, our enemies are now investing in information warfare (IW). Future conflicts are expected to be asymmetric, which means that IW forces will inflict substantial damage on large, computer-dependent adversaries.

In the Washington Times, the Chinese People's Liberation Army (PLA) publicly announced its plans to conduct Internet warfare against the United States. The PLA is gearing up for wartime computer attacks on networks and the Internet that will affect everything from banking to our military's communications structure.

In the past year, attempts to gain unauthorized access to the Army's networks have greatly increased—from the *Melissa* virus to computer attacks against the Pentagon by an Israeli hacker and two teenagers from California. The Army is now placing as much attention on protecting communications networks as it spent in preparing for the rollover to the year 2000 (Y2K). The U.S. Army Signal Center, Fort Gordon, Georgia, has responsibility for the combat developments of tactical, strategic, and sustaining base communications systems and the security systems that protect them. The Signal Center represents the warfighter in the development of information assurance (IA) tactics, techniques, and procedures to protect our tactical networks from our enemies.

During a recent IA Industry Day Conference, Lieutenant General David Kelley, Director, Defense Information Systems Agency (DISA), stated that an "Information Pearl Harbor" is imminent. It is not a matter of whether such an attempt will be made, but when. The Signal Center is taking this new threat into consideration as the Army migrates to the Warfighter Information Network–Tactical (WIN–T), which will replace the Tri-Services Tactical Communications (TRI–TAC) and the Mobile Subscriber Equipment (MSE) switch systems.

WIN–T is the Army's Force XXI command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) tactical communications network, and it will integrate joint, multinational, commercial, and battlefield networks into an intranet that provides mobile, secure, survivable, and multimedia seamless connectivity between all elements within the battlespace from theater to battalion level. WIN-T's backbone will support multiple security levels (MSL)—TOP SECRET/Special Compartmented Information (TS/SCI), SECRET, and Sensitive but Unclassified (SBU)—and various modes of information, including voice, data, video, and imagery.

Network-based monitoring technology within the Defense Information Infrastructure (DII) is being mandated on a large scale across the DoD. WIN-T will include IA security features throughout the network that will employ the DoD's defense-in-depth strategy to protect, detect, and respond to attacks on the military's information systems. IA offers authentication (verification of the originator), nonrepudiation (incontestable proof of participation), availability (unimpeded access to authorized users), confidentiality (protection from unauthorized disclosure), and integrity (protection from information damage).

The layering of IA technology solutions is the fundamental principle of the defense-in-depth strategy, which includes three key areas of protection: external perimeter, internal network, and local computer hosts.

Protected electronic perimeters are needed for local enclaves because many end-user systems have little built-in protection against external access. These systems are difficult to administer well enough to provide an effective defense. Protected perimeters are like castle walls and gates, which enable professional administra-

continued on page 16

The Army Prepares for the Next Generation of Warfare

continued from page 15

tors to control flow in and out. They also enable traffic through the gate to enter and leave at various levels during changing information conditions and allow specific services to be deactivated if they come under successful attack.

The external perimeter safeguards include firewalls, intrusion detection, inline encryptors, and where necessary, physical isolation. Internal network protection consists of a combination of security guards, firewalls, and/or router filtering devices to serve as barriers between echelons and/or functional communities. Host-based monitoring technologies can detect and eradicate malicious software (e.g., virus); detect software changes; check configuration changes; and generate an audit, audit reduction, and audit report.

The defense-in-depth strategy will provide a robust and resilient infrastructure designed to limit, contain, and repair damage that results from attacks. Fundamental criteria of the defense-in-depth strategy is that no single attack can lead to the failure of a critical function and that no critical function or system is protected by a single protection mechanism. This strategy is a key element in the successful implementation of IA in the WIN-T network.

The illustration below depicts the WIN-T's conceptual security architecture, which follows the layered protection strategy. Each layer will consist of a different configuration of IA tools designed to prevent a would-be intruder from gaining

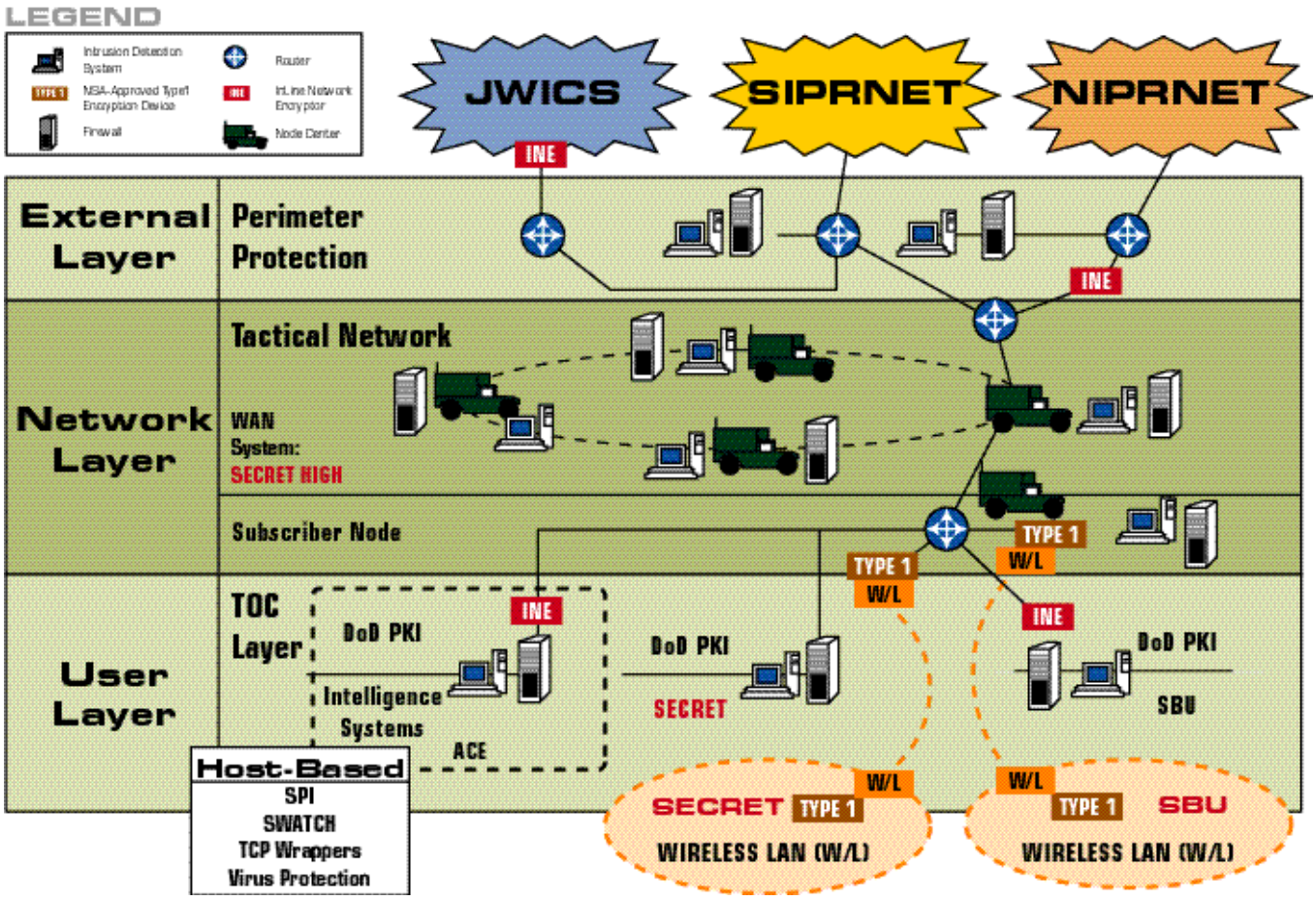


Figure 1. Layered Protection for a Secret High Backbone Supports Multiple Security Levels.

access to all systems by defeating one layer.

External Layer

The strongest layer of protection in the network, is the first line of defense in the defense-in-depth architecture. The primary focus of the perimeter is protecting the inside from the outside, but enclave boundaries also provide some protection against malicious insiders (e.g., those who use the enclave to launch attacks). Protection measures include firewalls, filtering routers, replication servers, strong authentication, authentication servers, Internet Protocol (IP) security/virtual private networks (VPN), and measures to defend against back doors that circumvent firewalls, such as internal use of cellular phones or modems (e.g., sending data through voice public branch exchanges). The external layer and its suite of IA equipment will interface with external connections, such as the Secret IP Router Network (SIPRNET), SBU IP Router Network (NIPRNET), and Joint Worldwide Intelligence Communications System (JWICS).

Network Layer

This layer focuses on network-based monitoring (intrusion detection), thereby providing the capability to identify attacks and suspicious network activity. It captures and forwards event data to a predefined IA cell or the Regional Computer Response Team (RCERT).

User Level

Command and control (C2) protect tools will be employed on the individual host workstations. Host-based monitoring will reside on servers and end-user systems and will detect attacks against individual hosts. The detect capability of this type of monitoring is more fine-grained than network-based monitoring and can be the best line of defense in detecting malicious insiders. Local host protection software consists of Transmission Control Protocol (TCP) Wrappers for individual access control, a security profile inspector (SPI), a Simple Watch (SWATCH) for alerting when audit anomalies occur in the profile, and McAfee virus protection. This C2 package is the last line of defense against unauthorized use and entry.

Voice subscribers will be able to place and receive secure telephone calls to subscribers located on switched networks that incorporate National Security Agency (NSA) Type I-approved devices. WIN-T will provide selected users with a handheld device that will connect via terrestrial and available satellite means to the WIN-T infrastructure, and via airborne platforms to communicate within the area of operations, both in and around command posts/tactical operations centers (TOC). It will have a secure (NSA-approved) capability that provides voice, data, and video communications.

Another form of IA that will be available to the user is the Public Key Infrastructure (PKI). PKI refers to the framework and services that provide for the generation, production, distribution, control, and accounting of public key certificates. It provides critical support to security applications providing confidentiality, authentication of network transactions, data integrity, and non-repudiation.

WIN-T is not designed to counter a specific threat. However, certain security IA components are designed to protect WIN-T from the IW threat. As part of this strategy, IA protects the Army's C2 information network from attempts to penetrate the network to obtain, disrupt, or manipulate the resident information. It allows simultaneous access and processing protection for users at different security levels.

IA and the security features within the WIN-T network will continue to change after the network is fielded in 2005. Even as technology evolves and the threat changes, the Army must continue to protect its vital communications networks.

Major Robert Turk, USA, is the acting Branch Chief, Switching and Networks Branch, Materiel Requirements Division, Directorate of Combat Developments, United States Army Signal Center. He received his B.S. and M.S. in Computer Science from Alabama A. and M. University, Huntsville, Alabama and Towson University, Towson, Maryland. He may be reached at turkr@emh.gordon.army.mil.

Captain Shawn Hollingsworth, USA, is the IA officer, Switching and Networks Branch, Materiel Requirements Division, Directorate of Combat Developments, United States Army Signal Center. He received his M.S. in Technology Management from Mercer University, Atlanta, Georgia. He may be reached at hollings@emh.gordon.army.mil.

Containing Contagion in Cyberspace

COL John C. Deal, USA
MAJ Gerrie A. Gage, USA
Ms. Robin Schueneman

The recent "denial of service" attacks against America Online, Yahoo, and other ISP and Content Providers suggests that computer networks are vulnerable to widespread attack from a variety of adversaries. Complicating these issues are the global nature of such activities and the disparate nature of the kinds of attacks these services have to guard against.

Critical to this discussion is the fact that the dispersal of the tookkits available to hackers makes it all but certain that sniffing out, tracking down, and eliminating these threats will occupy the best network minds for some time to come.

As webmasters, systems administrators, and network security managers rethink the problem, they will, out of necessity, focus a large part of their effort on mitigating virus attacks—in all their forms.

The similarity between computer network systems and biological systems is uncanny. This comparison is common both within Information Technology publications and among users of computer network systems. Addressing computer networks as living systems from the standpoint of health makes one recognize the plethora of vulnerabilities that exist. One of the greatest threats to the health of an organization's computer networks is computer viral infections or contagion. Containing these contagion and eradicating them before the health of a network is degraded requires understanding and real-time vigilance on the part of users, network administrators and software developers.

The Pathology of Computer Viruses

A computer virus is a program, or software code, designed to replicate and spread, generally with the victim being oblivious to its existence. The mere mention of "computer virus" sends computer novices and experts scrambling to download the latest update of Norton, McAfee, or IBM antivirus software. Their reaction is justified. Every large corporation and organization has experienced a virus infection—most experience them monthly. According to data from IBM's High Integrity Computing Laboratory, corporations with 1,000 or more personal computers (PC) now experience a virus attack every 2 to 3 months—and that frequency will likely double in a year.[1] The number of virus attacks may seem unusually high if it is viewed independently. However, when Symantec Corporation (a supplier of DoD antiviral software) defines and categorizes 21,389 known viruses and McAfee (the other supplier of antiviral software to DoD) categorizes more than 40,000 viruses—the number of virus attacks is put in a new light. These viruses, usually benign or annoying, can slow performance, absorb resources, change screen displays and in the end, disrupt or deny service to such an extent that it affects organizations' bottom line—profit or mission accomplishment.

Computer viruses come from a variety of sources and spread by attaching themselves to other programs (e.g., word processors or spreadsheet applications) or to the boot sector of a disk. When the infected file is activated or executed, or when the computer is started from an infected disk, the virus itself is also executed. Viruses can also lurk in computer memory, waiting to infect the next program that is activated, or the next disk that is accessed.

Dataquest's 1991 study of major U.S. and Canadian computer users for the National Computer Security Association found that most users blame infected diskettes (87 percent) as the source of a virus. Forty-three percent of the diskettes responsible for introducing a virus into a corporate computing environment were brought from home. Nearly three-quar-

ters (71 percent) of infections occurred in a networked environment, making rapid spread a serious risk. Seven percent of computer users said they had acquired their virus while downloading software from an electronic bulletin board service or Web site. Other sources of infected diskettes included demo disks, diagnostic disks used by service technicians, and shrink-wrapped software disks; these other sources contributed 6 percent of reported infections.[2] Although no new statistics are currently available, networking, enterprise computing, and inter-organizational communications are growing. Accompanying the growth in telecommuting and networking is an increase in infections.

Viruses are growing in complexity and variety. In 1986, there were just four known PC viruses. In today's virus rich environment, more than three viruses are created every day, for an average of 110 new viruses created in a typical month. There are several variations of viruses, but there are only three ways that a virus can access a system. "Computer Viruses: Past, Present and Future" describes these three methods as follows:

File Viruses

Most of the thousands of viruses known to exist are file viruses, including the *Friday the 13th* virus. These viruses infect files by attaching themselves to a file, generally an executable file—the .EXE and .COM files that execute applications and programs. The virus can insert its own code in any part of the file, provided it changes the host's code somewhere along the way, misdirecting proper program execution so that it executes the virus code first, rather than the legitimate program. When the file is executed, the virus is executed first.

Boot Sector / Partition Table Viruses

Although there are only about 200 boot sector viruses, they make up 75 percent of all virus infections. Boot sector viruses include *Stoned*, the most common virus of all time, and *Michelangelo*, perhaps the most notorious. These viruses are so prevalent because they are difficult to detect. They do not change a file's size or slow PC performance, so they are fairly invisible until their trigger event occurs. Events such as reformatting a hard disk or scanning a disk serve as a trigger. The boot sector virus infects floppy disks and hard disks by inserting itself into the boot sector of the disk, which contains code that is executed during the system boot-up process. Booting from an infected floppy allows the virus to jump to the computer's hard disk. The virus executes first and gains control of the system boot program code even before the operating system (OS) is loaded. Because the virus executes before the OS is loaded, it is not OS-specific and can infect any PC operating system platform—MS-DOS, Windows, OS/2, PC-NFS, or Windows NT. The virus enters the random access memory (RAM) and infects every disk that is accessed until the computer is rebooted and the virus is removed from memory. Partition table viruses attack the hard disk partition table by moving it to a different sector

continued on page 20

Trojan Horse

Like its classical namesake, the Trojan Horse virus typically masquerades as something desirable; e.g., a legitimate software program. The Trojan Horse generally does not replicate (although researchers have discovered replicating Trojan Horses). Rather, it waits until its trigger event and then displays a message or destroys files or disks. Alongside the Trojan Horse is the **Trojan Mule,** which fools authorized users into giving their LOGIN information, passwords, and user-IDs. Once a user types in the valid user-ID/password LOGIN information, the virus sends that information to the file implementers and displays a LOGIN error message. As the authorized user retypes the information, the virus has already exited, the real LOGIN program regains control, and the user never suspects that LOGIN information has been revealed. The difference between the Trojan Horse and Trojan Mule viruses is that the mule does not even try to perform a useful function (e.g., game, application) and it disappears from the system once its done its work, whereas the horse remains in the system until it is cleaned out.

File Overwriters

These viruses infect files by linking themselves to a program, keeping the original code intact and adding themselves to as many files as possible. Innocuous versions of file over-writers may not be intended to do anything more than replicate but, even then, they take up space and slow performance. And because file over-writers, like most other viruses, are often flawed, they can damage or destroy files inadvertently. The worst file over-writers remain hidden only until their trigger events. Then they can deliberately destroy files and disks.

continued on sidebar of page 20

continued from the side bar of page 19

Polymorphic Viruses

More and more of today's viruses are polymorphic in nature. The recently released Mutation Engine, which makes it easy for virus creators to transform simple viruses into polymorphic ones, ensures that polymorphic viruses will only proliferate over the next few years. Like the human AIDS virus, which mutates frequently to escape detection by the body's defenses, the polymorphic computer virus mutates to escape detection by anti-virus software that compares it to an inventory of known viruses. Code within the virus includes an encryption routine to help the virus hide from detection, plus a decryption routine to restore the virus to its original state when it executes. Polymorphic viruses can infect any type of host software. Although polymorphic file viruses are most common, polymorphic boot sector viruses have already been discovered.

Stealth Viruses

These viruses are specially engineered to elude detection by traditional anti-virus tools. The stealth virus adds itself to a file or boot sector, but when the host software is examined, it appears normal and unchanged. The stealth virus performs this trickery by lurking in memory when it is executed. There, it monitors and intercepts the OS's calls. When the OS seeks to open an infected file, the stealth virus races ahead, disinfects the file, and allows the OS to open it—all appears normal. When the OS closes the file, the virus reverses these actions, thereby re-infecting the file. Boot sector stealth viruses insert themselves in the system's boot sector and relocate the legitimate boot sector code to another part of the disk. When the system is booted, they retrieve the legitimate code and pass it along to

continued on the sidebar of page 21

and replacing the original partition table with the virus' own infectious code. These viruses spread from the partition table to the boot sector of floppy disks as floppy disks are accessed.

Multipartite Viruses

These viruses combine the ugliest features of both file and boot sector/partition table viruses. They can infect any of these host software components. And while traditional boot sector viruses spread only from infected floppy boot disks, multi-partite viruses can spread with the ease of a file virus—but they still insert an infection into a boot sector or partition table. This tendency makes them particularly difficult to eradicate. *Tequila* is an example of a multi-partite virus.

Although there are only three ways to infect a system, there are hundreds of variations of viruses. The sidebars (pages 17 through 21) contain descriptions of virus variations taken from "Computer Viruses: Past, Present and Future," "Demystifying Computer Viruses," and "Computer Security Basics." This list is not all-inclusive, but it describes some of the common variations to date.

Viruses affect computers and networks differently. The purpose of most viruses is to remain undetected, thereby allowing them to spread throughout the organization until they degrade performance or destroy data. Most viruses give no symptoms of their infection, thus driving the use of anti-virus tools. Anti-virus tools allow users to identify these quiet killers. However, many viruses are flawed and do provide some tip-offs to their infection. Here are some indications to watch for:[3]

- Changes in the length of programs
- Changes in the file date or time stamp
- Longer program load times
- Slower system operation
- Reduced memory or disk space
- Bad sectors on the floppy
- Unusual error messages
- Unusual screen activity
- Failed program execution
- Failed system boot-ups when booting or accidentally booting from the A: drive
- Unexpected writes to a drive.

This list of virus variations and symptoms is not all-inclusive. Additional information can be found at the following Web sites:[4]

- http://www.rootshell.com (exploits)
- http://www.insecure.org/sploits.html (exploits)
- http://ciac.llnl.gov/ciac/CIACVirusDatabase.html (virus information)
- http://www.snafu.de/~madokan/mvic/viruscont.html (virus creators)
- http://www.symantec.com/avcenter/index.html (virus information)
- http://vil.mcafee.com (virus information)
- http://www.virusbtn.com (virus information)

The viruses discussed above are only the most common variations of computer viruses and their symptoms. Computer viruses have cost companies worldwide nearly $2 billion since 1990, with those costs accelerating to $1.9 billion in 1994. This cost is directly related to virus cleanup, not loss of profit. Profit loss caused by

viruses is impossible to calculate. Organizations are combating the virus problem with antivirus software. The cost of this software is expected to grow from $700 million in 1997 to $2.6 billion by 2001.[5]

So what can an organization do to prevent computer viral infections, and what is the best response in the event of an infection? These questions are best answered by analyzing a real event. This event is current and represents the best possible response to date by the Federal Government, DoD, and industry. As reported by SANS (System Administration, Networking, and Security) Institute, the response of these organizations was "impressive."

Containing Contagion: A Case Study

History will remember several notable landings: the landing of the lunar module on June 20, 1969; the landing of ET the extraterrestrial in movie cinemas in 1982; the landing of Mark McGwire in record books with his 70th home run in September 1998; and the landing of Melissa in commercial, military, educational, and home PCs on March 26, 1999.

One might ask, "Who is *Melissa*?" The question is in fact, "What is *Melissa*?" *Melissa* is a virus, conceivably the fastest spreading virus PCs have seen since the infamous *Morris Worm*, which infected more than 6,000 computers in a matter of hours (ftp://coast. cs.purdue.edu/pub/doc/morris_worm/GAO-rpt.txt) in November 1988. By March 30, 1999, *Melissa* had successfully infected about 70,000 E-mails. It was the first virus to have prompted Federal law enforcement to send out a warning about computer viruses; the Federal Bureau of Investigation (FBI) joined with the National Infrastructure Protection Center (NIPC) to issue a warning in anticipation of the tidal wave of E-mails that *Melissa* was expected to generate.

Melissa is a **macro virus**, which means that its infectious code is resident in a macro (a symbol, name, or key that represents a list of commands, actions, or keystrokes) contained in a Microsoft Word document (see right side bar). In *Melissa's* case, the macro has instructions to disable macro detection capabilities, read the first 50 names in a recipient's Microsoft Outlook address book, and forward itself as an attachment to those individuals, or groups of individuals. When this forwarded E-mail message is received and opened, the macro begins again its cycle of E-mail generation, thus bogging down and potentially crashing mail servers through its exponential rate of infection. This type of attack is known as a **denial of service.**

While the shutdown of electronic mail servers is destructive enough, there is at least one other potentially hazardous result of this virus. *Melissa* is spread through a Microsoft Word document. However, this virus is constructed in such a way that it infects whatever document is open at the time the infected attachment is displayed, and that document is the one that is forwarded with the virus. Imagine this scenario: You are typing a classified document when you receive *Melissa*. When you open the attachment, i.e., the macro virus, it now places itself on

continued on page 22

accomplish the boot. Under examination, the boot sector appears normal, but the boot sector is not in its normal location.

Macro Viruses

Macros are, in essence, mini-programs that take much of the legwork out of repetitive or template-oriented documents. For example, to minimize the work involved in typing the date in correspondence, a user could program a macro to insert the day, month, and year all at once when the letter "D" is typed. Macro viruses are carried in the types of data files that business computer users most often exchange: word processed documents and spreadsheets. Also, because these data files are often exchanged by E-mail, they sometimes bypass the checks that virus-aware organizations already have in place. Experts estimate that 40 percent of virus attacks are made this way. Macro viruses are created with the aid of the macro routines contained within all word processing and spreadsheet application software, such as Microsoft Word and Excel. They attach themselves to any document files that include the macro code, so that they can then be executed through the application software. The whole purpose of macro languages is to insert useful functions into documents, which are then executed as the documents are opened. This is what makes macro viruses easy to write. But one of the reasons they have become so prevalent is the success of Microsoft Office, which has 80 percent of the global market for integrated packages—a tempting target for macro virus writers.

Memory-Resident Viruses

The memory resident characteristic is the most common among viruses. When viruses load into memory via a host application, they remain in memory until the computer is turned off. At

continued on the sidebar of page 22

continued from the side bar of page 21

this stage of their existence, viruses can easily replicate into boot sectors or subsequently launched applications.

Non-Memory-Resident Viruses

These viruses can infect the system only when the host application is running. When the host application is closed, the virus is closed down as well. Therefore, if applications are opened after a host application is closed, there is no danger of infecting the system with that specific virus at that time.

Companion Viruses

To understand this characteristic, it is helpful to have a basic understanding of the sequential order of how system files work. In launching an executable file, either the user manually issues a command or the interface executes a command. Most applications have a file-type (FT) extension of *.EXE. When invoking these commands, the user or the computer enters the name of the application without the extension. The computer executes other system files with the same name before executing the *.EXE application's FT. A companion virus creates a name that matches the *.EXE file name but with a different extension (e.g., *.COM). The *.EXE still executes; however, the *.COM (infected file) launches first and infects the system. Most antiviral software packages can identify this characteristic.

Bomb

A bomb is a type of Trojan Horse that is used to release a virus, a worm, or some other system attack. It is either an independent program or a piece of code that has been planted by a system developer or a programmer. A bomb works by triggering some kind of unauthorized action when a particular date, time, or condition oc-

continued on the sidebar of page 23

your already opened Word document and forwards THAT document to the first 50 addressees in your address book.

Several aspects of this virus have helped its seemingly global proliferation. One of the most significant aspects is its use of a user's own address book to forward the infectious E-mail. This means that an ordinary user, who would be suspicious of E-mail from an unknown source, receives the virus as if a friend, co-worker, family member, etc. sent it, thereby instilling a false sense of security. In addition, this virus is spread with the help of Microsoft Word and Microsoft Outlook, two programs that are resident in a vast majority of PCs today due to the overwhelming popularity of Microsoft Office.[6]

The DoD's and Services' Information Assurance processes helped ensure that *Melissa's* impact on DoD and the Services was minimal. The Army began receiving the virus shortly before 5:00 p.m. on Friday, March 26, 1999. Half an hour later, the Army Computer Emergency Response Team (ACERT) began receiving notices from its Regional CERTs (RCERT), and by 6:00 a.m., the virus had spread throughout DoD systems worldwide.

Once users began receiving E-mail from known acquaintances but with an "out-of-character" attachment, they began contacting their local systems administrators who, in turn, alerted the ACERT at Ft. Belvoir, Virginia, and the technical support staff at Microsoft (which created the software the virus was designed to run on), and McAfee and Norton, two anti-virus companies. After the virus was discovered, a restriction was placed on the size of E-mail attachments. A message was distributed to all E-mail users, instructing them to not open attachments or enable macros in Microsoft Word documents they received via E-mail unless they were sure of the document's origin.

Working in concert with industry, Government officials were able to detect and attack the virus and implement fixes that were distributed to systems administrators and users in record time. RCERTs went to a heightened level of management and detection, and the Army Signal Command directed the information management officials at 18 major facilities to scan E-mail servers using an application received from Microsoft and delete E-mail traffic infected with the virus. Throughout the night, ACERT coordinated reports, orchestrated solutions to the virus with McAfee and Norton, and assisted system administrators with installing fixes. By Monday, March 29, 1999, the virus was contained and eradication was well on its way. This reaction established a process termed "Positive Control," and the proactive efforts of all involved made this rapid containment happen, along with the close cooperation with the software industry.[7]

Disinfecting *Melissa* was actually a fairly simple process, even if labor intensive. Ordinarily, the fix would have merely involved retrieving the latest virus definitions from a reputable virus-scanning source, such as Norton or McAfee, and scanning client and server hard drives. The glitch in *Melissa's* case was that these virus-scan-

ners were caught relatively off guard with this virus. Normally, anti-virus software companies know about new viruses long before they are released and, therefore, are able to release updated virus definitions to their clients before the danger arrives. For some reason, *Melissa* was kept under close wraps until its release on March 26. In the end, the damage caused by *Melissa* will be measured in the millions of dollars. But the lessons learned from this attack are being institutionalized. Contagion in cyberspace can be contained.

Colonel Deal is the Commander, U.S. Army Information Systems Engineering Command, Ft. Huachuca, Arizona. He earned an M.S. in Electrical Engineering from the Naval Post Graduate School and an M.A. in National Security Studies from the Naval War College, and an M.A. in International Relations from Salve Regina University.

Major Gage is the Operations Officer for the News Systems Training Office, Directorate of Combat Development, 306th MI BN, Ft. Huachuca, AZ. She has a B.S. in Biology from Florida Southern College, an M.S. in Material Acquisition Management from Florida Institute of Technology, a M.S. in Engineering Management from University of Missouri-Rolla, and a M.A. in Computer Information Resource Management from Webster University.

Robin Schueneman supports the Army's Information Assurance Directorate of DISC4. She is the DISC4 lead to the Information Assurance Vulnerability Alert (IAVA) Compliance Verification Team (CVT). Ms. Schueneman earned a B.A. in Communications from UNC-Chapel Hill, North Carolina in 1994.

Endnotes

1. Symantec Corporation, *Computer Viruses: Past, Present and Future,* Anti-Virus Research Center, March 29, 1999.
2. Ibid.
3. Lowenthal, *Overview of Computer Viruses,* Information Paper, SAIS-IAS, March 1999.
4. Ibid.
5. Davy, Jo Ann, "Virus Protection," *Managing Office Technology,* 1998.
6. Schwartz, John, "New Virus Snarls E-Mail Systems," *The Washington Post,* p. E1 (March 30, 1999).
7. Singer, Jeremy, "*Melissa* blunted by response teams QUICK RESPONSE MAKES ARMY SYSTEMS VIRTUALLY IMMUNE TO E-MAIL VIRUS," *Inside the Army* (April 5, 1999).

Bibliography

Corbitt, Terry, "Datafiles in Danger," *Accountancy,* available online at: http://proquest.umi.com/pqdeb (January 1999).

Davy, Jo Ann, "Virus Protection," *Managing Office Technology,* available online at: http://proquest.umi.com/pqweb (1998).

Jarvis, Kenneth, "Demystifying Computer Viruses," *Management Accounting,* available online at: http://progquest.umi.com/pqdweb (April 1997).

Lowenthal, "Overview of Computer Viruses," Information Paper, SAIS-IAS (March 1999).

Russell, Deborah & Gangemi, G.T., Ed., "Viruses and Other Wildlife," *Computer Security Basics* (United States of America, O'Rilley and Associates, Inc., 1991) pp. 79-88.

SANS Newsbites, available online at: http://www.sans.com (March 1999) and http://securityportal.com

Schwartz, John, "New Virus Snarls E-Mail Systems," *The Washington Post,* p. E1 (March 30, 1999).

Singer, Jeremy, "*Melissa* blunted by response teams QUICK RESPONSE MAKES ARMY SYSTEMS VIRTUALLY IMMUNE TO E-MAIL VIRUS," *Inside the Army* (April 5, 1999).

Symantec Corporation, "Computer Viruses: Past, Present and Future," Anti-Virus Research Center available online at: http://www.symantec.com/avcenter/reference/corpst.html (March 29, 1999).

curs. There are two types of bombs: time and logic. A time bomb is set to go off on a particular date or after some period of time has elapsed. The Friday the 13th virus was a time bomb. A logic bomb is one that is set to go off when a particular event occurs. Software developers have been known to explode logic bombs at key moments after installation—if, for example, the customer fails to pay a bill or tries to make an illicit copy.

Spoof

This is a generic name for a program that tricks unsuspecting users into giving away privileges. Often, the spoof is perpetrated by a Trojan Horse mechanism in which an authorized user is tricked into inadvertently running an unauthorized program. The program then takes on the privileges of the user and may run amok.

Bacteria

These are programs that do nothing but make copies of themselves, but by doing so they will eventually use up all system resources (i.e., memory, disk space).

Rabbits

This is another name for rapidly reproducing programs.

Crabs

These programs attack the display of data on computer terminal screens.

Salami

Salami slices away (rather than hacking away) tiny pieces of data. For example, salami alters one or two numbers or a decimal point in a file, or it shaves a penny off a customer's bank interest calculations and deposits the pennies in the intruder's account.

Computing on the Virtual Border

.mil meets .edu

LTC Eugene K. Ressler, USA
COL Clark K. Ray, USA

The U.S. Military Academy (USMA) at West Point confronts a novel information age challenge—to balance the needs of a dynamic, technology-rich undergraduate experience for 4,000 cadets with the availability, security, and interoperability concerns for an enterprise local area network (LAN) operating within the Department of Defense (DoD) network infrastructure. Despite

Figure 1. Work at a Z-248, circa 1988.

resource, technology, and culture challenges, this balancing act has been unusually successful over an evolution spanning the 10 years since the USMA network was created in 1989. Perhaps surprisingly, cadets' education benefits from the moderate discipline imposed by operating the network in accordance with DoD requirements and professional best practices. Typical university data networks, by contrast, operate as mostly unfettered services in which almost "anything goes" with regard to hardware, software, protocols, and modes of use. Although this approach affords great individual freedom, its overall effect may be to reduce network usefulness. Recent trends in campus computing seem to be drawing the rest of academe closer to the computing model employed at West Point.

West Point occupies a rare crossroads of ".edu" and ".mil" domains. This is literal in the sense that many network hosts have names in each domain. Browsing www.usma.army.mil will take a virtual visitor to the same place as www.usma.edu and www.westpoint.edu. The Academy is first and foremost a primary commissioning source for Army officers. It is an Army post, and the post network is an Army information system. "Dot mil" naming and conformance to DoD/Department of the Army (DA) standards is expected and required. However, West Point is also a tier I, accredited academic institution with strong ties to the academic community for research and other professional exchanges. Military and civilian faculty members find that in some settings, an ".edu" address communicates the seriousness with which the USMA views its role in undergraduate teaching, learning, and research.

Attracting the best qualified of American's high school graduating class each year is an essential aspect of the West Point program. Among bright, knowledgeable high school students, sophisticated technological infrastructure is high on the list of criteria for college choices. After admission, cadet families expect and deserve electronic mail (E-mail) and other electronic contact with their cadets. It follows that a principle of information assurance (IA) at West Point is to support technology programs and systems that meet the expectations of diverse clients outside the gate. Connecting with the American public is essential to fulfilling its institutional mission, so West Point can seldom afford to escape risk by reducing access.

The military/educational duality continues inside the gate. Inquiry is the soul of learning, and inquiry has increasingly come to involve innovative uses of technology. The computing environment at West Point must provide cadet students and faculty members the freedom to experiment with hardware and software and to exchange information worldwide with great convenience while still providing information assurance. Cadets purchase their own computers and software much as they do textbooks and other tools of the academic program, so they have a reasonable expectation of control over their computers' configuration. On the other hand, the USMA network is a military facility where official business takes precedence. The Army reasonably expects to enforce usage policies and config-

uration management of network resources.

To be sure, universities and colleges share many of USMA's challenges. Although few have a dual presence on the Internet, each campus has business to conduct in security and with high reliability while also providing academic freedom of inquiry. Educating students on acceptable use of technology facilities is a shared concern. Students everywhere stay on the leading edge of new information services. Downloadable software of all varieties, music in "MP3" (compressed) form, and electronic stock trading illustrate developments that have put college officials in catch-up mode, deciding what students can properly and legally do, determining their own legal and ethical institutional responsibilities, and figuring out how to enforce their policies.

USMA differs from its peer academic institutions in the way it confronts IA challenges. A key example is the USMA approach to student computing. Although cadets do own and pay for their computers, the configuration is standard, chosen through a "best value" competitive government solicitation, with software installed in advance. Although some disk space is reserved for cadets to configure however they choose, a precondition for physical connection to the USMA network is use of a government-installed, controlled, managed, and monitored operating environment. For example, all cadet computers must currently run WindowsNT as their operating system when connected to the network, and except for selected individuals, users may not exercise full administrator privileges.

Acceptance of these limitations is a modest sacrifice for the services provided in return: Internet and intranet access; shared files, printers, and public bulletin boards; and standard directory and E-mail facilities. Configuration standards at West Point allow the organized planning and delivery of a wide spectrum of services, a range exceeding that at most schools. A current project will provide each cadet with a high reliability network home directory that is Web-accessible via Hypertext Transfer Protocol (HTTP). IA measures, such as antivirus software updates, operating system patches (often issued in response to Army Computer Emergency Response Team [ACERT] alerts), software upgrades, and necessary configuration changes are dispensed each time cadets log in to their network accounts. Army intrusion detectors alert USMA technicians to Internet attacks on cadet computers. Teams are usually able to clear or repair any damage before the cadet knows what has happened. The latest cadet computers include hardware features for central monitoring that have averted significant maintenance problems.

Figure 2. Typical cadet work space today.

Technical support is another difference. Most American students come to college with a computer of their own choosing. To an uncomfortable degree, they must fend for themselves in solving software, hardware, and configuration problems. Some institutions are currently finding that students on stipend can fill some of this gap in technology support. West Point has made cadet Information Systems Officers (ISO) part of the Corps of Cadet chain of command for more than a decade. A small team of government technicians mentors ISOs in a range of system administration tasks considered to be "second echelon" support (forgotten passwords, installation of hardware drivers, and the like). This structure provides an exceptional developmental experience for the ISOs and an effective, zero-dollar (although not zero person-hour) source of support. Government and con-

continued on page 26

tract personnel perform more sophisticated repairs. All cadets take a one-semester course in computing fundamentals in their first year. Additionally, each year as many as 20 percent of cadets select academic majors or sequences (minors) in disciplines directly related to information technologies, providing a level of expertise to classmates who share their living areas not found at many other institutions.

The ethical and moral aspects of cadet development programs are another essential part of IA at West Point. Inside the West Point firewall, designs to safeguard systems and data are able to assume that malicious intent on the part of users is a rare—and readily punishable—occurrence. Cadets are instructed to consider technology system abuses to be failings of personal conduct or ethics. In short, USMA's students are asked and required to be part of the IA effort. West Point's intranet security intends to "keep honest people honest" and to detect the occasional outlying bad behavior. On the other hand, most campus network designers frequently have no choice but to assume that many students will intentionally abuse institutional systems. The Athena project at the Massachusetts Institute of Technology (MIT) and the proliferation of virtual LANs and other elaborate security control mechanisms on campuses stand as examples.

The upshot of USMA's methods is better education and training for cadets. On any given day, approximately 99.6 percent of cadet computers are available on the USMA network. At other institutions, the popularity of campus-wide student computer purchase programs is growing. These often include limited standard configuration efforts. However, few published data measure overall availability statistics. Whereas most campuses sport an eclectic array of standards, West Point cadet, faculty, and staff computers run identical E-mail, office suite, mathematics, and multimedia software, allowing faculty members to give instructions and assignments that incorporate configuration details. Technology support and security costs are reduced, so available dollars can be focused on improving capabilities rather than on security and middle ware. Although cadets do not have complete freedom to connect devices and run disapproved software in the USMA network environment, cadets with bona fide educational needs to operate nonstandard configurations are able to do so in controlled circumstances under the guidance of a faculty mentor.

The lessons of experience are somewhat counterintuitive. The military and government environment of education at West Point benefit its cadet students rather than detracting from their experience. A comprehensive approach to IA for student computing is part of the solution, rather than a problem to be solved.

Lieutenant Colonel Eugene K. Ressler, Jr., is Professor of Computer Science and Associate Dean for Information and Educational Technology at the United States Military Academy (USMA) at West Point, New York. He has served as an Army engineer and computer scientist in various assignments. He graduated from the USMA in 1978 and received a master's degree in computer science from the University of California at Berkeley in 1984 and a Ph.D. in computer science from Cornell University in 1993. He may be reached at ressler@usma.edu.

Colonel Clark K. Ray is the USMA Computer Science Program Director in the Department of Electrical Engineering and Computer Science and has previously served in Army engineering and automation assignments. He is a 1976 graduate of USMA and received his master's and Ph.D. degrees in computer and systems engineering from Rensselaer Polytechnic Institute. He may be reached at ray@eecs1.eecs.usma.edu.

In Pursuit of the "Trustworthy" Enterprise

Mr. Sean P. O'Neil

Editor's Note: Inclusion of this product within the *IAnewsletter* does not constitute as an endorsement by IATAC or DoD.

Today's consumers may be immediately concerned with protecting their Visa card numbers during on-line purchases, and until just a few weeks ago, government information technology (IT) managers were primarily obsessed with exterminating the year 2000 (Y2K) bug. However, individuals in both private and public sectors feel growing apprehension about security threats from the Internet.

Shared Concerns—Inside and Outside the Beltway

Citizens and government managers alike recognize not only the potential dangers posed by hackers, computer virus writers, Web saboteurs, and other Internet attackers, but also the need to increase the soundness of overall Internet security infrastructure.

Just as businesses and consumers are beginning to tap the Internet's potential for electronic commerce (e-commerce) purposes, government agencies are leveraging the power of the Web to deliver enhanced services and information. However, with the efficiencies offered by the Internet come opportunities for disaster. As the world rushes into the Internet age, the opportunities for security breaches and cyber terrorism continue to escalate.

The Internet opens the e-commerce door to millions of users, while simultaneously exposing Web sites and placing at risk invaluable corporate data, mission-critical business applications, and consumers' confidential information. Web-enabling technologies also have the potential to compromise the integrity of government networks and crucial defense resources. The Internet may soon serve, in effect, to launch commercial hijackings and cyber terrorism directed against the U.S. national infrastructures.

A Real and Imminent Danger

According to the FBI, the average American corporation will experience a major electronic intrusion once every 2 years. On the government side, the General Accounting Office has warned that federal government systems such as tax collection, national defense, and air traffic control networks may face serious threats of severe disruption unless adequate defense measures are quickly put in place.

Fortunately, sophisticated tools are now available to protect E-commerce transactions, IT assets, and network resources. The most powerful of these e-commerce security tools are equally effective in sensitive government IT environments—where property and lives are at stake, not just dollars and credit ratings.

Computer Associates International, Inc., (CA) has developed such a tool. Its eTrust security solutions are used at government and commercial sites to safeguard information and maintain the integrity of vital enterprise resources. eTrust protects mission-critical IT resources and offers broad functionality, including risk assessment, attack detection, and consolidated administration of policy and audit trails. eTrust solutions can also be scaled to suit an environment of any size.

Government agencies and commercial entities deploy eTrust as either stand-alone products or as a comprehensive security suite. eTrust was designed to be used with CA's Unicenter TNG enterprise management solution, thus offering IT managers a consistent approach to building, deploying, and managing security as part of the larger IT administration and control task.

By supporting and exploiting security features of the OS/390,

continued on page 28

continued from page 27

UNIX, and Windows NT operating systems and applications, eTrust's open, expandable architecture allows organizations to leverage their existing technology investments. Public key infrastructure (PKI), LDAP, and smart-card products are a few of the standards-based technologies used by Global 2000 customers and government clients in conjunction with CA's enterprise management and security products.

When the Firewalls Come Tumbling Down

Together with network intrusion detection systems, firewalls have traditionally provided first-level defense against external attacks. However, holes must be punched through firewalls to grant legitimate access to Web-enabled applications. Implementing these applications concurrently provides an opportunity for hackers to exploit application or server vulnerabilities and breach security controls.

Equally disconcerting is the fact that moving to e-commerce and Internet-enabled environments has done nothing to eliminate traditional security threats. On the contrary, these developments have escalated vulnerabilities by increasing the number of people with access to specific internal services. For these reasons, conventional security devices are no longer effective by themselves. Simultaneously implementing several stand-alone security tools is also ineffective because it results in a patchwork solution that leaves weak spots unprotected.

Protecting Against Security Threats on All Fronts

Using eTrust, CA has partnered with government and commercial customers to provide a complete security solution tailored to specific requirements and organization goals, a solution that supports Internet use and also protects the infrastructure. Tight integration among eTrust offerings gives government agencies and business organizations enterprisewide security and also allows them to adopt incrementally eTrust solutions that seamlessly work with one another. Solutions include—

- eTrust Access Control, which provides policy-based control to determine who can access specific systems, what they can do with them, and when access is allowed
- eTrust Admin, which simplifies user and resource administration, reducing its complexity, expense, and susceptibility to error
- eTrust Audit, which collects enterprisewide security and system audit information
- eTrust Content Inspection, which safeguards systems connected to the Internet from malicious code attacks
- eTrust Directory, which ensures high performance and reliability of critical directory service applications
- eTrust Encryption, which seamlessly safeguards information against intrusion as it is transferred across a Transmission Control Protocol /Internet Protocol (TCP/IP) network
- eTrust OCSPro, which provides a scalable, distributed Online Certificate Status Protocol (OCSP) responder implementation, giving client applications the current status of a digital certificate from a trusted authority in real time
- eTrust Firewall, which controls Internet, intranet, and extranet access to mission-critical applications, excluding unauthorized users
- eTrust Intrusion Detection, which delivers advanced network protection and includes an integrated antivirus engine with automatic signature updates
- eTrust Policy Compliance, which enables organizations to protect against unauthorized usage or attacks by identifying potential weak points in security policies, automatically generating corrections, and constantly monitoring the network
- eTrust VPN, which delivers secure Internet communications and safeguards all virtual private network (VPN) uses.

CA also offers a Security Integrity Services (SIS) portfolio, which includes a complete range of consulting services for security assessment, policy development, product installation, support, implementation, and outsourcing. For further information on CA's eTrust products and services, see http://www.cai.com/solutions/enterprise/etrust.

Sean P. O'Neil is a freelance writer and President of Write Hand Communications, Inc. He holds an M.B.A. from Dowling College, as well as a B.A. in English from State University of New York at Albany. He may be reached at spoemail@aol.com.

Third International Information Hiding Workshop

Mr. Robert P. Thompson
Director, IATAC

IATAC recently attended the Third International Information Hiding Workshop in Dresden, Germany. This workshop is the primary forum for scientists engaged in the field of Information Hiding techniques, including steganography and digital watermarking. The workshop focused on algorithms and techniques, rather than on systems and policy. The information presented at this workshop is intended to provide a comprehensive view of the current state-of-the-art in data embedding research.

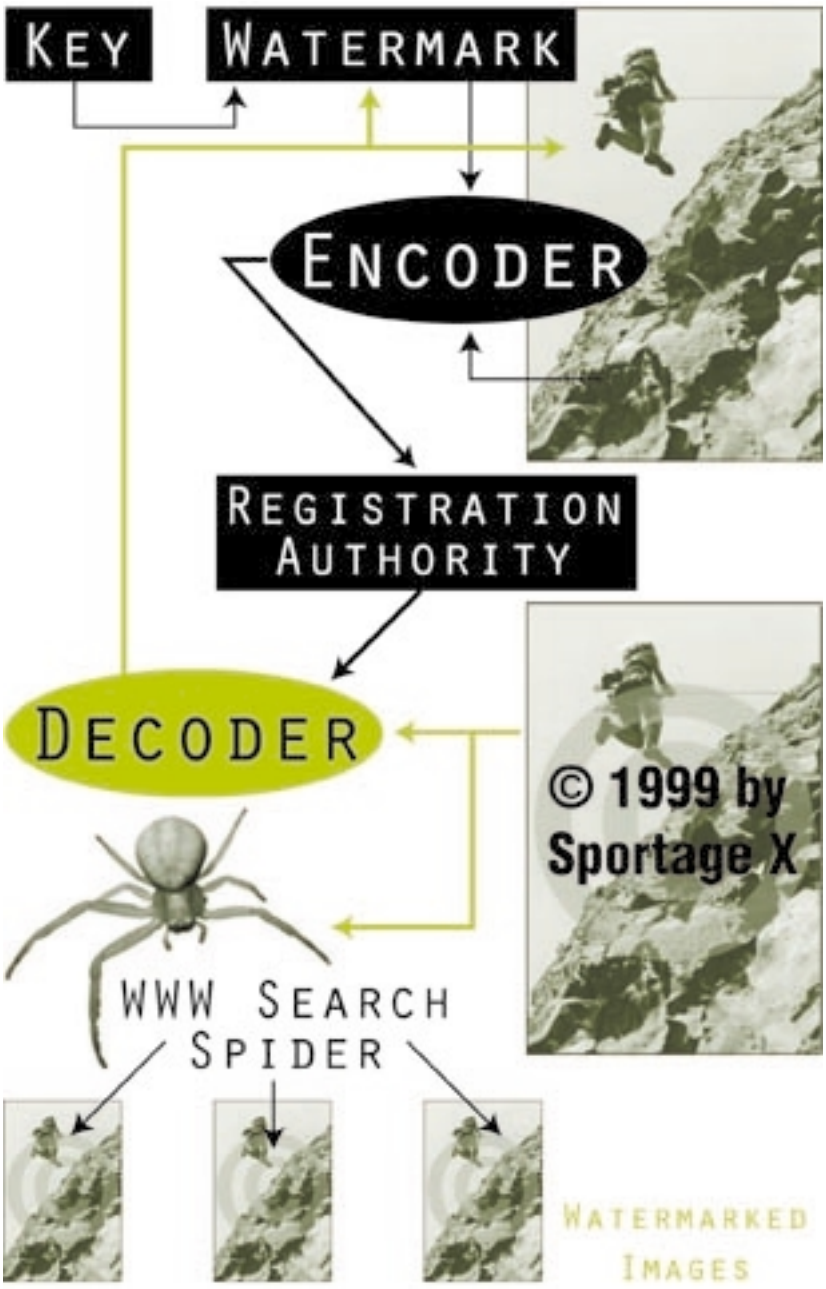


Figure 1. Watermarking System

Conference sessions were separated into steganography and watermarking tracks. The steganography track was divided into sessions on fundamentals, paradigms and examples, asymmetric steganography, engineering, and attacks. The watermarking track featured sessions on proofs of ownership, detection and decoding, watermarking techniques, protecting private and public watermarking information, new designs, robustness, and software and hardware protection.

The steganography sessions illustrated that steganography research is improving, and certain institutions are gaining expertise, along with more operational insight than is usually expected in academia. In general, steganography is designed to make it more difficult to detect embedded data. Researchers and developers are beginning to make more realistic assumptions about host data files; many are stating that initial assumptions about Least Significant Bit (LSB) substitution appear to be false and the security of these techniques is questionable. Algorithm developers are paying more careful attention to where to hide data, focusing on areas

continued on page 30

continued from page 29

with specific statistical properties rather than hiding data throughout the host file.

In the digital watermarking sessions, the IATAC state-of-the-art report on Data Embedding for Information Assurance concluded that advances in watermarking attacks were, in turn, forcing advances in watermarking techniques. Yet the research presented at the workshop largely ignored knowledge of common attack methods. Instead, the presentations described minor variations of existing techniques. There were several attempts to add theoretical rigor to watermarking techniques and protocols. While the mathematics presented were generally sound, the proofs made assumptions that had no strong basis in reality, and no attempt was made to prove that the assumptions were valid. Thus, it is hard to use the theoretical results to draw any conclusions about operational watermarking systems.

Ms. Elke Franz, from the Dresden University of Technology, presented a paper on "Steganography Secure Against Cover-Stego Attacks." The paper described techniques for avoiding steganography detection when the attacker has a copy of the overt host image (sometimes called the cover image). Ms. Franz proposed a steganography method that simulates the image scanning process. First, a scanner's statistics are modeled by repeatedly scanning the same image to obtain a "noise" profile of the scanner by observing the differences between each scanned image file. Ms. Franz described how an embedding algorithm had been designed to generate the same scanner model. She claims that the embedding process will be indistinguishable from an image obtained from a specific scanner.

Ms. Franz then provided the workshop attendees significant insight into the steganography detection process. She observed that the details of a digitized image depend on the acquisition method. Common open-source steganography methods ignore this fact. She also observed that the details of the embedded data, such as the compression and encryption methods used and the type of overt host, could affect the ability to detect embedded data. Ms. Franz explained two methods that an attacker might use to manipulate overt host and embedded data. The first method is to establish a Web site that is an attractive and convenient source of overt host data files, except that the files are selected to be poor candidates for embedding data. The second method is to seed freeware or shareware compression and encryption programs on the web. These programs would be designed to prepare embedded data in a way that makes it easier to detect.

For more information on the workshop and a summary of significant papers presented, contact IATAC at 703.289.5454 or via E-mail at iatac@dtic.mil.

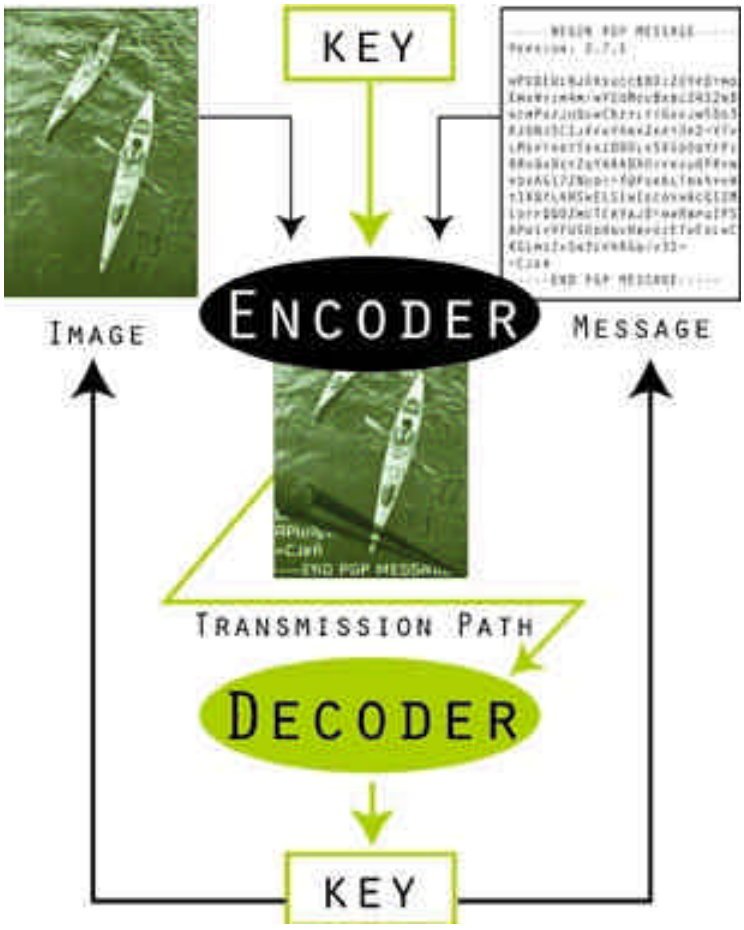


Figure 2. Example of a Generic Steganography System

IAC Awareness Conference

May 16, 2000
Hope Hotel
Wright Patterson AFB
Dayton, OH

"Key Challenges" to Meet Joint Vision 2010

The theme of this conference is "Key Challenges" that need to be conquered to enable us to meet Joint Vision 2010. The meeting is open to all Department of Defense (DoD) and associated industry personnel. This meeting will promote IAC Awareness with an emphasis on the needs of the warfighter.

The objective of this conference is to explore the strategic direction and the resulting requirements of information technology and services necessary to support DoD. To that end, an aggressive agenda with senior-level participants will provide an opportunity to discuss and share valuable insights between Research and Development and the warfighter community.

Those in attendance will include policy makers, DoD program managers, researchers, analysts, information providers, and information users. This conference will address the information needs of the warfighter, along with the current and future information technology initiatives to support those needs in the new millennium. The impact of changes in the policies, procedures, and technologies of information now and in the future and the subsequent impact on DoD will also be addressed.

DoD IACs will have exhibits in the display area highlighting their capabilities, products, and services.

Register Electronically at

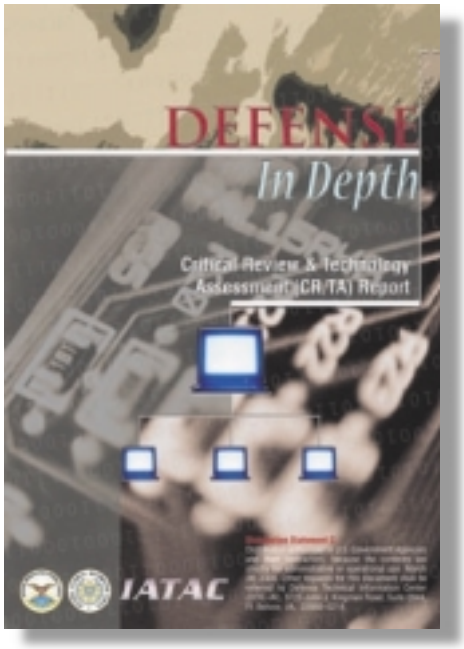
http://iac.dtic.mil/surviac/announce

Additional Information

Donna Egner, SURVIAC
937.255.4840
E-mail: degner@bah.com.

products

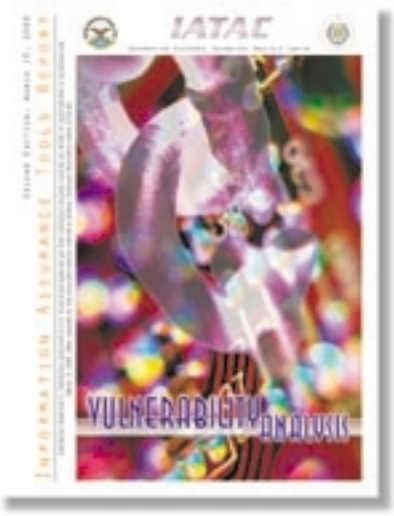
Defense in Depth Critical Review & Technology Assessment (CR/TA) Report



Attacks on DoD systems have expanded from simple wiretaps and viruses to session hijacks and trojan horses, and the types and sophistication of these attacks are constantly evolving. In response to these threats, DoD response has also evolved. In recognition of the growing threat and complexity of this problem, DoD developed the defense in depth strategy to protect its networks and information systems.

This report describes the impact of evolving technology on the defense in depth strategy. The execution of the strategy requires a significant number of different security and networking technologies. This report focuses on examining the trends and giving an overview of the relevant technologies. This report reviews the defense in depth strategy and discusses its implementation in the Defense Information Infrastructure (DII). Key elements of the strategy and current implementation of the strategy are discussed.

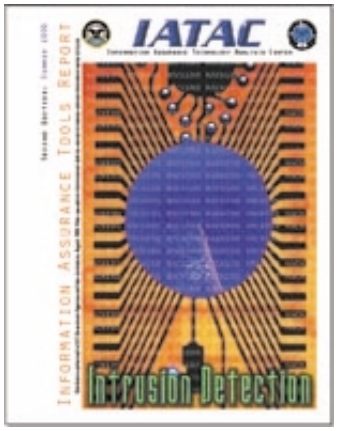
Vulnerability Analysis Tools Report 2nd Edition



This newly updated report provides an index of the vulnerability analysis tool descriptions contained in the IATAC Information Assurance Tools Database. It summarizes the pertinent information, providing users with a brief description of available tools and contact information. As a living document, this report will be updated periodically as additional information is entered into the Information Assurance Tools Database. Currently the IA Tools database contains descriptions of 38 tools that can be used to support vulnerability and risk assessment.

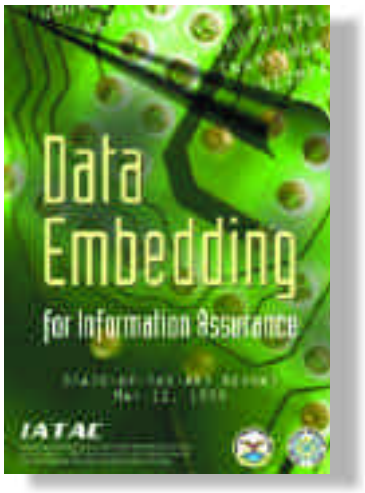
Data Mining CR/TA

This report provides an overview of data mining techniques, applications, and COTS data mining software products. Data mining is used to discover previously unknown and meaningful relationships by sifting through large amounts of stored data. Data mining has applications in marketing, information assurance, risk management, and fraud management. To help users select a product that best meets their objectives, data mining tool evaluation criteria are provided. A table summarizing the features of available products is also provided.



Intrusion Detection Tools Report 2nd Ed.

This newly updated report provides an index of intrusion detection tool descriptions contained in the IA Tools Database. Research for this report identified 46 intrusion detection tools currently employed and available.



Data Embedding for IA SOAR

Provides an assessment of the state-of-the-art in data embedding technology and its application to IA. It is particularly relevant to: information "providers" concerned about intellectual property protection and access control; information "consumers" who are concerned about the security and validation of critical information; and law enforcement, military, and corporate organizations concerned about efforts to communicate covertly. The report has been specifically designed for readers who are not experts in data embedding. For more in-depth information, the bibliography provides an extensive list of authoritative sources from which the reader can obtain additional technical detail.

Computer Forensics—Tools and Methodology

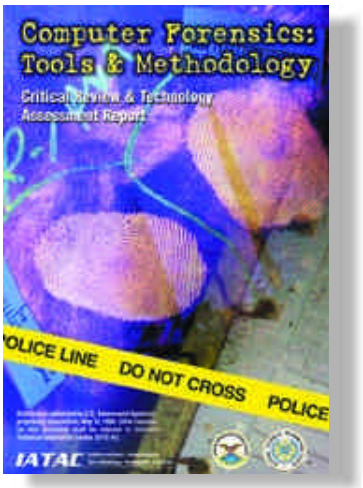
This report provides a comparative analysis of currently available software tools used in computer forensic examinations. It provides a useful introduction to this specific area of science, and offers practical high-level guidance on how to respond to computer system intrusions. This report provides a useful analysis of specific products, including their respective capabilities, unique features, cost, and associated vendors.

Firewall Tools Report

This report provides users with a brief description of available firewall tools and contact information. Currently the IA tools database contains 46 firewall tools that are available in the commercial marketplace.

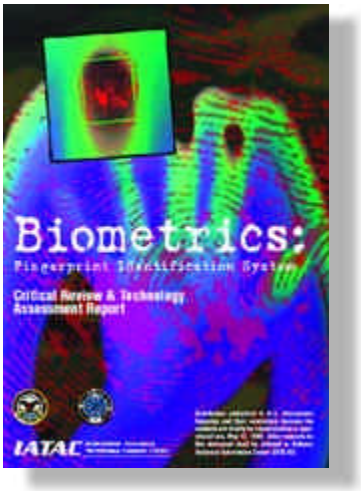
Malicious Code Detection SOAR

This report includes is a taxonomy for malicious software providing a better understanding of commercial malicious software. An overview of the state-of-the-art commercial products and initiatives, as well as future trends is presented. The report presents observations and assertions to support the DoD as it grapples with this problem entering the 21st century. This report is classified and has a limited release.



Modeling & Simulation Technical Report

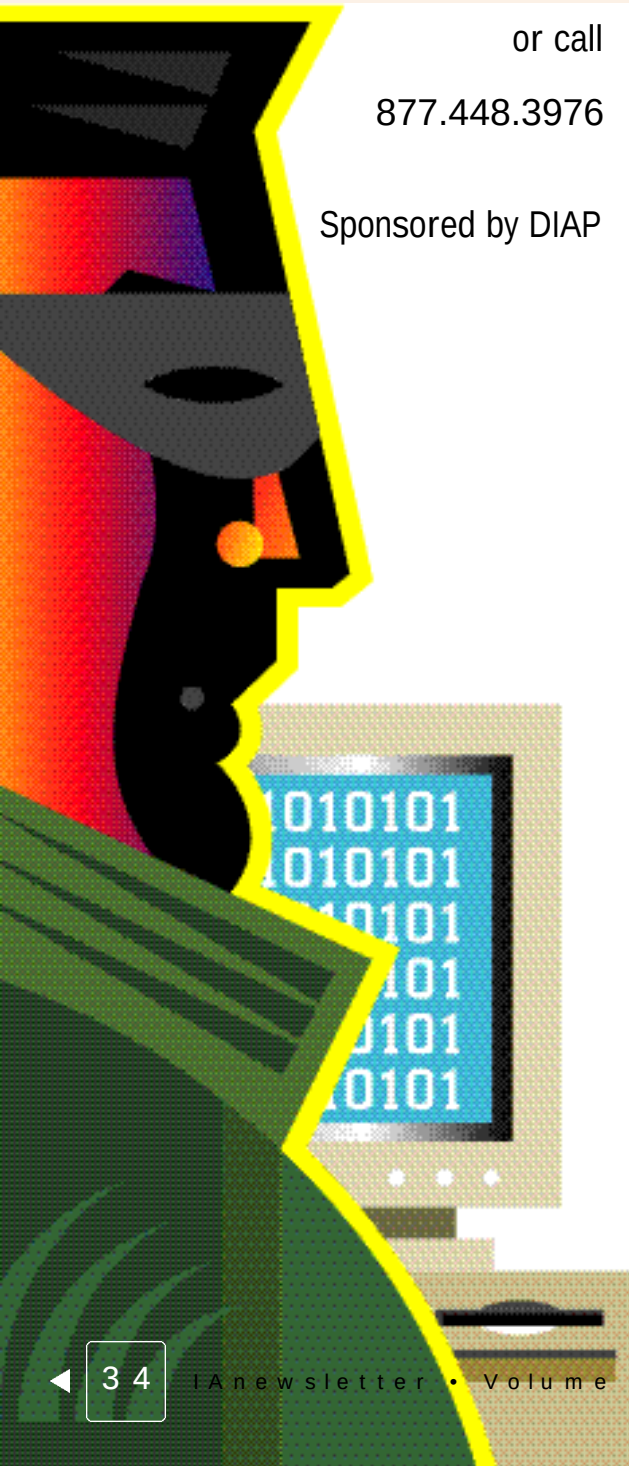
This report, released December 1997, describes the models, simulations and tools being used or developed by organizations within DoD.



Biometrics: Fingerprint Identification Systems

Focuses on fingerprint biometric systems used in the verification mode. Such systems, often used to control physical access to secure areas, also allow system administrators access control to computer resources and applications. Information provided in this document is of value to anyone desiring to learn about biometric systems. The contents are primarily intended to assist individuals responsible for effectively integrating fingerprint identification products into their network environments to support the existing security policies of their respective organizations.

Order Form on Page 35



Distributed Denial of Service Tools

continued from page 12

vice attack occurs, connectivity may have to be restored selectively starting with critical systems.

- **Define what is acceptable as an outage.** Most of the observed attacks have only lasted 3-5 hours. A possible response may be to wait for the attack to subside on its own. Any useful response may take several hours to diagnose and execute.

- **Be able to rule out normal network outages and configuration errors.** Most outages that a site experiences are the result of normal hardware failures and configuration errors rather than the result of a malicious attack. It is essential that the true cause of an outage be identified so the proper fix-action plan can be applied.

- **Be prepared to use a network sniffer/analyzer on the enclave's NIPRNET connection.** If a site is under a network attack, information from these tools will be invaluable in taking prudent countermeasures. Remember, remotely controlled/accessed sniffers will likely be inaccessible as a result of the attack.

- **Know who your upstream provider is.** If a site is under an attack, blocking the attack must happen upstream of the target to be effective. Sites should contact either their appropriate Service CERTs or the DoD-CERT for support in the event of an attack.

For more information

DoD-CERT has released both technical tool reports and situational awareness reports on the known Distributed Denial of Service tools on their homepage: http://www.cert.mil/reports/tools/index.html http://www.cert.mil/reports/sitaware/index.html

In addition, DoD-CERT and other security leaders from the industry attended a "Distributed-Systems Intruder Tools" workshop hosted by CERT/CC in November 1999. The results of the workshop may be obtained at: http://www.cert.org/reports/dsit_workshop.html

For up-to-date security information, users can visit the DoD-CERT Web site at http:/www.cert.mil. Users can also contact the DoD-CERT via the following methods:

Phone: 703.607.4700
800.357.4231
DSN 327.4700

E-mail: cert@cert.mil

1Lt Brian Dunphy, USAF, is on the Senior Technical Staff of the DoD Computer Emergency Response Team, Defense Information Systems Agency, Arlington, VA. He received his B.S. in Electrical and Computer Engineering from Carnegie Mellon University in May 1996. He may be reached at bpd@assist.mil.

order form

IMPORTANT NOTE: All IATAC Products are distributed through DTIC. If you are NOT a registered DTIC user, you must do so PRIOR to ordering any IATAC products. TO REGISTER ON-LINE: http://www.dtic.mil/dtic/regprocess.html.

Name_____DTIC User Code _____

Organization _____Ofc. Symbol _____

Address_____ Phone _____

_____ E-mail _____

_____ Fax _____

DoD Organization? O YES O NO If NO, complete **LIMITED DISTRIBUTION** section below.

LIMITED DISTRIBUTION

In order for Non-DoD organizations to obtain LIMITED DISTRIBUTION products, a formal written request must be sent to IAC Program Office, ATTN: Sherry Davis, 8725 John Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218

Contract No. _____
For contractors to obtain reports, request must support a program & be verified with COTR

COTR _____ Phone _____

Technical Reports

O Biometrics O Computer Forensics O Defense in Depth O Data Mining
O IA Metrics O Modeling & Simulation

IA Tools Report

O Firewalls O Intrusion Detection (2nd Ed.) O Vulnerability Analysis (2nd Ed.)

State-of-the-Art Reports

O Data Embedding for Information Assurance O Visualization

O Malicious Code Detection [o TOP SECRET o SECRET]

Security POC Security Phone

UNLIMITED DISTRIBUTION

Newsletters *(Limited number of back issues available)*

o Vol. 1, No. 1 o Vol. 1, No. 2 o Vol. 1, No. 3
o Vol. 2, No. 1 o Vol. 2, No. 2 (soft copy only) o Vol. 2, No. 3 o Vol. 2, No. 4
o Vol. 3, No. 1 o Vol. 3, No. 2 o Vol. 3, No. 3

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

_____

_____

Once completed, fax to IATAC at 703.289.5467

calendar

April 25—27

DISA Annual DII Conference
Arlington, VA
Call Ms. Linda Scofield
703.607.6514
disaco@ncr.disa.mil

April 25—27

Fiesta Informacion 2000
San Antonio, TX
Call J. Spargo & Associates
703.631.6200
COME SEE OUR BOOTH!

May 8 - 12

DoD Computer Crime Workshop
Colorado Springs, CO
Call 877.4IT.EXPO
(877.448.3976)
www.TechnologyForums.com

May 16

IAC Awareness and Business Meeting
Dayton, OH
Call Donna Egner, SURVIAC
937.255.4840
E-mail: degner@bah.com
COME SEE OUR BOOTH!

June 6—9

2000 Annual USPACOM IA Conference
Ilikai Hotel, Honolulu, HI
Call Maj Veronica Baker
808.477.1046
vlbaker0@hq.pacom.mil

June 8

Information Assurance Technical Framework Forum
Gaithersburg, MD
Subject: PKI/KMI
Call Mr. John Niemczuk
410.684.6246
http://www.iatf.net

July 20

Information Assurance Technical Framework Forum
Linthicum, MD
Subject: "Detect and Respond"
Call Mr. John Niemczuk
410.684.6246
http://www.iatf.net

IATAC

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