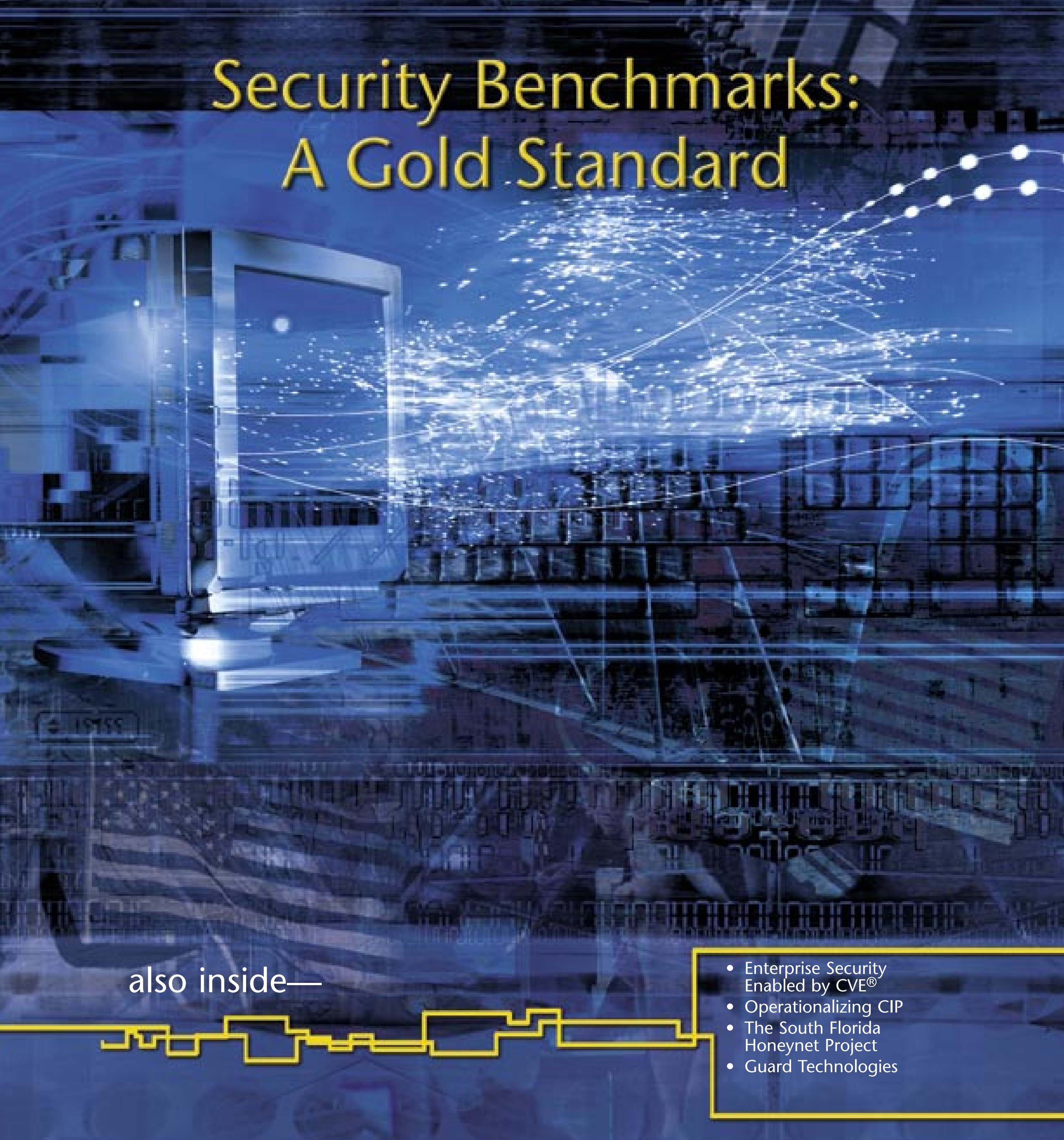
IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 5 Number 3 • Fall 2002

Security Benchmarks: A Gold Standard



also inside—

contents

feature

IA initiatives

in every issue

About IATAC & the *IAnewsletter*—

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

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

IATAC Director:	Robert J. Lamb
Inquiry Services:	Peggy O'Connor
Technical Analysts:	Abraham T. Usher April Perera Jim Peña

IAnewletter Staff—

Creative Director:	Christina P. McNemar
Art Director:	Ahnie Senft
Designers:	Maria Candelaria Holly Shipley Trang Dam

IAnewsletter Article Submissions

To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/news_events/author_submission.htm and download an "Author's 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—

Winter 2002/2003	3 January

Cover design:	Holly Shipley
Newsletter design:	Ahnie Senft

Distribution Statement A:

Approved for public release;
distribution is unlimited.

IATAC Chat

Robert J. Lamb, IATAC Director

This past July the IATAC Steering Committee met. During the course of that meeting a number of great ideas were put forth and IATAC has been moving forward to execute accordingly. With this column I'd like to highlight a couple of these initiatives for your information.

Many of you may have heard of the change to the *IA Digest* that we have undertaken as a result of recommendations from both the J6K of the Joint Staff and DIAP. The Digest was published monthly, in hard copy only with a limited distribution managed by the J6K. We had looked at a number of options for putting it on line, but routinely were confronted by copyright restrictions. We have resolved those issues and in the process expanded the Digest to be a twice weekly, electronically disseminated, HTML file linking subscribers to stories of interest. With IAC PMO, J6K, and DIAP concurrence, we have expanded distribution to a much wider audience. Since its inauguration in August, we have been inundated with subscription requests. Ultimately we will automate that process, but in the meantime if you are interested in receiving the IA Digest, please send an E-mail to iatac@dtic.mil and we will process it accordingly.

The Steering Committee also focused our research efforts on this year's reports. As in past years, there will be three of them—two Critical Review and Technology Assessments (CR/TA) and one State-of-the-Art Report (SOAR). The committee recommended we pursue the following topics—

Wireless Security

The objective of this report is to provide an overview, analysis, guidelines, and recommendations for security of wireless wide area networks. It will examine basic Wireless Wide Area Network (WWAN) technologies, the different security schemes implemented within each technology, the issues and concerns associated with each scheme, and current industry trends and best practices used to mitigate these concerns.

Insider Threat

The importance of the Internal Threat is axiomatic to the defense and intelligence communities. These communities contain multi-level security environments with policies mandating that entities could only access information up to its security level. An Internal Threat is defined as an entity that—

1. Is identified and authenticated by the environment
2. Is authorized to execute certain activities based on that authentication
3. Is executing unauthorized activities.

The original Internal Threat was a person with an assigned security level obtaining information classified at a higher security level. As the complexity of information environments has increased so has the sophistication of the internal threat. To efficiently deploy resources to enforce multi-level security policies that mitigated the internal threat was straightforward in paper-based environments, challenging (but obtainable) in centralized electronic environments, and formidable in distributed electronic environments.

Multi-level Security

Information fusion is similarly a topic of considerable interest. This report will explore the realization of information fusion framework for these communities within a multi-level security environment. A multi-level security environment contains, within its security perimeter, both information and entities with different security levels. A multi-level security policy is the basis for the operational and administrative procedures within this environment. The policy classifies information at a sensitivity level. In addition, information may receive a compartment that categorizes the content of the information. The security level of a document is the combination of both the sensitivity level and the set of content compartments. An entity (e.g., software, hardware, or an individual) also has an assigned security level. The policy mandates (by law) that an entity can access information up to its security level. The challenge is to introduce technology that supports the researcher/analyst and guarantees that the policy is enforced. This report will explore the realization of information fusion framework for these communities within a multi-level security environment, examining the challenges, policies, and technologies, for those operating in this environment.

Sign up for the IA Digest and look for these reports in the coming months.

Warmest Regards,

Bob

Consensus Minimum Security Benchmarks

A Gold Standard for Windows 2000 Professional Arises from a Public-Private Partnership

by Alan Paller, SANS Institute; and Clint Kreitner, The Center for Internet Security

The Gartner Group reported last May that at least through 2005, 90 percent of computer attacks will use known security flaws for which a solution is available. People don't fix the flaws because—

- knowledge about the flaws and how to fix them is not widely shared, and
- tools to measure whether they have been fixed were not widely available”

On July 17, the National Security Agency, Defense Information Systems Agency, the National Institute of Standards and Technology (NIST), the FBI's National Infrastructure Protection Center, the General Services Administration (GSA), the SANS Institute, and the Center for Internet Security (CIS) jointly announced minimum standards for securing computers using Microsoft Windows 2000 Professional, which is used on Windows 2000 computers functioning as workstations. The unprecedented announcement, led by Presidential Cyber Security Advisor Richard Clarke, is an effort to stop most common attacks against computer networks both inside and outside the Government. The new benchmark provides detailed configuration specifications for computers running Windows 2000 Professional and that are to be connected to networks. In field tests, application of the benchmark configurations have proven to eliminate more than 80 percent of commonly exploited vulnerabilities. (see *Measuring the Value of Security Guides* on page 10 for details on the effectiveness of the new benchmarks).

Government experts hope that the benchmarks will help eliminate two of the most troubling problems in computer security—problems that affect both federal and private computer networks—by eliminating holes that hackers already know about.

Two widespread problems

Unprotected systems are a massive challenge throughout Government and industry because of two practices common among companies that sell and install systems. First, the companies employ a distribution process in which months pass between the time a vendor creates a CD and a user installs the software. Even if you are the first to receive a new CD, the software on that CD may be two or three months old. Security vulnerabilities discovered in the intervening months are automatically installed with the software. Users may overcome this problem by downloading and installing the latest security patches from the vendor's Web site, but, not surprisingly, a large percentage of users do not take this step.

While the systems remain unpatched, they are highly vulnerable. More than two thousand automated attack programs are constantly scanning the Internet looking for vulnerable systems. Too many organizations have found that their systems are attacked and exploited (often with a Trojan horse program) before the users have had time to download and install the needed patches.

Second, the companies deliver their software with installation scripts that automatically install services that are unfamiliar to the user and may not be needed. Some of those services, like telnet, FTP, CGI scripts, and BIND/DNS are notoriously vulnerable to attackers. Others have more subtle vulnerabilities. All of them, if left enabled, provide a continuing fertile ground for additional vulnerabilities to be discovered and exploited. When users do not know they are running a service, they often do not look for security patches for those services.

The White House announces a standard for DoD and possibly other agencies

In announcing the new benchmark, President Bush's Special Advisor of Cyberspace Security, Richard A. Clarke, pointed out the most important aspect of the new benchmark, saying, “this is the model for Government and industry partnership.” The partnership combines the knowledge and buying power of the Government and more than 100 very large non-Government organizations. They agreed on specific minimum security settings for Windows 2000 Professional presented as a “gold standard.” Mr. Clarke also said that DoD organizations would be required to use the new standards and that the White

House is considering whether and how to require compliance by civilian federal agencies.

Consensus takes some of the uncertainty out of security

Most of the organizations involved in the partnership had published their own guides for securing Windows 2000, but all the guides conflicted in small ways. Since many user organizations looked to multiple sources for guidance, the differences between their guides meant that they were unable to move ahead with confidence.

The consensus benchmarks were forged by all the organizations identifying and resolving the differences among the various existing guides. The consensus guide empowers user organizations to move ahead with a high degree of confidence that they can have a solid foundation for security of their systems.

Tools to test and enforce the standards

As a part of the announcement, the partners also released an automated testing tool created by CIS that compares the security settings on a computer with the security settings in the benchmark and scores each machine on a 0 to 10 scale.

Benchmarks are complex documents and most system administrators and security practitioners have neither the time nor the breadth of expertise to test every aspect manually. Automated testing makes that job easy and reliable. The Center's tool also guides the user in the proper method of correcting configuration problems that lower the score.

U.S. Air Force plans to acquire safer systems

At the July 17 announcement, U.S. Air Force CIO John Gilligan announced that the U.S. Air Force was planning to integrate the new benchmarks into future procurements so that system administrators would not be burdened with having to play catch up on every new machine.

Where to find benchmarks and tools

The benchmarks and automated tools are available for immediate download from the CIS's Web site at http://www.cisecurity.org. Individuals may use the benchmarks and tools to check their systems, but organizations must be members of the Center to distribute the tools and use them across the entire organization. The GSA has purchased internal distribution rights for all Federal Government agencies (both civilian and Military), as well as for authorized federal contractors and sub-contractors, so that they may use the tools wherever and however they see fit on Government

...continued on page 9

Additional Benchmarks Currently Available from CIS

http://www.cisecurity.org

- **Cisco IOS Router**—The most popular router
- **Solaris**—The UNIX operating system used on Sun Microsystems computers
- **Linux**—The open source operating system gaining popularity in government and industry
- **HP–UX**—The UNIX operating system used on Hewlett Packard computers
- **Windows NT**—The most popular server operating system on Intel hardware prior to Windows 2000.

Training and Certification for Implementing the Windows Security Benchmark

The new security benchmarks will improve security only on the systems where they are applied. The ultimate value of the benchmarks, therefore, will be determined by the number of people who have the skills and knowledge to implement them.

Because that knowledge is not taught in Microsoft system administration courses for MCSA or MCSE certification, security experts from Australia to the U.S. to Europe have cooperated to build a hands-on education program that targets the necessary skills.

The course covers the benchmark, what it does, including registry keys, folder ACLs, user rights, and security policies. It also shows how to view, modify, and apply the standard. And the course provides hands-on experience in using the tools that enable administrators to be sure it is being applied correctly. It assumes the student is familiar with Windows 2000.

To reach a goal of training 150,000 people in applying the security benchmarks, five types of education have been deployed—

1. The course book is available from Amazon and is called "Securing Windows 2000 Professional Using the Gold Standard Security Template" by Bower, Farrington, and Weber, (ISBN 0–9724273–0–9).
2. Hands-on, instructor-led training has been run in more than 50 cities around the world both in public courses and in private onsite courses.
3. On-line training is available at any time with audio programs, visuals, and on-line quizzes.
4. Local-mentor programs are also being launched in more than 60 cities and on military installations. These programs combine on-line training with two or three meetings in which mentors help their peers work through the hands-on exercises.
5. Instructor-led on-line training is also being offered in which students take the live course with an instructor, but do so remotely.

Certification Program

Each student may demonstrate that both skills and knowledge have been mastered by completing a practical exercise and passing a test.

For information on the availability of DoD education programs for the new benchmarks, contact DISA, Maryann Dennehy at 703/882-1716. For more information on training programs open to all students, see the schedule posted at http://www.sans.org.

Training System Administrators in Using the New benchmarks

- **AIX**—The UNIX operating system used on IBM computers
- **Apache Web Server**—The most popular Web server software
- **Windows IIS Web Server**—The second most popular Web server software
- **Check Point FW–1/VPN–1**—The most popular firewall/VPN
- **Cisco PIX Firewall**—The second most popular firewall
- **Cisco CAT Switches**—The most popular networking switch

The Importance of Consensus Security

by Tony Sager and Brian Henderson

The Department of Defense (DoD) and many other components of the Federal Government look to the National Security Agency (NSA) for the means to protect vital communications and information systems. In today's Information Technology environment, the need is particularly acute for ways to counter security vulnerabilities found in popular commercial operating systems and applications. The NSA's Information Assurance Directorate (IAD) has responded to the challenge, in part by developing a very successful series of Security Configuration Recommendation Guides. And, in a real break from tradition, several of these Guides have been shared with the public through the NSA Web site http://www.nsa.gov. On July 17, 2002 at the press conference led by Richard Clarke, Cyber Security Advisor to the President, we joined with a number of our peer organizations to announce agreement on a "consensus" security benchmark for Windows 2000.

Several customers who had adopted our earlier NSA *Microsoft Windows 2000 Security Recommendation Guides* wanted to know if we had changed course. We reassured them that the content of the consensus benchmark is essentially identical to our prior NSA Guides. Here's the message that we asked them to take away from the press conference. This is a change in the development process for this type of security guidance, and that our goal is to reach agreement on baseline security configurations among peer organizations (the Defense Information Systems Agency [DISA], the National Institute of Standards and Technology [NIST], the FBI's National Infrastructure Protection Center, the General Services Administration [GSA], the SANS Institute, and the Center for Internet Security [CIS], etc.).

A shared problem

Why did we move towards a "consensus" model for developing and sharing security recommendations?

Fundamentally, it is because we believe that, at the security baseline level, network security is a shared problem between the DoD and the rest of the community. Not only is our security problem shared, but also we are each hopelessly dependent upon the security of others. If we have a shared problem, then we must pursue shared solutions.

There had already been a lot of technical sharing between several organizations that develop such standards (NSA, DISA, NIST, CIS, etc.). Here's the challenge we set before ourselves—if we could come to agreement on a common baseline, then the community would benefit in several ways. We could share labor on the development and the maintenance of security guidance. As the community following the guidance grows, "spin-offs" like training and tools become more viable for vendors to provide. Most importantly, we could minimize the confusion for system operators, who are already flooded with multiple authoritative sources and conflicting security guidance.

So this change in focus and attitude led to a surprising result—community agreement among a large number of security experts on prudent, baseline security settings for Windows 2000.

Consensus is nice, security improvement is better

But here's the reality check.

No security guidance document, however well intentionally and thoroughly tested, is inherently "good." Security guidance is only valuable when used and when it becomes a routine part of designing, installing, and operating our networks. This means that it must be easily integrated into operations, supported with tools and training, and provide a clear implementation of site and higher-level security policies, all in addition to providing specific value in improving security.

The bottom line? Security benchmarks are not the final answer for security improvement—they're just a beginning. Real improvement in network protection will come in many forms.

1 When system owners and decision makers move to adopt this consensus guidance for operational networks.

We're not starting from scratch. Each of the organizations involved in the consensus brings along a very large constituency. For NSA's part, we know that hundreds of organizations and major programs all across Government and the private sector have already adopted our guidance, formally as we support them through our mission, and informally by taking our recommendations from the Web site.

On July 17, U.S. Air Force CIO John Gilligan announced his intention to make the Windows 2000 Consensus Benchmarks the U.S. Air Force standard. The earlier NSA Guide, with essentially identical content, was declared the DoD Baseline Standard for Windows 2000. A number of other organizations are considering similar large-scale adoption.

If you follow security guidance for Windows 2000 available from DISA, NSA, NIST, CIS, or SANS, then you are already part of this consensus movement. The key difference is that the people giving you advice have agreed to share their ideas up-front, and reach agreement wherever possible.

2 When security engineers routinely start from and adapt consensus security benchmarks for their customers.

We know this is starting to happen across the community. MITRE system engineers supporting DoD (some of whom are directly involved in the development of the guidance) now routinely use the consensus benchmarks (or its predecessors like the NSA Recommendation Guides) as a starting point for advice to DoD programs. Anecdotally, we have heard numerous stories of use of the benchmarks from Microsoft senior engineers—using them as a starting point, and tailoring them to the specific operational and security needs of their customers.

3 When the consensus security benchmarks are supported with training.

SANS quickly had a course available based on the consensus benchmarks (their "Gold Standard" training), which is selling out rapidly. DISA is developing training based on this technical content, and the DIAP is exploring options for DoD-wide training. Large-scale, reasonably priced training from commercial sources integrated into Military schools is easily within reach.

4 When the consensus security benchmarks are supported by tools to help manage networks.

Consensus security benchmarks will not improve the security of networks on a large scale until they are embodied in a rich selection of tools to assist system administrators. Tools allow a system administrator to implement the benchmarks, and enable periodic or continuous reporting on the actual settings of every machine. The effect of configuration changes, and the resulting security improvement, can be scored, measured, and reported. This view of security status can then used as the basis for enterprise level security metrics.

A fundamental part of the CIS model is the development and release of freeware tools that measure compliance with their benchmarks (and with the consensus). But their real goal is to encourage a large market for commercial tool builders by certifying vendors whose tools accurately report on compliance with benchmarks. Based on technology that they already offer, commercial tool vendors can easily build compliance checkers that measure systems against these best practices. The vendor enthusiasm seems very high, and vendors like Bindview, Symantec, and NetIQ have already committed to this.

5 When consensus security benchmarks are available for each of the key components found in our networks.

A security benchmark for Windows 2000 is just the beginning. Most of the technical work is already done for Solaris and Cisco IOS, and these will be available and supported by CIS tools very soon. Several others are underway. Our mutual goal is to continue the consensus model, and share work wherever possible. This work can move quickly because organizations like NSA, DISA, and CIS are contributing existing documents as a "first draft" for the community.

6 When we can change our security decision processes.

With a defined baseline we can change how we purchase, deliver, and test software. If we think of the consensus security benchmarks as specifying the desired security behavior of a system and its applications, we can then provide a standard test environment for GOTS developers, and acceptance criteria for applications.

Key security decisions like accreditation, certification, and network "readiness" can become much more streamlined and meaningful. If we think of the benchmarks as representing the "best advice" of the security community, then—

- System architecture and design could start from such benchmarks for each component
- Security engineers could tailor the benchmarks based on program-specific security issues and operational constraints
- Documentation of the security-operational tradeoffs could serve as key evidence to decision makers about the security worthiness of the resulting system
- Continuous measurement of the tailored security benchmarks with tools can provide decision makers with a meaningful metric of the "readiness" of the network

Security "value"

Given the track record of the organizations involved, many people accept that the consensus security benchmarks for Windows 2000 are worthy of attention, if not adoption. However, we think that analytic organizations (including ours) owe the operational community and senior decision makers a clearer and more specific case for the potential security value of moving towards consensus benchmarks as a model for operating our networks. These are some of the questions that the operational community should pose about the potential security value of consensus security benchmarks—this is the sort of discussion that can get mired in philosophical debate and misleading statements (e.g., "this will stop 90 percent of all hacker attacks").

1 Do they "close" most of the known vulnerabilities in the component?

There's no final answer, but current informal studies, using different techniques for measurement, show that compliance with the consensus security benchmarks for Windows 2000 Professional (or predecessors like the NSA Guides) will conservatively close well over 80 percent of the known vulnerabilities in that component (see the feature article *Consensus Minimum Security Benchmarks: A Gold Standard for Windows 2000 Professional Arises From A Public-Private Partnership* on page 4). More detailed studies are underway at MITRE and elsewhere, including the mapping of common vulnerabilities and exposures (CVE) vulnerabilities against the benchmarks (see *Enterprise Security Enabled by CVE®* on page 12).

2 Do they "block" attacks against our systems?

Organizations that have collected and/or analyzed data about attacks against systems (e.g., the DoD CERT, CERT/CC, Gartner Group) all use very similar numbers—90 percent or more of the attacks or incidents against systems have taken advantage of known vulnerabilities with known solutions (e.g., patches or configuration options). In fact, it is typically reported that most attacks are based on a relatively small number of specific vulnerabilities. This is an area that deserves more study, and we believe that these two complementary communities—organizations that track, analyze, and report on attacks, and organizations that analyze technology and develop security recommendations—should jointly take this as their challenge.

3 Do they help me manage vulnerability information, by filtering through the "security noise" and helping me respond to new vulnerabilities?

The operational community does not have the luxury of time or resources to turn every system administrator into a security "wizard." If, in fact, compliance with consensus security benchmarks will close most vulnerabilities and block most attacks, then system operators can spend much less time sorting through the "security noise" of multiple vulnerability alerts, conflicting experts, and vendor claims. The effort of developing the consensus security benchmarks brings together security experts in both the public and private sectors to study vulnerabilities, develop countermeasures, and share the information in a form usable by system operators. As new vulnerabilities are uncovered, these experts should be able to quickly assess the effectiveness of prior guidance, and update it if necessary.

If compliance with the consensus security benchmarks will close most vulnerabilities and block most attacks, does this imply that the "consensus" organizations have discovered some magic ideas that everyone else missed? Of course not. In fact, our experience shows that qualified, independent groups (including the vendor) that develop security configurations for a component will typically reach very similar conclusions. This is not surprising, since all of us are studying the same "pile" of vulnerabilities, and the options for blocking problems at a component configuration level are relatively limited.

Therefore, the unique aspect of the security benchmark for Windows 2000 is the level of agreement among organizations, not the specific content of the benchmark. The benchmarks provide a vehicle to focus the experts, gain feedback from the operational community, and translate the hard-earned knowledge of vulnerabilities into a constructive, usable form that can improve security. In this way, everyone can spend less time sorting through the noisy pile of vulnerabilities, and more time on missions and operations.

No benchmark or guide will solve all security problems

Here are a couple of things that skeptical readers should point out about community-wide security benchmarks. There are no "magic bullet" solutions to the network security problem. For the Windows 2000 example, at best we can speak of closing almost all of the known vulnerabilities for only one component in a potentially very complex system.

However, it is a very significant subset of the applicable vulnerabilities for a key component of the network and, as discussed above, seems to easily meet the “80 percent solution” threshold. Given the state of network security today, an approach that can make much of the vulnerability management problem tractable and is “reasonable” in cost, training, implementation, and maintenance is an essential step.

Security is a system level problem, but we believe that without strong, known building blocks, system security is unattainable.

Benchmarks are not the long term solution

Gaining agreement among security experts and system operators is essential, gratifying, and has the potential to bring about large-scale security improvement. However, this strategy is essentially reactive—blocking problems after they are discovered, and doing the best that we can with existing technology. This approach is not the long-term solution.

However, benchmarks can be used to ”attack” the security configuration problem earlier in the life cycle. They can be used to specify how systems are configured out of the box, or delivered by our systems integrators. They can provide a testing baseline for applications developers, and as a means to collect community agreement on expected system behavior for the product developer. We are also developing closer linkage to the National Information Assurance Partnership (NIAP), to ensure that the development of more secure systems is closely matched to the secure operation of systems.

Summary

In our experience, the working-level cooperation between Government Agencies, private companies, and Microsoft that led to the success of the security benchmark for Windows 2000 is unprecedented, and the feedback has been overwhelmingly positive. The most gratifying feedback is from system administrators—the people on the front lines who have to make the technology work, and who rely on the security community for their help in securing systems.

The people involved in this project are representative of a growing security community, an extended network of professionals in and out of Government who have dedicated their careers to improving the security of our nation’s information and networks. Our collective sense of purpose has never been more focused, and the spirit of cooperation has never been higher. Working in partnership, we have the ability and the responsibility to improve the security of our nation’s information systems. ■

About the Authors

Tony Sager

Tony Sager serves as the Chief of the Systems and Network Attack Center (SNAC), located in the Information Assurance Directorate of NSA. The Center develops and releases to the public the NSA Security Recommendation Guides for several IT products (Windows 2000, Cisco Routers, etc.). Their security analysis of emerging network technology is sought and used by policy makers, network architects, and users across government. Tony recently celebrated 25 years with the NSA, holding a number of technical and managerial positions focused on Computer and Network Security. He holds a B.A. in Mathematics from Western Maryland College and an M.S. in Computer Science from the Johns Hopkins University.

Brian Henderson

Brian Henderson has been involved in information assurance since 1985. As a U.S. Naval officer and a graduate from the Naval Postgraduate School, he was assigned to the Department of Defense (DoD) Computer Security Center at the NSA. Following retirement from the U.S. Navy, Mr. Henderson worked for a small software support firm developing support plans for DoD information assurance products. He joined NSA in 1998 developing information assurance policy, then served on the NSA Chief Information Officer’s staff. Mr. Henderson joined the SNAC in 2001 as Chief of Staff and helped coordinate the center’s efforts to make security configuration guidance available to the public. He is currently a full-time student at the DoD Joint Military Intelligence College pursuing a Master of Science degree in Strategic Intelligence.

…continued from page 5

owned computers and contractor computers being used for Government tasks.

The bottom line

Turning the tide against cyber attackers will not be possible until the vast majority of systems on the Internet are free of common, easy-to-exploit vulnerabilities. The Gold Standard consensus benchmarks offer a means to accomplish that goal on both newly acquired systems and on systems already deployed.

The consensus benchmark process does not guarantee security—no one and no single action can. Rather they raise the bar for would-be hackers and crackers and dramatically reduce the vulnerability of all who apply the benchmarks and measure their systems, and all who connect to the them. ■

About the Authors

Alan Paller

Alan Paller is Director of Research at the SANS Institute. He leads SANS consensus research programs, was the expert witness in the MafiaBoy trial, has testified before both the House and Senate, and has chaired more than 60 national and international conferences on information technology. He may be reached at paller@sans.org.

Clint Kreitner

After serving in the U.S. Navy as Director of Computer-Aided Ship Design at the Bureau of Ships and Design Superintendent, Clint Kreitner has for the past 30 years been President and CEO of two information technology companies; ROH, Inc. and American Information Systems, Inc. (1971–1989); and numerous hospitals (1989–2000). Most recently he was President and CEO of the Southeastern Region of the Adventist Health System. He served as a Board Member and was Chairman of the Board of several of the hospitals. He is currently the President and CEO of The Center for Internet Security. Mr. Kreitner earned an undergraduate degree from the U.S. Naval Academy and graduate degrees from Webb Institute and American University.

Measuring the Value of Security Guides

by Trent Pitsenbarger

Why should I implement these security recommendations? What benefits do they provide? How much will they improve the security of my systems? These are the pervasive questions that we have been asked since we published our first security guide in 1997.

Historically, one of the primary missions of the NSA's Systems and Network Attack Center (SNAC) has entailed the provision of security consultancy services to the Department of Defense (DoD) and U.S. Government Agencies. These services have run the gamut from architectural guidance provided at the onset of network design to field evaluations of fully operational networks.

In the mid 1990s, demand for these services increased dramatically in response to the growing dependency of our customers on information technology (IT). Realizing that customer demand was beginning to outstrip our capacity, the SNAC began development of a series of security configuration documents that system administrators could use to help secure their networks. The goal was to offer the benefit of our knowledge and experience via the guides with the primary audience being those customers with which we could not directly interface. In 1997 the SNAC delivered its initial set of guides, covering Windows NT, Microsoft Exchange, and Lotus Notes.

From these rather humble beginnings the suite of configuration guides has grown dramatically. Presently 34 guides are available on the NSA Web site, covering a wide range of topics. The Web site is in its 17th month of operation and is currently enjoying over 1,000 unique visitors per day with over 2 million total downloads. The guides are used by a plethora of customers, are endorsed by the vendors whose products they cover, have formed the basis of commercially available tools used to assess and improve the security posture of networks, and have been endorsed by a variety of private sector security forums and key industry personnel. Most recently, these guides formed the basis for the development of the Windows 2000 Professional Consensus Baseline Security Settings.

Intuitively, these guides have been a remarkable success and while these are all strong indicators that the guides have been beneficial, is there a more quantifiable means of determining the value of these guides? The SNAC has postulated several methods of measuring value. One of the simplest, and most meaningful entails "before and after" vulnerability scans. In other words, what reduction in vulnerabilities is reported by vulnerability scans as a result of the application of the security guidelines?

In order to develop such hard and fast numbers, the SNAC utilized a popular commercial vulnerability scanner. This scanner monitors a computer under evaluation and reports on over 2000 known vulnerabilities, which it categorizes as being of high, medium, or low concern. The scanner reports on internal configuration settings, file and registry permissions, policy issues, and application level vulnerabilities. For our testing, the vulnerability scanner was run against an out-of-the-box configuration of Windows 2000 Professional and was then re-run after implementing the Windows 2000 Baseline Security Settings. As recommended in the guidelines, implementation of the settings included the installation of Windows 2000 Service Pack 3 and the cumulative patches for Internet Explorer and Windows Media Player. The implementation of these patches is critical. While the overall network architecture and configuration of a computer can, in some cases, mitigate problems addressed by security patches, there are many instances where the only practical countermeasure is to install the patch.

As a result of implementing the Windows 2000 Baseline Security settings and applicable security patches, the number of vulnerabilities in the "high" category dropped 95.5 percent while the overall number of vulnerabilities dropped 90.7 percent! Figure 1 illustrates the complete set of results from these tests.

In a related effort, the MITRE Corporation performed their own independent analysis of the value of the guides. The goal of this analysis was to identify the number of common vulnerabilities and exposures (CVE) issues present in various configurations of Windows 2000 Professional (see *Enterprise Security Enabled by CVE®* on page 12 for more information). The end result was that with Windows 2000 Service Pack 2 installed, post SP2 hot fixes installed,

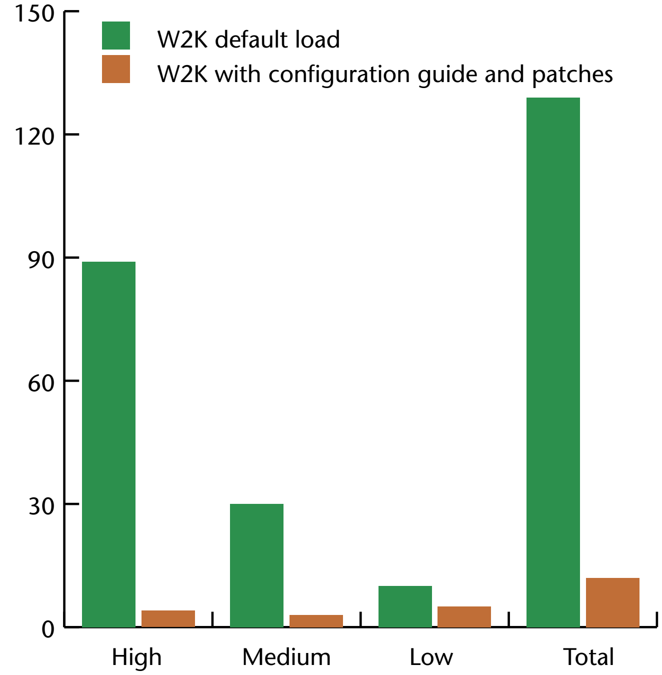


Figure 1. Windows 2000 vulnerability scanner results

and the consensus baseline settings applied, 83 percent of the CVE vulnerabilities were eliminated.

In both of the above studies, the figures were derived from analysis of systems within laboratory environments where operational considerations were not a limiting factor for implementing the security guides. However, it is important to note that similar results have been demonstrated based on the configuration and analysis of operational systems. A case study documenting these results is available from the Center for Internet Security's Web page http://www.cisecurity.org.

So what about the residual vulnerabilities not covered by patches and the Consensus Baseline settings? Several of these residual vulnerabilities are related to optional configuration settings that can be applied in high-risk environments when operationally feasible. However, most of the residual vulnerabilities are related to application level settings not covered by the operating system configuration guide. Implementing other configuration guides, such as the various SNAC application guides, would have reduced the vulnerability space even more.

To demonstrate this, similar tests were performed using Microsoft's Internet Information Server (IIS) software and the corresponding SNAC IIS guide. The vulnerability scanner that we utilized tests for a variety of configuration issues as well as checking the patch status of the IIS installation. Our testing showed that 50 percent of the vulnerabilities identified by the scanner where corrected by the application of the configuration settings alone, with all of the vulnerabilities addressed when both the guide and security patches were applied. These numbers reflect the nature of IIS security patches—they tend to be related to port 80 based buffer overflows against which IIS configuration settings are generally ineffective.

These numbers are impressive but we do not mean to imply that this is a "magic bullet" solution to network security. Proper configuration of the operating system and applications along with timely installation of security patches are just two elements of a sound and comprehensive security policy, but if followed universally would significantly raise the security posture of our networks. ■

References
1. The Windows 2000 Professional Consensus Baseline Security Settings can be found at http://www.cisecurity.org.
2. All the SNAC guides can be found at http://www.nsa.gov/snac/index.html.

About the Author

Trent Pitsenbarger

Trent Pitsenbarger has worked at the NSA for 18 years. For the last six years, he has worked as a technical leader in NSA's SNAC. In this role, he provides computer security consulting services to a wide variety of civilian and military organizations. He has a M.S. degree in Computer Science from James Madison University. He has authored numerous security configuration guides which have been published to the NSA's Internet Web site.

Enterprise Security Enabled by CVE®

by Robert Martin

In the world of hackers versus computer programmers, there are no small mistakes. Last year, a computer hacker took advantage of a coding mistake and broke into a hospital's computer system and downloaded thousands of medical records. The hacker's activities went unnoticed until the hacker went public, and even then, the hospital initially denied his claims. The next day, the hospital confirmed the intrusion. [1]

Mistakes in software code—anything from a typo, a math error, incomplete logic, poor configuration, or incorrect use of a function or command, to an oversight in the requirements guiding the design and coding—can result in security complications. When they do, the mistakes are referred to as vulnerabilities, or exposures. An entire industry of information security products and services now exist to help you protect your networks and systems from being exploited by the hackers and crackers who would use them to gain unauthorized access.

Vulnerability—A mistake in software code that can be directly used to gain access to a system or network.

Exposure—A mistake in software code that allows access to information or capabilities that can be used as a stepping-stone into a system or network.

MITRE's Information Security Group has played a significant role in this field through the creation of "CVE," or common vulnerabilities and exposures, a list or dictionary that provides a single, common name for a single security vulnerability or exposure. CVE's common names enable the security tools and services you use to protect your systems to communicate with each other in a way that did not exist prior to the creation of CVE. It also provides a way to compare which tools provide what coverage.

Protecting your network and systems

A vulnerability or exposure might exist in any single piece of software or hardware, or be created when one or more of these items are used together. A variety of tools exist to help you locate and fix such occurrences, including vulnerability databases, vulnerability scanners, intrusion detection systems (IDSs), and similar Internet-based services.

To keep their products up-to-date, tool and service providers have to continuously gather new vulnerability information. This data is researched by the organization itself, or is obtained from external sources—such as security newsletters, notification services, and public information Web sites that are made available to the public by commercial organizations, the Government, and other sources (see Table 1 on page 13).

The problem

While many sources exist for finding out about vulnerabilities, historically, each source or company has used its own approach for quantifying, naming, describing, and sharing the information about the vulnerabilities it found. This directly affects your networks and systems when tools and products from different companies are used together and each product refers to the same vulnerability by a different name (see Table 2 on page 13), resulting in confusion at the least, and incomplete coverage at the worst. Also, any vulnerabilities or exposures found within the systems then need to be fixed. Unless your software vendors use the same vulnerability descriptions and names as the sources in Table 1, it may be difficult to find the appropriate patch or fix.

The solution

In 1999, MITRE created CVE to act as a bridge between the different tools and services. Today, CVE is an international, community effort that has grown from the original 321 official CVE entries (also called "names") to more than 2,223 entries. In addition, CVE includes 2,900 CVE candidates, or CANs, which are those vulnerabilities or exposures under consideration for acceptance into CVE.

This means that there are currently 5,123 unique issues with publicly known names available on MITRE's CVE Web site—and the list is always growing. Approximately 100 new candidates are added each month based upon newly discovered issues.

Table 1. Vulnerability information sources

Site/Service Name	Type	Organization
arachNIDS	free IDS database	Max Vision Network Security/Whitehats
Bugtraq	E-mail list	Bugtraq
Bugtraq mailing list Database	mailing list database	SecurityFocus.com
Casandra	alerts	CERIAS/Purdue University
CERIAS Vulnerability Database	database	CERIAS/Purdue University
CERT Advisories	advisory	CERT Coordination Center
CyberNotes	monthly newsletter	NIPC
Fyodor's Playhouse	hacker Web site	Insecure.Org
IBM ERS	advisory	IBM
ICAT Metabase	free Web site	NIST
Microsoft Product Security Notification Service	advisory	Microsoft Corporation
Online Vulnerability Database	database	Ernst & Young's esecurityOnline.com
PacketStorm	hacker Web site	Securify, Inc.
Razor	advisory	Bindview Corporation
S.A.F.E.R.	monthly newsletter	The Relay Group
SANS NewsBites	email list	SANS Institute
Security Alert Consensus	email list	Network Computing and SANS
SecurityFocus Newsletter	newsletter summary of Bugtraq E-mails	SecurityFocus.com
SGI Security Advisory	advisory	Silicon Graphics, Inc.
Sun-alert	alert	Sun Microsystems, Inc.
SWAT Alerts	alerts	Symantec
SWAT Database	database	Symantec
Vigil@nce AQL	database	Alliance Qualité Logiciel
X-Force Alert	advisory	Internet Security Systems
X-Force Database	free Web site	Internet Security Systems

Table 2: The vulnerability tower of Babel

Organization	Name used to refer to the same vulnerability
AXENT	phf CGI allows remote command execution
BindView	#107 – cgi-phf
Bugtraq	PHF Attacks – Fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CA-96.06.cgi_example_code
Cisco Systems	HTTP - cgi-phf
CyberSafe	Network: HTTP 'phf' Attack
DARPA	0x00000025 = HTTP PHF attack
IBM ERS	ERS-SVA-E01-1996:002.1
ISS	http - cgi-phf
Symantec	#180 HTTP Server CGI example code compromises http server
Security Focus	#629 - phf Remote Command Execution Vulnerability

CVE Entry—The CVE entry (or "name") is an encoding of the year the name was assigned and a unique number N for the Nth name assigned that year. For example: CVE-1999-0067.

How CVE works

CVE is publicly available and free to use. Through open and collaborative discussions, members of the CVE Editorial Board decide which vulnerabilities or exposures will be included in CVE, and then determine the common name, description, and references for each entry. Editorial Board members come from numerous information security-related organizations around the world, such as software and tool vendors, research institutions, Government agencies, and academia.

Products and services that incorporate CVE names are referred to as "CVE-compatible," meaning that they can cross-link with other products and services that use CVE names. To be CVE-compatible, products or services—

1. Must be CVE searchable so that a user can search using a CVE name to find related information

2. Any output must be presented in a manner that includes the related CVE name(s) or CAN(s)

3. The standard documentation for the products or services must include a description of CVE and details of how customers can use its CVE-related functionality. CVE compatibility facilitates the exchange of vulnerability information and makes it easier to share data in a vendor-independent manner.

MITRE maintains the CVE List and Web site (http://cve.mitre.org), manages the compatibility process, moderates editorial board discussions, and provides guidance to ensure that CVE remains objective and continues to serve the public interest.

Enterprise security enabled by CVE

In a CVE-enabled process, CVE-compatible products and services act as a bridge. For example, in Figure 1 (see page 25), an organization is able to detect an ongoing attack with its CVE-compatible IDS system (A). In a CVE-compatible IDS, specific vulnerabilities that are susceptible to the detected attack are provided as part of the attack report. This information can then be compared against the latest vulnerability scan by your CVE-compatible scanner (B) to determine whether your enterprise has one of the vulnerabilities or exposures that can be exploited by the attack. If it does, you can then access a CVE-compatible fix database from your product vendor, or you can use the services of a vulnerability Web site, which lets you identify (C) the location of the fix for a CVE entry (D), if one exists.

Using CVE-compatible products also allows you to improve how your organization responds to security advisories. If the advisory is CVE-compatible, you can see if your scanners check for this threat and then determine whether your IDS has the appropriate attack signatures. If you build

...continued on page 25

Operationalizing Critical Infrastructure Protection

A Combatant Command Perspective

by LtCol Ted Ruane, USMC

It doesn't matter whether it's al Qaeda or a nation-state or the teenage kid up the street, who does the damage to you is far less important than the fact that damage can be done. You've got to focus on your vulnerability and not wait for the FBI to tell you that al Qaeda has you in its sights. [1]

Consider the following series of apparently random events—a backhoe accidentally strikes an underground fiber optics cable servicing a Combatant Command Headquarters. A tropical hurricane sweeps over an important military airfield. A dockworker strike shuts down sea ports along the West Coast. An isolated criminal act disrupts the Alaskan Pipeline. To many people, these recent infrastructure hazards may initially appear to have little impact on Department of Defense (DoD) warfighting missions and capabilities during a national crisis or contingency. However, these seemingly random events can be just as devastating on current and future DoD missions as a well-planned terrorist attack.

Within DoD, Critical Infrastructure Protection (CIP) is designed to ensure the availability of mission-critical assets through deterrence, detection, defense, and defeat of threats and hazards to commercial and Military infrastructures. The DoD defines "critical infrastructure" as "infrastructures essential to plan, mobilize, deploy, sustain, and transition to post-conflict operations." In simple terms, therefore, the primary purpose of the DoD CIP Program is mission assurance. This article discusses recent United States Pacific Command (USPACOM) efforts to institutionalize the DoD CIP Program with formal processes and tools to make critical infrastructure protection a reality. Most importantly, it will highlight how CIP is now being operationalized in support of deliberate and crisis action planning and mission execution in the Pacific Theater.

Background

Although the DoD CIP Program is relatively new, the concept of attacking and protecting infrastructure assets critical to a nation's warfighting capabilities is as timeless as war itself. History is full of examples of smaller forces defeating larger forces when the smaller force correctly identified and attacked a critical vulnerability in the larger force's warfighting capability. Today, most people recognize that the Achilles' Heel of the United States Military is its heavy dependence on a limited number of vulnerable military and commercial infrastructures. What infrastructures are most important to DoD? The DoD currently identifies ten different critical infrastructure sectors, including—

- Personnel
- Financial Services
- Health Affairs
- Intelligence, Surveillance and Reconnaissance (ISR)
- Space
- Logistics
- Transportation
- Public Works
- Command, Control, and Communications (C3)
- Defense Information Infrastructure (DII)
- Defense Industrial Base (Proposed)

Our Nation has experienced a rapid technology expansion during the past two decades, resulting in an explosion in physical and cyber-dependent infrastructures. Unfortunately, redundant backup capabilities did not keep pace with this trend. For example, today a typical bridge in the United States transports more than just vehicles and trains across a river; most bridges also transport fiber optic cables, water pipes, power lines, natural gas lines, and other critical assets. If the bridge is destroyed, multiple infrastructures are impacted.

Computer networks have revolutionized business processes throughout society with breathtaking improvements in data fusion. However, this heavy reliance on technology also has a serious downside—a web of dependencies has now been created making it infinitely more difficult to assess just how vulnerable the Military, public, and private infrastructures have become. The rise of the Internet presents unique and disturbing critical infrastructure protection challenges too. A typical Internet search today of important DoD infrastructures reveals detailed information about commercial power grid designs, military telecommunications site capabilities, and other data that a potential enemy of the United States can use to their advantage. A sobering example of this is the infrastructure data found by U.S. investigators on an al Qaeda laptop found in Afghanistan. The computers logs showed that al Qaeda operators spent considerable time on sites that offer software and programming instructions for the digital switches that operate power, water, transportation, and communications grids. [2] The DoD CIP Program is designed to identify these mission-critical physical/cyber assets, assess their vulnerabilities and dependencies, and implement appropriate protections plans.

The DoD CIP Program has its origins in the President's Commission on Critical Infrastructure Protection (PCCIP). Events during the past two years, most notably the terrorist attacks on September 11th, 2001 and the Y2K scare, have made many of the PCCIP findings listed in their 1997 document entitled, *Critical Foundations, Protecting America's Infrastructures* [3] a stark reality today. According to this report, the United States is vulnerable to devastating infrastructure attacks and most organizations simply do not recognize the seriousness of this problem. The report predicted that the United States has only a three to five year window, from 1997, to prepare before our enemies will exploit our infrastructure vulnerabilities. [4]

Given the seriousness of the report's findings, President Clinton issued Presidential Decision Directive 63 in May 1998, considered by many to be the birth of the National CIP Program. The DoD published its supporting CIP Plan and immediately established a CIP Directorate within the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence/Deputy Assistant Secretary of Defense for Security and Information Operations (OASD (C3I)/DASD S&IO/CIP). This DoD CIP effort, which began in August of 1998, was initially overshadowed by Y2K's shared sense of urgency, its known attack window, and the recognition of a clear end to the effort. In contrast, the CIP effort struggled to establish a shared recognition of a threat, an unknown attack window, the complexity of addressing ten distinct infrastructure sectors, and a fear that once started, the CIP effort would present a never-ending resource drain. With the success of the operationalized Y2K effort, OASD (C3I)/DASD S&IO began leveraging the lessons learned from that experience and implemented a Combatant Command CIP outreach initiative to expand the DoD CIP program.

USPACOM was one of several Combatant Commands who closely monitored both the National and DoD CIP Program efforts from 1998–2000, and consequently recognized the importance of CIP to both mission assurance and warfighting capabilities. In early 2001, senior leaders within USPACOM made an innovative decision—they created a CIP Branch "out-of-hide" within the Antiterrorism/Force Protection (AT/FP) Division where CIP could quickly become "operationalized" by leveraging many of the operational gains made by the AT/FP community. Since that time, the USPACOM AT/FP Division was renamed as the AT/CIP Division (J34) to better describe its dual role in the "people-protection" and "critical-asset protection" business.

CIP Appendix 16 requirements and training

On 24 August 2001, the Director of the Joint Staff requested USPACOM serve as the "lead supported Combatant Command" for development of the first CIP Appendix (known now as the CIP Appendix 16 Project) to an Operational Plan (OPLAN). USPACOM accepted the challenge despite lack of resources, manpower, and existing CIP processes and templates for building a first-ever theater CIP Plan. However, as a direct result of the terrorist attack of September 11th, 2001, OASD C3I received Defense Emergency Response Funding (DERF) in December 2001. A significant portion of this DERF was forwarded to USPACOM in late January 2002 for development of a first-ever Combatant Command CIP deliberate plan. The Joint Staff and USPACOM agreed to a deadline of 30 April 2003 for completion of the CIP Appendix 16 Plan. Other Combatant Commands were directed to closely monitor USPACOM's CIP efforts and use USPACOM's CIP Appendix 16 plan as a template for development of their own supporting CIP Plans.

As the lead Combatant Command for this project, Joint Staff planning guidance to USPACOM included the following specified and implied tasks that must be included the CIP Appendix 16 Plan—

- Develop a methodology for identifying mission-critical infrastructure assets
- Use existing DoD assessment organizations to conduct CIP Assessments. These assessments must identify: physical and cyber vulnerabilities, asset dependencies (both intra- and inter-sector), and single points of failure
- Develop an Indications and Warning process to monitor the assurance of mission-critical assets
- Develop plans for remediation of vulnerabilities
- Develop Infrastructure Protection Plans, including—
  - Mitigation Plans against the potential loss of a critical asset
  - Response Plans to defeat infrastructure threats
  - Reconstitution Plans to restore a critical asset's capability after loss

USPACOM hosted a DoD CIP Conference in January 2002 where key elements of the CIP Appendix 16 Project were first introduced to CIP representatives from OSD, the Joint Staff, the other Combatant Commands, Service Headquarters, and members of the USPACOM CIP Working Group. USPACOM also conducted four CIP Training Workshops designed to educate CIP Action Officers about CIP processes and CIP Appendix 16 requirements. These workshops were conducted at Camp Smith, Hawaii (April 02), HQ US Forces Korea (June 02), HQ US Forces Japan (June 02), and HQ Alaskan Command (July 02). USPACOM will host a second annual DoD CIP Conference and Combatant Command CIP Workshop in Honolulu from 27–31 January 2003. This event is already drawing significant interest throughout the DoD, and will be an opportunity for USPACOM to showcase early results of the CIP Appendix 16 project to the DoD CIP community.

The best possible mission assurance: the CIP event lifecycle

The CIP Appendix 16 Project is best described as an enterprise-wide assurance plan for critical infrastructure assets supporting USPACOM mission success. This description applies to all phases of any required OPLAN, CONPLAN, or crisis action plan. This infrastructure assurance plan follows the six-step DoD CIP Life-Cycle shown in Figure 1 (see page 16).

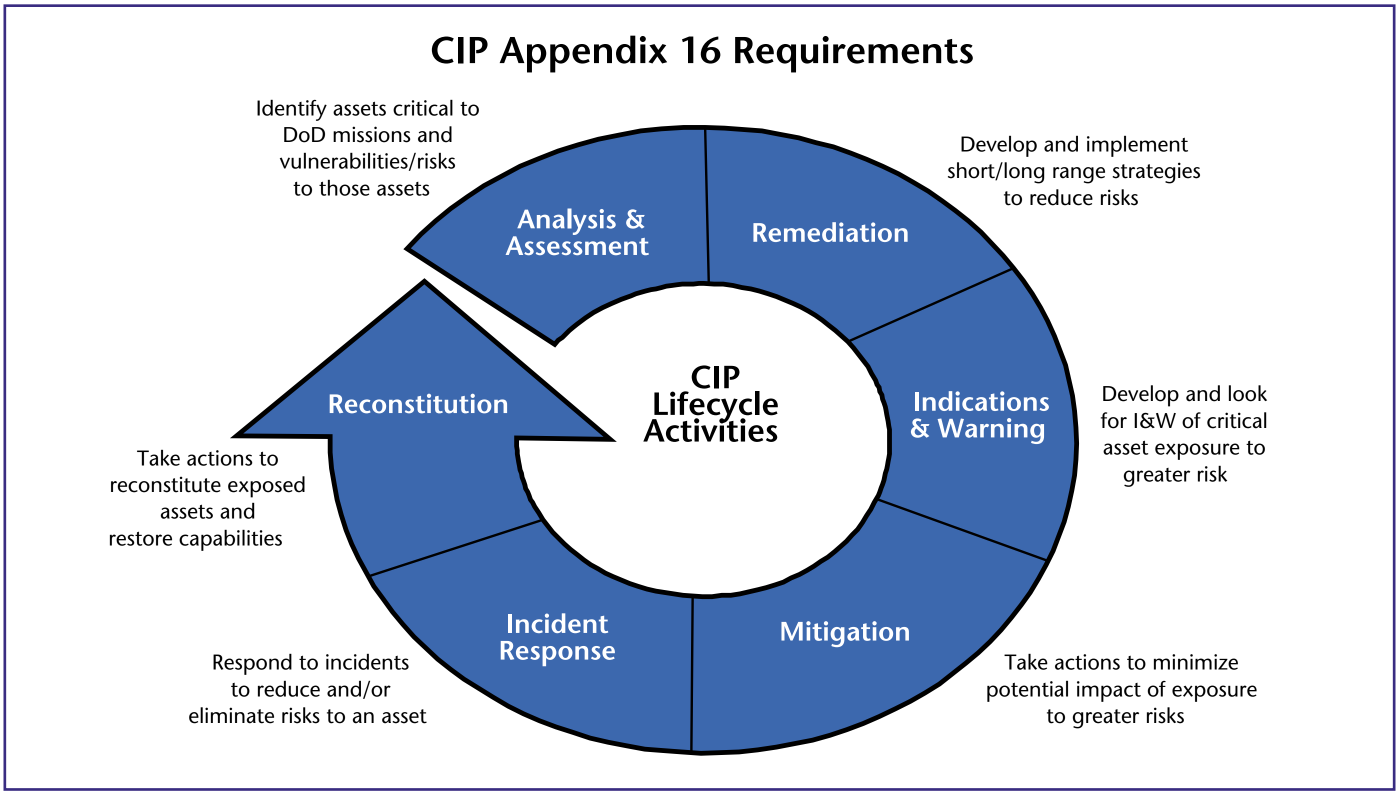

CIP Appendix 16 Requirements
Identify assets critical to DoD missions and vulnerabilities/risks to those assets
Analysis & Assessment
Remediation
Develop and implement short/long range strategies to reduce risks
Indications & Warning
Develop and look for I&W of critical asset exposure to greater risk
Mitigation
Take actions to minimize potential impact of exposure to greater risks
Incident Response
Respond to incidents to reduce and/or eliminate risks to an asset
Reconstitution
Take actions to reconstitute exposed assets and restore capabilities
CIP Lifecycle Activities

Figure 1. DoD CIP lifecycle activities

A brief description of the CIP event life cycle steps, and required sub-plans makes it clear how the individual activities build on one another to create a context for a comprehensive infrastructure assurance solution.

1. **Analysis and assessment**—This activity is the foundation, and most important element, of the six CIP lifecycle events. It is performed by functional experts at HQ USPACOM using a formal methodology for determining those assets absolutely critical to mission success (based on combatant commander mission-required capabilities and service component/commercial-provided assets) and whether these assets are vulnerable, based on CIP Assessments. Because this activity is so critical to the entire mission assurance process, it will be discussed in more detail later in this article.
2. **Remediation actions**—These actions are designed to fix known cyber and physical vulnerabilities identified during CIP assessments performed by the Defense Threat Reduction Agency (DTRA) the Joint Program Office-Special Technology Countermeasures (JPO–STC), other agency assessments, or self-assessments. Remediation may be no-cost, low-cost, or high-cost actions based on the nature of each vulnerability. Remediation may also require procedural or process changes.
3. **Indications and warnings**—These actions are designed to monitor the daily mission assurance capabilities of critical infrastructure assets supporting USPACOM missions. Indications are the preparatory actions indicating an infrastructure event is likely to occur based on tactical level (asset owner), operational level (sector), and/or theater strategic-level intelligence, law-enforcement information, and private sector input. Warning is the process of notifying asset owners of a possible threat or hazard.
4. **Mitigation actions**—These are actions taken before or during an infrastructure event by asset owners, installations, sectors, and others designed to minimize the operational impact of the loss of a critical asset.
5. **Response plans**—These are plans designed to eliminate the cause or source of an infrastructure event. USPACOM has established geographic security coordinators called Joint Rear Area Coordinators (JRACs) in Japan, Alaska, Guam, and Hawaii to provide Quick Response Forces (QRFs) for tactical-level antiterrorism and critical infrastructure protection requirements.
6. **Reconstitution plans**—The final lifecycle event involves actions required to rebuild or restore a critical asset capability after it has been damaged or destroyed. Admittedly, this CIP lifecycle activity is probably the most challenging and least developed process.

Determining what is mission-critical: the mission area analysis process

As mentioned earlier, the most important element of the six CIP life cycle events is Analysis and Assessment—determining what assets are important and identifying their vulnerabilities and dependencies. To conduct the initial analysis, USPACOM uses a staff process developed by JPO–STC known as Mission Area Analysis (MAA). The MAA is a systematic approach that ultimately links combatant command missions to infrastructure assets critical to a given OPLAN, CONPLAN, or Crisis Action Plan. This top-down, mission-focused approach begins by identifying and prioritizing Mission Essential Requirements (MERs) based on a specified plan. MERs are specific combatant command or joint task force capabilities essential for execution of a warfighting plan. MERs are linked to forces, functions, and tasks, and assist CIP assessment teams in determining which assets are truly mission-critical.

Due to time-sensitive and assessment scheduling challenges, the USPACOM CIP Working Group modified this MAA process. CIP assessment sites and installations are being selected prior to conducting the MAA process, rather than allowing the MAA process to determine assessment site priorities. Put another way, USPACOM is pursuing this MAA process from the inside out rather than from top to bottom.

The USPACOM process begins with the identified MERs. These MERs are linked to forces, based on the pre-selected assessment sites, then linked to the necessary functions and tasks supporting the forces. The end result of this effort is a mission area analysis that greatly assists in focusing scheduled assessment efforts. However, if resources and time permit, a complete JPO–STC MAA process, as described above, does result in a more mature process that can be duplicated by USPACOM and other Combatant Commands for other OPLANs and CONPLANs. The importance of this MAA process cannot be overstated—identify the wrong mission-critical asset, and a command stands a good chance of wasting time, resources, and manpower on a CIP assessment while a true (but unknown) mission-critical asset remains vulnerable to threats and hazards. Figure 2 shows a graphic example of this USPACOM MAA process.

Determining vulnerabilities and dependencies: CIP assessments

Soon after the USPACOM CIP Working Group completes its MAA, this data is provided to the CIP assessment team. The team uses the MAA to scope and focus the assessment efforts on those truly mission-critical assets at a designated installation or site. During the past year, USPACOM has relied on two different, but complementary, DoD organizations for CIP assessments. The Defense Threat Reduction Agency (DTRA) conducts Balanced Survivability Assessments (BSAs), normally a two-week mission-focused assessment at a Military installation or designated site. DTRA has completed four of these assessments in the USPACOM AOR, and will complete an additional six during the remainder of FY03. The Joint Program Office-Special Technology Countermeasures (JPO–STC) conducts Mission Assurance Assessments. These assessments are unique, since they focus on both commercial and military asset vulnerabilities and dependencies using an area assessment approach. JPO–STC recently completed a very successful island-wide Oahu assessment of mission-critical assets in October 2002. Plans are currently being made to conduct similar area assessments on Guam, Okinawa, and mainland Japan during FY03. Both organizations provide assessment reports to the USPACOM CIP Branch. The USPACOM CIP Working Group enters the data from these reports into the CIP Database, setting the stage for development of remediation and protection plans for mission-critical assets.

Turning data into useful information: the CIP database

The USPACOM CIP Database plays an integral role in both the overall CIP Program and continuing development of CIP deliberate and crisis action plans. This database is more than just a simple means of producing a quick list of critical infrastructure assets. It is an operational tool used for different risk-management purposes by different echelons within USPACOM command structure. For example, Service components, as asset owners, are more likely to use the CIP database for making tactical and operational asset protection decisions (i.e., mitigation, response, and reconstitution planning). However, the combatant command staff is likely to use the same database for theater-strategic purposes, namely, mission assurance by determining the "cascading effect" of an asset loss on other infrastructure assets.

The USPACOM CIP database began in late 2000 as a USPACOM initiative, but has recently become a joint partnership between USPACOM and JPO–STC based on their extensive technical expertise. USPACOM is developing the operational requirements and the required certification, accreditation, and fielding plans. JPO–STC is providing the technical development, training and maintenance support. Some of the most prominent features of this database include: an integrated DoD mission assurance tool, valuable CIP information sharing for crisis decision support, visualization of asset relationships, and the ability to leverage other protection initiatives such as antiterrorism, force protection, information operations and the fusion of asymmetric threats.

To ensure uniformity of information across ten infrastructure sectors and four Service components, asset data is sorted in the database following the six-step DoD CIP Event Life-Cycle. The goal is to create efficiencies in data presentation so the completed CIP Appendix 16 document can repeatedly refer to the CIP database for specific information about mission-critical assets. This data optimization approach eliminates the need to create documents containing thousands of data points spanning hundreds of pages.

Protecting critical infrastructures: the resource challenge

There are no magic formulas or templates for protecting critical infrastructures. Once the mission analysis, assessment, and identification of mission-critical asset processes are completed, USPACOM relies on commercial and Military asset owners to make important risk-management decisions to remediate vulnerabilities and develop protection plans to minimize loss. While many remediation options involve process or procedural changes, most vulnerabilities require resources. The DoD CIP Program competes with other important DoD programs for scarce resources, and there is a serious backlog of unfunded Antiterrorism/Force Protection (AT/FP), Information Assurance (IA), and other mission assurance resource requirements. The USPACOM CIP Branch serves as an advocate for con-

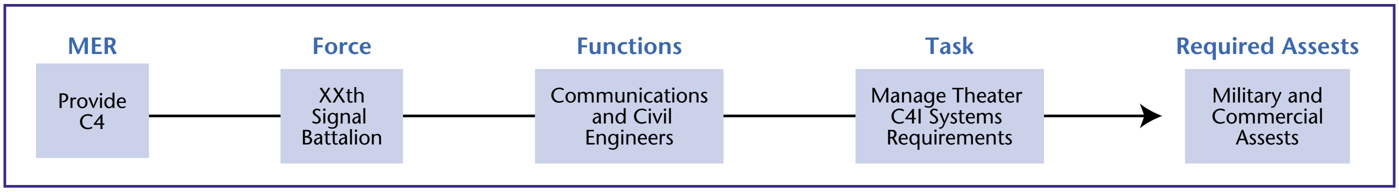

MER
Provide C4
Force
XXth Signal Battalion
Functions
Communications and Civil Engineers
Task
Manage Theater C4I Systems Requirements
Required Assests
Military and Commercial Assests

Figure 2. Mission Area Analysis (MAA) Process

tinued program resource support to ensure senior leadership understands the need for CIP, especially at a time when asymmetric threats to US interests are on the rise.

The endstate: an operationalized CIP program

What do USPACOM and the rest of the DoD CIP community gain on 30 April 2003 with the delivery of CIP Appendix 16? Following is a short list of CIP Appendix 16 deliverables, many of which are "firsts" within the DoD—

- Deliberate CIP Plan (Appendix 16) to be used as a template for all Combatant Command OPLANs, CONPLANs, and Crisis Action Plans
- USPACOM CIP Instruction prescribing CIP Roles and Responsibilities among the HQ Directorates, Service Components, and Sub-Unified Commands
- USPACOM CIP Operations Order "operationalizing" CIP throughout the USPACOM AOR and prescribing how CIP planning and execution is conducted
- Ten individually-tailored theater infrastructure sector assurance plans characterizing mission-critical systems, functions, and tasks
- USPACOM CIP funding plans articulating Combatant Command CIP resource requirements based on an increasingly mature and dynamic CIP Program
- Realistic CIP training events scripted into all major USPACOM exercises as a means of educating leaders and headquarters staffs in mission assurance through CIP
- A CIP Database identifying relationships between mission-critical assets, their associated vulnerabilities, and protection requirements
- Formalized CIP processes created and implemented, such as Mission Area Analysis and an institutionalized CIP assessment methodology
- Close integration of CIP activities with other operational USPACOM activities, such as the Current Operations, Future Operations, and Counter-Terrorism Divisions

Conclusion

> *The al Qaeda have spent more time mapping our (infrastructure) vulnerabilities in cyberspace than we previously thought. An attack is a question of when, not if. [5]*

This article began with a series of infrastructure threats, dependencies, and vulnerabilities. There are hundreds more threats and hazards to DoD missions now and on the horizon. We simply can't protect everything, everywhere. CIP is a program designed to help DoD efficiently determine the extent of our mission-critical infrastructure vulnerabilities and dependencies, and make informed risk-management decisions. Operationalizing CIP is a key element in ensuring DoD can continue to accomplish all assigned missions, especially in an age of increasing asymmetric threats and unconventional warfare. Due to the complexity of CIP as a program, it must not be stove-piped into a particular functional area such as logistics or communications—it cuts across numerous functional boundaries and traditional organizational charts. It must be operationalized to ensure there are no gaps or seams in our infrastructure protection efforts. USPACOM is working hard to institutionalize and operationalize critical infrastructure protection throughout the Pacific Theater through continuous planning, horizontal and vertical headquarters staff coordination, coordination with Host Nation, state/local, and commercial organizations, and integration of infrastructure protection activities necessary to assure the execution of National Military Strategy. With a formal program implemented and integrated within the master DoD CIP Plan, USPACOM is achieving its vision for operationalizing CIP within the Pacific Theater. ■

References

1. Richard A. Clarke, Special Advisor to the President for Cyberspace Security.
2. Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say; Barton Gellman, Washington Post, Thursday, June 27, 2002; Page A01.
3. DoD Critical Infrastructure Protection Plan, dtd 18 November, 1999, pg 5–6. The PCCIP submitted its report, Critical Foundations, in October 1997. An electronic version is available at http://www.pccip.gov.
4. DoD Critical Infrastructure Protection Plan, November 18, 1999, pg. 5–6.
5. Roger Cressey, Chief of Staff of the President's Critical Infrastructure Protection Board.

About the Author

LtCol Ted Ruane, USMC,

Lieutenant Colonel Ted Ruane, USMC, is the Critical Infrastructure Protection Branch Chief (J341) to the Deputy for Antiterrorism and Critical Infrastructure Protection (J34 AT/CIP) at the United States Pacific Command (USPACOM) Headquarters. He graduated from Iowa State University with a degree in Political Science and received a M.B.A. from Averitt University. He is a 1999 graduate of the USMC Command and Staff College, Quantico, VA, where he received a M.S. in Military Studies. Since 1999 he has worked in both the Force Protection and Infrastructure Protection programs for USPACOM. Following his assignment at USPACOM LtCol Ruane will take command of the Marine Expeditionary Unit (MEU) Service Support Group 15 of the 15th MEU at Camp Pendleton, CA. Lieutenant Colonel Ted Ruane can be reached at taruane0@hq.pacom.mil.

Contributing Authors

Jim Newport

Jim Newport currently supports the Deputy for Antiterrorism and CIP (AT/CIP) at the USPACOM. He holds a B.A. degree in Human Relations from Milligan College, TN, and a master's degree in Military Arts and Science from USA Command and General Staff College. He may be reached at jhnewpor@hq.pacom.mil.

Robert Lietzke

Bob Lietzke currently supports USPACOM Mission Assurance initiatives for CIP and Network Operations (NetOps). He holds a B.S. degree from the U.S. Air Force Academy and an M.S. from Chapman University. He may be reached at lietzke_robert@bah.com.

USPACOM CIP Conference

Hilton Hawaiian Village Hotel · Waikiki, Hawaii
January 27-31, 2003

USPACOM CIP Conference
January 27-29, 2003

Combatant Command CIP Workshop
January 30-31, 2003

Hosted by: USPACOM J34
Commercial: 808/477-0656
DSN: 477-0656

For registration and
additional information:
http://eNSTG.com/SignupNow

USSOUTHCOM's 2002 Information Assurance (IA) Conference

by Robert Munger

U.S. Southern Command (USSOUTHCOM) recently hosted their 2002 Information Assurance (IA) Conference in Fort Lauderdale, Forida on August 2, 2002. COL Benjamin F. Fletcher, J6 Director, kicked off the 2nd annual conference themed "Securing the Future." The objectives were to present current, pertinent IA issues, foster teamwork across the theater, and provide technical updates and points of contact.

Approximately 130 personnel, representing USSOUTHCOM, Joint Staff, White House Cyber Security Office, JTF–CNO, DISA, NSA, USSPACECOM, USPACOM, USEUCOM, and IA experts from all Services attended. Representatives from several IA related disciplines, such as the Defensive Information Operations, Information Assurance Professionals, Information System Security Managers and Officers, System Administrators, Network Operations, and Information Dissemination Managers also attended. This composition of professionals ensured expression of various viewpoints and enabled personnel with hands-on working experience to interact directly with policy makers. Additionally, the four-day conference featured 12 briefers sharing information concerning network attacks and security, the evolution of incident reporting and response, vulnerability patching processes, public key enabling technology and future network threats.

The Honorable Carol A. Haave, Deputy Assistant Secretary of Defense for Security and Information Operations, provided the keynote presentation. Ms. Haave characterized the current situation, as it pertains to IA, as a "patchwork protection against a global asymmetric threat." Her intent in the IA program is to "evolve to integrated assurance" defined as "full dimensional protection built on an operational capabilities foundation." The major objective is to build

...continued on page 24

The South Florida Honeynet Project

Yesterday, Today, and Tomorrow

by Richard La Bella

I never expected I would ever turn geek. But it happened. I purchased my first computer during the fall of 1993 to write comedy. At that time, I was a stand up comedian/actor living in New York City. When I wasn't running off to auditions and acting classes, or serving up cappuccinos at Bella Luna, I was spending hours at the computer. And I wasn't writing comedy. Instead, I was a die-hard AOL user with a screaming 9600 Baud modem.

One month later, I was introduced to Jon Lunning who would change my professional life forever. Jon was amazing because he was a UNIX guy who knew a lot about computers, networking, and programming. One day, I asked Jon "Is there something else I can run on my computer other than Windows for Workgroups 3.11"? Jon told me about an Open Source operating system in development called Linux. During the first quarter of 1994, I located my first Red Hat distribution in the computer books section of Barnes and Noble and the rest was history. I was hooked. I put the acting dream on hold, developed some new skills, and acquired a real job as an Internet Desktop Support person for an Internet café in the East Village. I held numerous IT positions from that point on which allowed me to acquire my MCSE in 1997, my CCSA and CCSE, and a CCNA certification.

Nine years later, May 2, 2001, I was laid off from a South Florida dot com nightmare. As a security professional in the South Florida area my priorities shifted from finding work to finding a way to learn and develop my own security skills immediately. I sensed that the longer I would go without work in information security, the harder it would be to keep up. That's when I discovered the Honeynet Project. I read the Honeynet Project was tracking hackers by deploying various operating systems, then analyzing the data captured so it could be documented and shared with the public. It was the coolest thing I had ever heard of. I pulled $8,000 out of my own pocket to purchase some new systems to get started.

The South Florida Honeynet Project yesterday

On September 28, 2001 I set out to build my first honeynet. With the help and support of Lance Spitzner and the Honeynet Project, my $8,000 investment turned into a Non Profit organization called the South Florida Honeynet Project. Members include Jeff Dell, Darren Bounds, Tyler Hudak, John Machado, Rob Wiley, Castor Morales, and Scott Kemp.

On December 5, 2001 the South Florida Honeynet Project co-founded the Honeynet Research Alliance. The Alliance was started by the Honeynet Project to bring together other honeynet organizations under one umbrella for sharing, learning, and growing honeynet research. To learn more about the Honeynet Research Alliance we encourage you to visit http://www.honeynet.org/alliance.

First generation (GenI) data control

From late December 2001 through June 2002 the South Florida Honeynet Project deployed first generation (GenI) honeynets. GenI honeynets use a shell script written by Lance Spitzner to control and capture packets moving in and out of the honeynet. The script is called Alert.sh and can be found at http://www.enteract.com/~1spitz/intrusion.html.

We ran this script on a Linux system configured to run Check Point Firewall-1 NG. We configured the script to copy our daily and monthly data capture logs over secure transmission to a centralized data collection system owned and operated by the Honeynet Project. These logs would then be viewed by other members of the Honeynet Research Alliance.

During the GenI days we learned a lot. I'll never forget our first incident on Superbowl Sunday, February 3, 2002. My daughter was sick that day. Twenty minutes into the excitement of discovering my first honeypot compromise my wife and I had to whisk my daughter off to the hospital to fight a high fever. While at the hospital, away from the compromised system, our GenI data control failed somewhere and the honeypot was involved in IRC (Internet Relay Chat) sessions via Germany and Belgium. The biggest lesson we learned that day was how important data control really was. For example, we could have gotten ourselves in trouble if our system was used to compromise a Government system. We were just lucky. My daughter got better; we fixed our data control issue and documented the attack. You can read "Superbowl Hack" at http://www.sfhn.net/whites/sbowl/sbowl/sbowl.htm.

GenI data control had one major limitation we don't have with GenII data control, which I will touch on in just a moment. The GenI data control script works by blocking any number of connections for any period of time. You set the parameters. For example, if we set the Alert.sh script to block all connections after the tenth outbound connection for ten hours then we protect ourselves from upstream liability issues. It's all about risk. The GenI Alert.sh script protects us from the risk of our system being utilized to attack and compromise other systems connected to the Internet. However, the drawback with GenI data control is our inability to learn anything more from our attacker once they have been blocked. You see, once the attacker has been blocked by the parameters you set in the script the attacker can quickly catch on that the connections are not getting out anymore. This can be learned while the enemy is sniffing the honeynet. The end result is our enemy or black hat leaves the scene of the crime, disallowing us to learn anything more about the black hat's motives, tools, and tactics.

The South Florida Honeynet Project today

Today, the South Florida Honeynet Project is in the process of implementing and documenting a juicer honeynet. Something we call covert honeynets. Covert honeynets are high value honeynets that leverage GenII data control and data capture developed by members of the Honeynet Project. First, I will discuss GenII data control and data capture then discuss what covert honeynets are. What you are about to read is an overview of GenII and how it compares to GenI. This is not a detailed article, nor a HOWTO for building a GenII system. Because GenII systems are pretty new to us, we still have more to learn before it can be properly documented. If you are looking for a more detailed description of GenII and GenI honeynets I will point you to the Honeynet Project's "Know Your Enemy: Honeynets" paper online at http://www.honeynet.org/papers/honeynet/.

Second Generation (GenII) data control

GenII data control uses two layers of data control we didn't have during the GenI days. GenII data control is more flexible, centralized, and less visible on the network. It's flexible because it allows us to integrate the functionality of two separate applications to control the level of risk we choose to assume against the level of our enemy's activities we expect to capture. It's a centralized system because all data control and data capture happens on one system. And it's less visible or hidden than GenI because a GenII system operates at layer two making it harder to detect. A GenII system bridges all ingress and egress traffic. There are no IP addresses bound to the network interfaces of a GenII system like there are on a GenI system.

So then, what makes GenII tick? First, we use an Open Source application called Iptables and Rob McMillan's Iptables firewall script, rc.firewall-genII for data control and data capture. The rc.firewall-genII script sets up all your rules and a logical bridging interface for moving packets between two physically connected network cards in the system. Secondly, we use another Open Source application called Snort and Jed Haile's Snort-Inline code for data control and data capture. Snort-Inline matches the packets payload against a set of intrusion detection signatures and makes a decision on what to do with the packet based on a signature match. When we combine the use of Rob McMillan's Iptables script and Jed Haile's Snort-Inline code with Snort we will gain a more flexible, centralized, stealthier system. In summary, we have more options for data control and data capture which can be built onto one system. Just a quick side note: This is not the only type of GenII system that can be built. Jed Haile the creator of Snort-Inline is also the creator of another GenII system called Hogwash (http://hogwash.sourceforge.net).

Going covert

A new concept in honeynets that we are developing is something we are calling "covert honeynets." Covert honeynets are crafted to look and feel like a real organization connected to the Internet. Covert honeynets have a real Web presence, a database of high value information, simulated covert traffic patterns, a mail server, an SMTP relay, an FTP server, split DNS, and high value information. An analogy for covert honeynets is to think of this type of honeynet as a smarter fishing lure to catch the bigger fish. We are using GenII data control to help us make data control seem transparent to the enemy, and we are deploying a high value honeynet so our enemy will have something to stick around for.

We are documenting covert honeynets and hope to have our paper released to the public in the next two months. You can see us speak live about covert honeynets November 7th and 8th at the Rio Hotel in Las Vegas, Nevada. For invitations visit the Web site at http://www.frallc.com/pdf/c104.pdf. ■

About the Author

Richard La Bella

Richard La Bella is the founder of the South Florida Honeynet Project. He currently works as a Security Engineer for Office Depot, Inc., specializing in deploying and managing firewalls and intrusion detection systems. He holds certifications as an MCSE, CCSA, CCSE, and as a CCNA. He has presented at several national conferences, which include the South Florida ISSA Conference, West Point Military Academy, Black Hat Convention, and will soon join his colleagues from Honeynet Research Alliance for a briefing at the Pentagon on October 22, 2002. The South Florida Honeynet Project team spends their free time documenting and deploying covert honeynets.

Guard Technologies

Connecting the Dots

by Kristina Winkler and Danyetta Fleming

The Department of Defense (DoD) has issued several mandates that are moving our forces toward a more network-centric approach to warfare. DoD goals have evolved over the past few years resulting in the need for an "end-to-end set of information capabilities," as noted in Joint Vision 2020.

The evolution of information technology will increasingly permit us to integrate the traditional forms of information operations with sophisticated all-source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign. The development of a concept labeled the global information grid (GIG) will provide the network-centric environment required to achieve this goal. The grid will be the globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel. It will enhance combat power and contribute to the success of non-combat military operations as well.

This vision has been filtering down to respective organizations to create a "joint picture of the battlespace," however, this requirement leaves a key question unanswered—*how do I connect the dots?* In other words, how does my organization link to other systems or agencies, coalition partners and the industrial base with which I need to share information? Sometimes this answer is simple, however, in most instances, the answer is more complicated. For example, if your requirement is to connect a classified network to the NIPRNET or to a coalition partner network, given current DoD guidance, a "direct connection" of networks or systems of differing classification levels is not permitted. This article focuses on one of the approved and accreditable methods for "connecting the dots"—the use of multi-level security technologies, and more specifically, a high assurance guard (HAG) that has been certified and approved for use. In this article, we discuss the HAG and the certification and accreditation (C&A) process considerations for these devices.

High Assurance Guards (HAG)—what they do

In today's world, sharing information may occur over a series of dynamic networking environments. Information such as electronic mail (i.e., E-mail), data files, and imagery is exchanged between networks to enhance communication among different organizations. Electronic transmission of this data between different security domains adds complexity to the problem because of the significant increase in security related needs.

A HAG is an IA device that offers a high-assurance solution for the transfer of data across differing classification domains. The functionality of a HAG can be likened to a border control scenario. For example, based on U.S. Customs policies, regulations, and directives, upon reaching a border, people must verify their identity to a border patrol person via a passport and state their need for crossing the border. In addition, their belongings are searched to ensure that no prohibited items are in their possession. Only after their identity has been confirmed, their personal items have been searched, and they have stated their "need" to enter a certain country are they allowed to pass across the border. The border patrol person(s) in this instance are the guardians of the border. Likewise, a HAG enforces policy and has its own communication, releaseability, and access requirements. A message must be checked against a HAG's security policy before the message will be allowed to pass; this prevents undesired data disclosure. A security policy is a statement of "what" it means for a computer system, a network, etcetera, to be "secure." Following this scenario within the context of DoD, our borders correspond to the interfaces between our high or low side networks. The exchange of information between a high or low side networks is dependent upon the interchange data requirements.

As further outlined in the scenario, information is allowed to pass through a HAG based on a security policy. An example of one of the parts of a HAG's security policy is the enforcement of releaseability requirements. Releaseability requirements for a guarding device may include—

- Allow only a properly labeled message to pass from the private level to the public level
- Allow only attachments that have been reviewed for security level at the user's workstation to pass from the private-to-public side
- Allow only selected application attachments to pass through it. This capability will be configurable to support a variety of application packages
- Perform word and/or phrase search
- Support rule-based sanitization (i.e., message content modification) of messages from high levels through low levels
- Ensure that only allowed data is distributed
- Validate proper message construction, including configurable verification of message content
- Remove classification labels, which were inserted into the E-mail body and attachments prior to delivery to the other side [1]

Information transfer between different security domains involves guarding technologies that are still evolving. There are trade-offs between cost, operational needs, convenience and risks. For instance, dependent upon data requirements, operational needs, and budget, it may be more beneficial to use a manual air-gap transfer (i.e., "sneakernet") than use a guarding technology. However, using a "sneakernet" can have the following risks associated with it—

- Time and expense of supporting physical transfer of data.
- Slow transfer rate, since data must be copied several times to and/from media.
- Human error in manually migrating data—
  - Incorrect data files may be migrated.
  - Due to various/multiple formats of data and/or different systems traversed in this process, data may become corrupted during transfer.
  - A user provides at best a visual scan to verify data was transferred correctly; it is difficult for a user to determine manually subtle inconsistencies in file attributes.

Although there are cost implications in buying and operating a HAG, many organizations find that the greatest benefit of this technology is that it offers the potential for an automated transfer of data across domains with a high level of assurance, that the transfer policy will be consistently enforced.

Now that we know what a guard can do to make the "joint picture" more a reality, the next question is, "What are the certification and accreditation challenges presented by adding this technology to an existing baseline or future architecture?"

Certification and accreditation (C&A) for high assurance guards

A discussion on multi-level guarding solutions within the context of DoD would not be complete without including a discussion concerning C&A practices. C&A is required for all DoD information technology systems in order to operate within the DoD information infrastructure. There are some unique attributes to the C&A of multi-level devices that will be addressed below.

The process for certification and accreditation of guarding technologies is dependent upon the system/networks classification, with policy dictating that the highest-level domain dictates the C&A process and requirements. What does this mean? Within DoD, this means following the DoD Information Technology Security C&A Process (DITSCAP) for Secret And Below Interoperability (SABI) connectivity or the DoD Intelligence Information System (DoDIIS) C&A for Top Secret And Below Interoperability (TSABI) connectivity. Note that each process serves different communities and therefore, has different requirements. Listed below are additional items of consideration, when following the formal C&A processes for multi-level devices—

1. **Accrediting Authority Involvement**—The Designated Approving Authority (DAA) and Certifying Authority (CA) are involved upfront. Whether you are using an already accredited guarding solution or looking to have one built to suit your specific needs, it is imperative to ensure that those with the knowledge of the requirements are involved during the design phases. Proper knowl-

edge is required by all parties to prevent a time consuming and costly mistake.

2. **Know your data**—It is critical to develop a very detailed understanding of what information your organization needs to pass from one domain to another. The characteristics of your data are used to determine what systems can meet your existing need and also determine the level of effort for creating the filters that will contain the security policy. Without a clear understanding of exactly what the data is and who can have access to this data, it is very difficult to tailor a guard solution to meet the requirement.

3. **Data Sharing Agreements**—Development of a Memorandum of Agreement (MOA) is required from the beginning of the C&A process. These documents should be among all parties, which will be sharing data between security domains. The MOA serves two major purposes—
   a. A MOA is required for data release—In coalition environments an explicit agreement needs to be documented as per DoD policy; this allows the information to be released to a second or third party nation.
   b. This document provides an agreement of both parties' responsibilities with respect to the data protection requirements.

4. **Security Requirements**—Ensure that the design of the guard meets DoD policies for multi-level requirements. These requirements will eventually become the benchmark by which the system will be certified. Therefore, these requirements should be incorporated from the start of any project looking to field a multi-security level solution.

5. **Penetration Testing**—One additional certification test and evaluation requirement for multi-level solutions is that they are required to undergo third party penetration testing.

Conclusion

In order to move our forces toward a network centric approach to warfare, multiple networks must be connected. To align these networks to the JV2020, there must be information flow between many systems with differing security domains. A solution to inter-domain collaboration can be either a cornucopia of various technologies or specific products such as HAGs. The multi-level challenge can be faced with appropriate C&A planning and an understanding of available and upcoming technologies that can make the "joint-picture" a reality. ■

References

1. IATF Release 3.0, September 2000
2. Joint Vision 2020

About the Authors

Kristina Winkler

Kristina Winkler is an Associate with Booz Allen Hamilton. She received her B.S. degree in Business Administration from the University of Arizona, a M.A. degree in Telecommunications from George Mason University, and is a Certified Information Systems Security Professional (CISSP). Ms. Winkler has over eight years of specialized experience in information systems security for government and commercial clients and currently provides guarding solutions support. She may be reached at winkler_kristina@bah.com.

Danyetta Fleming

Danyetta Fleming currently provides Certification Test and Evaluation (CT&E) support for Multi-Security Level (MSL) technologies. She received her B.S. in Engineering from University of Illinois Urbana-Champaign and is a Certified Information Systems Security Professional (CISSP). Ms. Fleming may be reached at fleming_danyetta@bah.com.

…continued from page 19

"war fighter trust…" To this end she stated, "IA is a journey, not a destination."

The hands-on hacking instruction was one of the several conference highlights. Two very knowledgeable and experienced penetration testers from the Information Assurance Technology Analysis Center (IATAC) presented a series of in-depth classes to the general session using an isolated, custom-built network of 27 laptops. The instructors led the group through numerous password-cracking techniques using a variety of publicly available hacking (kiddie) scripts. Other informative briefings included the White House Cyber Security Office perspective on the September 11th attacks, NSA analysis of future IA threats, and JTF–CNO explanations of IA policies.

Thanks to all who contributed to this year's highly successful and informative conference. The Information Assurance Division will use the accomplishments of information sharing and refining reporting procedures as a building block for the next IA conference. Essentially, this year's success was largely attributable to the active involvement of highly technical, experienced, and energetic individuals representing combatant commands, services, several DoD agencies, and the private sector. Remember, "securing information and information networks lead to securing our future." ■

About the Author

Robert Munger

Robert Munger is a configuration manager and action officer assigned to the Information Assurance Division at HQ USSOUTHCOM. He earned his B.A. in Communications from the State University of New York in 1987.

…continued from page 13

or maintain systems for customers, the CVE compatibility of advisories will help you to directly identify any fixes from the vendors of the commercial software products in those systems (if the vendor fix site is CVE-compatible). The result is a much more structured and predictable process for handling advisories than most organizations currently possess. To date, more than 400 CANs have appeared in vulnerability advisories from 28 organizations.

Conclusion

As with the CVE Editorial Board, the organizations working on or delivering CVE-compatible products is international in scope. Currently there are 67 plus organizations working toward compatibility for 104 plus products and services, including software vendors who have added CVE names to their alerts and to their software patch and update sites.

The changes in tools and services brought about by the adoption and support of CVE allow more systematic and predictable handling of security incidents. As more vendors respond to user requests for CVE compatibility, the complete cycle of finding, analyzing, and fixing vulnerabilities will be addressed—moving this part of securing the enterprise from art to science. ■

References

1. Sullivan, Bob, "Hospital confirms Hack Incident," MSNBC, December 9, 2002.
2. Refer to the CVE Web site at http://cve.mitre org for the most up-to-date information. An in depth white paper on this topic, "The Vulnerabilities of Developing on the Net," is available on the CVE Web site. Robert A. Martin is the CVE Compatibility Lead and a Principal Engineer in MITRE's Information Technologies division.

About the Author

Robert Martin

Robert Martin is the primary point of contact for CVE compatibility efforts, a co-lead for MITRE's Cyber Resource Center Web site, and a principal engineer in MITRE's Information Technologies Directorate. His focus is the interplay of cyber security, critical infrastructure protection, and e-business technologies and services. Mr. Martin received an M.S.E.E. from Rensselaer Polytechnic Institute and an M.B.A. from Babson College. He is a member of the IEEE Computer Society, the IEEE, the ACM, the NDIA, and AFCEA. He may be reached at ramartin@mitre.org.

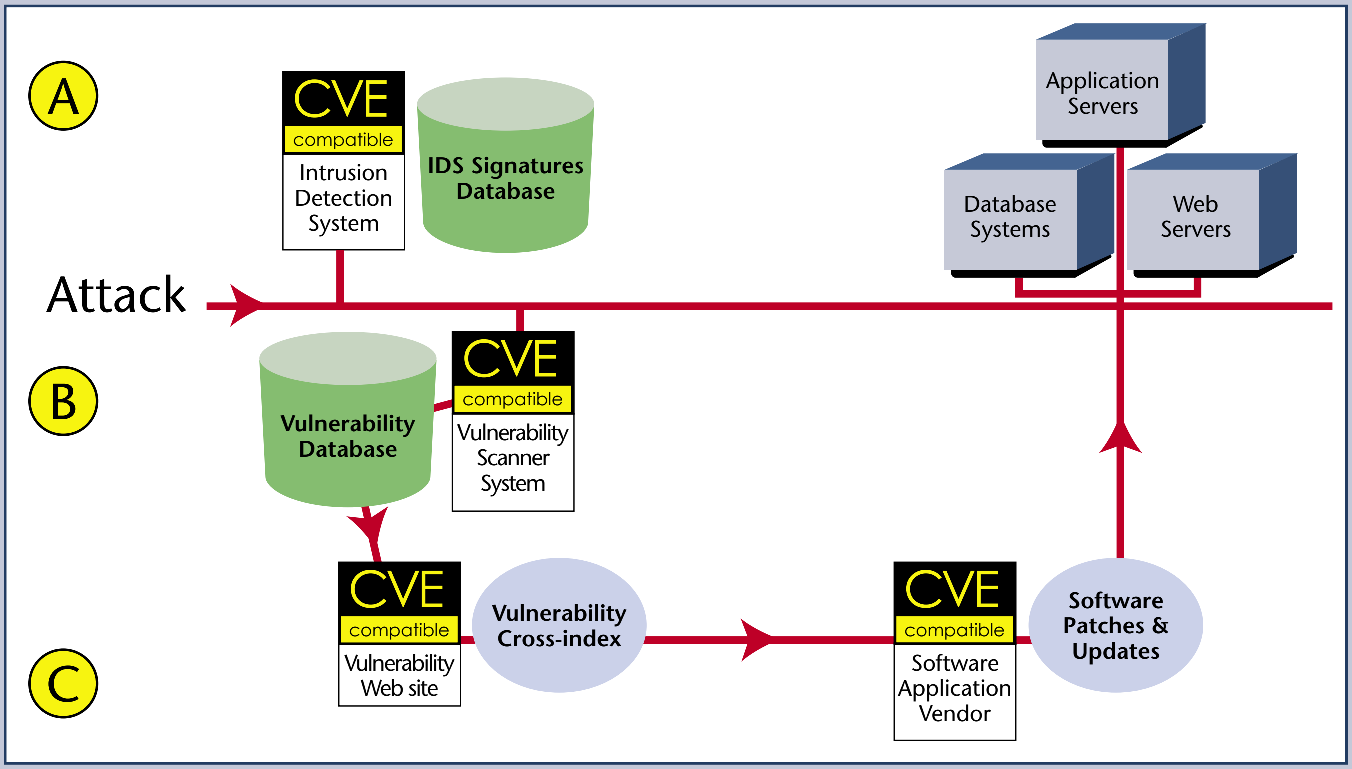
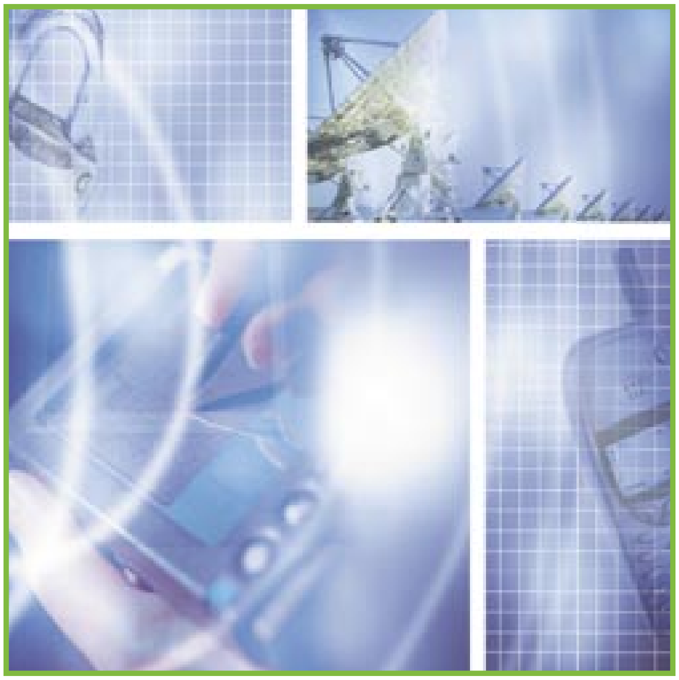


Figure 1: A CVE-Enabled Process



Wireless Wide Area Network (WWAN) Security

Over the past few years, the use of wireless data devices, such as the BlackBerry™ unit by Research In Motion (RIM), has greatly increased within the Federal Government.

The need for accessing E-mail remotely has been the primary market driver for this growth, although device-to-device communications has also been a significant contributor. However, this surge in wireless E-mail usage is not yet pervasive among most Federal mobile workers because of the requirement to carry another device, limited coverage, the cost of the extra device, the associated airtime, and the limited security offered. New developments are ongoing that will greatly reduce these limitations to help spur not only wireless E-mail and device-to-device communications usage, but also help increase wireless data usage in general over the next several years to include a wide range of applications and new users.

Perhaps the biggest catalyst behind this expected growth are the upgrades being made by the cellular carriers to 2.5 generation (2.5G) and 3rd generation (3G) systems. These upgrades are greatly improving the throughput of wireless data services to speeds at or above 56 kbps landline modem speeds. The networks are also more ubiquitous and have improved security over existing networks.

With the increased bandwidth being offered nationwide, often using the same device as a person may use for a cellular voice call, there is a wide-reaching effort by vendors to offer wireless end-to-end solutions. This effort is not just limited to the traditional wireless companies such as Nokia and Motorola, but traditional Internet and software companies such as Microsoft, IBM, Oracle, and Sun are also heavily investing in this area. As an example of the high expectations, when Sun Microsystems' CEO Scott McNealy was asked "What will be the next technology advance that radically changes the business landscape," he stated "Wireless is the next big thing. There's just no question about that." [Computerworld September 30, 2002]

The growth of Personal Area Networks (PANs) such as BluetoothTM is also expected to help drive wireless adoption. Presently, Bluetooth™ is offered as a standard option on only a few phones, but as it becomes standard on more phones and the price for Bluetooth "modem" cards for laptops become more inexpensive, more and more users will take advantage of the seamless connection Bluetooth offers to wirelessly access their remote data.

With the large expected growth of wireless, its tremendous capabilities, and with hundreds of thousands of Personal Digital Assistants (PDAs) lost or stolen per year [Gartner], security is a major concern. To exemplify this issue, a user may have entered all of his passwords into his PDA, have E-mails automatically forwarded from his desktop to his PDA, be able to remotely download files wirelessly, and not even have the password login feature enabled in the PDA. This scenario is troubling many IT administrators with good reason. This report was developed to address WWAN security with those administrators in mind.

The objective of this report is to provide an overview, analysis, guidelines, and recommendations for security of wireless wide area networks. After reading this report, a United States Federal Government Information Technology (IT) professional with minimal knowledge of wireless networks should understand the leading Wireless Wide Area Network (WWAN) technologies, the security issues from an Infrastructure Assurance perspective, the different security schemes implemented within each technology, current Department of Defense (DoD) policies, industry trends, and best practices used to mitigate these concerns.

It complements the National Institute of Standards and Technology (NIST) Special Publication 800-48 Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices document. This report will be released in December 2002. You may order it using the order form on the next page or by going to our Web site. ■

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 ______________________________

Organization ______________________________

Address ______________________________

____

____

DTIC User Code ______________________________

Ofc. Symbol ______________________________

Phone ______________________________

E-mail ______________________________

Fax ______________________________

Please check one: □ USA □ USMC □ UN □ USAF □ Command
□ Industry □ University □ DoD □ Gov't □ Other

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

____

LIMITED DISTRIBUTION

IA Collection Acquisitions CD–ROM

□ Summer 2002 ed.

IA Tools Reports

□ Firewalls (3rd ed.) □ Intrusion Detection (3rd ed.) □ Vulnerability Analysis (3rd ed.)

Critical Review and Technology Assessment (CR/TA) Reports

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

State-of-the-Art Reports (SOARs)

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

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

UNLIMITED DISTRIBUTION

IAnewsletters (Limited number of back issues available)

Volumes 1	□ No. 1	□ No. 2	□ No. 3	
Volumes 2	□ No. 1	□ No. 2 (soft copy only)	□ No. 3	□ No. 4
Volumes 3	□ No. 1	□ No. 2	□ No. 3 (soft copy only)	□ No. 4 (soft copy only)
Volumes 4	□ No. 1 (soft copy only)	□ No. 2	□ No. 3	□ No. 4
Volumes 5	□ No. 1	□ No. 2	□ No. 3	

Fax completed form to IATAC at 703.289.5467

December

NOAA IT Security Conference & Expo

December 3, 2002
Silver Spring, MD
http://www.noaa.gov

US, UK, Canada, Australia, and New Zealand Military Computer Network Defense (CND) Technical Conference

December 4–6, 2002
Booz Allen Hamilton Conference Center, McLean VA
https://www.enstg.com/Invitation
Code = "US,63594"

E-business Security: Information Assurance Technical Framework Forum

December 5, 2002
John Hopkins University, Applied Physics Laboratory, Laurel, MD
http://www.iatf.net/

A Strategic Summit on Auditing and Governance in the New Era of Accountability

December 9–12, 2002
Embassy Suites Hotel, New York City, NY
http://www.misti.com/northamerica.asp?page=4&disp=conf&region=1&subpage=2

18th Annual Computer Security Applications Conference

December 9–13, 2002
Las Vegas, NV
http://www.acsac.org/

National Threat Symposium and Security Awareness Fair

December 11–12, 2002
John Hopkins University, Applied Physics Laboratory, Laurel, MD
http://www.iaevents.com/natthreat02/newinfo.cfm

January

Defending America Together: The New Era

January 8–10, 2003
Riviera Hotel, Las Vegas, NV
http://www.federalevents.com/govcon/purpose.html

WEST 2003

January 11–16, 2003
San Diego Convention Center, CA
http://expo.jspargo.com/west03/expo.htm

SPACECOMM 2003

January 28–30, 2003
Broadmoor Hotel, Colorado Springs, CO
http://rockymtnafcea.org/2003/

DoD 7th Annual IA Workshop/Conference

January 28–30, 2003
Marriott Hotel, Williamsburg, VA
http://www.isoc.org/ndss03/

February

Conference on Mobile and Wireless Security

February 11–13, 2003
Scottsdale, AZ
http://www.misti.com

Homeland Security 2003: IT On the Frontline

February 26–27, 2003
Ronald Reagan International Trade Center, Washington, DC
http://www.AFCea.org/homeland03/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