IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 4 Number 3
Summer 2001

CERT/CC

Tracking, Preventing & Resolving Computer Security Incidents

also inside

- DIAP Reorganizes
- JTF-CNO Tactical Decision Exercises
- Time Based Security

contents

on the cover

ia initiatives

in each issue

IAnewsletter

Creative Director
Christina P. McNemar
Technical Editor
Robert J. Lamb
Information Processing
Abraham T. Usher
Inquiry Services
Peggy O'Connor

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 J. Lamb
Director, IATAC
703.289.5454

Submitting Articles

To submit your related articles, photos, notices, feature programs or ideas for future issues, please request an author's packet from—

IATAC
Christina P. McNemar
3190 Fairview Park Drive
Falls Church, VA 22042
Phone 703.289.5454
Fax 703.289.5467

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

Article Deadlines

Winter 2001	16 December 01
Spring 2002	15 February 02

Cover design—Maria Candelaria
Newsletter design—Christina P. McNemar
Illustrations—Holly Shipley

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

IATAC chat

by Mr. Robert J. Lamb, IATAC Director

Configuration Management CR/TA

This edition of the *IAnewsletter* includes an overview of our newest critical review and technology assessment (CR/TA) report entitled *Configuration Management Compliance Validation*. This CR/TA examines the complexities of configuration management (CM) through the system development and deployment processes and examines information assurance implications and applications of this process. The report is available for download on our Web site and hard copy editions may be ordered from that same site. All of our products are available electronically and may be requested using the order form at the back of this newsletter.

Steering Committee

IATAC hosted its annual Steering Committee meeting on 18 July 2001 in Washington DC. Representatives from across DoD volunteer to serve as members spanning the spectrum of IA professionals from the warfighter to R&D communities, Services, and agencies. The Steering Committee, chaired by Mr. Richard Hale, DISA, is charged with reviewing IATAC activities over the past year and providing advice and guidance on future IATAC operations. In addition to an update on IATAC initiatives, the Steering Committee received presentations on our two most recently published reports, *Information Modeling and Simulation*, and *Configuration Management Compliance Validation*, as well as an overview on the Fleet Information Warfare Center (FIWC) Commander's Guide to the Elements of Information Operations (20 March 2001) developed under an IATAC Technical Area Task.

During the coming months IATAC will present abstracts to the Steering Committee on potential topics for upcoming reports. Specific subject areas highlighted by the members included the following—

- **Enterprise Vulnerability Management.** Develop a state-of-the-art-report which addresses the technology and tools to help disseminate information on vulnerabilities, distribute fixes, sense status and progress of fixes, and assess effectiveness and maintenance of fixes.
- **Coalition Operations**. Examine the technologies and techniques for information sharing between modern coalition partners. Address the fluid and dynamic nature of those partnerships with respect to the level of trust, recognizing that the level itself may change. Address military, Government, and civil organizations. Recognize that it is more than just a set of VPNs.
- **Mobile Code Security.** Examine technologies as well as vulnerabilities and security issues of mobile code. Mobile code is software obtained from remote systems that is transferred across a network, and then downloaded and executed on a local computer (e.g., a computer with a Web browser) without explicit installation or execution by the recipient. Mobile Code technology has become a mainstream way of executing software.
- **Wireless Security.** Examine the technology and security of the spectrum of wireless devices and networks now in use and projected for the future. The growing popularity of Web enabled and wireless devices (e.g., cellular phones, personal digital assistants, etc.) is simultaneously exploding and opening potential vulnerabilities across DoD.

IAC Mission Success Stories

Each quarter all 13 DoD IACs submit success stories reflecting support provided to DoD. It's an opportunity for the IAC to present and describe specific achievements. Similarly, visitors may identify support they can leverage and contact the appropriate IAC. That Web site is http://iac.dtic.mil/mss.

CarnegieMellon
Software Engineering Institute

CERT® Coordination Center

Tracking, Preventing & Resolving Computer Security Incidents

by Tabatha Spitzer

The nightly news has put information and network security at the forefront of public awareness. From the challenges of Y2K to the newly recognized *Code Red Worm*, the nation has been forced to confront the fact that computer technology is not always as secure as we wish to believe and the costs of restoring that security can be staggering. Yet the media just grazes the surface of the network vulnerability issues. We have heard about *Melissa*, the "*love bug*," and distributed denial of service attacks that shut down Yahoo, Ebay and others. What about all the others we do not hear about? One organization that tracks and works to resolve, and in many cases prevent, these disruptions is the CERT® Coordination Center (CERT/CC).

The CERT/CC is an organization dedicated to the security of the virtual world. They study Internet security vulnerabilities, track computer security incidents, release security alerts, perform research for long-term taimprovements in network systems and develop information and training that help other organizations improve the security of their systems. The CERT/CC is part of the Networked Systems Survivability Program at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University in Pittsburgh, Pennsylvania. The Defense Advanced Research Projects Agency (DARPA) established CERT/CC in 1988 when the "*Morris worm*" shutdown approximately ten percent of the computers connected to what was the precursor of today's Internet.

With the growth of the Internet and computers came a corresponding growth in worms and viruses as well as increasingly sophisticated tools for causing damage and increased ease in obtaining and using those tools. During the past year CERT/CC examined 1,100 reported vulnerabilities and almost 22,000 reported incidents. The growth of the Internet and attackers has led the CERT/CC to broaden its focus to trend analysis and network survivability—the ability to perform essential functions even in the face of attacks or failures, as well as increase its attention to information security in industry through the Internet Security Alliance.

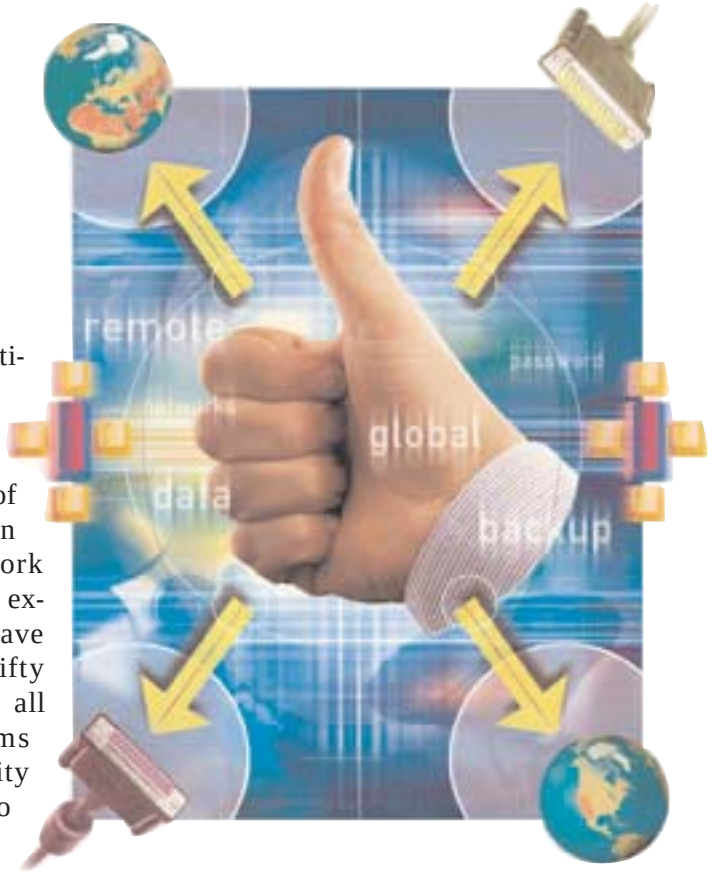
While CERT/CC is active in resolving incidents and cataloging vulnerabilities, it is equally committed to preventing problems. For example, the last Republican National Convention was the most connected in history. CERT/CC was called on to ensure that political party E-mail, public and confidential information, the intranet and the Internet were all protected.

Another valuable service CERT/CC offers is to post the latest security for free on their public Web site. Sharing their insights developed from examining thousands of incidents and vulnerabilities allows the public to learn what to do and how to avoid an attack.

In past editions of the *IAnewsletter* we have featured many of DoD's premier network security organizations including the DoD CERT, the Joint Task Force for Computer Network Operations and each Service's computer security incident response teams. CERT/CC is one of the many organizations strongly aligned with DoD's network security commands; two major beneficiaries are DISA and GSA. For this reason, this edition of the *IAnewsletter* features three articles from the security professionals at CERT/CC.

The security expertise provided by CERT/CC is dedicated to the integrity and survivability of computer networks and information systems. For further information on CERT/CC please visit their Web site at www.cert.com.

A Safe Bet
CERT® Security Practices



by Julia Allen and Eric J. Hayes

How many alarming headlines have we read in the last year? "Thousands of Computer Networks Compromised," "Stolen Laptop Computer Contained Classified Data," "Government Web Site Defaced Again," "E-mail Attachment Delivers Destructive Payload; Agency Mail Server Knocked Out." The threats to computer networks and systems are growing and anyone involved with a computer network had better shore up their defensive network skills and capabilities or face the potentially devastating consequence of a compromised system. People who attack computer networks and systems have a host of motivations, but for the manager or network administrator, they all spell trouble. Malicious intruders are armed with sophisticated tools and knowledge of the latest computer vulnerabilities.

Networked systems and the sensitive information they contain can be compromised despite an administrator's best efforts. Even when an administrator knows they should be devoting more time to security, they often don't have the time. Keeping systems functioning takes priority over securing those systems. What is the best way to protect computer networks and systems? Administrators need a clear and comprehensive set of security practices that are easy to find and follow.

The Networked Systems Survivability program at the Software Engineering Institute (SEI) is dedicated to finding solutions for keeping networked systems secure. A major element of the program is the creation of CERT[1] system and network security practices. Security experts working together have assembled more than fifty best practices to address all phases of securing systems and networks. CERT security practices are organized into five broad groupings based on the order in which they are performed. They are—

- Harden and secure
- Prepare to detect and respond to intrusions
- Detect intrusions
- Respond to intrusions
- Improve

The complete set of practices is available on the CERT Web site at http://www.cert.org/security-improvement/index.html. Also, on June 1, 2001 Addison-Wesley published a book entitled *The CERT Guide to System and Network Security Practices*, written by Julia Allen, a senior member of the technical staff at the SEI.

By adopting these practices, an administrator can act now to protect against today's threats, mitigate future threats, and improve the overall security of the organization's networked systems.

The Structure of CERT Security Practices

The topics addressed by the CERT practices were created to address 75 to 80 percent of the problems that are reported to the CERT/CC. Each practice consists of an introduction and a series of practical steps presented in the order of recommended implementation. Each practice also has a section describing policy considerations that complements the steps and helps ensure that they will be deployed effectively.

All practices assume the existence of—

- Organizational goals and objectives from which security requirements derive. These may require periodically conducting an information security risk analysis and assessment to help set

continued on page 6

continued from page 5

priorities and formulate protection strategies.
- Organization-level and site-level security policies that can be traced to these goals, objectives, and security requirements.

The practices do not make reference to any one operating system or version, so the principles will remain valid despite the rapid advances in specific technologies. However, many practices are linked to documents called implementations that discuss specific operating systems and software. Implementations are available from http://www.cert.org/security-improvement/#implementations.

Descriptions of the Five Steps

Following the all-important first step of creating a secure system configuration, steps two through five contain practices that describe what to do when something unexpected occurs on a network.

1 Harden and Secure

The recommended practices to harden and secure systems form a strong foundation by establishing secure configurations of networks, systems, critical data, and access to them. If this is done correctly and maintained, many of the common vulnerabilities used by intruders are eliminated. Following these practices can greatly reduce the success of many common, recurring attacks.

Systems shipped by vendors are very usable but, unfortunately, often contain many weaknesses from a security perspective. (This idea is depicted as Swiss cheese in figure 1.) This step yields a hardened (secure) system configuration and an operational environment that protects against known attacks for which there are designated mitigation strategies.

2 Prepare to Detect & Respond to Intrusions

This step starts with the assumption that there are many vulnerabilities not yet identified. An administrator must be able to recognize when an unknown vulnerability is being exploited. How can an administrator recognize what is not there? The major method to help recognize exploitation is to characterize a system so that an administrator can understand how it works in a production setting. Then, any deviations will provide the clue to notice unexpected or suspicious activity. Characterizing a system thus helps the administrator identify new problems and formulate new solutions.

The administrator learns about the expected behavior of a system by thoroughly examining and recording a known baseline state and noting expected changes at the network, system (including kernel), process, user, file, directory, and hardware levels.

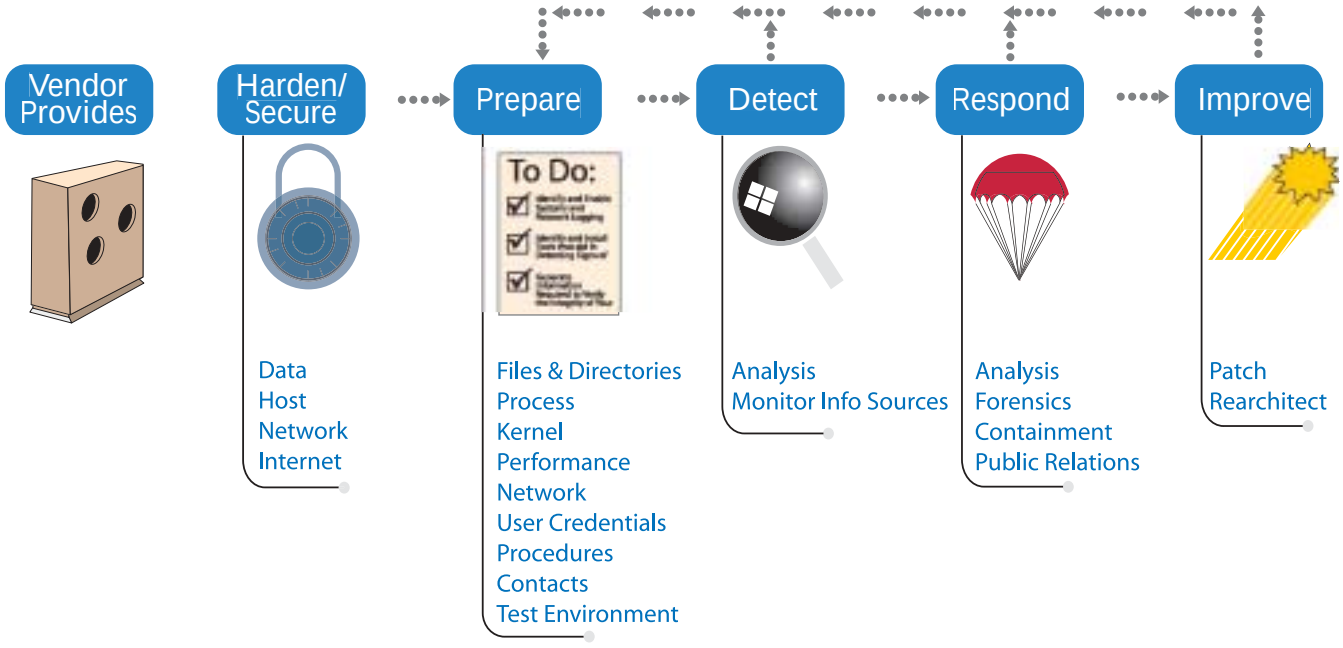


Figure 1. Securing Information Assets shown above illustrates how to secure and protect information assets (such as a network or Web server) using the CERT security practices.

In addition, the administrator and his or her manager must develop policies and procedures to identify, install, and understand tools for detecting and responding to intrusions well before they need to be invoked.

3 Detect Intrusions

This step occurs when an administrator is monitoring system or network transactions by, looking at the logs produced by a firewall system or a public Web server, for example. The administrator notices some unusual, unexpected, or suspicious behavior; learns something new about the asset's characteristics; or receives information from an external stimulus (a user report, a call from another organization, a security advisory or bulletin). These indicate either that something needs to be analyzed further or that something on the system has changed or needs to change (a new patch needs to be applied, a new tool version needs to be installed, etc). Analysis includes investigating unexpected or suspicious behavior that may be the result of an intrusion and drawing some initial conclusions, which are further refined during the next step, "Respond to Intrusions." Possible changes or system improvements an administrator could make include—

- Installing a patch (re-harden)
- Updating the configuration of a logging, data collection, or alert mechanism
- Updating a characterization baseline to add unexpected (but now acceptable) behavior or remove behavior no longer considered acceptable
- Installing a new tool

4 Respond to Intrusions

In this step, an administrator further analyzes the damage caused by an intrusion (including the scope and effects of the damage), contains these effects as much as possible, works to eliminate future intruder access, and returns information assets to a known, operational state. It may be possible to do this step while continuing analysis. Other parties that may be affected are notified, and evidence is collected and protected in the event it should be needed for legal proceedings against the intruder.

5 Improve

Administrators also need to take action to improve their systems following detection or response activities. In addition to practices contained in the step Detect Intrusions, improvement actions may include—

- Further communicating with affected parties
- Holding a postmortem meeting to discuss lessons learned
- Updating policies and procedures
- Updating tool configurations and selecting new tools
- Collecting measures of resources required to deal with the intrusion and other security business case information

Many times the process of improving a networked system will lead to a cyclical repetition of previous practices.

Conclusion

Even when system administrators know how to secure systems, they often don't have the time to take action. The CERT security practices, organized into five top-level steps, provide administrators with guidance that is easy to access, understand, and implement. The practices describe steps to securely configure an organization's computing assets and steps to take when an intrusion or something else unusual happens. Following these practices will help your organization keep its systems and networks secure.

Julia Allen is a senior member of the technical staff in the Networked Systems Survivability Program at the Software Engineering Institute (SEI). The CERT® Coordination Center is a part of this program. Allen is engaged in developing security improvement practices for network-based systems. Allen has more than 25 years of managerial and technical experience in software engineering. She received a B.S. in computer science from the University of Michigan, an M.S. in electrical engineering from the University of Southern California, and an executive business certificate from the University of California at Los Angeles.

Eric J. Hayes is a member of the technical staff in the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI). As a senior technical writer/editor at the SEI, his work includes editing security improvement modules, technical tips, and writing documents relating to computer security. Hayes received a B.A. in English writing from the University of Pittsburgh. At the graduate level, he has studied rhetoric at the University of Wisconsin at Milwaukee, technical editing at the University of Minnesota at Minneapolis, and technical writing at Carnegie Mellon University.

Endnote

1. CERT and CERT/CC are registered in the U.S. Patent and Trademark Office.

System Survivability Analysis

by Richard C. Linger

Modern society is irreversibly dependent on large-scale critical infrastructure systems to sustain quality of life, economic growth, and national security. As a result, society faces unquantified—but generally acknowledged as substantial—risks of intrusion and compromise with potentially serious consequences. Defense, telecommunications, energy, finance, health care and other key sectors are potentially affected. Critical infrastructure systems depend on large-scale computing and communication systems for operation and control. These systems exhibit powerful functionality that implements complex processes, extraordinary complexity that challenges intellectual control, extensive use of COTS components of uncertain reliability and quality, and potential cascade failure effects across interdependent systems-of-systems. Recognition of the growing consequences of failure has motivated interest in analyzing and improving system survivability as a prudent risk-management strategy.

As part of its Survivable Network Technology Initiative, the CERT Coordination Center is developing methods for analyzing and improving the survivability characteristics of network systems. Survivability is defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [Ellison 99]. In this article, survivability is discussed in terms of attacks and intrusions, in the knowledge that the methods can help deal with failures and accidents as well. Unlike traditional security measures that require central control and administration, survivability addresses highly distributed, unbounded network environments that often lack central control or a unified security policy. Survivability focuses on delivery of essential services and preservation of essential assets, even when systems are penetrated and compromised. As an emerging discipline, survivability builds on existing disciplines, including security, fault tolerance, and reliability, and introduces new concepts and principles. Survivability in adverse environments requires capabilities for intrusion resistance, recognition, and recovery. The Survivable Network Analysis (SNA) method [Mead 00] permits assessment of survivability characteristics at the requirements and architecture levels. Steps in the SNA method include system mission and architecture elicitation, essential capability definition, compromisable capability definition, and survivability analysis. Essential service scenarios and intrusion scenarios play key roles in the method.

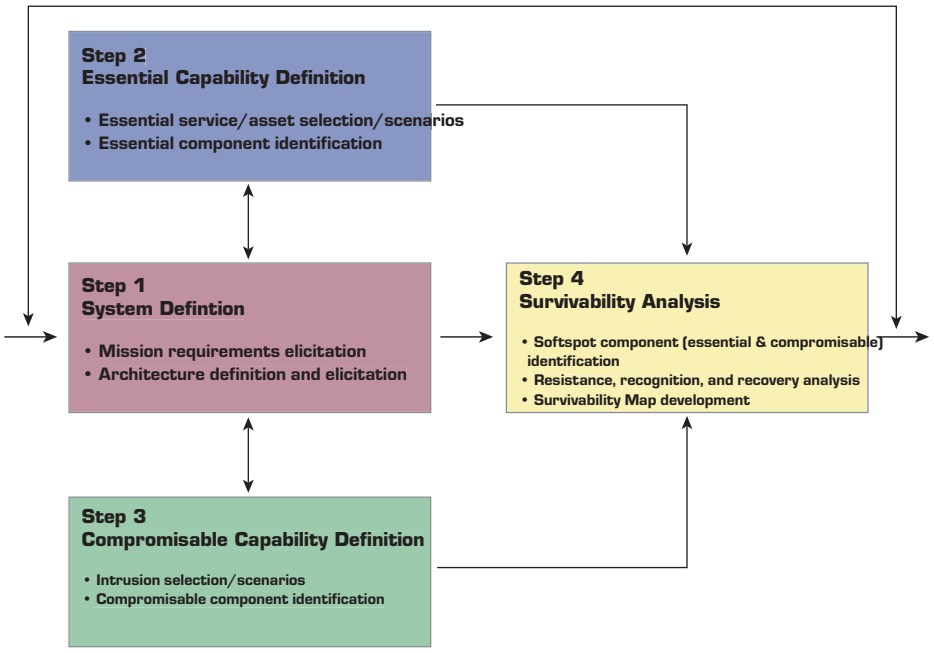


Figure 1. The Survivable Network Analysis Methodology Steps

The Survivable Network Analysis Method

A small team of trained evaluators can apply the SNA method to an existing or proposed system through a structured interaction with system

stakeholders. The method is composed of four principal steps, as depicted in Figure 1.

1 The mission requirements and architecture of the current or candidate system are elicited from stakeholders and system architects. Mission requirements concern the overarching goals and objectives that the system must satisfy. These requirements are typically elaborated into specific functional and non-functional requirements for system services. Architecture elicitation involves determination of network topology, hardware and software, and, in particular, connectivity with the outside world.

2 Essential services (services that must be maintained during attack) and essential assets (assets whose integrity, confidentiality, availability, and other properties must be maintained during an attack) are identified, based on mission objectives and consequences of failure. These services and asset uses are characterized by usage scenarios that are mapped onto the architecture to identify corresponding essential components (components that must be available to deliver essential services and maintain essential assets).

3 Intrusion scenarios are selected based on the system environment, assessment of risks and intruder capabilities, and the experience of the CERT organization. Attack trees, hierarchically organized intruder workflows that can result in survivability compromises, provide a taxonomy of potential intruder behavior and serve as valuable guides in the selection process. The representative intrusion scenarios are likewise mapped onto the architecture to identify corresponding compromisable components (components that could be penetrated and damaged by intrusion).

4 Softspot components of the architecture are identified as components that are both essential and compromisable, based on the results of steps 2 and 3. The softspot components and the supporting architecture are then analyzed for three key survivability properties, namely, resistance, recognition, and recovery. Resistance is the capability of an architecture to repel attacks. Recognition is the capability to detect attacks as they occur, and to evaluate the extent of damage and compromise. Recovery, a hallmark of survivability, is the capability to maintain essential services and assets during an attack, limit the extent of damage, and restore full services following the attack. The analysis of the "three Rs" is summarized in a survivability map, as depicted in Figure 2. The map enumerates, for every intrusion scenario and its corresponding softspot effects, the current and recommended architecture strategies for resistance, recognition, and recovery. The survivability map provides feedback for use in evaluating the original architecture, and may result in an iterative process of survivability evaluation and improvement.

Intrusion Detection	Softspot Effects	Architecture Strategies for ⊗	Resistance	Recognition	Recovery
(Scenario 1)		Current			
		Recommended			
(Scenario n)		Current			
		Recommended			

Figure 2. Survivability Map

The SNA method has been applied to several systems with good results. In each case, the findings have included recommendations for reconfiguration of network architectures to reduce the potential for intrusion and compromise and to increase recovery capabilities. The recommendations have also called for improving security policies to encompass survivability-related requirements for system deployment and operation. Additional information on the SNA process can be found at the CERT Web site, www.cert.org.

Richard Linger is a Senior Member of the Technical Staff at the Software Engineering Institute, Carnegie Mellon University, and a member of the faculty of the CMU School of Computer Science and the Heinz School of Public Policy and Management. He may be reached at rlinger@sei.cmu.edu.

References

Ellison, R., Fisher, D., Linger, R., Lipson, F., Longstaff, T., and Mead, N., *Survivable Network Systems: An Emerging Discipline,* CMU/SEI-97-TR-013, November 1997, revised May 1999.

Mead, N., Ellison, R., Linger, R., Longstaff, T., and McHugh, J., *Survivable Network Analysis Method,* CMU/SEI-2000-TR-013, September 2000.

by Christopher Alberts and Audrey Dorofee

Evaluating Information Security Risks Using octave℠

Today, virtually all information is captured, stored, and accessed in digital form. We rely on access to digital data that are accessible, dependable, and protected from misuse. Unfortunately, this need for accessible data also exposes organizations to a variety of new threats that can affect their information. Organizations need a way to understand their information risks and to create strategies for addressing those risks.

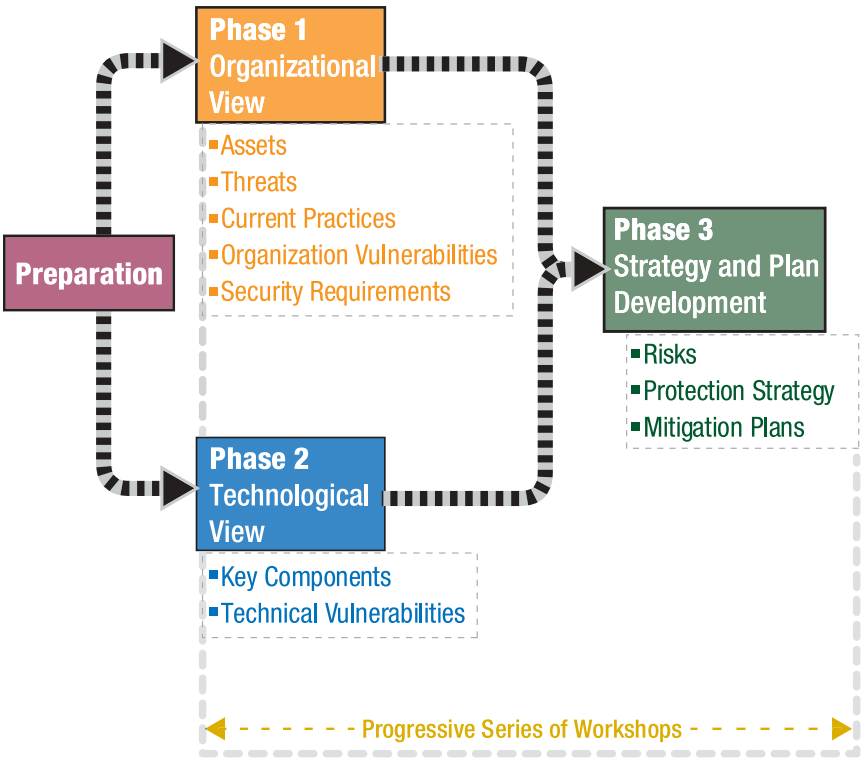


Figure 1. The OCTAVE Method

The confidentiality, integrity, and availability of information are critical to the missions of all organizations. However, many organizations form protection strategies by focusing solely on computing infrastructure weaknesses without establishing the effects on their most important information assets. This leads to a gap between the organization's operational and information technology (IT) requirements, placing the assets at risk. Current approaches to managing information security risks also fail to include all components of risk (assets, threats, and vulnerabilities). In addition, many organizations outsource information security risk evaluations, which may not be adequate or address their perspectives. Self-directed assessments provide the context to understand the risks and to make informed decisions and trade–offs.

An Approach for Assessing Information Security Risk

To manage risks, you must understand what they are and then build mitigation plans to reduce the risks. The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠) Method is a security risk evaluation focused on the organization's assets and the risks to those assets. It is comprehensive, systematic, context driven, and self directed.

OCTAVE℠ is led and performed by a small, interdisciplinary analysis team of business and IT personnel who make decisions based on risks to the organization's critical information assets. OCTAVE℠ requires workshops to encourage open discussion and exchange of information. During the evaluation, the following catalogs are used to measure organizational practices, analyze threats, and build protection strategies—

- Catalog of practices—a collection of good strategic and operational security practices
- Threat profile—a collection of major sources of threats
- Catalog of vulnerabilities—a collection of technology weaknesses based on platform and application

The OCTAVE Method

OCTAVE[SM] uses a three-phase approach (Figure 1) to examine organizational and technology issues, assembling a comprehensive picture of the organization's information security needs. Each phase consists of several processes. These phases and their processes are described below—

Phase 1
Build Asset-Based Threat Profiles

This is an organizational evaluation. The analysis team determines which assets are most important to the organization (critical assets) and identifies what is currently being done to protect those assets. The processes of Phase 1 are—

1 **Identify Senior Management Knowledge.** Selected senior managers identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.

2 **Identify Operational Area Management Knowledge.** Selected operational area managers identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.

3 **Identify Staff Knowledge.** Selected general and IT staff members identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.

4 **Create Threat Profiles.** The analysis team analyzes the information from Processes 1 to 3, selects critical assets, refines the associated security requirements, and identifies threats to those assets, creating threat profiles.

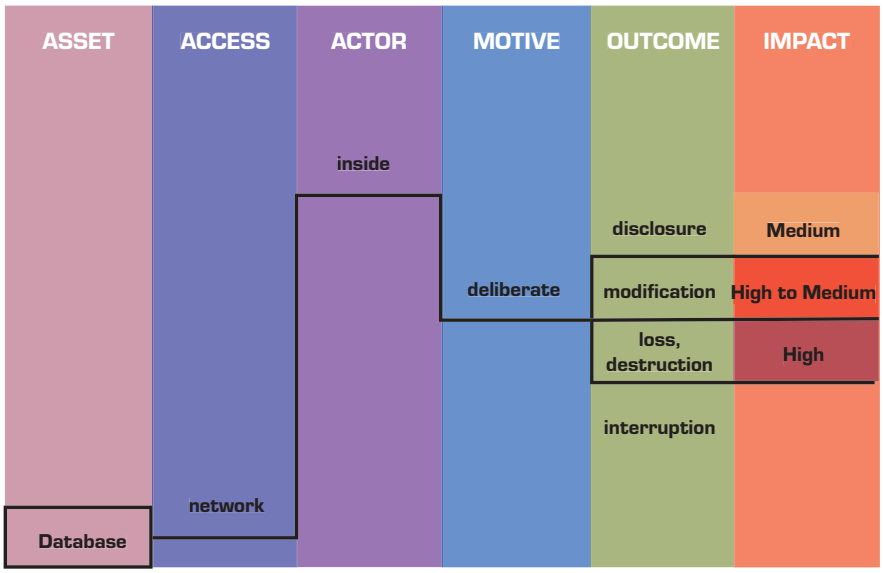


Figure 2. Partial Risk Profile for a Records Database

Phase 2
Identify Infrastructure Vulnerabilities

This is an evaluation of the information infrastructure. The analysis team examines key operational components for weaknesses (technology vulnerabilities) that can lead to unauthorized action against critical assets. The processes of Phase 2 are—

5 **Identify Key Components.** The analysis team identifies key information technology systems and components for each critical asset. Specific instances are then selected for evaluation.

6 **Evaluate Selected Components.** The analysis team examines the key systems and components for technology weaknesses. Vulnerability tools (software, checklists, scripts) are used. The results are examined and summarized, looking for the relevance to the critical assets and their threat profiles.

Phase 3
Develop Security Strategy and Plans

During this part of the evaluation, the analysis team identifies risks to the organization's critical assets and decides what to do about them. The processes of Phase 3 are—

7 **Conduct Risk Analysis.** The analysis team identifies the impact of threats to critical assets, creates criteria to evaluate those risks, and evaluates the impacts based on those criteria. This produces a risk profile for each critical asset. (See Figure 2 for a partial risk profile.)

8 **Develop Protection Strategy.** The analysis team creates a protection strategy for the organization and mitigation plans for critical assets, based upon an analysis of the information gathered. Senior managers then review, refine, and approve the strategy and plans.

continued on page 20

DIAP Reorganizes

Reflecting the DoD Defense-in-Depth Strategy

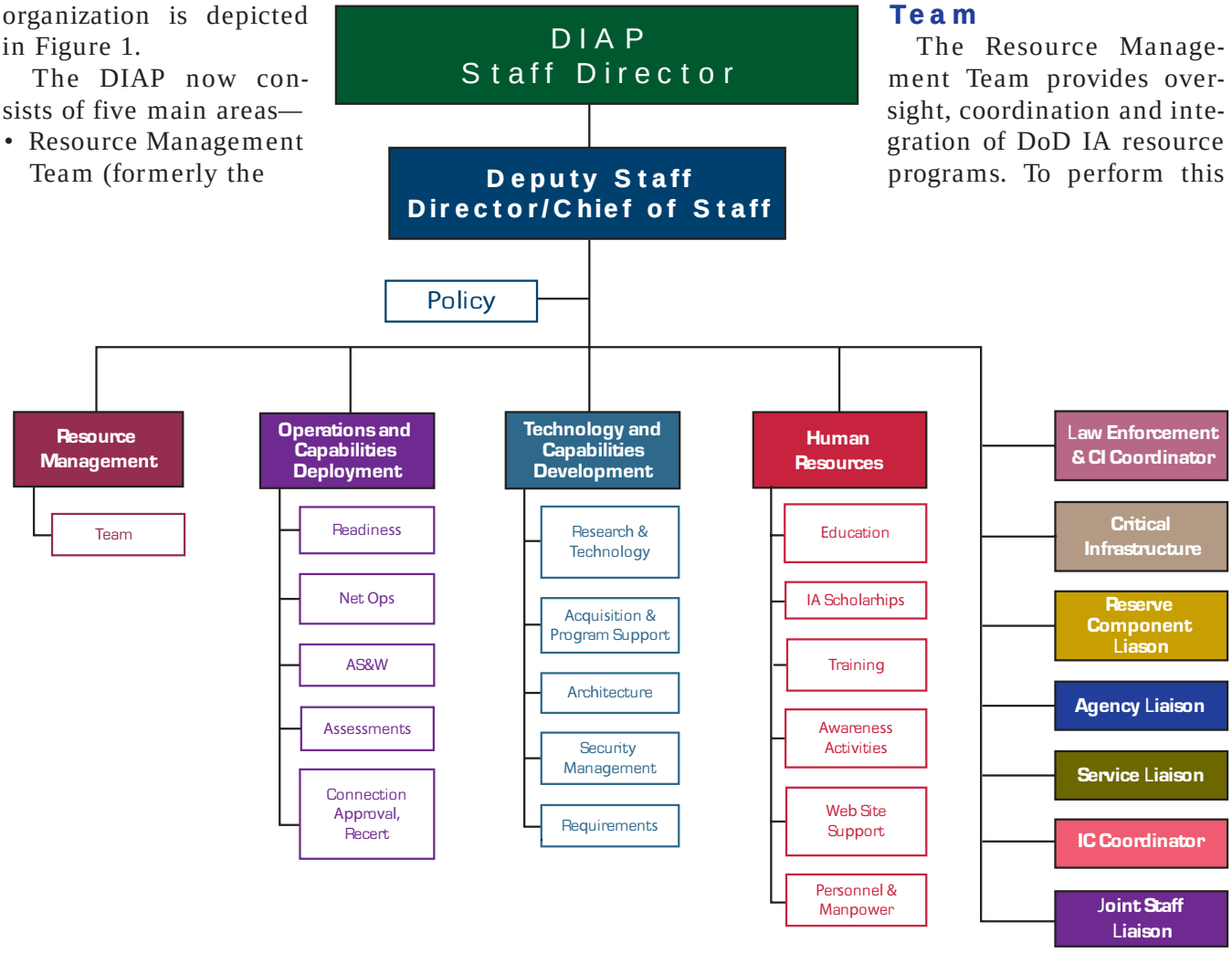
by CAPT J. Katherine Burton, USN

The Defense-Wide Information Assurance Program (DIAP) has gone through a number of changes since its inception in June 1998. As the organization grows in experience, providing oversight to the DoD IA programs, many different methods have been explored to provide the best view and accomplish the mission of the DIAP. One of the most important changes in the last year has been the reorganization of the DIAP to more closely reflect the DoD's Defense in Depth strategy. The new organization is depicted in Figure 1.

The DIAP now consists of five main areas—

- Resource Management Team (formerly the Program Development and Integration Team or PDIT)
- Operations and Capabilities Deployment Team
- Technology and Capabilities Development Team
- Human Resources Team
- Liaisons.

The former FEIT (Functional Evaluation and Integration Team) was broken up into areas that correspond to People, Operations and Technology and the functional areas contained within these three teams. The final area, Liaisons, formalizes the need to develop relationships with the DoD components and some unusual cross-functional areas such as the Law Enforcement/Counter-Intelligence Coordinator and the Reserve Component Liaison. The total structure provides a more understandable description of the various areas of concern that the DIAP must address. More details of what is covered in each area follows.



Resource Management Team

The Resource Management Team provides oversight, coordination and integration of DoD IA resource programs. To perform this

mission, the team develops IA program categories and transforms IA resources into operational capabilities. The team also is responsible for developing input to the Defense planning documents and for preparing the DIAP Congressional Justification Book (CJB) and the DoD CIO IA Annual report – a copy of which is available on the DIAP Web site. In its oversight role, the Resource Team monitors the IA plans, activities, and resources investments of Components and assesses the adequacy of the resources. In addition, the team prepares and coordinates responses to IA program queries from Congress; the Undersecretary of Defense, Comptroller; and the Office of the Director, Program Analysis and Evaluation (PA&E). Most recently, the Resource Team has been heavily engaged in the Quadrennial Defense Review (QDR), providing input to the various scenarios looking at IA capabilities as they are expressed in Defensive Information Operations. This activity has been in close cooperation with the CINCs/Services/Agencies to ensure realistic analysis is made with matching resources to capabilities.

Operations and Capabilities Development Team

The Operations and Capability Deployment Team provides the interface between OSD and the operational elements of DoD. Administratively organized into Readiness, Network Operations, Attack Sense and Warning, Assessments and Connection Approval Re-certification, the team addresses a broad area of issues related to IA in DoD network operations. Issues currently at the forefront include how to measure and report IA readiness, effectiveness of DoD and Service IA policies in protecting the networks, improvements in the IA Vulnerability Management process, and the operational impacts of proposed new policies and policy changes. The Team is also overseeing efforts to improve monitoring of DoD networks for intrusions and other attacks with an eye toward developing tools that will help predict upcoming network events to allow DoD to do proactive rather than reactive network defense. Additionally, the Operations Team provides advice to ASD/C3I on current and emerging cyber threats.

Technology and Solutions Development Team

Technology and Solutions Development Team is responsible for ensuring IA solutions are planned, designed, developed, and implemented for all DoD fielded Information Systems through a "cradle-to-grave", integrated, and systematic oversight approach. This approach incorporates IA policies and guidance within DoD regulations for Program Managers, developers, and information security professionals. The team engages program development efforts early on at the requirements definition phase to ensure compliance with IA policies and guidance. The goal is to ensure common IT architectures to leverage resources and enhance interoperability. The team also focuses the R&D community on developing IA solutions for the common good of the DoD and provides guidance to CINCs, Services, and DoD Agencies on implementing the DoD PKI, KMI, and Cryptographic Modernization roadmaps.

Human Resources Team

The Human Resources Development Functional Area addresses two interrelated concerns. The first relates to the training and certification of IA personnel. The goal is to develop and institutionalize the means for continually improving the education, training and awareness (ETA) of DoD personnel. The second relates to manpower and personnel. The goal here is to identify and tag IA billets, and to have career paths in place to ensure that IA billets are filled with personnel having the requisite knowledge, skills and abilities to perform the function. One initiative currently being given high priority is the DoD Information Assurance Scholarship Program (IASP). Scholarships will be available for non-DoD/government students as well as DoD military and civilian personnel. Information on the program is at http://www.c3i.osd.mil/iasp. The second high priority effort is development of a resource strategy to implement the recommendations of the 1999 Information Assurance (IA) and Information Technology (IT) Human Resources Integrated Process Team. Key recommendations of the IPT, listed here, will go a long way towards transforming the Department's IA work force to defend against cyberthreats today and in the future.

- Updating existing manpower and personnel databases to

continued on page 21

Tactical Decision Exer

by LtCol Michael Davis and Ms. Melissa Hathaway

The Department of Defense (DoD), like other public and private sector communities, is a computer and network dependent organization. The Defense Information Infrastructure (DII) and DoD computer networks that control and operate within it are becoming increasingly vulnerable to electronic attacks and intrusions. These vulnerabilities were highlighted during two major activities—Eligible Receiver 97 and Solar Sunrise. Currently, exercises relating to this challenge continue. However, we have moved beyond the need to expose the vulnerabilities and are now using exercises to develop practical and effective solutions to our network challenges.

DoD recognized this threat to the DII, and in response created the Joint Task Force for Computer Network Defense (JTF-CND). The JTF-CND was the department's initial focal point for the defense of its computer systems and networks. The JTF-CND achieved initial operational capability (IOC) on December 30, 1998, and full operational capability (24x7) in June 1999.

In October 1999, United States Space Command (USSPACECOM) assumed the CND mission and JTF-CND was resubordinated to that command. A year later, the Computer Network Attack (CNA) mission was similarly assigned to USSPACECOM through the Unified Command Plan (UCP). Upon the direction of CINCSPACE, the JTF-CND began the process of examining the requirements, mission, functions, organization, CONOPs, etc. to bring the CND and CNA missions together into one organization—the Joint Task Force for Computer Network Operations (JTF-CNO). Major General Dave Bryan, the Task Force Commander, called for a bottom up review of every process and paradigm, urging his staff to "think as warriors think" and to "consider all possible solutions, no matter how far 'out of the box' the solutions may seem." As the DoD focal point for network defense, he wants his command and people to be considered "world-class".

As part of this command focus, the J5 was directed to examine the established procedures for responding to everyday attacks against the DII and incorporating new training techniques to quickly bring staff to a level of ability to actively defend the networks, and plan if appropriate for measured response. To meet these needs the J5, assisted by IATAC personnel, commenced a training concept beginning with Tactical Decision Exercises (TDE) to help the command realize a new level of readiness.

TDEs are mini-exercises that provide the JTF-CNO with an immediate assessment of the organization's ability to accomplish its assigned mission in a focused area. Each TDE uses a scenario-based event-driven approach to focus on a particular training requirement, problem set, and/or staff section. At times, the TDE will include the entire command. TDEs are 2-4 hours in length and are currently being conducted monthly due to the influx of personnel and tempo of innovative attacks on the DII.

The J5 is using the TDEs to help refine current tactics, techniques, and procedures (TTPs) and validate the standard operating procedures (SOPs). The JTF-CNO is quickly growing and to capture the "corporate" knowledge and continue to sustain operations, it is necessary to document SOPs. Some TDEs highlight shortfalls in the policies and procedures,

cises Preparing the JTF-CNO for Mission Readiness

thereby enabling the command to document new procedures for future use. The JTF-CNO uses the TDEs to help validate the level of training required to be world-class and identify the training requirements necessary to sustain that stature.

The J3 (operations division) uses the TDEs to develop and practice Quick Reaction Plans (QRP) for crisis scenarios, such as malicious code handling procedures and response to unauthorized network activity. To accomplish this, it was determined that a TDE should be conducted in three phases. First, IATAC personnel would work with all staff sections of the JTF to develop a draft QRP. Second, after the draft QRP is produced, a mini-exercise is conducted to rehearse and validate the QRP. Finally, the QRP is reviewed to determine its effectiveness and adjusted if necessary. At the completion of this process, IATAC formats and delivers the final QRP for contingency execution.

The JTF-CNO has also found value in using the TDE concept to conduct no-notice recalls and examine its coordination procedures with Law Enforcement, Counter-Intelligence, and Intelligence communities. This has lead toward the development of measures of performance (MOP) and helping the command quantify its level of readiness.

Finally, TDEs provide a venue for improving DoD-wide understanding and knowledge of the JTF-CNO's capabilities. TDEs are used to prepare for CINC exercises and real world crises. The JTF-CNO has expanded its participation in these TDEs to include other commands, thereby introducing them to the support available for computer network defense and attack planning residing in the JTF-CNO. This also is helps ensure that military operations and campaign planning consider and integrate effective CNO capabilities.

TDEs are becoming increasingly important in assisting the JTF-CNO in improving its ability to defend networks. The TDEs and real world activities introduce challenging scenarios like the Red Worm virus to help staff polish their procedures. The importance of this is underscored daily as our military networks continue to confront attacks from adversary and criminal alike.

LtCol K. Michael Davis is the Director for Plans, Policy, and Exercises (J5/7) Joint Task Force Computer Network Operations. He received his B.S. (History) from the University of Louisville May 1979 and his M.A. (History) from George Mason University. He is a PhD Candidate in American History at George Mason University. He is a recipient of the Commendation with gold star/w Combat "V", Combat Action Ribbon. He has held a variety of command and staff assignment as a commissioned Marine Corps officer. He has been assigned to the JTF since it's activation in December 1998. LtCol Davis may be reached at davisk@jtfcno.ia.mil.

Ms. Melissa Hathaway is the IATAC Program Manager for all IO exercises and wargaming. She leads the IO Training & Exercise support team to the JTF-CNO. She has more than 12 years of experience in analysis, design, research, and development of IO and Command and Control Warfare (C2W) methodologies, training packages, wargames, system dynamics models, information systems, and databases. Ms. Hathaway earned a B.A. in International Studies and Government from the American University in 1990. She is a graduate of the Armed Forces Staff College, Joint Information Warfare Staff and Operations Course. She may be reached at iatac@dtic.mil.

It's About Time: A Metric for Availability

by Winn Schwartau

The destruction of the United States would be the ultimate in non-availability. To avoid that eventuality during the Cold War, the U.S. military defended the Nation with time.

If the Soviets got it into their heads to send over a six-pack of MIRV, the US had somewhere in the vicinity of 18-22 minutes to launch our thermonuclear response over the pole. The point was not to defend the citizenry; it was to destroy as much of their nation as we could in response to their attack. The 18 minute window was how long we had to respond before their nukes nuked our nukes. Yeah, a ton of people would die and then there was that 10,000 year uninhabitable planet issue to work out, but the real point was MAD: deterrence through Mutual Assured Destruction. Given the outcome of the Cold War, it seems to have worked.

Physical home and business protection is also measured in time and we see it in a staple of cops and robbers movies: A crook breaks into a jewelry store (or home). The alarm goes off. It dials the cops (20 seconds); the cops examine the call to make sure it looks real (20 seconds); the cops go to the scene of the crime, presumably not across the street from the police station (1-5 minutes). To be on the safe side, the robbers give themselves a maximum of two minutes for the whole heist. The quantifiable question is, how much can they steal in two minutes?

At the office, time is often the first tier of protection. You unlock the door, open it and then run like heck to the supply closet so you can enter the security code into the alarm system. You have 25 seconds to do that or, in theory, the rent-a-cops come a running in a few minutes.

But There is No Protection

The history of conflict has been based upon the military concept of Risk Avoidance through Fortress Mentality. How high can we build the walls to keep the marauding masses out of our wheat fields, lakes and castles? Did that approach work? The Great Wall of China was an historical insignificance. The Berlin Wall was purely symbolic and the Maginot Line was ignored by the Germans. Hunkering down in defense for an attacker's seven year siege hasn't worked (e.g., Troy, Hussein) and the same approach hasn't worked for the Internet-style hunkering down we have attempted to defend against online punkersterism. Just look at what's happening out there!

Using Fortress Mentality in computer and network technology as a defensive method assumes that things will work as they should – but we all know they don't and won't. Take a look—

- Increasing complexity causes software and networks fail regularly in unpredictable ways.
- Networks grow and thus change every day, changing network security posture no matter how hard we try.
- Administrators do not know every single network ingress and egress of their network. Modems, PC Anywhere, unknown phone lines and secret subnets plague organizations.
- Connecting enterprise networks to partner organizations with unknown security weakens a network's defensive strength.
- Seemingly harmless applications often innocently create security vulnerabilities.
- New hacks appear daily against leading applications, operating systems and security mechanisms. Organizations have a difficult time keeping up with every new one.
- It takes time and effort to install new patches to enhance security, and they don't always work.
- Well-designed security mechanisms are all too often installed incorrectly and/or completely misconfigured.
- Administrators often turn off security controls during audits and maintenance and forget to turn them back on.
- Testing the protective value of a network with any degree of assurance is valid only for the exact moment it was tested.
- Measuring the efficacy of security products or protec-

tive systems is not possible – yet. *(Read on!)*

Phew!

What that means is, no matter how many firewalls, passwords, policies or OS patches you apply, it's a sure bet that you won't be 100% protected. There is no silver bullet, right?

"What about perfect firewalls that only keep the bad guys out?" I often get asked. "Fine," I'll answer. "Show me a good IP and a bad IP address."—"Oh."

Sure, you can put in the perfect security—an air gap—but that defeats the whole purpose of networks in the first place; allow businesses to seamlessly communicate and interact with as many other networks and people as they can for whatever purpose they choose.

So, if the conventional protection mechanisms of "Fortress Mentality" don't work, what will? Let's go back to the jewelry store—

The owners know that the store's plate glass windows represent no defense or protection at all to their millions of dollars in jewelry. It's there for show and to keep the honest people out, not the criminals.

Now, for a bit of math. Let's say that Protection **(P)** equals '0', where **P** is measured in time. One hammer and it's all over; the bad guys are inside in an instant.

For our network analysis purposes, let's assume that all of our protective security efforts are for naught for the reasons listed above; they only serve to keep the good guys honest. Thus, as above, the Protection value in time, **P = 0.** (That is, of course, unless your favorite security vendor is giving a written guarantee to the contrary.) From a risk management standpoint, how can we say anything different? Do we have any confidence or proof or trust that our security mechanisms will hold up in light of new hacker attacks or glitch discovery? And for how long can we feel secure with the latest OS service pack? One week? One minute? One microsecond?

Our jewelry store, though, probably has good detection mechanisms to detect the bad guys doing bad guy things—taped windows, cameras, heat, sound and motion detectors. This represents another piece of the Time Based Security (TBS) approach—Detection, where **D** is also measured in time. In this case, a detection should occur in something less than a second; after all, smashing though a plate glass window is no small sonic event. So, let's say that in this case D = 1 second.

The next and last component in the store's security is Reaction, or **R.** The reaction has several steps—

- Dial the cops (or security force)—20 seconds
- The cops analyze the call—20 seconds
- The cops call a cop car to respond—20 seconds
- The cop car comes to the jewelry store—1-4 minutes *(These are wildly optimistic figures, to be sure, but from the bad guy's viewpoint, it is better to remain conservative and not to underestimate your adversary.)*

So, the robbers are assuming R = 2 minutes—that they have 120 seconds to commit the crime and hightail it out of the area.

Since we assume a value of **P = 0,** (no protection), the store's entire defensive posture is then measured by **D + R,** the combined time it takes the detection and reaction systems to work. In this case, **D + R = 121 seconds.**

If, however, we had any confidence in the protection value of the plate glass window (bullet proof, hammer–proof), we might use the following Time Based Security formula—**P > D + R** which says, "if the time value afforded me by a protection device is greater than the amount of time it takes to detect and respond (repair, halt) to an attack, then I have a secure environment."

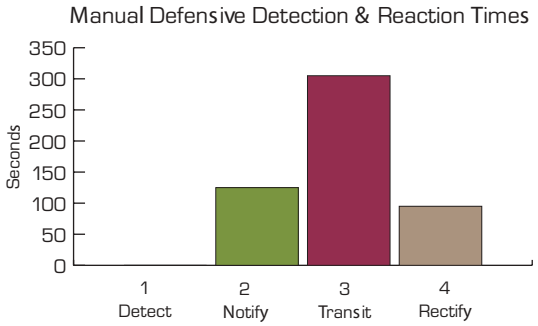


Figure 1. Total Exposure Time

The time value of **P** is the common metric in many physical examples of protection. In banks or for home security, the amount of security that vaults offer is measured in time: how long will it take a given oxy-acetylene torch of a given temperature to burn through the metal wall? These numbers provide a good metric base for choosing what kind of P-products, D-products and R-products to use in a complete defensive system.

But, since we do not know the measured protective strength **(P)** of systems in the networking world, we conservatively assign P a value of 0, thus giving us a new formula—

If **P = 0,** then **D + R = E,** where **E** represents Exposure, measured in time.

For the jewelry store their **E,** or exposure time, means that their greatest risk is how much can be stolen in 2 minutes. That value is no longer an information security number but one to be used by the bean counters, risk analysts and actuarial management who assess insurance rates. Assuming the **D + R** systems work, **E** becomes a quantifiable risk-measuring tool. The goal of course, is to make good business decisions which do not eliminate risk, but lower it to acceptable limits. Thus, in Time Based Security or TBS, we want **E → 0,** or Exposure time to approach zero.

To use TBS in the network world, then, we merely have to apply the same logic.

Detection: Let's say that your network is using really a whiz-bang Intrusion Detection System (IDS) and that it can detect any known attack in the universe in 10 seconds. In truth, such a system does not yet exist. Many organizations choose to implement several IDS to provide better coverage. For the sake of discussion, assume **D** = 10 seconds.

Now for reaction, **R,** which consist of three parts, Notification, Transit, and Rectification—

Notification: The IDS has to do something. Based upon more than 30,000 live audience members, that is generally to notify the administrator in charge either via page, E-mail or telephone. The average time value for this step is 2 minutes, or 120 seconds. This assumes someone is on duty. In some cases this value is as high as 64 hours.

Transit: The notified person has to get to a place where he can do something about the problem. Nominally let's allow five minutes. But consider the real world; corporate campuses, lunch hours, on the highway/airplane, midnight at home, weekends. How long does it really take?

Rectification: System Administrators will typically fix common problems in fairly short order, say less than two minutes. As with the transit time, we are using an optimistic time estimate to make a point.

So the **R** (reaction) component now equals 2 minutes + 5 minutes + 2 minutes = 9 minutes, for a total Exposure time of—9 minutes and 10 seconds.

E = D (10 sec.) + R (9 min.) = 9 minutes, 10 seconds

The question the systems administrator in combination with his risk management equivalents, legal staff, and auditors need to ask is: "How much damage can occur to our networks and our company in 9 minutes and 10 seconds of unlimited access by a bad guy." *(We're not looking at the insider problem yet.)*

Only you can come up with that answer...

Putting it Together

The TBS technique creates a new view of networks and their vulnerabilities by providing a common metric—time—to be used to gauge both risk and security under the same umbrella. We know (or should know) how fast our existing Detection and Reaction process is, even if we have no earthly idea how strong or weak our protective products and processes are.

The quantification of time to lost revenues, profits and image is not an exact science, but the distributed denial of service (DDoS) attacks of February 2000 demonstrated that big e-commerce sites are already looking at time = money in web site terms.

Now the acute reader will have already thought that TBS does not equally apply across the CIA infosec triad, and he is right. TBS does work in each case, but each one needs to be thought through and measured separately as breaches occur in different ways and over different time periods. There are charts and processes to apply TBS to each security fundamental.

Nonetheless, the most critical component of TBS is reaction, a completely overlooked component of security. The following matrix is representative of this component. Some reactions are automated, whereas others require system administrators to act. Note the time components;

these contribute to the **Exposure** time. Just as companies need to have a policy to implement security, they need to develop and be prepared to use a policy for reactions. Developing a reaction matrix is crucial for solving real-time security problems, but also for follow-up forensics, legal involvement, law enforcement investigation and prosecution.

The administrator needs to get the buy-in from management that under detected condition 'A' it is corporate policy for him to take reaction 'B', and then call management, the lawyers, police of aliens if necessary. I have seen companies come to a virtual halt because of a hacking incident because they lacked policies or procedures to respond. Ideally, someone will always be on duty or available in a short period to manage security events.

Unfortunately some people think that buying the strongest firewall or other security device is the solution. **Wrong.** The first steps are to measure existing detection and reaction systems, then determine if they are acceptable. Getting several values to approach 0 is core to TBS.

$$D \rightarrow 0$$
$$R \rightarrow 0$$
$$E = (D + R) \rightarrow 0$$

Only when we understand how the detection/response systems work with respect to our time metric can we realistically begin to choose the appropriate, risk managed choice, or protective systems.

There are many more Time Based Security formulas, which really help make the information security process quantitative rather than mere guesswork, but are outside the scope of this short article—

- How to determine exactly which files in a network are vulnerable
- How to protect those files with non-traditional security techniques that require few products.
- Solving Denial of Service
- Applying Defense in Depth to Time Based Security
- Extreme Intrusion Detection
- Protecting against the insider
- Tracking down the culprits

The offensive information warrior can also take advantage of the math of TBS. We have also developed a set of equations to measure the potential for successful attacks against target systems. If the target CND system also uses TBS, then it really comes down to the best implementation of TBS to see who wins.

Time Based Security is not a panacea to solve all security problems, but it does offer tools to rethink the traditional view of security, and adds the necessary dynamics to reflect defense in ever-changing environments. Perhaps most importantly, TBS adds a common metric to security, where we can measure each aspect of our security environment, quantify, replicate, and use them as benchmarks for performance today in the future.

If you have any comments or thoughts on how TBS can be expanded or improved, I look forward to hearing from you.

Reaction Matrix

Detected Event (Anomaly)	Chosen Reaction	Desired	Measured
3 Bad Password Attempts	Log and Notify Admin	1 second	2.40 seconds
3 Bad Password Attempts	Turn off Account/Notify Admin	1 second	0.94 seconds
Multiple Port Scan	Initiate Trace Route	250 ms	1.50 seconds
Internal User - Audit Behavior #1	Involve HR Immediately		
Ping of Death	Contact ISP to block IP[s]		
Syn-Ack Attack	Reaction #23		
Mail Bombs	Reaction #81		
Firewall Breach Attempt	Autofilter Source	100 ms	2.70 seconds
Traffic 2X Anticipated	Log and Notify Admin		
Multiple Site Attack	Shut Down Network	3 seconds	2 days
Shut Down $ Server	Isolate Network	1 minute	2.40 hours

Figure 2. A Reaction Matrix is critical for effective enterprise security.

As an acknowledged global expert in the field of information security, Mr. Schwartau has testified before Congress, advised committees and has consulted as an expert witness. He has written numerous books, including Cybershock, Time Based Security, and Information Warfare: Chaos on the Electronic Superhighway. He has appeared regularly on popular US, European and Asian television shows, (CNN, BBC, ABC, CBS, NBC, CNBC), as well as hundreds of radio shows nationwide. He is President of Interpact, Inc. and founder of NiceKids.Net, Inc. www.nicekids.net, *a cyber-ethics Web site for kids, parents, families and teachers. He also founded Infowar.Com (*www.infowar.com*) and the US/EU InfowarCon Conferences. He is one of the country's leading experts on information security, infrastructure protection and electronic privacy is often referred to as "the civilian architect of information warfare." Mr. Schwartau may be reached at 727.393.6600 or* winn@interpactinc.com.

Endnote

1. Based upon the book, *Time Based Security*, Winn Schwartau, Interpact Press, 1999, 2001. ISBN: 0-9628700-4-8

Evaluating Information Security Risks Using Octave

continued from page 11

Results of Pilot Tests

The SEI completed early testing of OCTAVE[SM] using a lightly facilitated version of the method. Later tests focused on training analysis teams to conduct their own evaluations. The testing has shown that the method works as designed. Our findings include the following—

- The analysis team was able to analyze the data and make decisions that fit best with their missions, consulting with additional personnel as needed.
- The single most critical success factor is senior management sponsorship.
- A major benefit for analysis team members was learning about their organization and about information security.
- The catalog of practices was beneficial in educating participants about good security practices.
- The threat/risk profile enabled the analysis team to perform a gap analysis between perceived threats and possible threats.

Summary

OCTAVE[SM] is a security risk evaluation focused on the organization's assets and the risks to those assets. It is comprehensive, systematic, context driven, and self directed. It enables people at all levels of an organization to work together to identify and understand their security risks and to make the right decisions about mitigation and protection.

Christopher Alberts is a member of the technical staff in the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI). Alberts is the team leader for security risk evaluations and is responsible for developing and delivering information security risk management methods, tools, and techniques. He is currently leading the development of Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE[SM]), an information security risk assessment technique, designed to be self-directed by organizations. Alberts has B.S. and M.E. degrees in engineering from Carnegie Mellon University.

Audrey Dorofee is a senior member of the technical staff in Survivable Network Management Project in the Network Survivable Systems (NSS) Program at the Software Engineering Institute (SEI). Dorofee is currently working on OCTAVE[SM], a self-directed Operationally Critical Threats, Assets, and Vulnerabilities Evaluation. She was previously a project lead and senior MTS for the SEI Risk Management and Software Engineering Process Improvement programs, where she was an author of the Continuous Risk Management book, training courses, and transition products. Dorofee received a B.S. in computer science from the Florida Institute of Technology and an M.S. in computer science from the University of Houston at Clear Lake City.

Endnote

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University. See www.cert.org/octave/ for more information.

continued from page 13

track personnel with IT/IA expertise performing IT/IA functions
- Implement recruiting and retention incentives for military and civilian personnel in IT/IA specialties
- Establishing minimum mandatory education and training requirements for personnel in IA functions
- Standardizing criteria for certification of personnel performing IA functions.
- Including contractor personnel in certification requirements
- More information on IPT recommendations is in the "Information Center" of the DIAP Web site www.c3i.mil/org/sio/ia/diap.

Liaisons

DIAP maintains many liaison positions that enable it to work more effectively with the various CINCs/Services/Agencies (C/S/A). These liaisons allow DIAP to address issues specifically related to a particular activity and to initiate, coordinate, s and oversee IA activities. DIAP has liaison elements to the following communities—

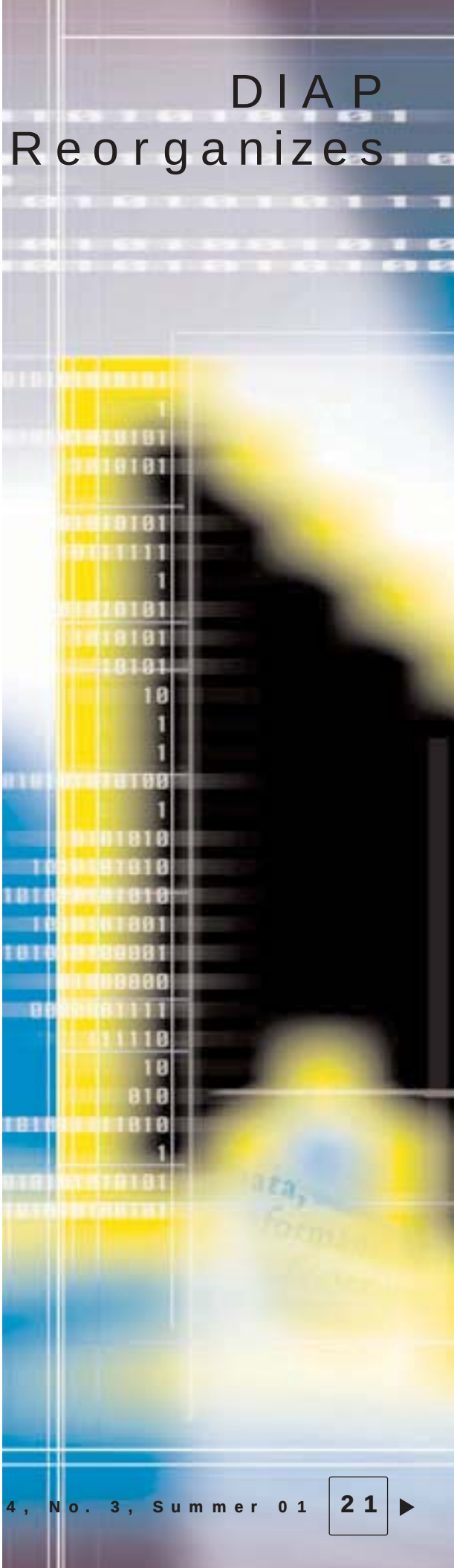
- Law Enforcement and Counterintelligence
- Intelligence
- Critical Infrastructure Protection
- Joint Staff
- Reserve Component Services Agencies

The liaisons form a critical link between the functional and programmatic resource areas and the actual activities.

The DIAP will continue to evolve both in form and in function as Information Assurance becomes more embedded in the DoD's processes. I have enjoyed participating in this evolution for the last three years and getting to know the IA experts throughout DoD. We have all grown together and everyone's efforts have all contributed to the significant improvement in the Department's IA posture. As I get ready to hand over the reins to my relief, Colonel Gene Tyler, U.S. Army, I want to thank everyone with whom I have had the pleasure to work. I know Colonel Tyler will continue to carry on the work we have all begun and take the DIAP to even greater accomplishments during his tenure as the DIAP Staff Director.

Captain J. Katharine Burton graduated from the University of Oklahoma (OU) in May 1976 with a B.A. in English Literature. Captain Burton is a 1998 graduate of the National War College where she received an M.S. in National Security Strategy with a certificate from the Information Strategies Concentration Program. She also holds an M.A. in Management Information Systems from George Washington University and is a 1986 graduate of the Armed Forces Staff College. Since 1997 she has been assigned as the Staff Director, Defense-Wide Information Assurance Program (DIAP), in the Information and Infrastructure Assurance Directorate of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I). CAPT Burton has recently been assigned as the Assistant Deputy Manager, National Communications System.

DIAP Reorganizes



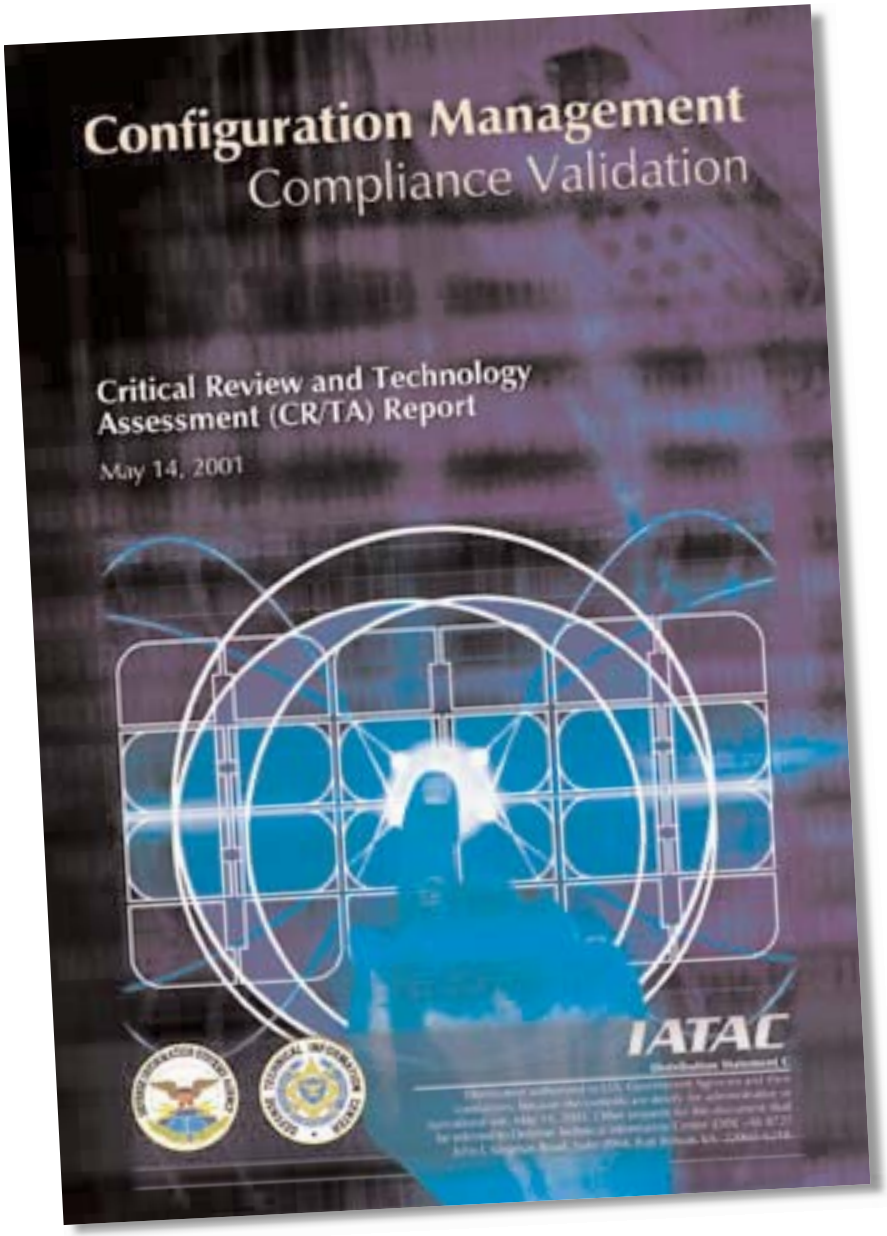
Configuration Management Compliance Validation

by Thomas J. Perrault

On February 7, 2001 the Under Secretary of Defense (Acquisition, Technology, and Logistics), Systems Engineering Office approved the Military Handbook, *Configuration Management Guidance, MIL-HDBK-61A(SE)* for use by all DoD Departments and Agencies. Although this document can only be used for guidance, it helps to ensure that the application of product and data configuration management to defense material items is utilized in each phase of their life cycle.

A shift has occured from Government imposed requirements on the contractor to the Government asking contractor how they intend to apply standard management practices to a given program and evaluation of those practices by industry standards.

- Limiting the focus of Government configuration control to performance requirements rather than detailed design solutions.
- Basing Government oversight of contractor practices on process rather than inspection of product.



The second significant transition of configuration management results from the rapid advance of information technology. The change from paper to digital and the concepts for automated data access, transfer, and sharing, increases the Government and industry capability to integrate from distributed sources. This is leading to a virtual enterprise need for configuration management (CM) to establish productive Information Assurance (IA).

The increasing technological sophistication leads to potentially crippling vulnerabilities and makes CM a critical element in minimizing the disruption, denial, degradation, destruction or disclosure of information. To maximize the efficiency of each system, commanders and leaders at every level should have a working knowledge of the CM process. This Critical Review and Technology Assessment (CR/TA) provides an overarching understanding of CM and the challenges to meet the needs. Figure 1 provides an overview of the CM Process

Model and the critical elements it contains: Inputs; Constraints; Mechanisms/Facilitators, and Outputs/Results.

This CR/TA is divided into the Introduction and eight main areas covering: CM Background; CM Standards, Requirements, and Guidance; CM Evolving Objectives, Information Assurance (IA) Perspective; Education and Training; National Consensus Standard Matrix for CM, and Current and Future Assessment of CM. In addition, the appendices provide: Abbreviations; Terms and Definitions; Overarching Configuration Management (CM) Sources; IEEE CM Reference Material; Selective CM Tools; U.S. Department of Dense and NATO Reference Material; U.S. Federal Government Reference Material; International Standards Organization (ISO) CM Reference Material; International Reference Material; Education and Training Courses; Conference Listings, and Various Societies, Institutions, Associations, and Documentation.

The basic principles that drive the CM discipline have been developed over the past thirty to forty years and are now stable and well defined. However, due to the automation and rapid applications development capability, CM practitioners will be challenged to break new ground in the design and implementation processes, particularly within computerized systems in the IA arena. Increasing enterprise wide management is based upon detailed integration and coordination. Selection of new powerful CM software products will provide the tools necessary to meet rapid applications development and reduced life cycle time.

Future trends indicate that CM is now and will continue to be driven by changes and advancements in information technology. IA professionals can obtain powerful methods to verify and validate each facet of infrastructure operation and establish baselines for effective IT defense perimeters. CM is a broad based pallet of capabilities to manage, document, and report the "cradle to grave" aspects of the IT environment. Therefore, it is given that these tools should be exploited to their full potential.

Mr. Thomas J. Perrault holds an M.S. degree in Information Systems Telecommunications from the Naval Postgraduate School and a B.A. from Salem State College, Salem, and Massachusetts. He has extensive Configuration Management (CM) experience in DoD, healthcare information management systems, and international Command, Control, Communications, Computer and Intelligence (C4I) systems. Mr. Perrault is providing technical support to the DISA Standard Perimeter Defense Task to develop a CM Plan that describes the installation, maintenance and operation, and activities and schedules for firewall administration within DISA. He may be reached at iatac@dtic.mil.

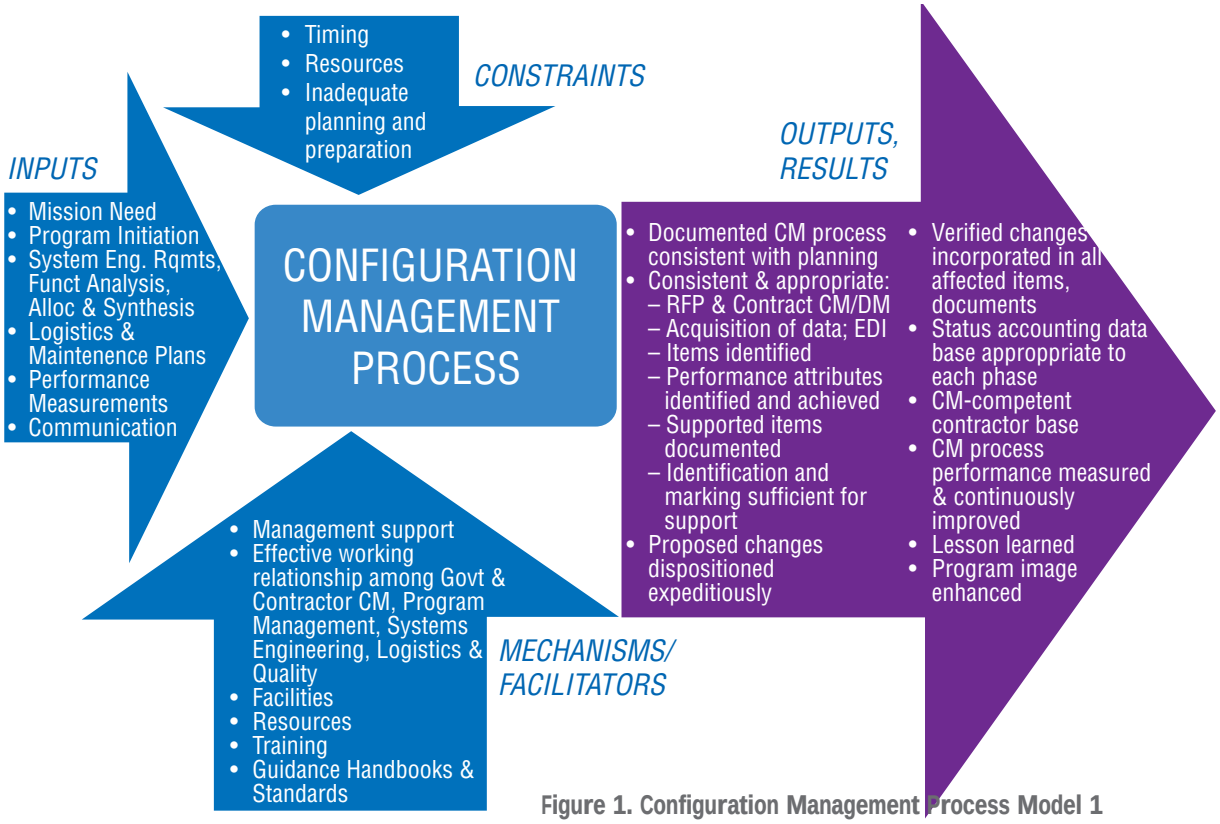
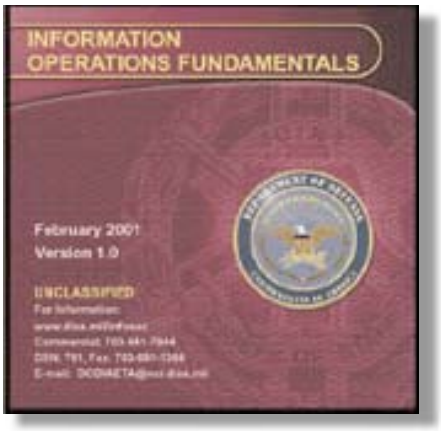


Figure 1. Configuration Management Process Model 1

DISA Implements Web Based Training

NOTE: *These products are Web-deliverable, using html and Flash technology. They can be loaded on Web servers for delivery via the Internet or intranet. As with our traditional products, they also run on a LAN or from a CD-ROM drive.*



IO Fundamentals

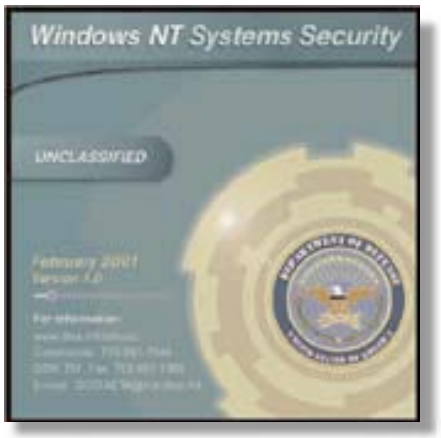
IO Fundamentals provides an overview of IO in the joint context throughout the range of military operations. It addresses IO principles relating to both offensive and defensive IO and describes responsibilities for planning, coordinating, integrating, and deconflicting joint IO. This product is based on Joint Publication 3-13, "Joint Doctrine for Information Operations." IO Fundamentals is an update and expansion of INFOWAR Basics.

Secret and Below Interoperability (SABI)

This product explains SABI, a network-centric process that incorporates risk management into all decisions for secret and below connectivity. It discusses the core functions and goals that have been established for the SABI process. The roles and responsibilities of the SABI community are addressed in detail.

UNIX Security for System Administrators

This product provides a basic understanding of UNIX Security. It is designed to help the beginning to intermediate-level administrator understand what makes up a secure UNIX system, what tools exist to protect the system, and provide assistance in the day to day tasks of monitoring and securing the network. At the completion of this course, the user will understand different UNIX environments and their origin, various UNIX threats and appropriate countermeasures, and basic encryption and security concepts. In addition, the user will learn fundamental system administration concepts, including basic commands, specific tools, network maps, sniffers, and network vulnerabilities. The resources section features links to relevant computer security web sites and a glossary of terms. Virtual hands-on exercises are provided throughout. While the exercises are based on Solaris, comparable commands in Linux Red Hat and HP-UX are demonstrated.



Windows NT Security

Windows NT Security details the steps necessary to safeguard system resources in a standalone or networked Windows NT operating environment. It provides virtual hands-on exercises to reinforce instruction of key security features. The target audience for the product is system administrators, ISSOs, and other personnel responsible for information systems administration. The user should have a basic hands-on understanding of computer systems and applications. The Resources section contains a library of Windows NT security documents to support and augment the content and exercises in the modules. There are also links to web sites related to Windows NT security.

To order go to www.iase.disa.mil

CyberProtect

CyberProtect is an interactive computer network defensive exercise with a video game look and feel. It is intended to familiarize players with information systems security terminology, concepts, and policy. Players learn about defensive security tools, which must be judiciously deployed on a simulated network. They then face a spectrum of security threats and must make practical decisions for allocating resources (in quarterly increments) using the elements of risk analysis and risk management. Play is divided into four sessions (simulating a fiscal year). After each session, players receive feedback on how well they are doing. At the end of the last session, players are given a report detailing their cumulative operational readiness rating. The report also details every attack by type, origin, and effectiveness of defensive tools.

Designated Approving Authority (DAA) Basics

This interactive CD-ROM highlights the duties and responsibilities of the DAA (in industry, the Chief Information Officer (CIO) may have these responsibilities). The user will learn about members of the DAA's team, including the Information Systems Security Manager (ISSM), General Counsel, Program Manager, Information Systems Security Officer (ISSO), User Representative, and the Certification Agent. This presentation covers the acquisition process, certification & accreditation (using the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) as a representation), legal and regulatory issues, and risk management. Roles of team members are discussed throughout. A glossary of terms and a resources section with relevant Web sites and documents are provided for reference. The information in this product can also benefit mid level and senior managers.

DoD INFOSEC Awareness

This interactive CD-ROM explains the need for information systems security and cites recent examples of security violations. The user will learn the definition of information systems security, along with relevant public laws and government policies pertaining to information security. Other topics include external threats to information security, the evolution of information systems security, user roles and responsibilities, and malicious logic. A glossary of terms and a directory of where to find help within the Department of Defense (DoD) are provided for reference.

To order go to
www.iase.disa.mil

Information Age Technology

This interactive CD-ROM provides an overview of basic information technology infrastructures, such as the Defense Information Infrastructure (DII), National Information Infrastructure (NII), Global Information Infrastructure (GII), and Intelligence Information Infrastructure (III). Elements of information transportation, such as speed, throughput, security, cost, and distance are considered. The hardware and resources used to support these information infrastructures, with an emphasis on communication devices used to access, process, and transmit information across telecommunications systems are highlighted. There is a module on transportation modes for information flow via local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). Tools for managing network resources are also discussed. Examples and real life analogies are given throughout the presentation. The resources section contains several web sites to learn more about topics discussed in this CD-ROM.

What's New

I want to take just a moment to encourage our readership to visit the IATAC Web Site http://iac.dtic.mil/iatac.

Hosted by the Defense Technical Information Center (DTIC), we've made a number of major changes during the past year, which has resulted in an exponential increase in visits. Some of those changes include posting our various products (Tools Reports, CR/TA, state-of-the-art reports (SOAR), and newsletters), automated inquiry support, and feedback to IATAC. Please visit and if you have suggestions for continued improvement, don't hesitate to engage.

During the past few months we added responses to inquiries along the lines of "frequently asked questions" or "FAQs." We have also posted abstracts of work executed under the Technical Area Task (TAT) program as a reference point. Items that appear useful or interesting may be requested from IATAC within the prescribed bounds of the document's distribution statement set by the supported organization.

New Products

IATAC's new Configuration Management Compliance Validation CR/TA is now available. The article on page 22 describes the report. It may be ordered on our Web site or by completing the order form on page 27.

Malicious Software

Today in 2001, the danger presented by malicious software to our nation's computer-based mission critical systems is greater than ever. The number of malicious code incidents continues to increase and, in several well-publicized instances, the impact to commercial information technology (IT) infrastructures has been substantial. A legitimate question arises; what does this mean to the DoD and its readiness to defend the nation and project force throughout the world.

IATAC will be releasing the Malicious Software SOAR this Fall. The approach taken to bound and develop this SOAR was influenced by the answers to the following questions—

- Should the report mirror the structure and content focus of the first report or changes be made?
- Should the report focus on yet-to-be-proven technologies and tools?
- Should the report continue to present trends that are synthesized from more recent commercial and DoD events, activities and capabilities?

The report provides insight into the DoD malware problem by making various assertions in the form of observed trends. The trends are intended to be of significant consequence to the target DoD audience. Those stakeholders were also interviewed to determine existing or planned efforts to combat malware and to uncover concerns and views regarding malware.

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 (unless you are DoD or Government personnel). TO REGISTER ON-LINE: http://www.dtic.mil/dtic/regprocess.html.

Name _____ **DTIC User Code** _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

LIMITED DISTRIBUTION

IA Collection Acquisitions CD-ROM

❑ Fall 2001edition

Critical Review and Technology Assessment (CR/TA) Reports

❑ Biometrics ❑ Computer Forensics* ❑ Defense in Depth ❑ Data Mining

❑ IA Metrics ❑ **Configuration Management—NEW!**

IA Tools Report

❑ Firewalls (2nd Ed.) ❑ Intrusion Detection (3rd Ed.) ❑ Vulnerability Analysis (2nd Ed.)

State-of-the-Art Reports (SOARs)

❑ Data Embedding for IA ❑ IO/IA Visualization Technologies ❑ Modeling & Simulation for IA

❑ **Malicious Software (Release due Fall 2001)**

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

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	❑ Vol. 3, No. 3	❑ Vol. 3, No. 4
❑ Vol. 4, No. 1	❑ Vol. 4, No. 2	❑ Vol. 4, 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

Sep 26—27

Security Cooperation 2001 Conference
Ritz Carlton Hotel,
Pentagon City, Arlington, VA
Hosted by the Defense Security Cooperation Agency (DSCA)
POC: Mr. Glenn Lazarus,
703.601.3855
http://ocl.nps.navy.mil/dsca

Oct 22—26

Information Warfare Seminar
IRM College,
National Defense University
Secret (US Only) seminar offers information warriors the latest developments in IO doctrine, policy and strategy.
http://www.ndu.edu/irmc

Oct 28—31

MILCOM 2001
Sheraton Premiere at Tysons Corner, VA
COME SEE OUR NEW BOOTH!
http://www.milcom.org/2001

Oct 30

Information Assurance Technical Framework Forum Meeting
Kossiakott Center, John Hopkins Applied Physics Laboratory
POC: John Niemczuk,
410.684.6246
http://www.iatf.net

Dec 10—14

Computer Security Applications Conference
New Orleans, LA
http://www.acsac.org/2001

Jan 15—17

WEST 2002
San Diego, CA
http://www.west2002.org

Mar 10—24

Computer Emergency Response Team Operation Training Experience (CERT OTE)
Regional Training Institute (RTI), Camp Johnson, Colchester, VT
A 15-day resident course to train Local CERT members to respond to intrusions and protect computer networks. Contact your training section to register under school code 1019.
POCs: Jeanette Martin-Smith, 802.338.3283
MAJ Dan Molind, 802.338.3283

IATAC

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