REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE Fall 1999	3. REPORT TYPE AND DATES COVERED Newsletter Vol. 3 No. 2

4. TITLE AND SUBTITLE
IA Newsletter
The Newsletter for Information Assurance Technology Professionals

5. FUNDING NUMBERS

6. AUTHOR(S)
Information Assurance Technology Analysis Center

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

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

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 Words)*

IA Newsletter 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). Featured in the issue:
Defense in Depth
DoD Y2K Computer Security Tips
Special Section: JTF-CND Component Commands

14. SUBJECT TERMS
Information Security, Information Assurance, Defense in Depth, Information Operations, Computer Security

15. NUMBER OF PAGES
27

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	None

DTIC QUALITY INSPECTED 4

20001027 068

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

01001001SECUREMESSAGING100100010010

Fall 1999 • Vol. 3 No. 2

Defense in Depth

page 3

also inside

DoD Y2K Computer Security Tips

Special Section on the JTF-CND Component Commands

1001001010100100010011NTRUSIONDETECTION01001001010

0100CERTIFICATION&ACCREDITATION1001001001

101000100ISTRONGPASSWORDS1010010010

contents

on the cover

ia initiatives

in each issue

Information Assurance Through

Defense in Depth

Our armed forces increasingly rely on critical digital electronic information capabilities to store, process, and move essential data in planning, directing, coordinating and executing operations.

Lt Col (Select) Bradley K. Ashley, USAF
Gary L. Jackson , Ph.D.

The physical analogy for this strategy is the formidable layered defenses of the medieval castle.

However, many of these systems have security weaknesses that can be exploited by powerful and sophisticated threats, which could result in unauthorized access, destruction, disclosure, modification of data, or denial of service. Such system vulnerabilities can jeopardize our most sensitive information capabilities. With deep, layered defenses we can reduce vulnerabilities and deter, defeat, and recover from sustained, skillful, and penetrating assaults.

Network Operations (NETOPS) provides the framework and procedures to manage the emerging Global Information Grid (GIG) of networked information capabilities. By integrating information assurance through Defense in Depth with Network Management and Information Dissemination Management (IDM), NETOPS is a key enabler for CINCs to achieve information superiority and accomplish their missions.

A good physical analogy of the fully developed medieval castle offers two valuable principles for designing Defense in Depth of information systems: 1) formidable layered defenses; 2) means to fight back actively. These castles were positioned to control the most significant terrain, serving to secure critical logistics bases and command and control centers for armed forces. Castles were built on strong foundations and often on high ground. They employed successive barriers, including water obstacles (moats), ditches, successive rings of strong and high walls, and towers. This defense structure allowed a relatively small force of well-supplied personnel, sentries, and men-at-arms to fight back and prevail against a much larger adversary. Just as a castle protected critical military resources in the Middle Ages, we must defend and protect our vital military information today.

The Defense in Depth approach employs and integrates the abilities of people, operations, and technology to establish multilayer, multidimensional protection—like the defenses of a castle. The approach employs successive layers, using a variety of methods

at multiple, key locations, to prevent the potential breakdown of barriers and penetration to the innermost areas of the system. In a simple successive-barriers strategy, the barriers might all use the same method, presenting an adversary who breaks down one barrier

Network Operations (NETOPS) Model

with another, and another, and another. But a simple strategy of redundancy will probably have little effect against different attack methods. To counter the variety of attack methods that may be used today, we must employ a comprehensive variety of security mechanisms that provide redundant protection. To block attempts to gain access and do harm at different locations in the protected environment, we must also deploy defenses at multiple locations. No critical sector or avenue of approach into the sensitive domain of the information system should be uncontested or unprotected.

People

To establish this protection, Defense in Depth integrates the abilities of people, operations, and technology.
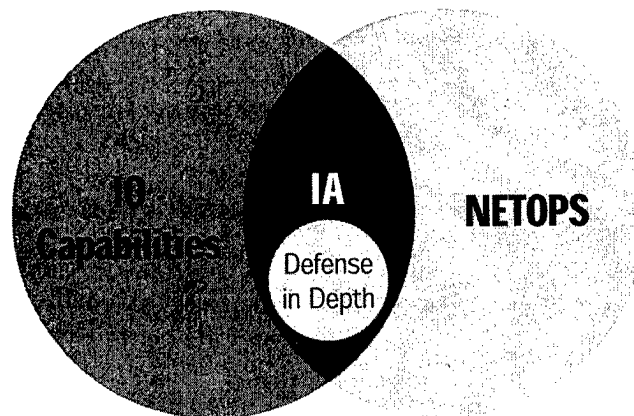
People using technologies to conduct operations are the strategy's central element. People design, build, install, operate, authorize, assess, evaluate, and maintain protection mechanisms. To gain and maintain the knowledge and expertise needed to perform these vital tasks, a comprehensive program of education, training, practical experience, and awareness is needed. We must recruit, retain, and wisely assign the best talent available. We also need a highly reliable personnel security system of appropriate background investigations, security clearances, credentials, and badges to ensure that only trustworthy persons have access. Finally professionalization and certification are important tools in

Information Operations
Capabilities

Network Operations of the
Global Information Grid

How NETOPS Fits with Information Operations

developing a validated and recognized cadre of experts and providing additional motivation for staff.

Operations

IA operations, the second element in the strategy, involves policy, procedures, and execution. IA policy drives operations by establishing goals, courses of action, and standards. It formally states the security requirements for information systems, what must be protected, how resources are used, and what must be done and not done. Policy also establishes standards that define uniform and common features and capabilities of security mechanisms, the rule or basis by which to measure the various dimensions of information assurance, and the desired or required level of attainment. Standard operating procedures (SOP) are then needed to ensure adequate implementation of the prescribed policies. The SOP should define system configuration, deployment, routine operations, and incident response and reporting. Defined

procedures for addressing incidents are particularly critical. After an intrusion is detected, incident information must be reported through established channels to appropriate authorities and specialized analysis and response centers. Incident response should then begin with immediate local emergency damage-limitation and survivability actions. These steps should all be stated in the SOP and implemented promptly. Regional and national experts might need to become involved when more sophisticated methods are necessary to confirm attacks, determine effects, and track down perpetrators. Execution of these tasks may be quite difficult when distributed, coordinated, low-visibility network-based attacks occur across many systems over an extended period of time. Careful, effective, and timely decisions must be made concerning appropriate additional responses, such as: declaring a higher level security situation or information operations condition (INFOCON), isolating affected systems, or pursuing legal, diplomatic, economic, or military actions. Operations also includes improving situational awareness, conducting IO-related exercises, and performing vulnerability assessments to improve our security posture.

Technology

The technology element of Defense in Depth focuses on four major areas

- Networks that link enclaves
- Enclave boundaries
- Local computing environments, or enclaves, and
- Supporting infrastructures.

Technology to Defend Networks

Redundant and multiple data paths offer more than one available alternate physical medium or route for data transport. These measures serve to ensure continued transmission when intermediate enclaves or network components are degraded or inoperable. Enclaves should be able to disconnect from external networks in a crisis, filter traffic to prevent the use of risky message segments, and control throughput. Provisions against denial of service should be included in agreements for commercial services—to avoid a single point of failure. In addition, automated tools for system monitoring and management should be employed on the network to collect and analyze observable phenomena and maintain knowledge of the status of systems. These tools should be able to detect disruption and degradation that can indicate security problems.

Technology to Defend the Enclave Boundary

Defense of the enclave boundary is geared toward ensuring that all outside systems that seek access meet the security criteria of the enclave. Boundary defenses protect inside data and services from outside dangers. They also protect systems within the enclave that do not have their own self-defense capabilities. Some of the technologies to defend the enclave boundary are:

- Identification and authentication tools,
- Personal Identification Numbers (PINs),

- Passwords,
- Biometric mechanisms,
- Firewalls,
- Malicious code and virus detectors,
- Intrusion detection and response tools, and
- Guards.

Technology to Defend the Local Computing Environment

In defending the local computing environment, the IA challenge is to provide selected mechanisms (such as protected distribution systems) for protection. In addition, effective tools must be used to deepen the defense by protecting the end-systems and capabilities and their internal components and associated peripheral devices. Technologies used for this purpose include:

- Passwords, PINs, tokens, and biometrics,
- Encryption,
- Digital signatures,
- System monitoring and management tools,
- Intrusion detection tools,
- Malicious code and virus detectors,
- Backup technologies, and
- Software with its own access control features.

Supporting Infrastructures

All military organizations and operations, including IA, require a logistics structure to provide essential resources and support for maintenance, repair, and other vital services. Many of these services are provided across garrison and deployed environments. IA Defense in Depth also requires specialized support from
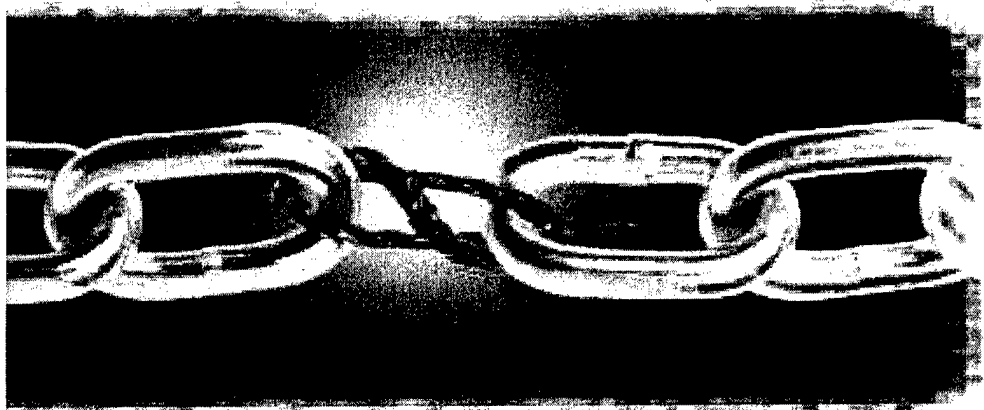
unique cryptographic capabilities and organized incident reporting and response.

The cryptography function must be resourced and managed to meet or exceed all requirements without disclosure or theft. We must continue to design and field equipment and must be delivered to organized capabilities in the chain of command, especially at the Military Department and Service, regional, and national/ global levels. Intrusion detection information must be forwarded to specialized structures with the ability to perform more sophisticated analysis and correlation of indi- in all types of operations. At the same time, however, adversaries will be able to acquire and use these technologies against our critical and mission-essential systems. Therefore, we must maximize the contributions of certified experts, employ disciplined operations guided by policies and using sound successful procedures, and field proven, reliable technological solutions. In these efforts, the human factor is and will continue to be essential. It takes people to make and use technologies and to conduct IA operations. IA Defense in Depth depends on each of us. We must master new technologies, watch for new and changing threats and vulnerabilities, and continue vigorous efforts to build a formidable IA Defense in Depth.

Lieutenant Colonel (Select) Bradley K. Ashley, US Air Force, is the Senior Information Operations (IO) Policy and Doctrine Officer, Joint Staff, C4 Systems Directorate (J-6), Washington, D.C. He is also the lead Joint Staff Officer for Information Assurance (IA) policy and doctrine, IO education, training, and awareness, Joint and CINC IO exercises, and a member of the IO Response Cell responding to real-world DoD computer network attacks. He received his M.S. from the U.S. Naval Postrgraduate School in 1990. He may be reached at ashley-bk@js.pentagon.mil.

Gary L. Jackson received his Ph.D. in Government from Georgetown University in 1985. He is a former staff Fellow in Political-Military studies at the Center for Strategic and International Studies (CSIS) and a retired U.S. Army Military Intelligence officer. Doctor Jackson supports the Joint Staff (J6) C4 Systems Directorate as a senior systems engineer working in the field of information security. He may be reached at 703.676.4160.

We are only as strong as our weakest link!

associated software that are reliable, fast and secure. There must be a strong system to produce, distribute, and manage public and private keys as well as digital certificates. Efforts are under way to improve the system by merging the current primary infrastructures for classified keys (Electronic Key Management System) and unclassified public keys (DoD Public Key Infrastructure).
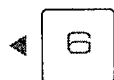
Detection, reporting, and response infrastructures are essential in discerning whether an intrusion is a local, isolated event or part of a more widespread, sustained, dangerous attack. The outputs from local use of tools and intrusion detection and response actions cations from a range of sources and agencies. DoD is now constructing and improving a global infrastructure to manage incident reporting and enable a coordinated, coherent response. Efficient operation of this infrastructure requires standardized reporting formats and procedures, automated support to transfer and analyze relevant data, and effective interface with other response capabilities.

The information assurance Defense in Depth approach will give us the ability to meet the tremendous IA challenges we face today and will face in the future. The complexity and power of electronic digital computing and telecommunications systems will increase, and our forces will continue to take full advantage of these capabilities

Matrix Mission Planning
in Information Operations

n 1995 I left the comfort and sanctuary of the Navy's EA-6B community at Whidbey Island, Washington, to assume the post of Fleet Electronic Warfare Officer of the U.S Second Fleet in Norfolk, Virginia. On the way, I attended a newly created course at the Armed Forces Staff College (AFSC) in Norfolk called Command and Control Warfare (C2W). Little did I know when I attended this course that within a month of my arrival at Second Fleet I would be up to my neck in what is now known as information operations (IO). My assignment as fleet Electronic Warfare officer was twofold. First, draft the first-ever C2W appendix to a large force exercise operations order (OPORD). Second, develop a fully integrated Joint Task Force (JTF) C2W strategy supporting the commander's intent and objectives. The first task was a snap. My training at AFSC provided me with the fundamentals I needed to breeze through the OPORD writing process. The C2W appendix was completed in record time. The remaining task, however, was daunting to say the least. I was overwhelmed. AFSC taught me the goals of a C2W strategy but never showed me how to actually build one. Since I was the only trained C2W guy on the Second Fleet's staff, the task of executing C2W doctrine fell squarely on my shoulders. **Enter Matrix Mission Planning (MMP).**

It soon became readily apparent that the one thing an information operations planner needs most is information—and lots of it. I studied the objectives of both the Commander-in-Chief (CINC) and the JTF Commander to derive a clear understanding of the operations timeline and the implied and specified tasks of the subordinate commanders. Armed with this knowledge, I still could not

CDR Mark L. Nold, USN

could use this format to balance C2W capabilities with JTF objectives and tasks (Figure 2 on page 8). I could now easily lay out a general C2W strategy that truly complemented JTF objectives and fully integrated C2W in support of the campaign. Our meager staff of three worked

Figure 1. Matrix of JTF Objectives and Tasks

tie all the information together. After a number of frustrating attempts, I began to lay out JTF objectives and tasks in a matrix to visualize the sequence of events that would take place in the operation (Figure 1). Lightning struck! I realized that I

diligently to develop the general C2W strategy that we would present to the JTF commander (see Figure 3 on page 8).

The boss was impressed and we embarked on the development of specific matrices (Fig-

ure 3) for each of the C2W capabilities in our arsenal (OPSEC, military deception, PSYOP, destruction, and electronic warfare). The matrices provided us with detailed plans for each capability, which were synchronized along the same timeline with the general C2W strategy, allowing us to identify showstoppers, specify required assets, and ensure that our strategy was sound and executable (Figure 4). In addition, we created specific matrices for other capabilities that would be integral to the strategy (Special Operations Forces support, surveillance, and C2 Protect) (see Figure 2).

Once the C2W (IO) Cell was established aboard the flag ship (U.S.S. Mt. Whitney), the general and specific matrices were submitted for refinement and finalization of the strategy. The finished product allowed the cell to generate the C2W target set needed for facilitating the strategy and to begin lobbying component representatives to rank our targets high on the Joint Integrated Prioritized Target List (JIPTL).

We had done it!

But we still had to see our plan through to execution. There were a thousand moving parts, each one critical to the plan. To manage this behemoth, we pulled every event from the matrices and created a single execution checklist (Figure 5), which described each event in detail in terms of date, time, executing unit, target, linked or other dependent events, and objectives. The Current Operations branch of the cell (not a

Figure 2. Balancing C2W Capabilities with JTF Objectives

doctrinal entity) tracked the progress of this checklist. Current Operations then provided feedback to the cell, where the strategy was reassessed and modifications were developed based on its success or failure in particular events.

The exercise was a success from an IO point of view, and matrix planning was the key. The process has evolved since that first effort, but the approach pioneered in the initial attempt has been repeated successfully several times since its creation.

Figure 3. C2W Capability-Specific Matrices

Matrix mission planning can work for you. It provides a sound mechanism that ensures that IO is fully integrated as it was intended—as a synergistic, supporting strategy that optimizes capability in relation to need. As the IO arena expands, the need for an organized approach to IO strategy planning becomes more and more critical. MMP is a vehicle that can ensure future capabilities are integrated seamlessly and effectively in information operations.

Matrix Mission Planning methods are now taught as part of the Armed Forces Staff College Joint Command and Control and Information Warfare School (JCIWS) curriculum. ⌄

Figure 4. Executable Checklist

Commander Nold received his B.S. in biology from Fort Hays State University in 1978 and commissioned a Second Lieutenant in the U.S. Marine Corps. In 1989 he transferred to the U.S. Navy. CDR Nold obtained his M.B.A. in Business Administration (Quality Management) from City University in 1994 and assumed command of the Electronic Attack Weapons School in April of 1999. He may be reached at noldml@yahoo.com.

Figure 5. Detailed Planning

ACERT/ ARFOR-CND

MAJ Glen Teasley, USA
MAJ David Papas, USA

As the Army expanded its efforts against hackers, the Army Computer Emergency Response Team (ACERT) expanded its protection of the Army's electronic highways using the latest in technology and the best in expertise. The ACERT is the Army's operational element for computer network defense. It conducts command and control protection operations in s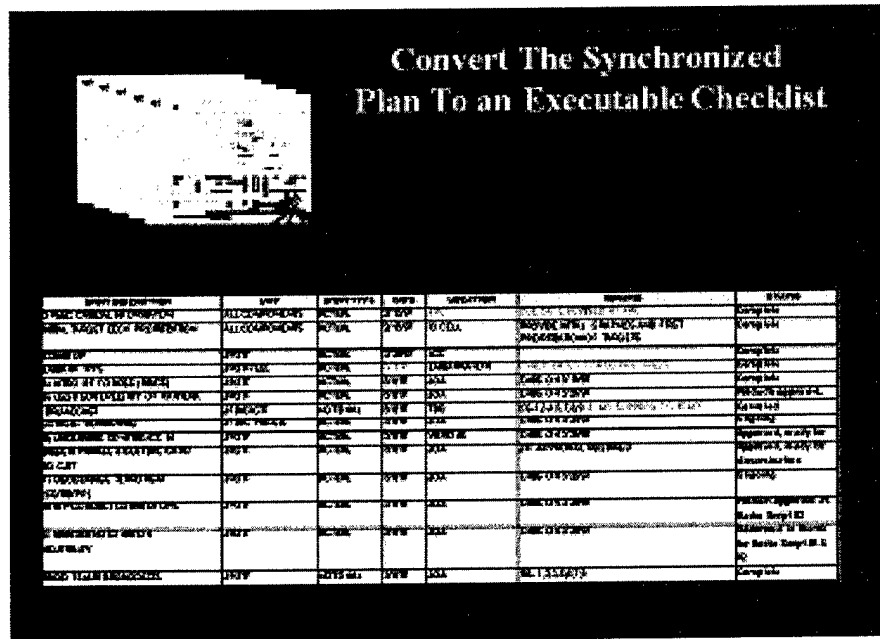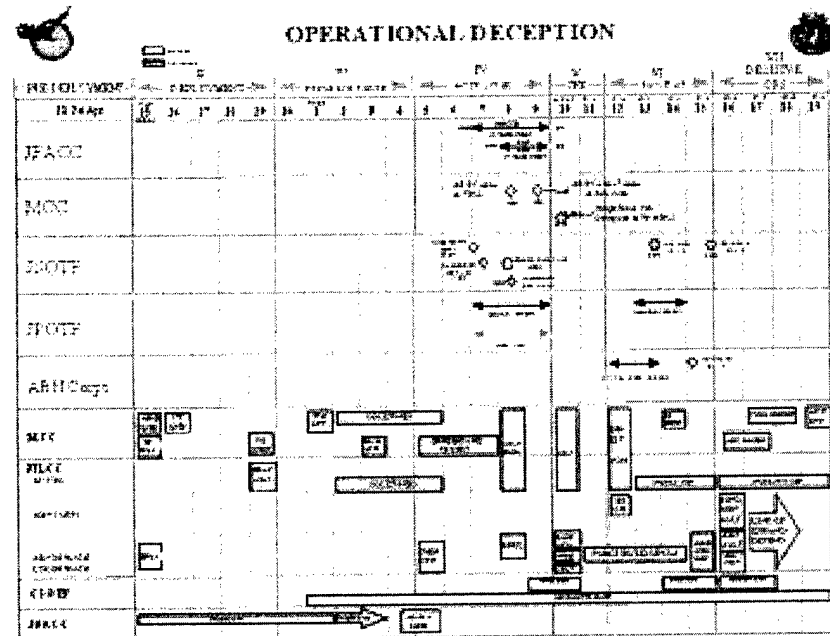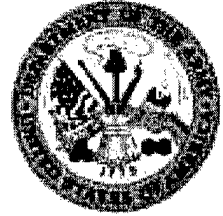upport of the U.S. Army to ensure the availability, integrity, and confidentiality of the information and information systems used by commanders worldwide. The ACERT is a division of the Land Information Warfare Activity (LIWA) located within the U.S. Army Intelligence and Security Command at Fort Belvoir, Virginia.

The ACERT consists of three branches: the regional CERT (RCERT) branch, the coordination center branch, and the computer defense assistance branch (Figure 1).

The RCERT branch manages the functional and operational support requirements of the four field RCERTs—RCERT Pacific at Fort Shafter, Hawaii; RCERT Europe in Mannheim, Germany; the RCERT Continental United States (CONUS) at Fort Huachuca, Arizona; and RCERT Korea in Taegu, Korea. The RCERTs are co-located with Army Signal Command's (ASC) Theater Network and Systems Operation Centers (TNSOC). By leveraging both the ASC's network operational function and the ACERT's network security function, each area of responsibility receives enhanced network support and constant vigilance for network security. The close working relationship between the ACERT, RCERTs, and the TNSOCs ensures the Army's ability to communicate worldwide is successful and accomplished in a secure manner.

The coordination center branch receives computer incident and intrusion reports, conducts analysis of vulnerabilities, provides technical assistance to network and system administrators and managers, analyzes new viruses and anti-virus software, and monitors network intrusion devices that support the Criminal Investigation Command (better known as CID) investigations.

The computer defense assistance branch provides a tool for Army commanders and their staffs to use in assessing their network security. The program is designed as a "white hat" external assessment; the results are shared only with the unit assessed. Commanders use the information to improve their network
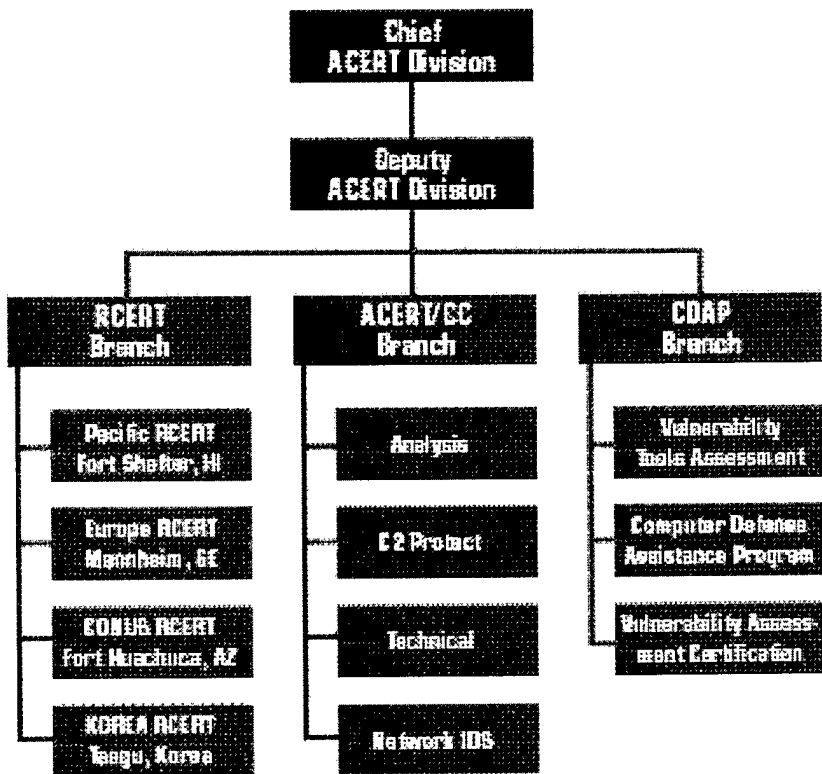

Figure 1. ACERT Organizational Structure

security and lessen the vulnerabilities that may allow unauthorized access.

Program objectives focus on ensuring the overall security configuration of the networks and identifying potential points of unauthorized access into networks. Objectives also focus on validating vulnerabilities and assessing the depth and degree of a potential compromise, and recommending methods, techniques, and configuration modifications needed to secure the scanned networks.

In December 1998 the Army deputy chief of staff designated the ACERT as the Army force for the Joint Task Force – Computer Network Defense

(JTF-CND). In this capacity, the director of the LIWA serves as the commander of Army forces and ensures the security of all Army networks. On a daily basis, the ACERT is fully engaged as a synchronized component of the JTF-CND team, protecting Department of Defense (DoD) networks worldwide.

The ACERT, in its mission to protect Army networks, coordinates daily with organizations both internal and external to the Army. Coordination within the Army includes the offices of the deputy chief of staff for operations, Office of the Director of Information Systems for Command, Control, Communications and

Computers (ODISC4), Deputy Chief of Staff for Intelligence, ASC, and CID. The ACERT coordinates with the following organizations and agencies outside of the Army: Air Force CERT, Navy Computer Incident Response Team, DoD CERT, Marine Corps' Marine Intrusion Detection Analysis Section (MIDAS), Coast Guard CERT, Federal CERT, Carnegie Mellon University (CMU) CERT, and the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center. Coordination encompasses collaboration and technical efforts involving vulnerabilities and their recommended solutions.

Army Information Assurance Vulnerability Process

Triggers:

- DISA MSG
- ODSC4 Directed
- Reported Case of NEW VIRUS
- Vendor-Identified Vulnerabilities
- CERT-Identified Issues
- Incident/Intrusion Analysis

RCERTs AOR Validation

ANSOC Network Validation

ACERT MSG via LISTSERVER & SENSER

MACOM Suspense to Acknowledge Receipt

MACOM Suspense for 100% Compliance

Verification & Validation

Average of 5–7 Working Days

Average of 14–30 Working Days

ACERT Web Page

Distributed Visibility   Centrally Managed

ACERT Maintains MACOM Reporting Compliance

Total   None
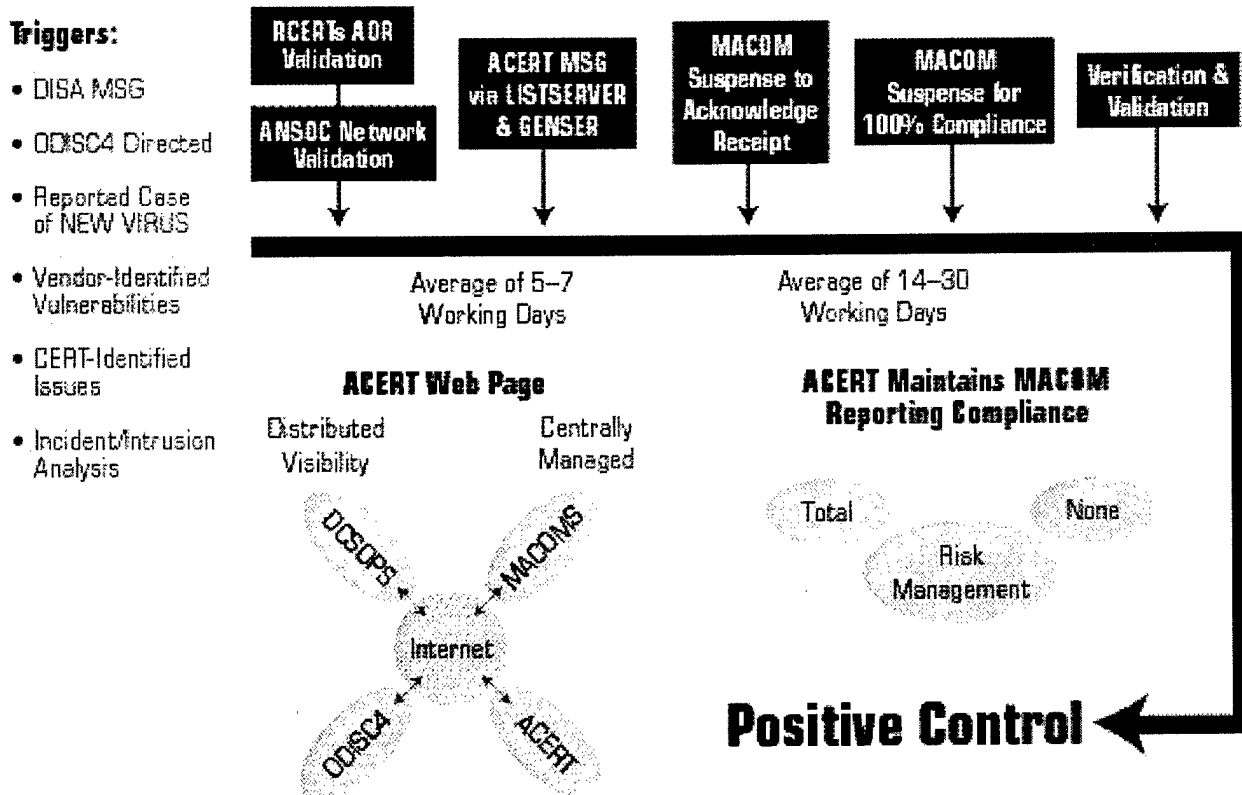Risk Management

Internet

Positive Control

Figure 2: Army Information Assurance Vulnerability Process

Contacting the ACERTs and RCERTs

ACERT

Commercial   1.888.203.6332
Internl. DSN: 312.235.1113
Comm. Fax: 703.806.1152
DSN Fax: 656.1152
Secure Fax: 703.806.1004
DSN Secure Fax: 312.656.1004
E-mail:
    acert@liwa.belvoir.army.mil
SIPRNET E-mail:
    acert@liwa.army.smil.mil
SIPRNET URL:
    www.acert.belvoir.army.mil

RCERT — CONUS

DSN: 879.2482
Commercial: 520.538.2482
E-mail: rcert@hqasc.army.mil
SIPRNET E-mail:
    anssm@ns1.army.smil.mil

RCERT — Europe

DSN: 380.5232
Commercial: 011.49.0621.730.5232
E-mail:
    rcerte@hq.5sigcmd.army.mil
SIPRNET E-mail:
    5sig001@66mi.army.smil.mil
URL: www.iwsc.5sigcmd.army.mil

RCERT — Pacific

DSN: 315.438.3121/7999
E-mail:
    pacrcert@shafter-emh3.army.mil
SIPRNET E-mail:
    pacrcert@shafter-emh51.smil.mil

RCERT — Korea

DSN: 315.725.9967
Commercial: 011.82.2.7915.9967
NIPRNET E-mail:
    rcert@aseswho1.korea.army.mil
SIPRNET E-mail:
    rcert@swwnv.army.smil.mil

To capture the massive amounts of data required to maintain situational awareness, the ACERT has developed a database that stores data on all reported or identified incidents and intrusions to Army automated information systems. In addition, the JTF-CND and the service components have developed the Joint CERT Database. This database will allow the ACERT, other service CERT/CIRTs, DoD CERT, and the JTF-CND to share information and conduct analyses on incidents. In this way, all DoD CND elements can share information and protect against identified possible threats.

A system administrator/operator who detects any automated information system security incident is required by regulation (AR 380-19) to immediately report it to the information systems security officer, who will notify the installation systems security manager. Concurrently, the system administrator /operator will notify the appropriate RCERT and request technical assistance. The RCERT verifies that an incident or intrusion has occurred and reports it to the ACERT. If an intrusion has occurred, the ACERT reports it to DCSOPS Information Warfare Office (DAMO-ODI), ODISC4, DoD CERT, and Joint Task Force-Computer Network Defense. The ACERT also notifies both the Army CID's Computer Crime Resident Agency and the Army Central Control Office, U.S. Army Intelligence and Security Command.

The ACERT monitors the Army's Information Assurance Vulnerability Alert (IAVA) process. The IAVA process is a DoD-mandated process for disseminating information and required actions on serious vulnerabilities to or attacks on DoD automated information systems. The ACERT publishes IAVA messages to disseminate information and required actions on new and critical vulnerabilities to automated information systems. IAVA messages are disseminated by a general service message (GENSER) to all Army major commands and by the ACERT list server to all subscribers. IAVA messages are directed by the DoD CERT, Army ODISC4, or the ACERT.

The IAVA process for the Army requires that information assurance officers at major commands report receipt of an IAVA message within 5 days and report compliance with the required actions or submit a waiver within 30 days. This timeline can be accelerated based on the criticaliness of the vulnerabilities addressed (see figure 2 on page 11). The status of major commands' IAVA compliance is monitored in the Army by both the ODISC4 and deputy chief of staff for operations, and in DoD by JTF-CND and the deputy secretary of defense.
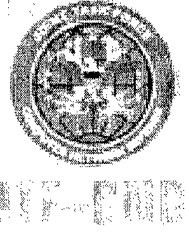
Two initiatives guide ACERT into the future: a fully integrated incident database and predictive analysis.

The predictive analysis process identifies potential attacks against Army networks. Predicting network attacks provides the commander a
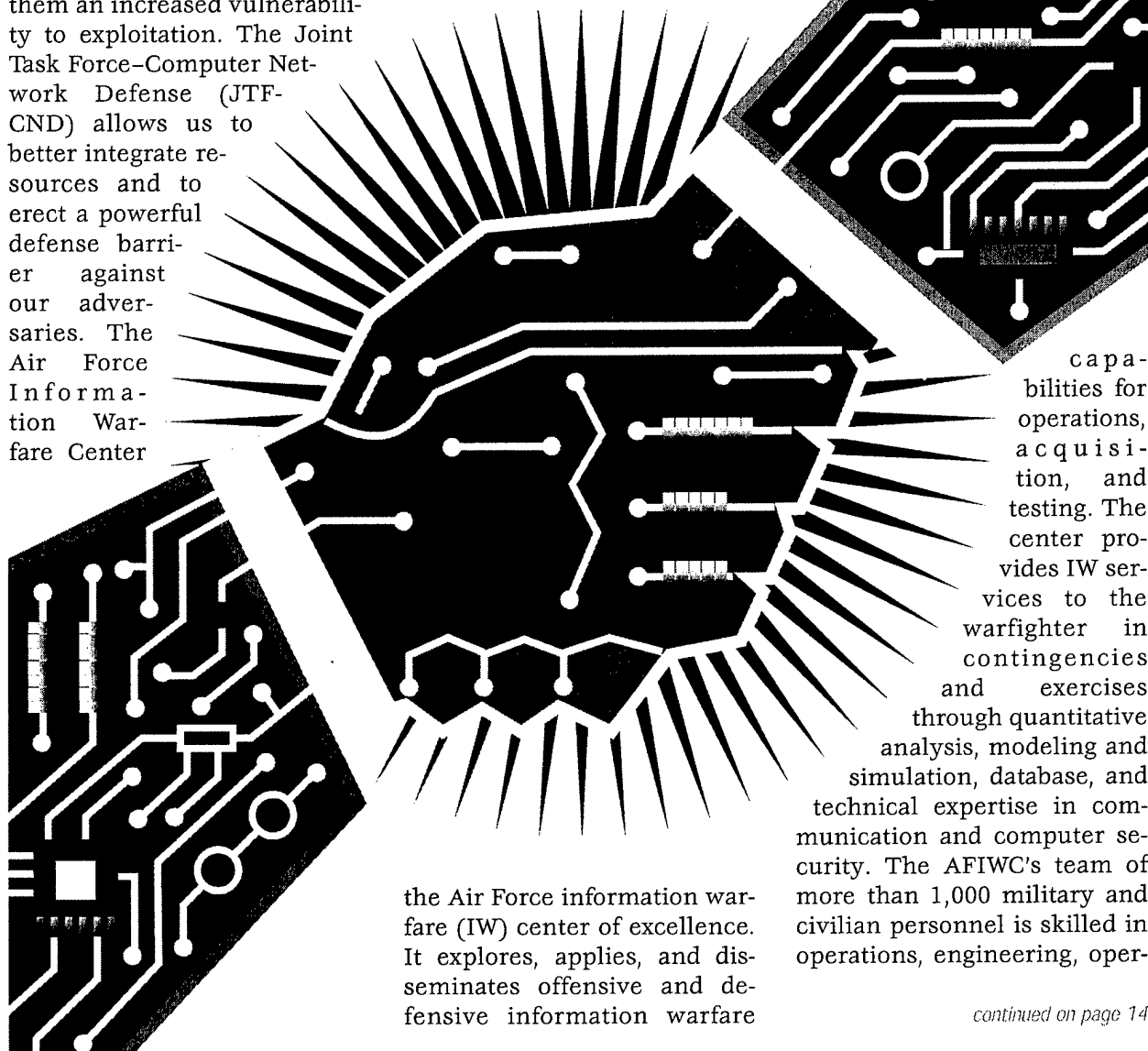
JTF-CND and AFCERT

Allies in the Information War

Capt Karl Grant, USAF
2nd Lt Becca Legé, USAF

With the constant threat of computer attack looming in today's expanding realm of information operations (IO), it is vital that we employ the most advanced tactics in computer network defense (CND). The expansion of global communication lines and the development of new technologies bring with them an increased vulnerability to exploitation. The Joint Task Force–Computer Network Defense (JTF-CND) allows us to better integrate resources and to erect a powerful defense barrier against our adversaries. The Air Force Information Warfare Center

(AFIWC/CC) has been designated as Commander Air Forces (COMAFFOR) for the JTF-CND. Among its responsibilities is coordination of joint defense against computer attacks on DoD information systems.

The AFIWC, co-located with the Air Intelligence Agency, is the Air Force information warfare (IW) center of excellence. It explores, applies, and disseminates offensive and defensive information warfare capabilities for operations, acquisition, and testing. The center provides IW services to the warfighter in contingencies and exercises through quantitative analysis, modeling and simulation, database, and technical expertise in communication and computer security. The AFIWC's team of more than 1,000 military and civilian personnel is skilled in operations, engineering, oper-

ations research, intelligence, radar technology, communications, and computer applications.

Within the AFIWC, the Air Force Computer Emergency Response Team (AFCERT) under the COMAFFOR is the execution element for the JTF-CND. Established in 1992, the AFCERT is the oldest organization of its kind in the Department of Defense and is the focal point for information

Since its inception, the AFCERT has grown and refined its intrusion detection techniques to counter the constantly changing threat to Air Force networks. The team's 94 military, civil service, and contractor personnel monitor networks at more than 120 locations worldwide. The monitoring of these sites is an enormous undertaking. For example, an estimated 6 billion connections were screened in 1998. Of those connections, 68 were identi-

both a real-time warning and detailed information about the activity. The warning and information enable commanders to know where any suspicious activity originates, whether critical information has been compromised or changed, and whether the system in question can be trusted.

On the preventive side, the AFCERT conducts vulnerability assessments on Air Force networks with a software tool set called On-line Survey (OLS). OLS looks for security holes in a network and can detect vulnerabilities that a hacker may use to gain access to an Air Force system. In addition, because OLS operations appear to users and system administrators as unauthorized activity, OLS is used to exercise the bases' or units' activity, detection, and reporting ability.

Incident response is one of AFCERT's most important services. When a suspicious or malicious activity on a system meets a predetermined threshold, the AFCERT - DESIGNATES IT AS AN INCIDENT, initiating a flurry of activity in a very short time. First, the chain of command is notified by the using organization (with the help of the Incident Response Team and the Air Force Officer of Special Investigations [AFOSI]). Depending on the criticality of the affected computer system, a decision is made on whether to isolate the system and pull it off the network. If the computer system is not deemed mission-critical, it may be left on-line so more information can be collected about the hacker. If any type of illegal

Captain Jay Schwitzgabel oversees Staff Sargeant Todd Michael's review of suspicious network connections.

protection of Air Force networked command, control, communications, and computer systems. The AFCERT's primary mission is to provide intrusion detection, vulnerability assessments, and incident response operations 24 hours a day, 7 days a week (24x7).

fied by the AFCERT as attempts to disrupt or exploit Air Force operations.

To aid in screening connections, the AFCERT relies on a tool called Automated Security Incident Measurement (ASIM). ASIM looks for suspicious or malicious traffic crossing Air Force networks, providing

activity is found, the AFOSI gets involved. AFOSI has the option of initiating its own on-site monitoring and pursuing prosecution. The AFCERT provides technical assistance to AFOSI investigations as needed. If it is determined that the base does not have the resources to secure the system or return it to normal operations, the base commander may request AFCERT augmentation. AFCERT and its sister divisions' joint incident response teams stand ready to recover such systems and can deploy to any location with less than 2 hours notice.

To perform intrusion detection, vulnerability assessment, and incident response operations effectively, the AFCERT relies on several organizations. The AFIWC's Countermeasure and Computer Security Engineering Teams provide research and red-teaming support to Air Force organizations and can augment AFCERT operations during OLS assessments, incident responses, and peak periods. AFIWC's Threat Analysis branch provides intelligence inputs, and the 690th Intelligence Operations Squadron's Cyberwatch provides indications and warning data. The Air Force's Network Operations Center is the Air Force's execution element for blocking connections recommended by the AFCERT at the Air Force enterprise-wide routers. Network Operations and Security Centers (NOSCs) and Network Control Centers (NCCs) provide Major Command–level and base-level support thereby channeling vital information to the AFCERT and ensuring that downward-directed

tasks are completed. The continued success of the AFCERT is due in part to the outstanding assistance and support that these organizations provide.

As the Air Force component lead to the JTF-CND, the AFCERT reports intrusion detection and incident response information and coordinates Air Force support to meet JTF-CND directives. In addition, the AFCERT assists with policy and procedural development and implementation. The AFCERT and AFIWC have been involved in several JTF-CND initiatives to standardize reporting processes across the Unified Command Commander-in-Chief (CINC)–Service–Agency (C/S/A) spectrum. Among the many projects to which the AFCERT, its sister divisions, and the AFIWC have contributed are the Joint Threat and the Joint CERT databases. These are two systems that will improve the JTF-CND's ability to correlate incoming information and coordinate an appropriate response to suspicious activity that crosses C/S/A boundaries. The AFCERT, its sister divisions, and the AFIWC have represented Air Force interests at numerous JTF-CND conferences and exercises and will continue to provide the support needed for the successful defense of Air Force and DoD network systems.

The interface between the AFCERT and operational units is the Information Warfare Flight (IWF) at the Numbered Air Forces. It is critical that the CINCs have the tools and the knowledge they need to make informed decisions for their units about CND. One of

the roles of the IWF is to provide this support by integrating IW activities into the normal campaign planning and execution process. By giving AFFOR a single IW focal point, the IWFs provide the structure to plan and execute IW for the warfighter. In doing so, they provide the reach-back capability to enable units to conduct 24 x 7 operations real-time. As Col Richard Stotts, AFIWC/CC, said in his address to the Armed Forces Communications and Electronics Association Symposium, "To operationalize [Defensive Counter Information], we must look at all the resources necessary to promote our information resource as a weapon system if we are to achieve the greatest use and protection of our information." With the AFCERT's support and resources to the IWFs, we can ensure that our units are well informed and prepared to handle any attack on their networks.

Information superiority is critical in today's defense of DoD computer systems and networks. Coordination of effort in the JTF-CND and integration of DoD resources in all facets of IO enables us to fight aggressively and win the information war. ✓

Captain Grant received his B.S. in Computer Science from Embry-Riddle University, Prescott, Arizona. He supports AFCERT Operations at the Air Force Information Warfare Center. He may be reached at 210.977.3158.

2nd Lieutenant Legé received her B.S. in physics from Loyola University, New Orleans, Louisiana. She may be reached at ralege@afiwc.aia.af.mil.

Marine Forces
Computer Network Defense

MARFOR·CND

Any Marine will tell you that the Fleet Marine Force (FMF) is the place to be if you want to be a real Marine. Operational commitments, deployments, leadership in the face of adversity—all the activities you've read about—happens out in the FMF. Unfortunately, a set of orders to report to a job inside the beltway (the highway surrounding the Washington, D.C. metropolitan area) is usually the first step toward a lifelong commitment as a desk jockey and sworn enemy of the nation's forests. You trade all
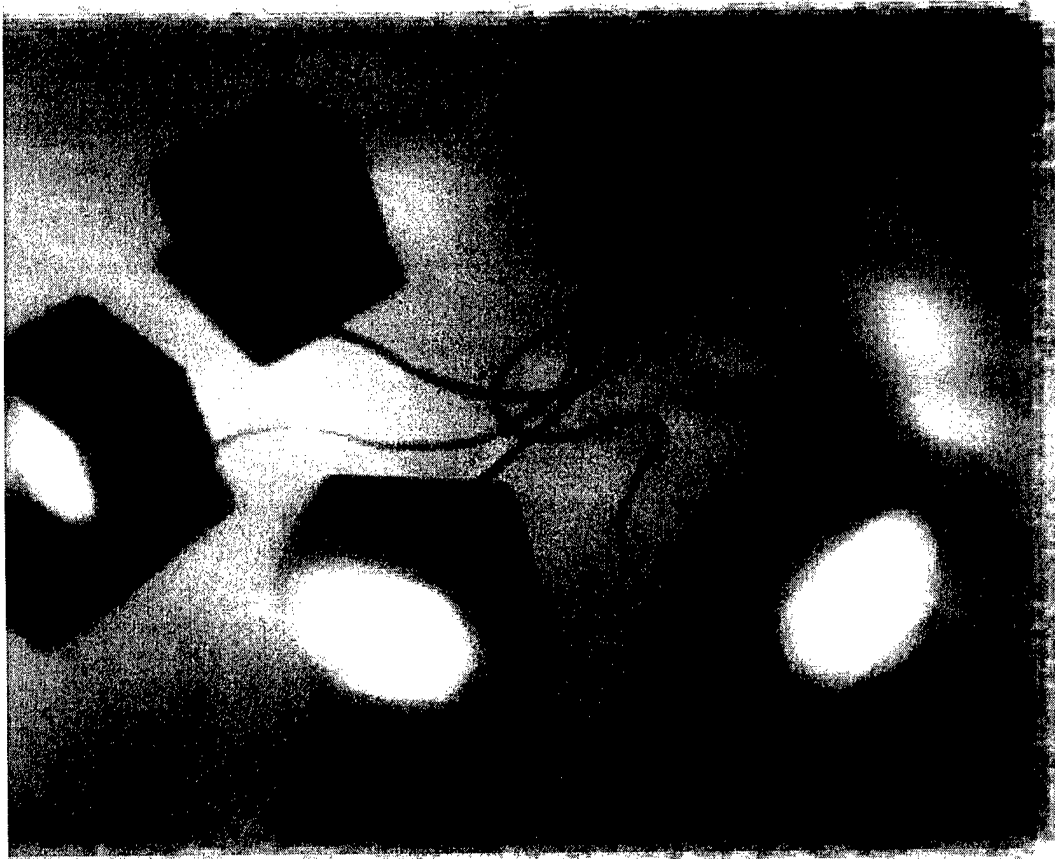
the fun of being an FMF Marine for 2 hours a day in a Route 95 van pool that now dictates the exact number of hours you spend at work. The Marines with whom you sweated, struggled, and persevered in the streets of Pohang are now replaced by government service employees and contractors who really don't understand what's so enjoyable about pulling CAT 5 through the sands of SWA at 02:00 while in MOPP 4. But just within the past year, the establishment of the Joint Task Force–Computer

Major E. H. Ted Steinhauser, USMC (Retired)

Network Defense (JTF-CND) along the sheltered suburban streets of Washington, D.C., helped bring back some of the operational feel of wearing a set of utilities at the crossroads of the Corps.

The JTF-CND was the result of Presidential Decision Directive 63 and events such as Eligible Receiver and Solar Sunrise, Protection of the Nation's Critical Information Infrastructure. Under its charter, the JTF-CND is responsible for establishing a fully operational JTF capable of coordinating the defense of the Defense Information Infrastructure (DII). Each service was tasked with providing a component to the JTF in mutual support of the DII subordinate elements. The Marine Forces Computer Network Defense (MARFOR-CND) is the Marine Corps component of a standing JTF. No set working hours, no predictable schedule—MARFOR–CND even has a real enemy, which is not only perceived to be "out there" but also routinely probes the Listening Posts (LPs) and Observation Posts (OPs) to see if they're awake. A

renewed sense of purpose has been instilled in the Marines working to support the connectivity for the Marine Corps Enterprise Network (MCEN).

The easiest part of bringing the MARFOR-CND on line was recognizing that it had an outstanding high ground from which to defend. Those of us in the information security business all know that to achieve anything resembling a secure network, we must view the system from the perspective of pessimistic vulnerability hunters who are unwilling to accept that today's working solution will stand up against tomorrow's emerging threat. The Marine Corps did it right, as they've always done. Nearly from its conception, the MCEN was engineered with security in mind. The big picture was thoroughly examined to ensure an understanding of why the system was brought into existence, and built the system with the aim of providing global support to the deployed commander. By dismissing the complexity caused by geographical separation, the Marines employed the fundamental aspects of true enterprise network symmetry and simply put, did what needed to be done. From the first scribbles of a few network engineers on restaurant napkins, to lengthy conversations over a couple of beers, the plan to construct a global network that was sustained, maintained, administered, protected, and defended from a central location was put into place.

In conjunction with the truly expeditionary nature of the Marine Corps, the MARFOR-CND Marines want to expand their capability beyond the MCEN garrison network. In a continued effort to protect the Marine Corps—deployed information architectures, the Marines will be fielding deployed security interdiction devices (DSID) to the FMF communication battalions. The DSID is designed to provide a defense in-depth, boundary-level architecture, composed of "best of breed" commercial off-the-shelf (COTS) security technologies. This design will enable the next generation of Marines to carry with them to the field technology that allows a tactical computer network defense in depth.

The instrumental catalyst that makes the Marine Corps component unique among the JTF components is operations security (OPSEC). This article did not include many details about the way in which the Marine Forces Component achieved this success, because we know that any information about the tools of information system security success is merely a new essential element of information (EEI) for our enemy to use against us. The Marines understand tactics well. Although the successes produced by the MARFOR-CND are unlikely to result in a new verse of the Marines Hymn, the Marines have assumed this newest mission with as much seriousness and intensity as they have applied to any past battle. 🔒

Mr. Steinhauser has been actively engaged as the MARFOR-CND Plans Officer in the conception and establishment of the Marine Corps' component of the Joint Task Force–Computer Network Defense. He may be reached at steinhauserth@noc.usmc.mil.

ACERT/ ARFOR–CND

proactive means for selecting the best course of action for protecting networks. The ACERT analytical sections predictive analysis capability is integrated into a multi-faceted LIWA analytical architecture. This structure also includes vulnerability assessment analysis via the information operations vulnerability assessment division and Computer Defense Assistance Program, reverse engineering and technical analysis of hacker tools via the LIWA Laboratory, and threat analysis via the intelligence branch.

As a key Army element responsible for ensuring information assurance, the ACERT, in its capacity as the ARFOR-CND, maintains a vigilant watch for the numerous risks and threats to Army automated information systems and networks. 🔒

Major Glen Teasley is the ACERT Operations Officer for the Land Information Warfare Activity at Fort Belvoir, VA. He holds a _____ in _____ science from the Penn _____ State University and is a _____ the Army's Computer Science _____. He may be reached at gateasl@liwa.belvoir.army.mil.

Major David Papas is the Chief, ACERT Coordination Center for the Land Information Warfare Activity at Fort Belvoir, VA. He holds B.S. degrees in computer science, software programming and systems engineering from the University of Southern Mississippi and is a graduate of the Army's Computer Science School.

Navy Computer Network Defense

The Navy Component Task Force–Computer Network Defense (NCTF-CND) is a component of, and directly supports, the CND mission of the Joint Task Force–Computer Network Defense (JTF-CND). NCTF-CND missions include—
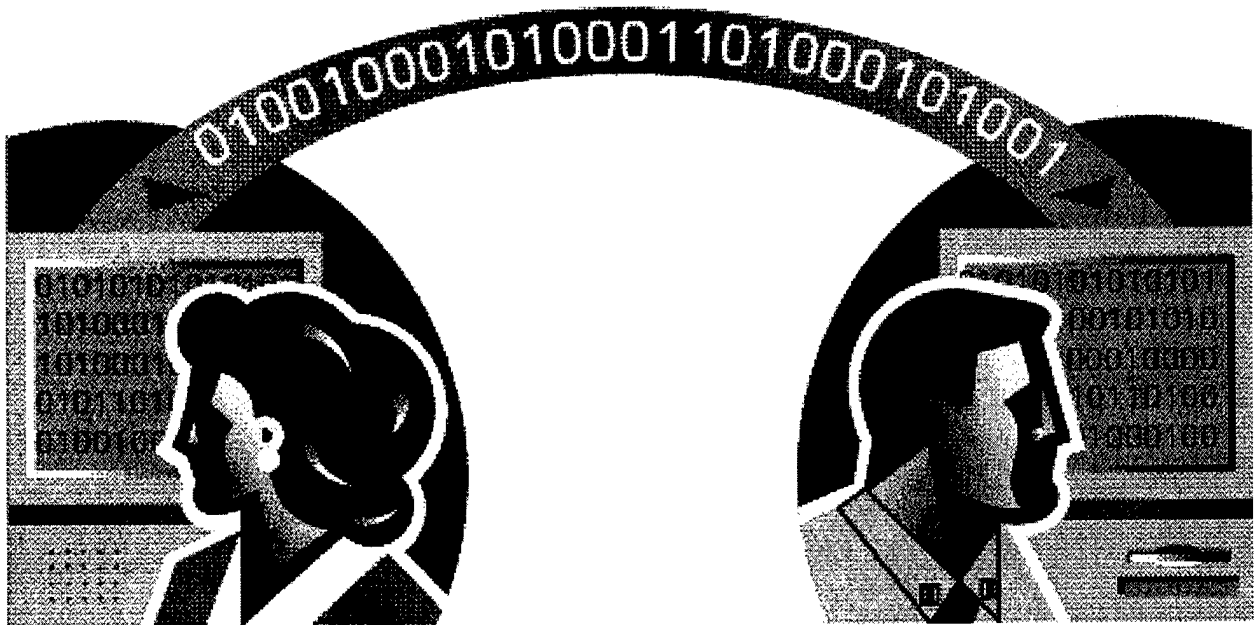
- Determining when Navy systems are under computer network attack (CNA), assessing an attacker's impact on military operations and capabilities, and notifying the JTF-CND and the user community of the threat
- Coordinating and directing appropriate Navy actions to stop CNA, contain damage, restore functionality, and provide feedback to the user community
- Developing contingency plans, tactics, techniques, and procedures to defend Navy computer networks and supporting the CND planning of Fleet Commanders-in-Chief (CINCs)
- Assessing effectiveness of defensive actions and maintain current assessment of operational impact on the Navy
- Coordinating as required with the Naval Computer and Telecommunications Command (NCTC), the Fleet Information Warfare Center (FIWC), the Naval Security Group, the Office of Naval Intelligence, the Naval Criminal Investigative Service (NCIS), and other agencies and private sector partners to defend Navy networks
- Monitoring status of Navy computer networks
- Monitoring Computer Incident Response Team (CIRT) alerts, warnings and advisories, and serving as a critical node in the indications and warnings (I&W) reporting cycle
- Participating in Navy exercises to conduct computer network defense training
- Assessing threats to Navy computer systems, based on all-source fused intelligence, from potential CNAs against Navy computers and networks
- Providing information to, and receiving direction from, the CJTF-CND and providing liaison to Navy organizations, as required
- Coordinating and directing appropriate actions to ensure that Navy pages resident on the World Wide Web are in compliance with prescribed DoD and Navy doctrine or policy

- Serving as the Navy's reporting agent for Information Assurance Vulnerability Alert (IAVAs).

The NCTF-CND is comprised of 14 officers, enlisted persons and civilians. It is colocated with the NCTC to provide a comprehensive view of Navy networks. This network operations view, in combination with the network security picture provided by FIWC, allows NCTF-CND to rapidly identify threats to computer networks.

In its first trial, NCTF-CND, working closely with the FIWC's Navy Computer Incident Response Team (NAVCIRT), was able to disseminate critical, timely information about the Melissa virus, which contributed to the rapid containment of the virus on Navy networks. In comparison, many civilian networks were taken off-line for days or weeks to recover from the damage this virus did.

NCTF's partnership with the NAVCIRT division of FIWC extends beyond this one incident. As Navy's information operations center of excellence, FIWC conducts forensic analysis of computer intrusion incidents and provides technical assistance to commands to restore networks. NAVCIRT also conducts on-line surveys of networks to identify vulnerabilities to command leadership, users, and system administrators.

NCTF-CND has also been vested with several significant network security–related missions, including Information Operations Condition (INFOCON), Navy Web-page Risk Assessment (NWRAC), and IAVA and compliance reporting.

As the manager of the INFOCON program, NCTF-CND, through the Chief of Naval Operations (CNO) N6, issues guidance Navy-wide on implementation of the program and makes Service-level INFOCON posture recommendations to CNO. NCTF-CND coordinated a Navy-wide INFOCON exercise, which was conducted from late November to early December 1999 to ensure that INFOCON-level implementation and the associated operational impacts are well understood by all Navy commands. NCTF-CND also has responsibility for assessing the operations security posture of publicly accessible Navy Web sites. In collaboration with FIWC and Commander, Naval Security Group, the Commander, Naval Reserve Security Group is developing a Web-based database and reporting mechanism that significantly improves Naval Reserve Security Group operators' ability to check web pages for compliance with established DoD and Navy instructions and their ability to expeditiously notify commands of their findings.

IAVAs alert DoD network users to vulnerabilities in operating system and application software and direct corrective measures. NCTF-CND has assumed the IAVA mission and, with system development support from NCTC, is implementing a Web-based compliance tracking system that significantly improves the timeliness and quality of IAVA compliance.

At the vortex of Navy network operations, the NCTF-CND has coordinated with all Navy second-echelon com-mands on the performance of several data collection efforts in support of the Navy–Marine Corps intranet and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence [ASD (C3I)]–directed Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)/ Internet gateway survey.

Early on, NCTF-CND recognized the need to create a tool to capture critical network and organizational information, marrying network Domain Name Service (DNS) server information and Internet Protocol addresses with organizational and chain-of-command information. The result is better and more timely dissemination of network defense information and direction Navy-wide and improved reporting timeliness of compliance with JTF and NCTF tasking and direction.

The preceding examples highlight the NCTF-CND's diverse missions. The first line of network defense is still the skill and operational awareness of network system administrators and users. A well-trained, well-informed cadre of system administrators and users, coupled with a system of rapidly disseminated advisories and direction, are key ingredients in the success of the computer network defense mission. As DoD and Navy move forward together into the next millennium, NCTF-CND will play an increasing role in the development and implementation of strategies that ensure that Navy networks are available when needed in peace, crisis and war, and the return to peace.

Monitoring and Protecting the Global

The protection and defense of operational networks is the mission of the Global Network Operations and Security Center (GNOSC), which is part of the Defense Information Systems Agency (DISA) operations directorate. The GNOSC consists of five branches. The Field Security Operations branch, at Letterkenny Army Depot, provides security services to the Defense Megacenters and to the Commanders in Chief (CINCs). The Plans branch provides long-range strategic planning for the Defense Information Infrastructure (DII). The Support branch provides support for daily internal operations of the GNOSC. The Operations branch, located at DISA headquarters in Arlington, Virginia is responsible for the day-to-day management of the DII. The remaining branch, the Department of Defense Computer Emergency Response Team (DoD-CERT) is the joint-level CERT for DoD.

MAJ Rod Laszlo, USA
CW5 Bruce Gardner, USA

Within the GNOSC, direct day-to-day monitoring and protection of the DII is the job of the Operations branch. This branch, which is staffed 24 hours a day, 7 days a week, is responsible for managing, by exception, network faults or outages in all components of the DII, including the Unclassified-but-Sensitive Internet Protocol Router Network (NIPRNET), the Secret IP Router Network (SIPRNET), the Integrated Digital Network Exchange (IDNX), the Defense Red Switched Network (DRSN), commercial and military satellites, video teleconferencing, and applications such as the Global Command and Control System and the Defense Message System. These networks are managed through five subordinate Regional Network Operations and Security Centers (RNOSCs), provide network management and control and CERT support by region, including the European, Pacific, Central Command, and United States areas of responsibility. In the event of a crisis, the GNOSC can manage, coordinate, and direct the actions of the RNOSC.

Photo by: Robert Flores, DISA

The GNOSC also is the DoD component responsible for the Joint Task Force–Computer Network Defense (JTF-CND). In this role, it synthesizes and reports CND-related information from all DoD organizations—CINCs, Services, and Agencies—and provides direct access to technical and engineering expertise throughout DISA. The JTF-CND is co-located with DISA, and the JTF-CND Watch Officer sits in the same command center where the GNOSC performs network management. This relationship allows the JTF-CND to obtain real-time information about the networks that it defends, and permits the GNOSC, in coordination with the JTF-CND, to suggest appropriate responses to an attack against the networks.

The networks that the GNOSC manages and protects can be likened to a weapons system. They must be monitored, managed, and manipulated so that they can be protected. One key to such network protection is the correct identification of the causes of network incidents. Network faults, outages, and congestion can appear to re-

sult from computer network attacks, but might also be due to a cable cut caused by a backhoe. Immediate analysis and deconfliction of events is essential for development of proper courses of action, in-

The DoD-CERT, the fifth branch of the GNOSC, provides network defense services through sensor monitoring, correlation of intrusion incident data, anti-virus product support to DoD, and reme-
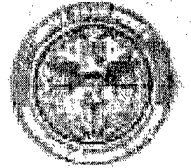
Network

cluding recovery and reconstitution. The co-location of the JTF-CND and the GNOSC facilitates such network defense.

The GNOSC Operations branch also includes a Computer Network Defense Assessment Team, a Worldwide Network Manager, and a Worldwide Satellite Manager. Each of these functions provides information to the Systems Control Officer (SCO), who ties all events together and is the customer's contact at the GNOSC. The SCO plays a crucial role in determining whether an event is a network or a security problem. To ensure quality of service for the customer, the GNOSC Operations branch addresses network performance issues and security. On the performance side, the Network and Satellite Managers monitor the global network picture and work closely with the RNOSCs to ensure that customers have a responsive and supportive network for a multitude of applications traversing the networks. On the security side the Computer Network Defense Assessment Team, working closely with the customer, the JTF-CND, and the DoD CERT, helps to assess and prioritize the customer's problem and refer it to the proper branch of the DoD-CERT.

diation of the effects of intrusive activity. It is the joint-level DoD-CERT for strategic technical coordination among all of the other Service and Agency CERTs and Computer Incident Response Teams (CIRTs) in DoD, and is the focal point for all computer incident and event reporting. Thus, it is the first place where a worldwide assessment of the status of CND throughout the DoD can be made. The DoD-CERT can correlate data from all Services and from the RNOSCs with data gathered directly by network sensor devices and then assemble a global picture of the defensive state of the network.

In closing, the synergy that results from the co-location of the JTF-CND and the GNOSC cannot be overestimated. It is critical to the ability to see the networks that are being defended, and the ability to gauge the impact of an attack on a network by seeing its components. The synergy of the JTF-CND and the GNOSC is also critical to seeing how best to stop or contain an attack. But just as important are the relationships forged by working side by side, every day, allowing the JTF-CND and the GNOSC to react as one in protecting the DII.

Major Laszlo is Deputy Operations Manager at the GNOSC. He received his B.S. in Geography from Portland State University in 1988. He is currently working toward completing his M.S. in Information Resource Management from Central Michigan University. He may be reached at laszlor@ncr.disa.mil.

Chief Warrant Officer Gardner is an information assurance officer at the GNOSC. He received his B.S. from Brown University and his M.B.A. from the University of Utah. He is currently completing a M.S. in computer science from James Madison University. He may be reached at garderb@ncr.disa.mil.

Photo by Robert Flores, DISA.

Military and civilian professionals in DISA's Global Network Operations and Security Center monitor the health and welfare of the Defense Information Infrastructure.

DoD Computer Security Tips for Y2K Preparation

Capt Elizabeth A. Siemers, USAF
DoD-CERT

With less than one month before the Year 2000 (Y2K) rollover, many DoD and non-DoD organizations have asked the DoD-CERT how to protect their computer systems from security threats during the Y2K rollover period. In response, the DoD-CERT has put together some tips and recommendations for administrators of DoD computer systems.

The DoD-CERT and many computer security experts warn system administrators that they can expect the following types of problems during the Y2K rollover:

- Intruders may use the Y2K rollover period as a window of opportunity for intruding on DoD computer systems

- Y2K problems may mimic a denial of service (DOS) attack

- There may be an increase in "network noise" (probes and scans)

- There may be an increase in malicious code infection (e.g., viruses, Trojan horses, and worms)

- Intruders may exploit system administrators' fears that a Y2K fix did not work or that Y2K testing was inadequate.

The following 10 recommendations address new variants of malicious activity occurring on the Internet today (e.g., denial of service and E-mail tunneling attacks), as well as attacks intending disruption during Y2K (e.g., logic bombs). These recommendations are geared toward countering the actions of malicious insiders and outsiders who may initiate incidents during the Y2K rollover.

Recommendations

1 Security Patches–Implement all of the latest security fixes or patches, especially for mission-critical systems and servers that are likely targets. For information on current Information Assurance Vulnerability Alerts (IAVAs), see http://www.cert.mil.

2 Anti-virus Signatures–Update all virus and intrusion detection signatures. For current DoD anti-virus products and signatures, see http://www.cert.mil/virus/avirus.htm. For current intrusion detection signatures, contact each product's vendor.

3 Anti-virus Software on Mail Servers–This is a good time to implement anti-virus scanning at E-mail gateways, where it is not already in use.

4 Secure System Configuration–Verify the security of system configurations, paying particular attention to countering the vulnerabilities and exploit scripts described in advisories leading up to the Y2K rollover period. Ensure that all systems are backed up before the Y2K rollover. For additional computer security advisories, see http://www.cert.org and http://ciac.llnl.gov.

5 Verify Trust Relationships–Verify and confirm all remote access accounts, and delete all remote access accounts that cannot be positively verified.

6 Identify Mission Critical Systems–Identify systems that will be needed by legitimate users during the holiday period and ensure that protection of these systems is properly prioritized.

7 Verify and Enforce Security Policy–Warn all users and administrators not to install any patches during the Y2K rollover period without confirmation from an authorized source that the patches are authentic. This effort is designed to counter an expected increase in hoaxes that warn of the urgent need to install Y2K or other patches or to update virus signatures.

8 Standardize Network and System Time–Synchronize time on all systems and networks from a trusted source, such as tick.usnogps. navy.mil or tock.usnogps. navy.mil, to ensure that incident reporting is not complicated by timing inconsistencies.

9 Minimize Network Traffic–Limit non-mission-critical network traffic (e.g., Web surfing) during the rollover period so that problem areas on the networks can be more quickly identified.

10 Establish a Normal Baseline–Just before the Y2K rollover period, observe system performance metrics and establish baselines for ordinary activity. Use the baselines to gauge unusual levels of disk activity, central processing unit (CPU) use or network traffic, thereby allowing earlier detection of viruses and denial of service attacks.

The DoD-CERT and all regional and Service CERTs and CIRTs will maintain 24-hour-a-day operations during the Y2K rollover period to support the field CERTs and will maintain heightened awareness concerning all computer security-related events that may occur during that time.

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

DSN 327.4700
Commercial 703.607.4700
800.357.4231

Unclassified E-mail:
cert@cert.mil
Classified E-mail:
cert@cert.disa.smil.mil
DSN Fax: 327.4009
Comm. Fax: 703.607.4009

Captain Elizabeth A. Siemers, USAF, is the Chief of Plans and Standards for the DoD Computer Emergency Response Team, Defense Information Systems Agency, Arlington, VA. She received her B.A. in history with a certificate in business administration from Indiana University in May 1995. Capt Siemers is now pursuing her M.S. in engineering management, with concentration in systems engineering, from George Washington University in Washington, D.C. She may be reached at eas@cert.mil.

SHERLOCK

A Third Generation Log Analysis Tool

Keith J. Jones

The typical computer network includes a variety of components, often including: routers, firewalls, intrusion detection systems (IDS), network sniffers, clients, and servers. Each of these components is capable of producing network activity logs of various types. These logs are often in a proprietary format, adhering to no single standard. Depending on the level of auditing and the activities monitored, logs can range from a few hundred kilobytes to several gigabytes in size. Furthermore, log formats may differ among different versions of the same product.

Modern security professionals and computer crimes investigators have only a few log analysis tools at their disposal, none ideally suited to the task. The crudest method correlates activity entries across many different log printouts. With this method, even a highly trained individual can perform only limited analyses when the log files are very large. First-generation search tools (grep, perl scripts, etc.) are a better approach for performing searches on large data sets but require considerable skill to use. The tools must be configured for each log format and search effort. This approach offers more efficiency, but skill and human error are still large factors.

Several vendors of network security products have created second-generation log analysis tools. These tools are capable of more sophisticated searches and limited correlation analysis but typically work only with

the vendor's proprietary log devices. Such tools are unsuitable for heterogeneous networks because of their inability to analyze different log formats generated by other vendor's products.

A new third-generation tool, produced by Sytex, addresses some shortcomings of the earlier generation of products. This product, called SHERLOCK, can operate in heterogeneous network environments and import multiple types of log formats into standard databases.

Sherlock has a platform-independent, Web-based interface and provides point-and-click generation of Structured Query Language (SQL) queries. It can be used by multiple investigators to query multiple network logs simultaneously.

Sherlock has features that facilitate both immediate and retrospective analysis of network activity. For instance, it captures log data directly from network devices, permitting immediate analysis of, and response to, potential intrusions. (Administrators can thus detect a port scan and then block the offending source Internet Protocol.) In addition, data are stored in read-only form to preserve intruders' footprints in system logs.

Sherlock was designed as an advanced network security analytical tool, but it can be scaled to handle various types and sizes of log analysis efforts. Information on Sherlock may be obtained from the Sytex Information Warfare Center at www.iwce.net or, by phone at 410.312.9114.

Keith J. Jones holds the position of "Software Development Team Leader" at Sytex, Inc. He currently works out of the Columbia, MD office with the rest of the technical operations team. Previously, he has completed two B.S. degrees in computer engineering and electrical engineering, and an additional M.S. degree in electrical engineering. Keith can be reached at the following e-mail address: kjones@sso.sytexinc.com.

iatac chat

Leveraging the Technical Area Task (TAT) Program

Robert P. Thompson
Director, IATAC

ne of the objectives of the Department of Defense (DoD) Information Analysis Center (IAC) Program is to maintain technical centers of excellence that can be called upon to facilitate use of existing scientific and technical information (STI) to meet DoD research, acquisition, operational, and logistics requirements. As a DoD institution, IATAC provides the foundation through which data gathering, studies, analyses, and other scientific and technical activities can be accomplished.

IAC operations are comprised of core functions and technical area task (TAT) activities. Core functions include basic services such as the collection of scientific and technical information (STI), inquiry support, data base operations, current awareness activities (e.g., IAnewsletter), and generation of technical reports. TATs fall within the scope of the IAC mission but are not funded as a part of the IAC's basic services. Typically technical and analytical in nature, TATs are more labor intensive and complex and may involve extensive gathering or creation of STI, analysis, and preparation and dissemination of the information.

IATAC services available via the TAT program support a broad spectrum of information assurance technical disciplines. These capabilities include policy and doctrine development, research and analyses, studies and reports, training and exercises, and conference and event planning. Technical disciplines (see fiugre below) include various aspects of information assurance and information operations to include certification and accreditation, computer forensics, biometrics, infrastructure protection, malicious code, penetration testing, psychological operations, public key infrastructure, and secure enterprise management to name a few. IATAC is providing TAT support to the plans and policy, research and development, acquisition, and operational communities.

The products generated via the TAT are developed in response to requirements delineated by the requesting activity. In addition, products are entered into the IATAC collection thus contributing to the growth of the information assurance (IA) knowledge-base. Other DoD organizations can access the STI developed through the TAT and leverage prior research and analyses to support their IA requirements. Releasability of TAT products are coordinated with the originating organization to ensure compliance with secondary distribution instructions. For more information on available products generated through the TAT program, contact IATAC at 703.289.5454 or iatac@dtic.mil. ✔

CAPABILITIES

Policy & Doctrine

Studies & Reports

Meetings & Conferences

Research & Analysis

Training & Exercises

EXPERTISE

Certification & Accreditation
Computer Forensics • Data Embedding
Information Assurance/Operations
Malicious Code Detection
Ops Security • Penetration Testing
Public Key Infrastructure
Security Test & Evaluation
Vulnerability 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

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 fu-

ture 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.

Vulnerability Analysis Tools Report

This report summarizes pertinent information, providing users with a brief description of available tools and contact information. Currently the IA Tools database contains descriptions of 35 tools that can be used to support vulnerability and risk assessment.

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 _____

Organization _____ Ofc. Symbol _____

Address_____   Phone _____

_____   E-mail _____

_____   Fax _____

DoD Organization? ❑ YES ❑ 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
❑ Biometrics   ❑ Computer Forensics   ❑ Data Mining   ❑ Modeling & Simulation

IA Tools Report
❑ Firewalls   ❑ Intrusion Detection (2nd Ed.)   ❑ Vulnerability Analysis

State-of-the-Art Reports
❑ Data Embedding for Information Assurance

❑ Malicious Code Detection [❑ TOP SECRET ❑ SECRET]

Security POC   Security Phone

UNLIMITED DISTRIBUTION

Newsletters *(Limited number of back issues available)*

❑ Vol. 1, No. 1   ❑ Vol. 1, No. 2   ❑ Vol. 1, No. 3

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

❑ Vol. 3, No. 1   ❑ Vol. 3, No. 2

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

February

3
IA Technical Framework
Forum Meeting
Linthicum, MD
Call Mr. John Niemczuk
410.684.6246
http://www.iatf.net

8–10
DISA 4th Annual IA Workshop
Holiday Inn Hampton Hotel
Hampton, VA
Call Maureen Premo
703.681.5789 or
Tracy Grubar 703.681.7933

9–11
AFCEA West 2000
San Diego Convention Center
San Diego, CA

22–25
SPACECOM 2000
Space Communications—Key to
Information Operations
Colorado Springs, CO
Call Michael J. Varner
719.590.1051
COME SEE OUR BOOTH!

March

14–16
Federal Information Systems
Security Education Assoc. Conf.
Gaithersburg, MD
http://csrc.nist.gov/organizations
/fissea.html

March

16
Information Assurance
Technical Framework Forum
Linthicum, MD
Call Mr. John Niemczuk
410.684.6246
http://www.iatf.net.

27–31
DoDIIS IA Training Forum
Bolling AFB, Washington DC
Call Mr. Paul Woeppel
210.977.3396 or
Mr. John Venit 202.231.5818

April

3-5
InfoSec World Conf & Expo
Orlando, FL
Call 508.879.7999
www.misti.com

25–27
Fiesta Informacion 2000
San Antonio, TX
Call J. Spargo & Associates
703.631.6200
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

IATAC

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