IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 6 Number 3 • Winter 2003/2004

A New Strategy— A New USSTRATCOM

also inside—

- The Road Ahead for Computer Network Defense Service Providers
- Zen and the Art of Scanning Networks
- INFOSEC Research Council
- SARS, Tylenol™, and Malicious Code
- A Framework for IA

contents

feature

4 **A New Strategy—A New USSTRATCOM**
by USSTRATCOM Public Affairs
The "strategic" in U.S. Strategic Command (USSTRATCOM) is no longer synonymous with the term "nuclear." Rather, the new command offers a wider range of strategic and globally oriented warfighting options—both conventional and non-conventional within a compact period of time.

IA initiatives

6 **The Road Ahead for Computer Network Defense Service Providers**
by Dr. Buzz Walsh and Ralph Ghent
The OASD for Network and Information Integration, together with DISA and NSA, chartered a project to collect, deconstruct, and analyze relevant DoD and commercial training to assist DoD components preparing for certification and accreditation.

12 **Zen and the Art of Scanning Networks—A Tour of Scanrand 2.0**
by Dan Kaminsky, CISSP
Enormous quantities of assets, supporting critical operations distributed worldwide, remain managed through only rough estimate and the occasional disruptive audit. Radio Frequency Identifier (RFID) technology truly promises to make assets in the real world just as easy to centrally manage as nodes on a digital network.

18 **INFOSEC Research Council—What is the INFOSEC Research Council?**
by John Davis
The INFOSEC Research Council (IRC) provides informal technical coordination of Information Security research plans and programs across the DoD, the Intelligence Community, Homeland Defense, and the other Federal Civil agencies.

20 **SARS, Tylenol™, and Malicious Code**
by Tom Ward, April Perera, Tim Madden
Comparing the commonalities shared by biological causes, criminally depraved intentional acts, or mischief within the cyberworld can provide insight into better preparation against malicious code attacks.

23 **USSTRATCOM/JTF–CNO 1st Semi-Annual JTF–CNO Computer Network Defense (CND) Community of Interest (COI) Conference**
by Tim Madden
The purpose of the conference was to promote intelligence community support for a variety of CND needs, from strategic to operational.

24 **A Framework for Information Assurance**
by Abraham T. Usher, CISSP
The growing dependence of these three groups on public information and communication assets requires greater vigilance in protecting these resources. This article presents a framework for thinking about IA in a simple, yet comprehensive manner.

in every issue

3 **IATAC Chat**

31 **Product Order Form**

32 **Calendar of Events**

About IATAC & the *IAnewsletter*—

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

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

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

IATAC Director: Robert J. Lamb
Deputy Director: Abraham T. Usher
Inquiry Services: Peggy O'Connor

IAnewsletter Staff—

Creative Director: Christina P. McNemar
Art Director: Ahnie Senft
Designers: Maria Candelaria, Holly Shipley
Editorial Board: Abraham T. Usher, April Perera, Jim Peña, Brad Soules

IAnewsletter Article Submissions

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

IAnewsletter Address Changes/Additions/Deletions

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

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

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

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

Deadlines for future Issues—
Spring 2004 January 30, 2004
Cover design: Maria Candelaria
Newsletter design: Ahnie Senft

Distribution Statement A:

Approved for public release; distribution is unlimited.

IATAC Chat

Robert J. Lamb, IATAC Director

Over the past several months, we have been working to enhance our subject matter expert (SME) database. With the encouragement and support of the IATAC Steering Committee, we have expanded our database considerably and are continuing to do so. Our objective is to make this database a resource for the IA community to leverage.

IATAC's SME database is comprised of a diverse group of Information Assurance (IA)/Information Operations (IO) professionals from academia, Department of Defense (DoD), Government Agencies, research and development (R&D) institutions, and industry.

Our objective for the SME database is to provide a resource for the IA and IO communities to query for expertise and support in solving problems. We've done a couple of things towards populating the database, which I wanted to share with you in this newsletter.

One of the first questions we had is what constitutes an expert and how should we organize the SMEs into a coherent construct of IA topics or domains that are both manageable and useful.

First, what constitutes an SME? In general we identified five criteria: knowledge, skill, experience, education, and training, with some criteria or guidelines to help gauge that expertise.

- **Knowledge**—Published one or more articles or books, spoken at one or more professional forums, served on a blue ribbon advisory committee
- **Skill**—Satisfied the skill demonstration requirements for industry certification at the journeyman or master level; satisfied the skill demonstration requirements for Government certification at the journeyman or master level; possess a professional license in the subject area
- **Experience**—Amassed eight or more years of professional experience
- **Education**—Holds an advanced degree from an accredited university in the subject area
- **Training**—Completed sufficient training in the subject area to satisfy the training requirements for industry certification at the journeyman or master level; satisfied the training requirements for Government certification at the journeyman or master level.

The SME domains are based on the Institute for Information Protection (I3P) taxonomy and are broken out into 114 different subject areas related to IA (see http://www.thei3p.org for more information about I3P). The 10 top-level categories are—

1. General Information Assurance (5 pillars of confidentiality, integrity, availability, authentication, non-repudiation)
2. Information warfare
3. Malicious code
4. Policy, standards, and guidance
5. Security testing and evaluation
6. Risk assessment
7. Wireless security
8. Information operations (psychological operations, computer network operation, operational security, electronic warfare, physical destruction, etc.)
9. Security tools (IDS, firewall, vulnerability scanners, forensics, etc.)
10. Cybercrime

While not a perfect match, it provides an organizing construct from which to work. SMEs that have skills that don't cleanly fit into a category have the option of entering their skills in an "other" category.

We would ask that if you are interested in becoming a part of the SME database and willing to provide technical support to others in your domain expertise, please contact us at iatac@dtic.mil and we will send you a URL to complete the SME application.

Second, if you have a technical question, please exercise this resource by contacting us and we will work to link you with the SME best suited to helping you solve the challenge at hand. And, if you have any questions about the program, please don't hesitate to contact us. ■

A New Strategy—A New USSTRATCOM

by U.S. Strategic Command, Public Affairs Office

Those passing by U.S. Strategic Command (USSTRATCOM) headquarters likely will not notice anything different. The same U.S. Air Force and U.S. Navy missiles point to the Nebraska sky in front of the LeMay Building main entrance. Electronic gates and security forces stand guard at the entrances. But appearances can be deceiving.

The large complex across from the Offutt Club that rests on top of the hill with the Minuteman and Trident missiles is, today, more than just a nuclear command post. The "strategic" in U.S. Strategic Command, for example, is no longer synonymous with the term "nuclear."

Rather, the new command offers the President a wider range of strategic and globally oriented warfighting options—both conventional and non-conventional within a compact period of time.

The need to integrate missions increased dramatically following the unification of the former USSTRATCOM with U.S. Space Command (USSPACECOM) October 1, 2002. The former USSTRATCOM served as the command and control center for U.S. nuclear forces. With the merger, USSTRATCOM added all Department of Defense (DoD) space operations and space support to its mission and became the DoD lead for computer network defense (CND).

Previously unassigned missions

The evolution of USSTRATCOM continued with announcement last year by President Bush that the command would assume responsibility of several previously unassigned mission areas—

- Global strike
- Integrated missile defense
- DoD integrated information operations (IO)
- Command and control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR)

USSTRATCOM has moved from a planning-focused headquarters to a command that oversees global operations. All of the changes are designed to help USSTRATCOM efficiently meet its global mission requirements for the joint warfighter. The following outlines how the four directorates and Joint Force Headquarters for Information Operations support the new USSTRATCOM mission areas.

- **Global Operations**—The Global Operations Directorate coordinates the planning, employment, and operations of DoD strategic assets and combines all current operations, global command and control operations, and intelligence operations. The directorate includes all Command Center operations, the Joint Intelligence Center, Current Operations, and the National Airborne Operations Center. Intelligence is an operational "output" of the new USSTRATCOM, closely aligned with other day-to-day operations in order to do its mission and improve the use of intelligence data in other mission areas.
- **Combat Support**—The Combat Support Directorate provides the organization and functions required to direct the support necessary to provide the staff with acquisition, contracting, combat logistics and readiness, C4 for strategic forces, intelligence, and global C2 in support of all assigned missions.
- **Policy, Resources, and Requirements**—This directorate is responsible for developing overarching policy to support execution of all the command's missions. It is also responsible for the articulation and development of all command requirement processes to ensure that USSTRATCOM has the tools to accomplish its mission, and it ensures appropriate decision support tools and assessment processes are in place to enhance operational capabilities.
- **Strike Warfare**—The Strike Warfare Directorate includes the Targeting Intelligence Center and three divisions: Global Strike, Combat Plans, and Planning/Targeting Tools. This directorate provides integrated global strike planning, and command and control support to deliver rapid, extended range, precision kinetic (nuclear and conventional), and non-kinetic (elements of space and information operations) effects in support of theater and national objectives.

- **Joint Force Headquarters–Information Operations**—Joint Force Headquarters–Information Operations incorporates, integrates, and synchronizes the various IO disciplines that enable the commander to use defensive and offensive IO in support of USSTRATCOM missions.

Relying on space

One of USSTRATCOM's challenges is to apply the operational experience gained during the global war on terrorism to flesh out the use of space forces in theater operations.

The ADM emphasizing the importance of space capabilities in achieving warfighting objectives stated—

"Space is essential to everything we do. Space support covered the entire landscape of Operation Iraqi Freedom and provided a level of precision that gave coalition forces the ability to not only understand first but to act first as well."

ADM James O. Ellis, Jr.
USSTRATCOM Commander

Space capabilities are often transparent—even to those who depend on them. Global positioning information, for example, allowed coalition forces to fight during sandstorms and take out military targets with minimal impact on civilians. U.S. forces were able to deliver global positioning system (GPS) munitions within minutes of receiving intelligence data.

The command, however, can't rest on its laurels, said Ellis. He said the command would now strive to further refine its support to the nation's warfighters.

Only by integrating the command's aggregate strengths will USSTRATCOM bring its entire range of global capabilities—space, missile defense, planning, communications, information operations, kinetic and non-kinetic strike, and intelligence—and ensure the U.S. military stays one step ahead of any adversary, he said. Coordinating the application of the command's vast capabilities and providing a single source for space-based capabilities that cuts across military and space boundaries is vital.

In previous operations, space support has been applied when and where needed but required too much time and effort by a theater commander to synchronize, said Ellis.

"Until now, theater support in our mission areas has been supplied a la carte…It's like single riders from a frontier cavalry troop arriving simultaneously or nearly so from all points of the compass at the same time."

For example, Ellis said USSTRATCOM is now uniquely positioned to help plan and support an effort to combine military and national security space operations. Streamlining the chains of command and avoiding duplication in space operations is one of the command's key priorities.

"Our vision must be a unified cavalry capable of a coordinated charge,…That means our professionals plan, train and execute side-by-side with regional warfighters so they are ready to deploy forward when called upon to bring unique USSTRATCOM capabilities to bear."

A fresh look at IO

As the revamped USSTRATCOM moves into its second year, its leaders are focusing on new challenges that accompany burgeoning space capabilities and, in light of those challenges, are calling for a "fresh look" at IO.

As displayed in recent operations in Afghanistan and Iraq, combatant commanders today must operate in a multidimensional battlefield with IO missions that include computer network operations, electronic warfare, psychological operations, military deception, and operational security. Yet each of the military Services and national security agencies has some type of IO program.

continued on page 17…

The Road Ahead for Computer Network Defense Service Providers

by Dr. Buzz Walsh and Ralph Ghent

Very shortly, the Department of Defense (DoD) will publish a new manual, O–8530.1–M, which outlines the certification and accreditation process for computer network defense service providers (CNDSPs)—organizations informally known as CERTs or CIRTs. [1] This emerging process, signed into policy last December, will impact not only the operation of department computer network defense (CND) but also how DoD trains the personnel that safeguard its computer networks. In anticipation of this new requirement, the Office of Assistant Secretary of Defense (OASD) for Networks and Information Integration, together with Defense Information Systems Agency (DISA) and National Security Agency (NSA), chartered a project to collect, deconstruct, and analyze relevant DoD and commercial training to assist DoD components preparing for certification and accreditation (C&A). A systematic evaluation regime and database were created to identify any gaps in current training opportunities and to construct a sustainable system for continued use in assisting service providers seeking to identify and tailor their particular training needs.

Much has transpired in the last 15 years. Early department organizational efforts were ad hoc and the rapidly evolving threat and security environments challenged standardization of terminology, techniques, and training for several years. The Department's enterprise security efforts now include safeguarding the myriad daily business and e-business transactions that enable support to the warfighter. The commencement of a formal certification and accreditation process marks a significant historical milestone in the maturation of securing DoD networks.

CERTs to CNDSPs—the CERT® Coordination Center

The CERT/CC was established in late 1988, after a Cornell University graduate student released the "Morris Worm," which disabled much of the Internet and demonstrated the emerging network's vulnerability. [2] Once the group of researchers assembled from government and academia successfully contained the worm, a series of meetings were held to discuss how to prevent and respond to potential occurrences in the future.

The Defense Advanced Research Projects Agency (DARPA), which created the Internet, subsequently funded development of a coordination center for Internet security incidents at Carnegie Mellon University's Software Engineering Institute (SEI). [3] DARPA tasked the SEI with establishing a capability to quickly and effectively coordinate communication among experts during future security emergencies and to build awareness of security issues across the Internet community.

DoD used the CERT/CC as a template as it organized to handle the growing awareness of internal computer network incidents. Each of the military Services constructed an organizational capability based on the rough template established by the CERT/CC. A strong partnering relationship between DoD and CERT/CC continues today. [4] DoD formally adopted the Computer Network Defense Services Provider (CNDSP) (vice CERT) nomenclature when DoD Directive O–8530.1 was published in early 2001. [5]

CND service provider—certification and accreditation

In the next few months, the maturation of DoD CND will plateau when selected CNDSPs begin to be evaluated in four areas, arranged by phase, by 146 metrics measuring services provided to DoD subscribers. The metrics were collaboratively developed by a working group representing all the services and four pilot evaluations were conducted to vet the metrics, certification, and accreditation process and procedures. A unit self-evaluation will precede any activity by the certification authorities (see Table 1).

The CNDSP C&A process is based on a four-phase approach leading to accreditation by the accreditation authority, United States Strategic Command (USSTRATCOM) (see Figure 1). The four phases of the certification and accreditation process are—

1. Registration
2. Verification
3. Validation
4. Post accreditation

Table 1. Computer network defense services.

Computer Network Defense Services			
Protect	**Monitor, Analyze, and Detect**	**Respond**	**Capability Sustainment**
Vulnerability Analysis and Assessment (VAA) Support	Network Security Monitoring/ Intrusion Detection	Incident Reporting	Memorandums of Understanding (MOUs) and Contracts
CND Red Teaming	Attack Sensing and Warning (AS&W)	Incident Response	CND Policies/Procedures
Virus Protection Support	Indications and Warnings (I&W)/Situational Awareness	Incident Response Analysis	CND Technology Development, Evaluation and Implementation
Subscriber Protection Support and Training			Personnel Levels and Training/Certification
Information Operations Condition (INFOCON) Implementation			Security Administration
Information Assurance Vulnerability Management (IAVM)			Primary CNDSP Information Systems

CND Service (CNDS) Accreditation—Formal declaration by the Accrediting Authority that the primary CNDSP operates at a level meeting or exceeding CNDS certification standards and is approved to carry out CNDS in accordance with DoDI O–8530.2. [6]

The process provides DoD with a standard method to assess a CNDSP's capability level based on performance criteria organized into 146 metrics. These metrics are based on IA best practices, self-assessment tools, and DoD requirements.

Registration

The CNDSP initiates the certification and accreditation process by applying to the CND Architect who reviews the package, and if the applicant appears ready for certification and accreditation, selects either DISA or NSA as the Certification Authority depending on whether the CNDSP is supporting General Services (GENSER) or Special Enclave networks.

Figure 1. CND service provider certification and accreditation process.

Registration
1. Application Package Submission
2. Application Package Review
3. Application Package Acceptance
Verification
4. On-Site Evaluation
a. In-brief
b. Evaluation
c. Out-brief
Validation
5. Reporting
6. Certification
7. Accreditation Award
Post Accreditation
8. C&A Maintenance

Verification

The Certification Authority conducts an on-site evaluation of the CNDSP including an assessment of any additional CND service organizations under the purview of that CNDSP. The CNDSP will receive an out-brief at the conclusion of evaluation.

CNDS Certification—An evaluation of the technical and non-technical services of a primary CNDSP completed in support of the CNDS Accreditation process. The evaluation determines the extent to which a CNDSP performs specified CNDS criteria. The certification integrates CNDS standards, self and independent assessment processes, improvement methods and tools, and information exchange among the CND Certification Authorities and CNDSPs. [7]

Validation

The evaluation team prepares a deficiency report based on their assessment, recommending whether the CNDSP should be certified and writes a certification report for the CND Architect. The CND Architect then makes an accreditation recommendation to USSTRATCOM. Validation culminates with an accreditation decision by USSTRATCOM. If certification is denied, a Provider Improvement Plan must be prepared by the CNDSP and approved by the Certification Authority and the CND Architect.

Post accreditation

CNDSP activities are monitored for consistency with evaluated and assessed standards of performance and changes to the CNDSP mission or subscriber population. Periodic self-assessments may be conducted.

CNDSP education training and awareness

To assist CNDSPs in their preparation for C&A, an evaluation of existing training opportunities was conducted with the training mapped against evaluation metrics. The results are available to interested DoD organizations. The department had previously directed the training of CND personnel and the establishment of a CND service C&A process under the supervision of the CND Architect. [8, 9]

The purpose of the training evaluation was to identify an available curriculum, assembled from multiple sources that can assist CNDSP both in preparation for the C&A process and in the remediation of identified deficiencies after the C&A process is complete. [10] The curriculum was then analyzed for gaps in training against the 146 metrics in order to prioritize new efforts for information assurance (IA) training. The analysis of training focused on the collection, deconstruction, and analysis of existing courseware and excluded the development of new course material. Follow-on initiatives will be identified and prioritized consistent with its value within the context of the emergent CNDSP C&A process.

The governing context of IA duties was collectively established by the DoD community and published in the Chairman, Joint Chiefs of Staff Manual (CJCSM) 6510.01, DoD Instructions 8500.2 and O–8530.2. [11, 12, 13]

Categories of IA responsibilities

The first four responsibilities listed are defined as individual responsibilities. These responsibilities are migrating toward individual skill certification and commercial adjudication. [14] The individual skill baseline is being used by DoD Directive 8570 to codify IA skills and responsibilities for DoD-wide training. [15] CJCSM 6510.01 and DoD Instruction 8500.2 articulate the responsibilities of four distinct individual IA functions (see Table 2)—

1. Authorized Users
2. Privileged User with IA Responsibilities (System Administrator)
3. IA Officers
4. IA Managers

as summarized in Appendix B. [16, 17] The fifth responsibility, CNDSP, is the sole focus of this curriculum development effort. Like the other responsibilities, it is essential that the CNDSP performance requirements be grounded in policy. Unlike the other four responsibilities, CNDSP is an aggregated or group responsibility. The criteria for the performance responsibilities for evaluating CNDSPs were the evaluation metrics defined in DoD Manual O–8530.1–M. [18]

Both commercial and DoD course offerings are dynamic in number and content. The primary commercial information technology (IT) training sources were examined for relevant offerings.

Table 2. Categories of IA Responsibilities

Categories of IA Responsibilities	
Authorized User Privileged User w/IA Responsibility (Sys Adm) IA Officer (formerly ISSO)	CJCSM 6510.01
IA Manager (formerly ISSM)	DoDI 8500.2
CNDSP	DoDI 0-8530.2

There will likely be multiple training opportunities associated with each evaluation metric. The responsibility rests with the CNDSPs to determine the best fit or value within the context of their specific situation. The best training value will likely be a function of the specific individual's professional background, IT certification, the timing of course availability, etc. A training opportunity matrix was assembled that organizes training opportunities against the certification and accreditation evaluation metrics.

Several commercial training providers were identified, such as Learning Tree, Software Engineering Institute, SANS, and International Information Systems Security Certification Consortium, Inc. (ISC2). Collectively, the training providers offer a wide range of courses that address general CND topics, with individual providers offering between two and twenty courses each. The commercial courses that were examined all were provided in a classroom setting, with durations ranging from one day to several weeks. However, not all classes are available all the time and are subject to technology changes. Information on 61 commercial courses (e.g., overviews, syllabi, master course lists, plans of instruction, and course training task lists) was collected where available. These courses represent a wide range of CND topics (e.g., vulnerability management, software evaluation, and network configuration). A total of 75 training opportunities provided by DoD were identified and subsequently divided into two major providers: service schools and DISA.

Training framework

Since a DoD policy vehicle codifies the metrics, they are relatively static. However, the dynamics of the IT field could quickly render any technical metrics obsolete. The solution to this challenge is to separate the metrics from the training opportunities with an intermediate pedagogical construct—the skill set. As particular technology-driven courses evolve, the skill sets can evolve while maintaining their linkage with the static evaluation metrics that are dictated by policy.

By focusing training decisions on skill sets, as opposed to metrics, CNDSP supervisors are able to aggregate their training needs, which are often distributed across multiple individuals. This allows CNDSP supervisors to identify overlaps in training opportunities and therefore maximize training value. The overarching analytic challenge was to establish an appropriate level of detail in defining the skill sets. If the skill sets were too tightly tailored to their corresponding metric, then it would be difficult to aggregate the skill requirements and identify appropriate training opportunities. If the skill sets became too generally defined, despite the ease of matching training opportunities, their linkage to the metrics would be tenuous. As a result, satisfactory completion of the training course may not adequately support passing the metric evaluation. [19]

The goal of the analysis was to balance the efficiency of fewer skill sets with the utility of easily matching skill sets to identified training courses. This analysis ultimately converged to the 37 discriminating skill sets illustrated below. This number was determined to be a good balance of the competing forces of pedagogical efficiency and field utility. The majority of the 37 definitions are grounded in DoD or commercial standards and policy (see Table 3). [20]

To assist supervisors seeking to match training against identified skill sets (and metrics), a training matrix was designed. The matrix correlates individual metrics with their associated skill sets. Where a skill set matched the analyzed curriculum of a training course, an annotation was made. Thus, the training matrix could be used to map individual C&A metrics to specific training courses.

The training matrix

The purpose of the training matrix is to provide a visual depiction of the intersection of required skill sets and available courses. On the main matrix, the vertical axis is comprised of the 146 CNDSP Evaluation Metrics. The horizontal axis is comprised of government and commercial courses. The skill sets were then plotted against courses that offer training in that skill set. A small portion of the matrix is illustrated in Table 4. [21]

Table 3 Skill Sets

Skill Sets			
Accreditation	Incident Mitigation	Network Security	Security Awareness and Training
Anti-Virus Software Configuration and Maintenance	Incident Reporting	Operational Security (OPSEC)	Software Configuration Management
Attack Sensing and Warning (AS&W)	Incident Response	Operating System (OS) Configuration and Maintenance	Software Evaluation
Classified Network/System Configuration, Maintenance, Policies and Procedures	Intrusion Detection	Personnel Security	Standard Operating Procedure (SOP) Development and Implementation
Continuity of Operations (COOP)	Malicious Code Handling	Physical Security	Testing/Exercises
Documentation	Network Analysis and Tools	Policy Development and Implementation	Threat Awareness and Identification
DoD Policy Awareness	Network Configuration	Project Management	Vulnerability Management
DoD Policy Compliance	Network Configuration Management	Providing IA/IT/Security Policy, Awareness and Training	
Firewalls	Network Monitoring	Quality Assurance (QA)	
Incident Analysis	Network Operations	Red Teaming	

The training matrix is a tool to assist in determining training options, not as a decision matrix. An indication that a skill set is mapped to a certain training class simply means that some aspect of that skill is taught in that class. It is not an indicator that the class provides the specific training necessary in that skill set to fully pass the metric. The matrix does not, by itself, provide sufficient information to make decisions regarding training. Rather, it is intended to provide a starting point from which further analysis can be done. The matrix provides a general guideline as to which classes address some part of the skill set in question. It serves as a guide to narrow the number of class syllabi that must be examined in order to determine the appropriate training opportunity. Once the number of classes has been narrowed down, the user must then determine the specific deficiency areas of the given skill set. This can then be compared against the syllabus of each class to determine if the class will meet the specific skill set requirements.

The matrix is also a useful tool in examining general coverage of the subject matter. However, due to the generalized nature of the mapping, it is not possible to be specific in the analysis. The courses are only mapped to the skill sets to the degree that the course being assessed teaches some aspect of the given skill set. Additionally, the skill sets have been mapped to the metrics to the degree that they are general skill sets required to satisfactorily perform the function that the metric is measuring. Coverage of a skill by a given course or courses is not a guarantee that the specific skill set needed to satisfactorily address the metric is taught.

For example, Metric 2.1.2 states—

Does the CNDSP perform intrusion detection monitoring on all subscriber mission-critical networks?

The skill sets associated with this metric include Intrusion Detection. The matrix indicates which courses provide intrusion detection software training. However, looking at the metric in greater detail shows that this metric requires both host-based and network-based Intrusion Detection Software (IDS) installation. The matrix does not have the fidelity necessary to determine whether the specific skill set of network based IDS is included in any given course.

A training database was developed to help look for gaps in the training opportunities. The database reports are also useful in identifying potential training and its utility against the metrics used in an organization's evaluation. The reports cross index the certification and accreditation metrics to skill sets and list associated training opportunities.

Conclusion

DoD has advanced the state of CND significantly since the pioneer days of DARPA and CERT/CC. Training and techniques have been continually challenged by the advancing threat and the department's increasing dependence on its networks. The upcoming C&A of CNDSPs is the next major step in DoD's ongoing effort to safeguard its computer networks. The commercial sector has a treasure of training opportunities available to supplement DoD courses and has been widely used by service trainers to prepare individuals for IT roles and responsibilities. Soon these same professionals will be tasked with preparing organizations for collective roles and responsibilities and training individual staff members in preparation for an evaluation of unit performance. Tools now exist that may assist supervisors and trainers in preparing individuals and units to take this next step down the road ahead for CNDSPs. ■

About the Authors

Dr. Buzz Walsh

Dr. Buzz Walsh is a senior staff member at IATAC and a retired U.S. Air Force Officer. He played a foundational role in Computer Network Defense and Information Assurance at the Joint Task Force for Computer Network Operations (JTF–CNO), the Joint Staff, and the Air Staff from 1993 to 2001. He received a Ph.D. in Computer Science from Michigan State University and a M.S. in Electrical Engineering from the University of New Mexico.

Dr. Walsh has published in a number of different forums including an award-winning critical analysis paper for Joint Forces Staff College in 1997, and an award-winning text for Air University in 1994 that remains in its core curriculum. He has served as faculty, adjunct faculty, guest lecturer or visiting professor at the National Defense University, Joint Forces Staff College, Army War College, Army Command and General Staff College, Air University, and the Air Force Academy.

Ralph Ghent

Mr. Ralph Ghent is the DoD CND Architect. As a retired U.S. Army Signal Corps Officer, his military experience includes Battalion Command, serving on the Joint Staff, and leading the C/J–6 communications planning for U.S. Forces, Korea. He has also taught at the U.S. Military Academy and the U.S. Army War College. He holds a B.S. from the U.S. Military Academy, an M.S.E.E from Georgia Tech, and a Masters in National Strategic Studies from the Navy War College. He is also a licensed Professional Engineer and a certified DoD Chief Information Officer from the National Defense University.

In his position within the Information Assurance Directorate of the Office of Assistant Secretary of Defense for Network and Information Integration (OSD–NII) he develops and provides oversight to this Program and CND Architectures for the DoD.

References

1. DoD Manual O-8530.1–M, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process, Draft, Fall 2003.
2. http://www.cert.org/
3. Ibid.
4. IA Newsletter, Volume 4 Number 3, IATAC, Summer 2001.
5. DoD Directive O–8530.1, Computer Network Defense, 8 January 2001.
6. DoD Manual O–8530.1–M, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process, Draft, Fall 2003.
7. Ibid.
8. DoD Directive O–8530.1, Computer Network Defense, 8 January 2001.
9. DoD Instruction O–8530.2, Support to Computer Network Defense, 9 March 2001.
10. Computer Network Defense Service Provider Education, Training and Awareness Program Final Report, 26 September 2003.

Table 4. Sample from CND training matrix.

			Air Force On-site Training					Navy On-site Training		
Skill Area	Metric	Skill	Infrastructure Technology Systems 300 (ITS 300)	Network Management Systems 200 (NMS 200)	Computer Systems Management	Base Information Protection 200	System Network Support 100 (SNS 100)	Information Systems Security Manager (ISSM) (CIN: A-531-009)	Network Security Vulnerability Technician (NSVT) Course (CIN: A-531-022)	Advanced Network Analyst (CIN: A-531-0045)
Vulnerability Analysis and Assessment Support	1.1.1 Does the CNDSP assist subscribers in identifying types of VAAs that may be performed within the serviced area and by whom?	Vulnerability Management				■		■	■	
		Documentation			■	■		■		
	1.1.2 Does the CNDSP assist subscribers with VAA self-assessments?	Vulnerability Management				■		■	■	
		SOP Development and Implementation				■		■	■	
		Documentation			■	■		■		
	1.1.3 Does the CNDSP have policies and procedures for the use of Vulnerability Analysis Scanning (VAS) tools?	Vulnerability Management				■		■	■	
		Documentation			■	■		■		
		SOP Development and Implementation				■		■	■	
	1.1.4 Does the CNDSP assist subscribers by identifying negative impacts to subscriber network operations because of VAS tool usage?	Vulnerability Management				■		■	■	
		Documentation			■	■		■		
		SOP Development and Implemenation				■		■	■	
		Software Evaluation						■		
		Network Operations	■	■		■	■	■	■	■
		Network Configuration	■	■		■	■	■	■	■
	1.1.5 Does the CNDSP obtain written permission from the DAA/network owner/subscriber before executing VAS tools? (Alternately, CNDSP has approval in writing by higher authority)?	Policy Development and Implementation								
		Documentation			■	■		■		
		SOP Development and Implementation								

11. CJCS Manual 6510.01, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), 26 March 2003.
12. DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.
13. DoD Instruction O–8530.2, Support to Computer Network Defense, 9 March 2001.
14. CJCS Manual 6510.01, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), 26 March 2003.
15. DoD Directive 8570, Information Assurance Training, Certification and Workforce Management, Draft, Fall 2003.
16. CJCS Manual 6510.01, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), 26 March 2003.
17. DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.
18. DoD Manual O–8530.1–M, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process, Draft, Fall 2003.
19. Computer Network Defense Service Provider Education, Training and Awareness Program Final Report, 26 September 2003.
20. Ibid.
21. Ibid.

Zen and the Art of Scanning Networks

A Tour of Scanrand 2.0

by Dan Kaminsky, CISSP

Author's Note: The tool described in this article is Open Source under the Berkeley Software Distribution (BSD) License, and may be acquired at the following URL: http://www.doxpara.com. The author may be reached at kaminsky@avaya.com, and welcomes any feedback or questions.

The scale is massive—the chaos, sometimes more than we'd like to admit. Enormous quantities of assets, supporting critical operations distributed worldwide, remain managed through only rough estimate and the occasional disruptive audit. But there is hope—a revolution is coming to inventory control, as Radio Frequency Identifier (RFID) technology truly promises to make assets in the real world just as easy to centrally manage as nodes on a digital network.

Unfortunately, it just so happens that nodes on networks are surprisingly tricky to manage en masse. As networks scale through hundreds of thousands, if not millions of potential addresses for devices, traditional tools and approaches simply bog down to the point where they can only be used for intermittent action—more for emergency intervention than consistent management. Of course, it's to the credit of Internet protocol (IP) (which has ultimately subsumed every other major mechanism for transferring bits from point A to point B) that not only is it capable of growing without an effective centralized manager, but that freedom distributed to the endpoints actually makes it more robust.

Supporting this robustness is a critical and often forgotten requirement, but security issues have become a significant contributor to network outages, the fact of which cannot be ignored. Worms are the most expensive computer security threat as of the writing of this article. Spreading rapidly from host to host, they quickly discover and infect all potentially vulnerable devices. Attackers now possess a mechanism for rapidly discovering and infecting vulnerable nodes across massive networks, and unlike defenders, they can usually ignore the collateral damage their approach might cause. It is therefore more critical than ever that defenders have a means for at least identifying the resources available on their network—to rapidly populate and update what I refer to as a "security knowledge base," no matter the scale of the infrastructure. Attackers can already find what they're looking for—it's time to provide defenders with the tools they need to compete.

What I shall describe in this article is no panacea, no quick fix to the problem of managing security across a wide network. While the tools discussed are indeed much faster than traditional solutions—the open source (BSD licensed) Scanrand's first revision was capable of locating 8,000 web servers across 65,536 addresses in approximately four seconds—they are merely components of a larger security architecture, one that ultimately must mirror the usability and functionality constraints of the particular context network. Given such deference to elegance, scanrand can be a very useful component, particularly for massive network against which little else scales.

Table 1. Requirements for a generic efficient TCP scanner

1.	**Selector**—Identifies targets to be scanned and order in which to scan.
2.	**Sender**—Transmits connection requests (SYNs) to each host.
3.	**Receiver**—Verifies incoming responses, analyzes connection acceptances (SYN | ACKs) and rejections (RST | ACKs) from each target, and reports to an external.
4.	**Reporter**—Analyzes received data, possibly trending across time and network space.

Stateless transmission control protocol (TCP) scanning

Scanrand 2.0 is, at its core, an unusually efficient TCP service detector, with the added capability of offering high speed traceroutes as well. Scanrand achieves its speed through a stateless implementation of TCP, almost entirely bypassing the kernel's standard mechanisms for connecting to TCP-hosted services (such as HTTP, SSH, or SMTP) and spawning the packets itself. Architecturally, Scanrand splits the two halves of any scan—the transmission of

Table 2. Reflecting payloads from a SYN to a SYN | ACK, RST | ACK, or ICMP time exceeded.

Field	Bitsize	Scanrand Use
Full Freedom		
TCP Source Port	16 bits	Relative Timestamp
TCP SEQ#	32 bits	Security
Minor Freedom		
TCP Dest Port	16 bits	Service Selection
IP Dest	32 bits	Target selection
IP Source	32 bits	Listener selection
IP DF Bit	1 bit	N/A (unreliable)
ICMP Error Only*		
IP ID	16 bits	original QoS/TTL
IP Protocol	8 bits	N/A (meaningful, dangerous to Cisco routers)
IP QoS	8 bits	N/A (meaningful)
IP Fragment	16 bits	N/A (may not route)
IP Options	312 bits**	N/A (may not route)
IP Checksum	16 bits	N/A (should not route)
IP Len	16 bits	N/A (should not route)
IP TTL	4-6 bits	N/A (decrements en route)

* *ICMP errors contain the entire IP packet that spawned them. As such, many of the fields within IP itself can be abused for reflectance purposes.*

** *8 bits are consumed selecting an unused IP Option type.*

requests, and the reception of responses—into two disconnected processes, kept in sync not through cached context

Table 3: Services scanned per level of bandwidth.

```
    64   B/s: . . . . . . . . . 1   services per second
    10  KB/s: . . . . . . . . 160   services per second
   100  KB/s: . . . . . . . 1,600   services per second
 1,000  KB/s: . . . . . . .16,000   services per second
```

but through additional data tucked into requests that is repeated in responses.

One of the risks inherent in any stateless architecture is that since context is not stored but returned from afar, false context might be sent and somehow parsed. This risk is commonly addressed through a memory-for-bandwidth trade-off—a cryptographic "cookie" is embedded in the SYN connection request, to be validated in the SYN | ACK connection acceptance or RST | ACK connection rejection. This cookie is a simple SHA–1 hash of predictable values in any response—IP Source and Destination, as well as TCP Source and Destination Ports, combined with a secret synchronized between the sender and receiver processes. The hash is truncated to the 32 bits that fit in the TCP Sequence Number Field, and is recovered in responses inside the TCP Acknowledgement number.

Scanrand 2.0, besides bringing an entirely revamped internal architecture (complete with libpaketto, a library simplifying complex network manipulation), is more efficient at pushing packets—so much so that bandwidth management became a high priority. While the tool can successfully operate across a wide range of speeds, note that the very packets being sent are astonishingly small, and as such even slow scans can support high speed data acquisition.

```
# sample scan an internal (RFC1918) network at
# 100 kbyte/sec for 30 common ports
scanrand2 -b100k 10.0.1.1-254:quick
```

Bandwidth limitation is not the only technique employed in Scanrand to minimize the disruptiveness of the scanner. To more effectively manage devices that preal-

locate resources for every SYN they see passing on a network—mainly certain firewalls and NAT devices—Scanrand 2.0 was given the ability to actively order such devices to release their resources using a reset, or RST packet, sent some number of seconds after the SYN connection request. This procedure can safely enable much higher speed scanning, at a cost of double the overall traffic.

```
# Search a class B for available LANs. Send RSTs
# towards each destination five seconds after
# sending a SYN.
scanrand2 -b10k -O5 10.1.1-254.1,63,127,191,254:
80,53
```

Besides being a security tool, Scanrand 2.0 includes several features designed specifically for network administrators. New is the ability to measure the end-to-end latency of every single response received—this was done by embedding a timestamp in the TCP source port, to be analyzed when the packet returned. One technique enabled by this allows for a sort of "spread spectrum" latency measurement, implemented by ordering Scanrand to fan packets out in many directions and record the return latency from each. By this means, the quality of a network link can be determined, quickly, versus a large number of samples—

```
scanrand2 -b30k -l10 64.1-254.1-254.1:80
```

An interesting mechanism was also added for the management of Voice-over-IP networks. Such networks are often critically dependent on Quality-of-Service, or Diffserv values being respected. Often, not only are such values ignored, but they're corrupted en route. By altering the QoS of scanrand's stateless route tracer, it is simple to expose any node that is changing the QoS value of a packet en route—the ICMP Time Exceeded message sent by the next router down will lack the pre-programmed QoS.

```
# Trace path eight hops out to a number of
# destinations, setting QoS to 47.
scanrand2 -b10k -l1-8 -q47 10.1.1-254.1:80
```

Operational advantages

The most useful addition to Scanrand 2.0, though, is also the simplest—database integration, not by supporting any particular API but by simply dumping raw SQL that can may directly piped into any database. This is not the normal mechanism for exporting data, but the approach is extraordinarily portable and unusually flexible. For example, it becomes quite trivial to integrate the results of scans executed from remote sites into a centralized knowledge base. Instead of exposing the code to complex API's and the network to various mechanisms for remote database access, the data can be acquired both trivially and securely simply by executing the scan over SSH and piping the results into the appropriate database or vice versa—

```
# Scan a remote network, piping the results into
# a local database
ssh user@remotehost scanrand2 -b10k 10.0.1.1-254:
quick -T remotenet -H -M1 | mysql db

# Scan a local network, piping the results into
# a remote database
scanrand2 -b10 10.0.1.1-254:quick -T remotenet -H
-M1 | ssh user@host mysql db
```

But does this scale? Not in terms of network bandwidth—scanrand is more than fast enough—but how can we actually build processes around these capabilities? Split mode is probably the most important function for actually operationalizing the tool. As discussed earlier, the process of sending packets and the process of receiving them are actually quite different. Scanrand allows the two functions to be run through separate executables—

- The listener, daemonized, translating each valid incoming packet into a line of SQL for a database.
- The sender(s), automated perhaps through cron jobs, spawning the queries that will elicit responses from the network.

The following examples are simple shell script; a more likely operationalization would use perl, python, or php as a driver—

```
# Collect scans in the background...
scanrand2 -L -s secret_1 -t0 -T table -H -M1 |
mysql db &

# Scan various targets
scanrand2 -S -b5k -O2 -s secret_1 192.168.1.1:
1-65535

scanrand2 -S -b100k -s secret_1 10.0.1.1-254:
quick

# Spawn a scan on a remote host, requesting
# packets be sent locally
ssh user@host scanrand2 -S -s secret_1 -i
$LOCAL_IP 10.0.1.1-254:quick
```

At this point, the database has been populated with the results of the last three scans, and may be queried for reports.

Large scale deployment

A basic deployment of scanrand is trivial, and it's probably one of the few scanners that can directly scale to rapidly evaluating a class A network—both as fast as possible, and over the course of a month, simply by varying the bandwidth level and not crashing. But the basic deployment can be perceived as stressful on networks. Put simply, depositing large amounts of traffic into hosts or even subnets that don't exist is not looked upon kindly, no matter the amount of traffic sent. In fact, empirical evidence has shown failure to use discretion when scanning a network results in less accurate results (i.e., other administrators find cause to block the scans). Avoiding this fate requires a multi-tiered approach, whereby subnets, hosts, and services are each identified using similar but unique methods.

The adaptive process significantly cuts down on the total number of probes that need to be sent—unsurprisingly, the fewer packets need to be sent, the quicker the job. More surprising is the fact that larger networks can enable faster scans. It is simple to execute multiple copies of scanrand, as each invocation requires a minimal amount of resources. Multiple invocations, each slowly transmitting packets towards a given subnet, can achieve significant speeds in aggregate while amortizing the impact of those

speeds across the entire network. It is through this method that we can meet constraints such as—

- Approximate 50 class B networks (3M addresses) identified as within target network
- No more than 8 packets per empty class C network,
- No more than 6 packets per empty IP address on a validated subnet,
- No more than 60 packets per host,
- No more than 10 kb/s to any LAN,
- No more than 100 kb/s across the backbone
- 30 ports scanned per target
- +10,000 nodes detected
- +50,000 services identified
- Scantime: 20 minutes

…as was achieved during the testing of Scanrand 2.0. The following examples demonstrate the procedure used—very basic, and though it could have been done with the aforementioned scripting languages of perl or php, the following code is meant to illustrate the mechanisms by which Scanrand 2.0 is capable of being driven in relatively few lines of code.

Given a set of Class B (a.b.) addresses, determine routable Class C's.*

Example 1—Net ID "Subnet Identification"

The idea behind this scan is to emit an extremely light set of packets towards each Class C (a.b.c.*), marking whenever we get a response from an address that's commonly associated with a subnet router. This is a notoriously tricky process to optimize, but the most important constraint that must be met is that scanning rights—ownership—must be at least plausible. It's often tricky to determine simply by network traits which administrative domain a given network operates within, particularly for fragmented networks. (It is at best rude to scan outside one's domain, and at worst illegal). Both out-of-band information sources and snmp scans, particularly those that allow one to crawl route tables, can be enormously useful here.

First, make sure the database is initialized and ready for scan results. We'll be using mysql on Knoppix, but similar processes can be designed for many DBMS's—

```
# execute as root
/etc/init.d/mysql start
mysqladmin create db
```

Next, start the SQL listener. We're using the -e option to scanrand, which stores a result whether the service was up or down.

```
scanrand2 -L \ # Listen only -- do not send
-s secret_1 \ # Accept responses with this key
-e \ # Log services whether up or down
-t0 \ # Disable timeouts
-T net_id \ # Name SQL Table "net_id"
-H \ # Output SQL Schema
-M1 \ # Output SQL
| mysql db & \ # Send to mysql
```

Given a file containing network entries such as—

```
10.1
10.2
10.10
192.168
```

Not only can scanrand read entries from a file, but it can append an arbitrary trailer to each line. This is meant to improve maintainability of the list files.

```
scanrand2 -S \ # Only send packets
-s secret_1 \ # Sign requests with this key
-b10k \ # Send packets at 10 Kilobytes/sec
-f net_list.txt+1-254.1-254:80,53 \ # Acquire
# targets from file
-v \ # Verbose mode -- watch packets get sent
```

Depending on the size of the network being scanned, one may wish to separate net_list.txt into several files, and scan each with their own invocation of scanrand. The process of creating separate lists is left to the reader; however, it should be noted—

- Core bandwidth/Per-LAN bandwidth determines number of simultaneous processes that may be run (presuming scan is source near the backbone).
- Certain networks may be arbitrarily given higher or lower bandwidth counts, in case of locality or international pipes.

It is also possible to execute a series of traceroutes to each live network, then extract every class C that was routed through. These addresses may be very interesting, they may be owned by external providers, or both. This scan is simple, but rather noisy (a more intelligent design would complete a binary search, looking for address ranges that caused consistent changes in routes).

```
scanrand2 -S -s secret_1 -b10k -l1-15 -f
netlist_txt+1-254.1-254:80,53
```

Given a set of class C (a.b.c.) addresses, determine addressable hosts.*

Example 2—Host Id "Host Identification"

Now, one may acquire a list of hosts that were seen in that particular network scan.

```
# Get sample hosts
echo "select dst from net_id group by dst" |
mysql -N db > temp.txt

# Get crossed nets
echo "select trace_mid from net_id group by
trace_mid" | mysql -N db >> temp.txt
```

…which we can then filter down to unique Class C's…

```
cat temp.txt | cut -d. -f1-3 | sort | uniq >
class_c.txt
```

…which we can now scan with a bit more depth (after starting up a new listener and a new table).

```
# start new listener
scanrand2 -L -s secret_2 -e -t0 -T host_id -H -
M1 | mysql db &
```

```
# scan target
for i in 80 139 22 23 # Could also be $1
do scanrand2 -S \ # Only send packets
-s secret_2 \ # Sign requests with
this key
-b5k \ # Send packets at 5
Kilobytes/sec
-O5 \ # Send proactive resets 5
seconds later
-f class_c.txt+1-254:$i \ # Acquire
targets
# from file
&
sleep 10;
done
sleep 10;
```

After some time (which can either be calculated, or acquired by making the final scan block), we will have a fully populated host list. Now, onto network services.

Table 4. Approximate bandwidth* required for various scans (single pass).

	Ports	x	Hosts	x	Subnets	=	KB
Class B Subnet Detection	2	x	4	x	254	=	127
Class C Host Detection	4	x	256	x		=	65
IP Address Service Detection	30	x	1	x		=	2
Alternative datapoints							
IP Address Mid Service Detection	1,150	x	1	x		=	74
IP Address Full Service Detection	65,536	x	1	x		=	4.2 MB
Quick Scan per subnet	30	x	120	x		=	230
Mid Scan per subnet	1,150	x	120	x		=	8.8 MB

* 64 bytes assumed per packet, as this is the minimum frame size on Ethernet

Example 3—Service Id "Service Identification"

Given a set of IP (a.b.c.d) addresses, determine TCP services available on hosts—First, we need the list of IP addresses—

```
echo "select dst from host_id group by dst" |
mysql -N db > ip_addr.txt
```

Then it's a matter of—

a. Parsing the file,
b. Separating it out into some number of threads, each running at -b bandwidth
c. Waiting less time than if each address was scanned in sequence.

```
# start new listener
scanrand2 -L -s secret_3 -e -t0 -T serv_id -H -
M1 | mysql db &

# Spew traffic
scanrand2 -S \ # Only send packets
-s secret_3 \ # Sign requests with this key
-b10k \ # Send traffic at 10k/s -- no overload
# needed, as there's a live host here
-f ip_addr+:quick \ # Send traffic to 30 most
# common ports
-y 10 \ # Spread scan across ten threads
-z 60 \ # Wait 60 seconds between each thread
```

Caveats—Of bandwidth and reliability

The power of Scanrand does not come without cost. What Scanrand may do quickly, other tools (such as Fyodor's trailblazing nmap) can do simply and more reliably—just significantly slower. Scanrand's power ultimately comes from exposing very fine grained control to the user regarding the precise network behavior of the application. Nowhere is this control more noticably demanding than in the design of reliable scanning procedures for massive networks. The sequential design of most tools allow for dropped packets to be quickly identified and retransmitted, on a per-host and per-stream basis. By contrast, the split nature of Scanrand (the sender and receiver don't even need to be on the same host!) makes it significantly trickier to alter sender characteristics based on received data of any sort. Potentially more worrisomely, unlike normal TCP traffic, Scanrand floods do not back off in the face of congestion. Luckily, we simply don't need to push networks that hard to complete extraordinarily fast scans, and more importantly, the aggregate bandwidth for a scan is so small that we can generally afford to run the scans multiple times. **Split mode particularly facilitates redundant senders to facilitate resilience against dropped packets, as data elicited from each sender will be merged into the same database for analysis purposes**. Conceivably, one could drive followup scans by matching outgoing requests to a failure to respond. Such outgoing requests can be logged in the database by adding the–g flag to any command that causes packets to be sent.

The implementation of this whole-scan scale error correction approach is left as an exercise for the reader (or a future article).

There are also issues that occur as scans escape the Class–A threshold and start sweeping the entire Internet, as I am presently doing with the cooperation of the Opte fast mapping project. Accurate and fast bandwidth measurement is a major area of research for future versions of scanrand, as completely saturating a given link may cause failures even repeated scans can't see through. However, one interesting saving grace is that only collisions or dropped packets of the SYN request are troublesome for us—given a bandwidth crunch on the way back, the remote TCP stack will repeatedly and semi-reliably retransmit the message until such time as we receive it (and our kernel, being quite confused at the incoming response, RST's away the responder).

Service actions

From this point, one has a fully populated database of common services on the network. Other applications can be driven from this database. For example—

```
echo "select dst from serv_id where port = 80
and stat = 'UP' group by dst" | mysql -N db >
webservers.txt;
```

```
for i in `cat webservers.txt`; do nikto.pl -host
$i -o $i.txt; done
```

Or simple reports can be generated—

```
echo "select port,count(port) as num from serv_id
group by port order by num" > common_ports.txt
echo "select dst,port from serv_id group by
dst,port" > simple_portlist.txt
```

Conclusion

Scanrand 2.0 allows network and security adminstrators to acquire data, almost in realtime, about the service capacity of their network. It integrates well with relatively complex processes designed to minimize scan intrusiveness, reducing the risk that scans will be blocked technically or administratively. It is also under active development, with several significant features (such as mass network visualization, similar node aggregation, and UDP service support) coming soon. The ultimate message is that, given some degree of thought and design, large networks can be rapidly and accurately evaluated, and ultimately even the largest architectures will be reasonable instrumentable with a sort of "network tripwire," able to drive further investigation and evaluation by security resources. While not a panacea, Scanrand 2.0 should be a helpful addition to any administrators toolkit. ■

About the Author

Dan Kaminsky

Mr. Dan Kaminsky is a Senior Security Consultant for Avaya's Enterprise Security Practice, specializing in large scale network operations, information visualization, and converged security. He is a graduate of Santa Clara University, receiving his degree in Operations and Management of Information Systems. Dan is well known in the security community for his "Black Ops of TCP/IP" presentations, unveiling the new and interesting modalities for TCP/IP he deploys in his "Paketto Keiretsu" suite of applications. Dan has also contributed to several books, including "Hack Proofing Your Network" and "Stealing The Network: How To Own The Box," and founded the cross-disciplinary DoxPara Research in 1997.

continued from page 5…

A New Strategy—A New USSTRATCOM

"The difficulty comes when a warfighting commander is in the middle of a crisis and he has to turn to multiple sources to obtain the IO assets [he needs]."

Lt Gen Thomas Goslin
USSTRATCOM Deputy Commander and Commander, Joint Force Headquarters–Information Operations.

In the face of that challenge, USSTRATCOM is working "to give every commander the equivalent of a big red button that says—push here for information operations," the general explained. Just as the command is now the ultimate source of DoD's space capability, it will be the ultimate source of IO capabilities.

Since IO missions are broad and stem from numerous sources, working in an interagency environment is essential, said Goslin. IO must be integrated into processes across the full military and national security spectrum, he added.

The command is now working with numerous organizations, including the Defense Information Systems Agency (DISA), the Joint Information Operations Center (JIOC), and the Joint Task Force for Computer Network Operations (JTF–CNO), and others to project an inter-departmental focus for IO.

"Fully integrating the information operations will allow us to provide a comprehensive and deliberate plan that includes assessment of battlefield damage and specific consequences of execution."

The Pentagon should handle with care the operational opportunities presented by rapidly advancing space technologies and capabilities, Goslin said.

"While our space access gives us the ability to cut through an adversary's operational security measures, an adversary's access to space presents new operational security and deception challenges to us. The availability of commercial imagery and communications requires that we understand better than anyone else…the challenges that a space-faring nation presents to its enemies."

At USSTRATCOM, Goslin and other command leaders are now working diligently to hash out the operational security piece of IO.

"We want to make sure that we can trust and use our information systems at any time. We also want to make sure that we can deny our adversaries some or all the trust and use of their systems. Space assets give our forces the freedom to operate our computer networks on the fly around the world, and we must be able to defend those as well as exploit those networks." ■

by John Davis

What is the INFOSEC Research Council?

The INFOSEC Research Council (IRC) provides informal technical coordination of Information Security research plans and programs across the Department of Defense (DoD), the Intelligence Community, Homeland Defense, and the other Federal Civil agencies. Originally convened by the National Security Agency (NSA) in 1996, it brings together U.S. Government sponsors of information security research at bimonthly meetings in the Washington, D.C. area and provides a forum to discuss critical information security issues, to convey the research needs of their respective communities, and to describe current research initiatives and proposed courses of action for future research investments. Each participating agency brings a unique perspective and set of priorities to the IRC. The IRC helps identify high priority areas of research to develop a common, shared view of the significant and challenging information security problems of the day.

How does it work?

The IRC accomplishes its mission through information exchange, identification of shared problems, conduct of forward-looking studies of mutual interest, and maintenance of a shared database of project information.

The Research Hard Problems List is a document maintained by the group that itemizes a consensus set of prominent INFOSEC problems that could benefit from additional research investments. It grew out of a study performed by IRC members and selected national experts in INFOSEC R&D. "Hard problems" are problems which will be of enduring significance for 5–10 years, requiring innovative research.

The list was initially available to anyone in the government and is now released to the public via the IRC's public Web site (http://www.infosec-research.org). The IRC periodically focuses on one of the hard problems during a meeting to identify progress and determine whether that problem should continue to be a focus of research funding. The IRC has recently commissioned an extensive study to update the Hard Problems List and expects results by the summer of 2004.

Table 1. Summary version of Hard Problems List

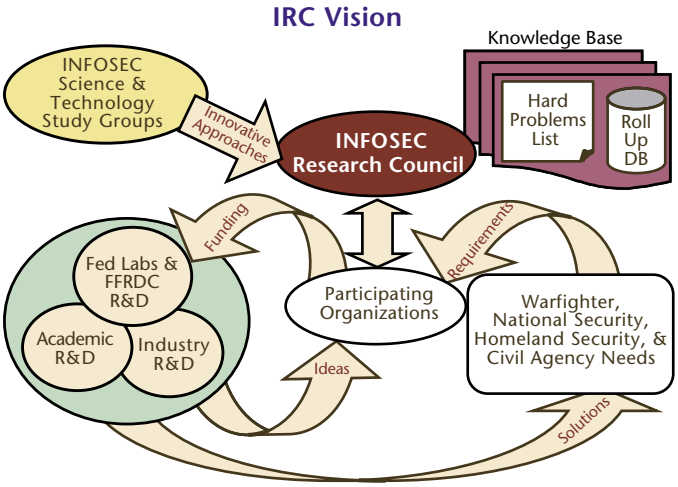
Operational Hard Problems	Design and Development Hard Problems
Intrusion and Misuse Detection	High Assurance Development
Intrusion and Misuse Response	Secure Systems Composition
Security of Foreign and Mobile Code	Metrics for Security
Controlled Sharing of Sensitive Information	
Application Security	
Denial of Service	
Communications Security	
Security Management Infrastructure	
Information Security for Mobile Warfare	

From time to time, the IRC convenes Information Security Technology Study Groups (ISTSG) to conduct forward-looking investigations of a particular problem or technology of interest to the members, potentially as a candidate for future research. These groups comprise national experts in particular technologies of interest, IRC members, and other appropriate government participants. A recent ISTSG was conducted on the topic of Malicious Code and delivered a publicly released report on this topic.

If you are interested in becoming part of the INFOSEC Research Council, contact the IRC Executive Agent, John Davis at john.davis@mitretek.org. ■

Table 2. Goals of the INFOSEC Research Council.

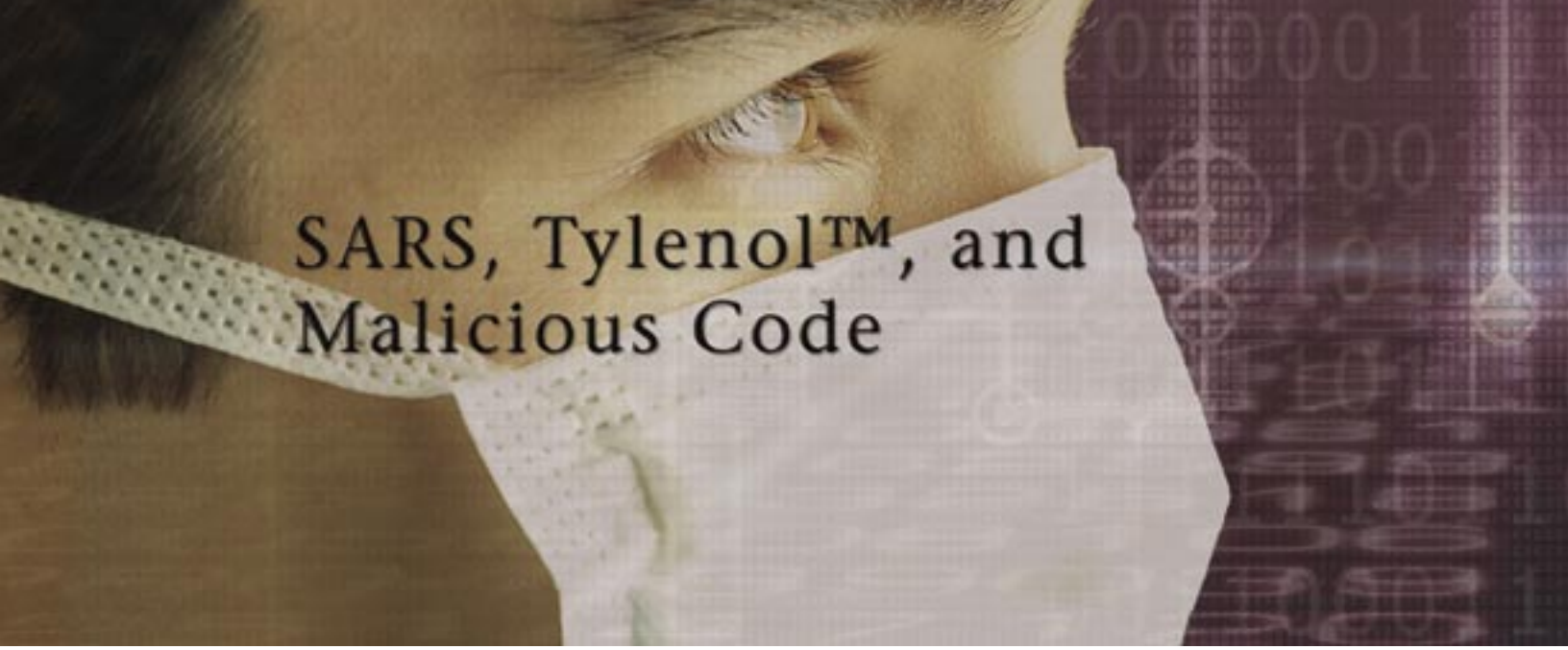
Enable knowledgeable, intelligent INFOSEC research investments
Increase efficiency and effectiveness of U.S. Government INFOSEC research
Support consolidated identification of high value research targets



About the Author

John Davis

Mr. John Davis is the Executive Agent of the Information Security Research Council. He received a B.S. in Physics from Pennsylvania State University, an M.S. in Physics also from Pennsylvania State University, as well as an M.S. in Electrical Engineering from Johns Hopkins University. Mr. Davis worked in the National Security Agency for over 30 years including assignments as Director of the National Computer Security Center (NCSC) and Deputy Chief of Research and Technology. He also served as the director for the Center for Information Security and Privacy at Mitretek Systems and now is a senior manager. He may be reached at john.davis@mitretek.org or 703/610-1945.



SARS, Tylenol™, and Malicious Code

by Tom Ward, April Perera, and Tim Madden

Damaging outbreaks happen, whether we are prepared for them or not, and they can affect all walks of life. Such events also have different origins, arising from malevolent biological causes, criminally depraved intentional acts, or mischief within the cyberworld. Comparing the commonalities shared by these events can provide insight into better preparation for identification and warning of, and defense against, malicious code attacks.

The SARS outbreak—biological malevolence and bureaucratic indifference

The source of the SARS outbreak is believed to have been within the Guangdong Province, China in November 2002. Two months after the first case of SARS was identified, Guangdong health officials and party functionaries had already documented 300 cases of a SARS-related illness. At that point the outbreak only affected Guangdong Province—by January 2003 SARS began to proliferate outside of Guangdong.

A little over three months after the first documented case of SARS (February 2003), the Hanoi French Hospital notified the World Health Organization (WHO) of a puzzling respiratory ailment. The exact reason the Hanoi French Hospital notified WHO is not documented. However, the rapid spread of the ailment—a type of atypical pneumonia—was puzzling to health workers in that area. As WHO began to monitor the disease, SARS spread to Hong Kong, Vietnam, Singapore, and Toronto, quickly transforming a local anomaly into a global outbreak. Many health care workers were unaware of their own exposure to SARS, thus contributing significantly to the population of infected individuals.

Alert and warning

According to WHO, SARS was a particularly urgent threat for a number of reasons—the causative agent was unknown, health workers were highly susceptible, no cure or treatment was identified, there were high numbers of respiratory failure, and it was quickly spreading around the world. [1] WHO was able to identify and monitor the outbreak by tapping into an existing indication and warning (I&W) infrastructure. There are two primary networks WHO uses to gather and disseminate intelligence data regarding outbreaks throughout the world, the Global Outbreak Alert and Response Network (GOARN) and the Global Public Health Intelligence Network (GPHIN) (see Figure 1). GPHIN collects and mines real-time data from news feeds and discussion groups from around the world to detect any patterns. [2] Once WHO identifies an official outbreak, GOARN can be used to send out alerts to over 100 networks around the world. [3] The speed and security of these networks is essential to timely dissemination of outbreak information.

The technology available to WHO and other health organizations was crucial in controlling the SARS outbreak. GOARN and GPHIN were the critical systems needed to disseminate information on a timely basis to international health organizations. In addition, the media played a large role in educating individuals on how to defend against SARS. SARS is an example of a high visibility outbreak, whose potential hazardous payload motivated individuals and governments to take precautions to defend themselves for fear of chaos and even death. Delayed reporting contributed to the speed with which SARS spread. Had WHO been alerted when the outbreak was first observed in Guangdong, SARS might not have become an international problem. In this case, hesitancy to alert the appropriate organizations created a problem that magnified its impact. To avoid similar outbreaks, an international environment needs to be created in which countries are willing to declare when they have an outbreak, and are able to effectively communicate with other governments and organizations to create a comprehensive response. [4]

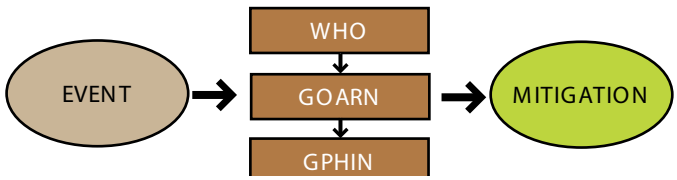


Figure 1.Events must be processed in order for mitigation to work.

The Tylenol™ case—depraved indifference

In 1982, Johnson & Johnson experienced a major crisis when it discovered that numerous bottles of its extra-strength Tylenol™ capsules had been laced with cyanide. By the end of the crisis, seven people had died. The poisoned capsules had apparently been placed on shelves in six different stores by a person intent on killing innocent people at random.

How J&J dealt with this situation set a new precedent for crisis management. The company was lauded for its quick decisions and sincere concern for its consumers. Despite initial losses, J&J regained and exceeded its previous market share within months of the incident.

In the midst of the crisis, J&J made a decision that would set a new standard for crises involving product tampering—the company ordered a massive recall of more than 31 million bottles at a cost of more than $100 million. It also temporarily ceased all production of capsules and replaced them with more tamper-resistant caplets. The company was able to use the crisis and its drastic response to demonstrate to customers its commitment to customer safety and to the quality of its product. In addition, the company's willingness to be open with the public and communicate with the media helped the company maintain a high level of credibility and customer trust throughout the entire incident. J&J's president also maintained a high profile by repeatedly assuring the public of the company's commitment to its customers' safety. [5]

Malicious mischief in the cyberworld

Despite early warnings of the Blaster worm, a large percentage of PC users had their systems infected by the worm. On July 17, 2003 approximately a month before Blaster was discovered in the wild, the Federal Computer Incident Response Center (FedCIRC) issued an advisory and patch for a buffer overflow vulnerability in Microsoft's Remote Procedure Call (RPC) Implementation [6] based on a July 16 Microsoft Security Bulletin (MS03–026). [7] Other vulnerability alert organizations, such as Carnegie Mellon's Computer Emergency Response Team/Coordination Center (CERT/CC) and Symantec issued advisories as well. The "Last Stage of Delirium" research group originally uncovered the vulnerability and disclosed the information to Microsoft. The company announced the vulnerability to the public and to security professionals in ample time with heavily publicized instructions and advice on how to install the appropriate patches.

Blaster was discovered in the wild on August 11 and once on a system, the worm used the host to attempt denial of service attacks on http://www.windowsupdate.com. (Ironically, this Web site is only a redirector site. The URL to Windows updates is http://v4.windowsupdate.microsoft.com.) The worm quickly spread around the world primarily affecting users of Windows 2000 and Windows XP. Blaster's presence was evident through high network bandwidth and system failure.

The information security community's actions prior to the Blaster worm outbreak provide an excellent example of how to identify a potential problem and disseminate information about it. Through organizations like FedCIRC, CERT/CC and Symantec, PC users were given enough time and information to defend themselves against potential threats.

On the other hand, the main methods of mitigating Blaster involved executing defensive measures at the user level. User indifference regarding what may have seemed like just another software vulnerability likely added to the proliferation of the worm. Like the boy who cried wolf, with so many vulnerabilities and alerts issued by Microsoft and other organizations, users soon become inured to warnings and made no attempt to differentiate between a critical patch and a less significant one. The responsibility of defending networks ultimately falls on individual users, who are often apathetic.

The issue in this case involves execution of defensive measures at the user level. Users are not necessarily going to be concerned about malicious code for a variety of reasons. For one, some users cannot comprehend the potential damage that can be caused by malicious code and therefore ignore vulnerability warnings. Additionally, users may not want to take the time to patch a system, especially when they are not able to differentiate between a critical

patch and an insignificant one. The Blaster worm is yet another lesson for all computer users on the importance of timely system patching and updating.

Conclusions

Despite constant vigilance within operating environments there are no safety and security guarantees—no way to absolutely, with 100 percent confidence, predict or prevent dangers or threats to our well-being, be they cultural, personal or technological. At some point early in any outbreak defenders must inaugurate a decision process that combines foresight, intuition, and forensic analysis of previous events. This should compel the appropriate entity to formulate a meaningful warning message and broadcast it to a wide audience.

Other organizations and agencies can be expected to devise countermeasures to mitigate the effects of the outbreak and still others can create defensive measures to prevent reoccurrence. In the instance of SARS, those entities were the Centers For Disease Control (CDC) and WHO; with Tylenol™, they were J&J along with the retail sector of the economy; and, for the Blaster worm, they were the CERT/CC, the Department of Defense (DoD) CERTS, and the Joint Task Force–Computer Network Operations (JTF–CNO).

Within each of the outbreaks discussed, detection is a vital component (see Figure 2). Not only does an entity have to discern that there is a malevolent event unfolding, the same watch and warning entity must also be able to intuitively establish that the rapid proliferation of the outbreak could have devastating effects downstream. In each of these outbreaks, countermeasure and protective decisions included the centralized formulation of actions/countermeasures, coupled with decentralized execution of protection and mitigation measures involving agencies, governments, and individuals. In each of these outbreaks a defensive posture had to be formulated by a given entity—based on incomplete data in a rapidly emerging crisis environment. It is important to note that despite incomplete or inconclusive data, timely decisions had to be and were made; this emphasizes the importance of coupling I&W functions with an authoritative decision-making entity that has both the means and the will to take action as quickly as possible given the circumstances.

Figure 2. Effective defense begins with cooperation.

Maintaining a prudent and persistent I&W entity along with supporting processes is fundamental to any effort designed to protect the public. The I&W process must also be linked with a response entity that has the authority and capacity to reach a diverse, widely dispersed audience with competent and timely warning and instructions.

The JTF–CNO computer network I&W system has proven its ability to detect and deter while providing timely warning to worldwide users within the Department of Defense. This capability is critical to sustaining the uninterrupted flow of information to warfighters deployed throughout the world. ■

About the Authors

Tom Ward

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

April Perera

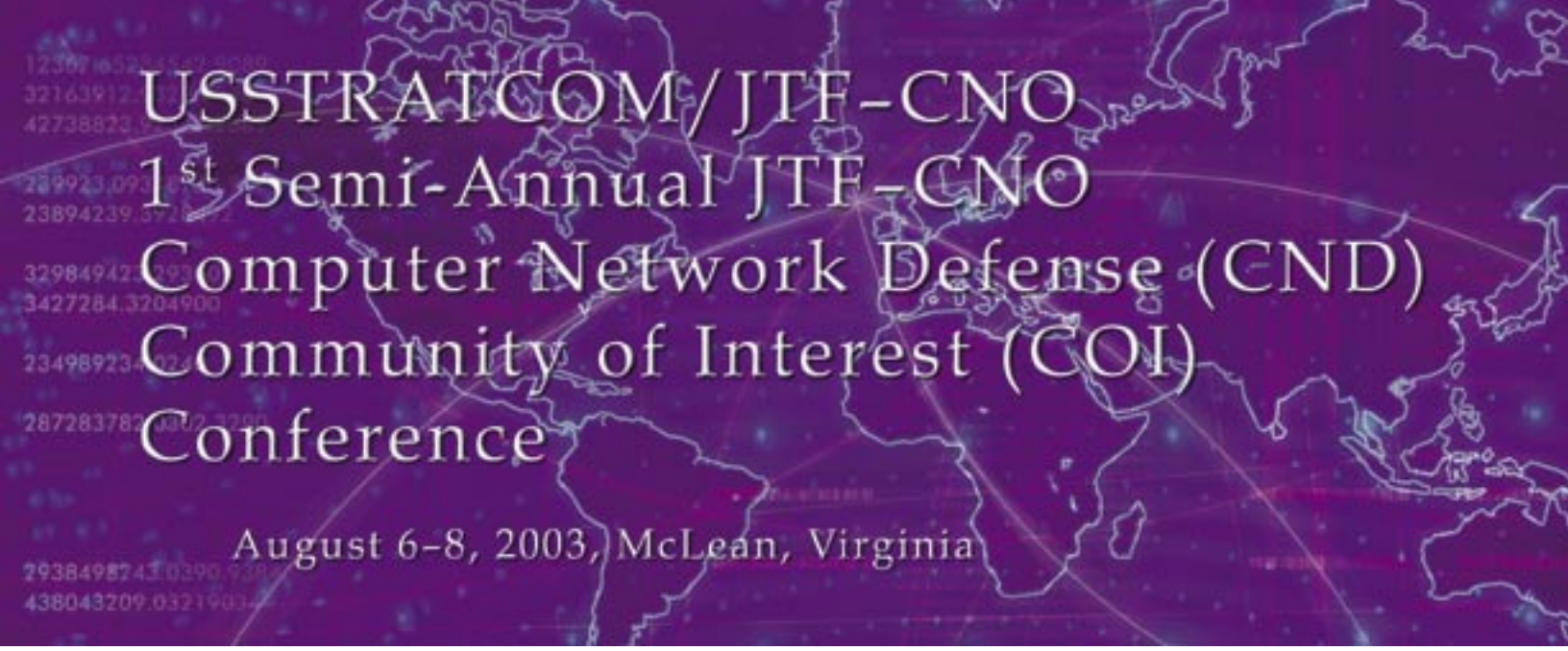
Ms. April Perera is a Research Analyst at the Information Assurance Technology Analysis Center (IATAC). She holds a B.S. from the University of Virginia. Ms. Perera can be reached at iatac@dtic.mil.

Tim Madden

Mr. Tim Madden is the public affairs and protocol officer for the Joint Task Force for Computer Network Operations, U.S. Strategic Command. He holds B.A. degrees in journalism and literature and can be reached at maddent@jtfcno.ia.mil.

References

1. World Health Organization (2003). Severe acute respiratory syndrome (SARS): Status of the outbreak and lessons for the immediate future [Online]. Available: http://www.who.int/csr/media/sars_wha.pdf.
2. Ibid.
3. Ibid.
4. Nullis, Clare. (May 27, 2003). SARS Shows Need for New International Health Regulations, Says WHO. Canadian Press [Online]. Available: http://mediresource.sympatico.ca/health_news_detail.asp?channel/id=16&news_id=1396.
5. Buchanan, Andrew. (November 11, 2001). Chemical terrorism that changed America—the unsolved Tylenol™ cases, a generation before anthrax scare. Associated Press [Online]. Available: http://www.s-t.com/daily/11-01/11-17-01/a02wn024.htm.
6. FedCIRC (2003, July). DHS/FedCIRC Advisory FA–2003–16 Buffer Overflow in Microsoft RPC. Retreived August 2003, from FedCIRC Web site: http://www2.fedcirc.gov/advisories/FA-2003-16.html.
7. Microsoft (2003, July). What You Should Know About Microsoft Security Bulletin MS03–026. Retreived August 2003, from Microsoft, Security and Privacy Web Site: http://www.microsoft.com/security/security_bulletins/ms03-026.asp.



by Tim Madden

The U.S. Strategic Command (USSTRATCOM) and the Joint Task Force–Computer Network Operations (JTF–CNO) jointly hosted a Computer Network Defense (CND) Community of Interest (COI) Conference in McLean, Virginia, August 6–8, 2003.

The purpose of the conference was to promote Intelligence Community (IC) support for a variety of CND needs, from strategic to operational. The nearly 120 participants represented four nations (Australia, Canada, England, and the United States), three U.S. Unified Commands (Central, Transportation, and Strategic), three U.S. Departments (Defense, Energy, and State), and 24 other commands, offices, organizations, and agencies.

CDR Michael Greenwood (USN), JTF–CNO J2/ Directorate of Intelligence, kicked off the conference with a charge to "fulfill the [JTF–CNO] Commanding General's vision" of doing CND better.

> *"The Intelligence community has been doing pieces and parts, with no coherent, consistent management of Intel support to the CND process…"*

he noted in his opening remarks.

> *"STRATCOM [U.S. Strategic Command] wants us to move forward in a coordinated, synchronized fashion that is inclusive and that enhances our best practices. STRATCOM is something like a velvet hammer—there's real power behind the quiet urgings to focus on the issues that move us forward together, rather than on what differentiates us. This is a new CND, proactive and aggressive, and it requires a new mind-set: don't shoot first and ask questions later, but be discerning, inclusive, and thoughtful. In short, what we need to accomplish over the next three days is answer the question, 'How do we fulfill the Commanding General's vision, that no attack will go undetected, no attack will go undefended, and no attack will go unanswered?'"*

Col Jeffrey Brown (USAF), JTF–CNO Chief of Staff and J3/Directorate of Operations, delivered the keynote address in place of MG J. David Bryan (USA), Commander, JTF–CNO. The General's message, Col Brown said, was that

> *"There is a new environment—Technological advances are progressing faster than ever and the operational tempo and threat environment are getting higher every day, which heightens the need for joint and coalition interoperability to support a new generation of warfighter."*
>
> **Col Jeffrey Brown (USAF)**
> **JTF–CNO Chief of Staff and**
> **J3/Directorate of Operations**

The fundamental need, he said, is for better information provided faster on the attributes that differentiate intruders, and "attribution with a legal degree of certainty."

Other speakers on the first morning—

- CDR Dan Driscoll (USN) Chief, Space/Information Operations Intelligence (IO) Division, STRATCOM, whose message was the importance of creating a capable IO organization.
- LCDR Kevin Hinton (USN), Chief of the Fusion Branch, JTF–CNO J2, who emphasized the necessity of breaking out of stovepipe thinking and practices to reach a fusion of analysis and understanding.
- Jeff Wright, JTF–CNO International Liaison for Information Assurance (IA) of CND, who spoke about the push "to create cooperative execution of common CND processes" on an international scale.

The second morning session of the conference began with an address by Dr. Michael Cohen, Senior Technical Advisor, Information Security Group, Australian Defence Signals Directorate. Dr. Cohen discussed the operations of his country's Computer Network Vulnerability Team, noting that CND "is a difficult problem that needs a complete security policy and strong forensic support."

continued on page 26…

A Framework for Information Assurance (IA)

by Abraham T. Usher, CISSP

Information Assurance (IA) has become an increasingly important topic to the military, government, and commercial industry in the past decade. The growing dependence of these three groups on public information and communication assets requires greater vigilance in protecting these resources. As America and other post-industrial nations become increasingly "information centric" economies, the relative importance of protecting information assets increases. This article presents a framework for thinking about IA in a simple, yet comprehensive manner.

In 1991, John McCumber created a framework for considering Information System Security (INFOSEC) issues in a holistic fashion. [1] INFOSEC came to be defined as—

> *Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.*

However, as the need for information and information resources has increased, INFOSEC evolved into information assurance (IA), defined by the National Security Telecommunications and Information Systems Security Committee as—

> *Information operations (IO) that protect and defend information and information systems be ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.*

Why bother with a new framework? It is useful to have a comprehensive model to consider how to best achieve information assurance objectives. I propose a framework that extends the previous work of a group of researchers at West Point (Ragsdale, et. al.) [2]. This framework has three main component parts—

- Information states
- Security services
- Security countermeasures (see in Figure 1).

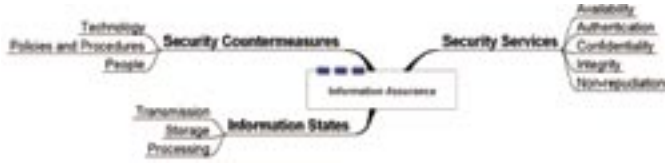


Figure 1. IA framework

Information states refer to the primary forms that digital information can exist in, including transmission, storage, and processing. **Transmission** refers to sending data from one subject to another. Storage refers to information located on a non-volatile, persistent source such as a computer hard drive. **Processing** refers to information that is undergoing usage by the CPU and exists in a volatile state (e.g., RAM).

Security services describe the five main countermeasures that are used to protect information resources—

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authentication.

Security countermeasures are the people, policies and procedures, and technologies that are combined as part of a defense-in-depth strategy to provide security services.

This framework provides a way of organizing the technical and non-technical elements of IA as they apply to achieving various security services. If the five security services are combined with two of the three security countermeasures, it yields a relationship diagram that looks like Figure 2. (People are left out of the diagram, as they are an implicit component of every security architecture.)

The usefulness of the information in Figure 2 is that a security professional may consider which IA objectives they need to achieve, such as confidentiality or integrity, and which technical mechanisms, policies, and procedures may

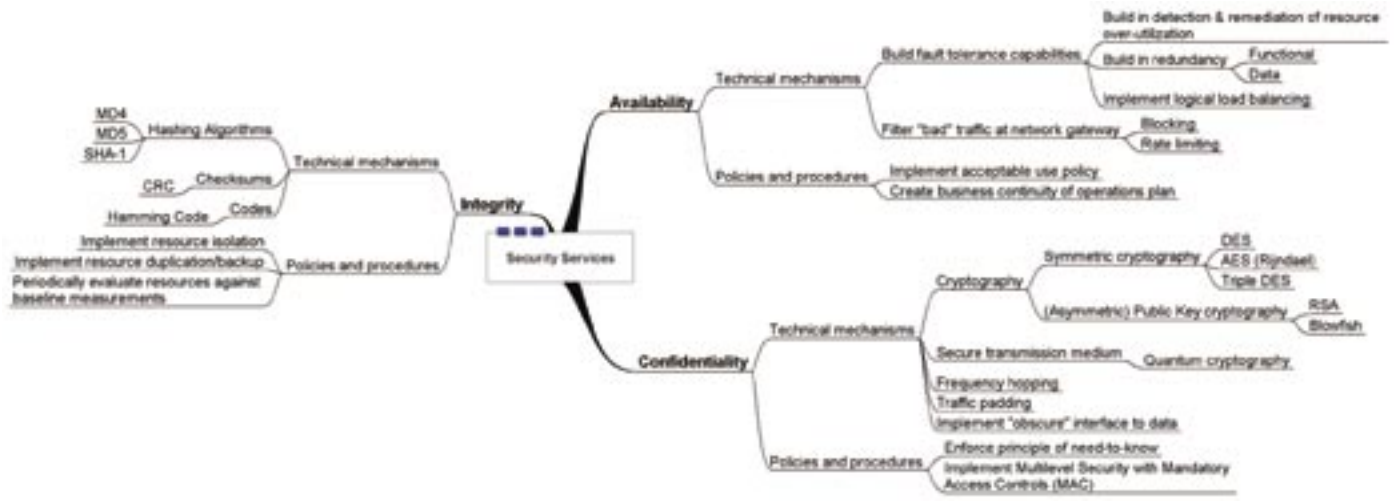


Figure 2.

be combined to achieve their objectives. Two examples of this process are presented below.

Example 1: Securing transfer of information across the public Internet

Alice wants to send an E-mail to Bob that includes an attachment that has sensitive financial information. Alice is concerned that a malicious interloper might intercept the data while it is in transmission by sniffing traffic on her local area network. To prevent interception of the data, Alice uses a product called PGP (Pretty Good Privacy) with her E-mail and encrypts the data with Bob's public key. Upon receiving the E-mail message from Alice, Bob decrypts the message using his private key.

Notes on Example 1

In this example, Alice was primarily concerned with the confidentiality of information that was to undergo transmission. She decided to use a technical mechanism to achieve her objective of confidentiality. In this specific case, she used asymmetric cryptography through the E-mail product PGP (see Figure 3).

It is important to realize that although Alice achieved a level of confidentiality for the transmission of her information, the PGP encryption did not afford any confidentiality once the message was received and decrypted by Bob and stored on his hard drive. In other words, once the information *changed states* (from being encrypted and in transmission, to being unencrypted and stored) a new set of security measures became necessary to ensure its confidentiality.

Alice could have improved the confidentiality of her E-mail message by using additional mechanisms, policies, and procedures related to confidentiality. A higher level of confidentiality could have been achieved by sending the E-mail across a secure transmission medium that is resistant to data interception (e.g., fiber optic cable). A non-technical way to improve confidentiality would be denying users access to Alice's network unless they had a specific authorization and need-to-know related to the resources on the network.

Figure 3. Selecting mechanisms for confidentiality.

Figure 4. Selecting mechanisms for availability.

Example 2: Maintaining the availability of a Web-based resource

Now consider a different scenario—Alice is a Web administrator, trying to ensure that important public information on her Web site http://www.alice.com remains available to other organizations. In this example, Alice is not interested in confidentiality of information as much as she is concerned with its *availability* (a public Web site that is not available for viewing by the public would not be very useful!). To prevent the Web site from being overloaded from legitimate traffic, Alice implements a system architecture with several redundant Web servers (see Figure 4). A load-balancer re-routes traffic dynamically to ensure that all incoming Web "hits" are evenly distributed across all of the servers. To protect against malicious Denial of Service (DoS) attacks, Alice purchases a protective system that allows her to limit the rate of bandwidth consumption

continued on page 26…

continued from page 23…

USSTRATCOM/JTF–CNO 1st Semi-Annual JTF–CNO Computer Network Defense (CND) Community of Interest (COI) Conference

Other speakers on Day 2 included—

- LTC Ed Sbrocco (USA), J3/Operations Directorate, who discussed the implications and demands of CND Response Actions (CND/RA), whose concepts are still being debated and whose range of activities is still being determined.
- Lt Col Timothy Evans (USAFR), Deputy Staff Judge Advocate, JTF–CNO, who took the audience through the legal ramifications of intelligence oversight in regards to CND and CND/RA.
- Jason Jurand, Military Infrastructure Office, IO Threat Analysis, Defense Intelligence Agency, who discussed the "fusion of strategic and tactical warning data."
- Louis Ramone, Intelligence Analyst, JTF–CNO Law Enforcement and Counterintelligence Center (LECIC), who detailed the nature of the relationship between JTF–CNO and LECIC and its agents and analysts.
- Mike Valerius, USTRANSCOM, who reminded the attendees that transportation "impacts mission capability" and is "the Achilles Heel of CND."

The Working Groups established during the conference included—

- Roles and Responsibilities (Lead: CDR Driscoll)
- Indications and Warning for Computer Network Attack Methodology (Lead: Mike Potaski of DIA)
- Collection and Requirements Management (Lead: Rich Hasbrouck, USSTRATCOM)
- Analysis and Reporting (Lead: LCDR Julie Welch, USSTRATCOM).

Attendees agreed that there should be a follow-on conference in late February 2004, with STRATCOM and JTF–CNO/J2 host, with all combatant commands, Services, and intelligence agencies invited to participate. ■

About the Author

Tim Madden

Mr. Tim Madden is the public affairs and protocol officer for the Joint Task Force for Computer Network Operations, U.S. Strategic Command. He holds B.A. degrees in journalism and literature and can be reached at maddent@jtfcno.ia.mil.

continued from page 25…

A Framework for Information Assurance

of suspicious traffic (e.g., if a client connection suddenly request 1 million Web pages, the system reduces the available bandwidth to that connection).

Notes on Example 2

As illustrated in Figure 4, the mechanisms for protecting the *availability* of information are very difference that the mechanisms for preserving *confidentiality*. In this particular example, Alice used to technical mechanisms, added redundancy and traffic filtering, to attain her objective of availability. Using encryption would have been inappropriate in this example, as encryption does directly not help attain availability.

For more a more comprehensive availability plan, Alice should have included additional measures. To provide a legal basis for discouraging users from abusing her Web site, she could have created an acceptable use policy that defines how external users may draw on her Web resources. To prepare for natural disaster such as a power outage or flood, Alice could create a business continuity of operations plan that describes how her Web site would be restored under emergency conditions.

Conclusion

The two examples presented in this article are a trivial example of using my framework for choosing mechanisms to achieve specific IA objectives. Real world information systems usually demand multiple IA objectives to achieve an acceptable level of assurance. This article only presents an abridged version of my IA framework. The full version of the framework is available through IATAC. ■

About the Author

Abraham T. Usher

Mr. Abraham T. Usher is the Deputy Director of the Information Assurance Technology Analysis Center (IATAC). He graduated from the U.S. Military Academy in 1996 with a B.S. double major in Modern Standard Arabic and German language studies and he also received a M.S. in Information Systems from George Mason University. Mr. Usher is a Certified Informational System Security Professional (CISSP) and may be reached at iatac@dtic.mil.

References

1. McCumber, John. "Information Systems Security: A Comprehensive Model," Proceedings of the 14th National Computer Security Conference. National Institute of Standards and Technology. Baltimore, MD. October 1991.
2. Maconachy, V., Corey, S., and D. Ragsdale. "A Model for Information Assurance," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. U.S. Military Academy. West Point, NY. June 2001.

product order form

Instructions: All IATAC **LIMITED DISTRIBUTION** reports are distributed through DTIC. If you are not a registered DTIC user, you must do so **prior** to ordering any IATAC products (unless you are DoD or Government personnel). **To register On-line:** http://www.dtic.mil/dtic/regprocess.html.
The *IAnewsletter* is **UNLIMITED DISTRIBUTION** and may be requested directly from IATAC.

Name _____ DTIC User Code_____

Organization _____ Ofc. Symbol _____

Address_____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ❑ USA ❑ USMC ❑ USN ❑ USAF ❑ DoD
❑ Industry ❑ Academia ❑ Gov't ❑ Other

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

_____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)

❑ Firewalls ❑ Intrusion Detection ❑ Vulnerability Analysis

Critical Review and Technology Assessment (CR/TA) Reports

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

State-of-the-Art Reports (SOARs)

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

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

UNLIMITED DISTRIBUTION

Hardcopy *IAnewsletters* available

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

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

Fax completed form to IATAC at 703/289-5467

February

8th Annual Information Assurance (IA) Workshop "Fighting the Net: Securing Today's Battlefield"
February 2–5, 2004
Atlanta, Georgia
http: www.iaevents.com, http://iase.dia.mil

West 2004
February 3–5, 2004
San Diego Convention Center, California
http://www.west2004.org

Information Operations T&E Workshop
February 9–12, 2004
Windemere Hotel & Conference Center,
Sierra Vista, Arizona
http://www.itea.org

National Threat Symposium
February 10–11, 2004
National Nuclear Security Administration,
Nevada Operations Office, Las Vegas, Nevada
http://www.iaevents.com

Spam Technology Workshop
February 17, 2004
NIST Gaithersburg Campus, Building 101,
Green Auditorium.
http://csrc.nist.gov/spam/

RSA Conference 2004
February 23–27, 2004
Moscone Center, San Francisco, California
http://2004.rsaconference.com/

Information Assurance 2004
February 24-26, 2004
Arlington, VA
www.idga.org/2108-01/g995.

AFCEA Homeland Security Conference
25-26 Feb 04
Ronald Reagan International Trade Center,
Washington, D.C.
http://afcea.org/homeland04/

March

Federal Information Systems Security Educators Association (FISSEA) Conference "Awareness, Training, and Education - The Driving Force behind Information Security"
March 9–11, 2004
Inn and Conference Center, University of
Maryland University College (UMUC),
Adelphi, Maryland
http://csrc.nist.gov/organizations/fissea/conference/2004/index.html

PEO EIS Industry Day 2004 "Integrating IT for Warfighters"
March 17–18, 2004
Sheraton National Hotel, Arlington, Virginia
http://www.fbcinc.com/event.asp?eventid=Q6UJ9A005ULY

Fose 2004
March 23–25, 2004
Washington, DC Convention Center
http://www.Fose.com

DTIC 2004 Annual Users Meeting and Training Conference
March 29–30, 2004
Hilton Alexandria Old Towne,
Alexandria, Virginia
http://www.fbcinc.com/event.asp?eventid=Q6UJ9A0074YI

Joint Warrior Interoperability Demonstration (JWID) 2004 Final Planning Conference
March 29 – April 2, 2004
Holiday Inn Chesapeake, Chesapeake, Virginia
http://www.jwid.js.mil

April

Fiesta Informacion 2004 "Transformation: A Journey, Not a Destination"
April 19–21, 2004
Henry B. Gonzalez Conference Center,
San Antonio, Texas
http://www.afcea.org/fiesta2004/default.asp

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

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