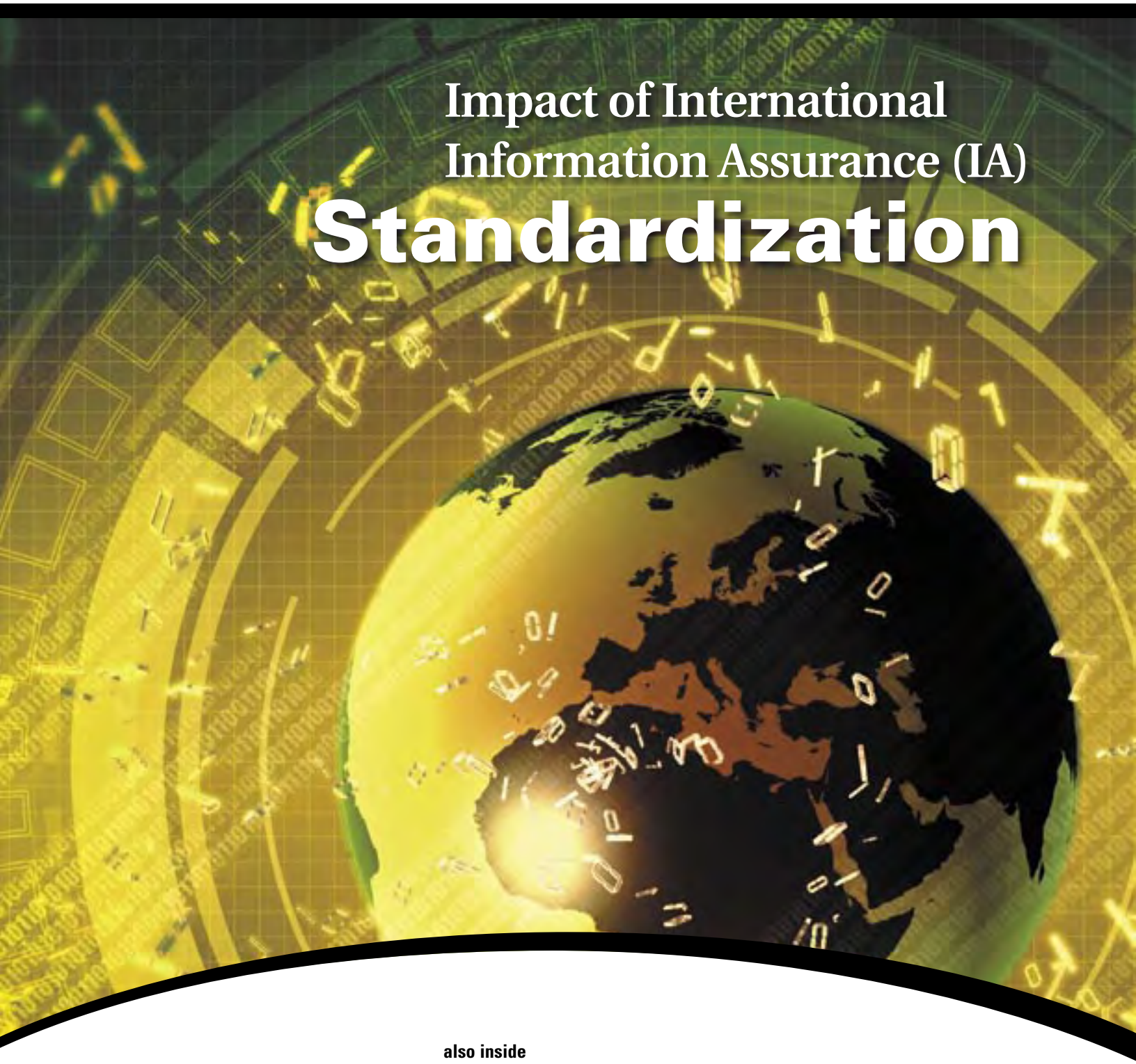
8/4

Volume 8 Number 4 • **Spring 2006**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



Impact of International Information Assurance (IA) Standardization

also inside

IATAC

contents

in every issue

DDRE

About IATAC and the *IAnewsletter*
The *IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Director, Defense Research and Engineering (DDR&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, or DDR&E. The mention of commercial products and/or does not imply endorsement by DoD or DDR&E.

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

IATAC Director: Gene Tyler
Deputy Director: Greg McClellan
Inquiry Services: Peggy O'Connor

***IAnewsletter* Staff**
Promotional Director: Christina P. McNemar
Creative Director: Ahnie Jenkins
Art Directors: Bryn Farrar, Don Rowe
Copy Editor: Diane Ivone
Designers: Steve Green, Dustin Hurt, Brad Whitford
Editorial Board: Greg McClellan, Jim Peña, Ronald Ritchey, Tara Shea, Gene Tyler

***IAnewsletter* Article Submissions**
To submit your articles, notices, programs, or ideas for future issues, please visit http://www.iatac.org/IA_newsletter.html and download an "Article Instructions" packet.

***IAnewsletter* Address Changes/ Additions/Deletions**
To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at:

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

Phone: 703/984-0775
Fax: 703/984-0773

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

Deadlines for future Issues
Summer 2006 April 7, 2006

Cover design: Dustin Hurt
Newsletter design: Bryn Farrar, Donald Rowe

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

IATAC Chat

Gene Tyler, IATAC Director

I'm sure the new year has brought much change for everyone, and by now you may be aware, IATAC has been involved in some changes of our own.

At this point, we are all settled in our new Herndon, VA location. For years, IATAC's home has been our Falls Church, VA office. While Fairview Park was a great location, our new One Dulles location is better suited to facilitate our continuing enhancements to IATAC. Along with a new home, we are also involved in creating a new, more polished look for IATAC. You may have already noticed the new face of this edition of the *IAnewsletter*. We've come a long way since our first days of creating this publication. For a retrospect of how far we've come, please take a peek at the insert on pages 16. You will see that we we've gone from a "fine" publication, to the award winning newsletter we have today. The *IAnewsletter* is just one of several improvements to be on the look out for within IATAC; one other I want to note is our IATAC Web site.

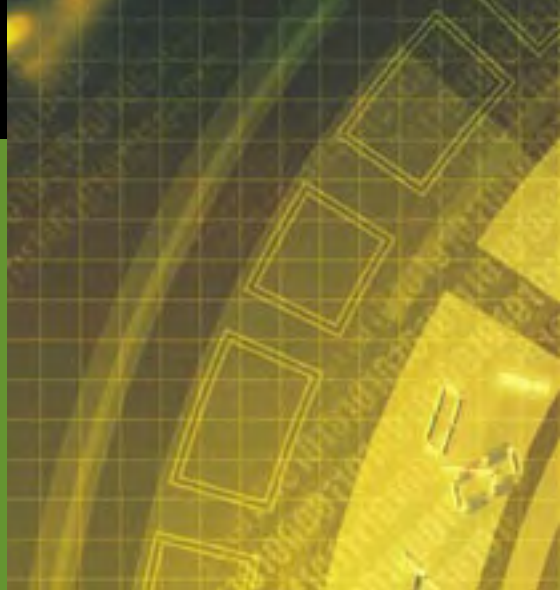
We are all extremely exited for the debut of our new, robust IATAC Web site, which will be coming very soon. Stay tuned to our next edition for a full update and review on our move and transformation.

Also in this edition, you will find some very exciting and interesting articles, including one which is slightly more technical than our norm. *DOWN with Trusted Devices* is a fascinating article which focuses on a security policy—Decrypt Only When Needed (DOWN). Although a relative uncomplicated security policy, this article details the impact that DOWN has on computer architecture and Key-Distribution Schemes. I encourage everyone to learn more about this policy for realizing trusted computers. In addition, the author of this article is from Mississippi State University, which happens to be our featured institution in this edition.

Finally, I would like to point out, the *Letter to the Editor.* The question in this edition came to us after the 2006 DoD Cyber Crime Conference, asking for information about DoD 8570.1 Directive and Manual. You will find the question and our response on page 31. DoD 8570.1, *Information Assurance Training, Certification, and Workforce Management*, is a policy that is likely to effect everyone in the IA community; for this reason, we have reached out to the Defense-Wide Information Assurance Program (DIAP), who will be featuring an article in our next edition.

As always, should you have any questions or concerns for me or the IATAC team, please do not hesitate to contact us. ■

Impact of International Information Assurance (IA) Standardization



by Nadya Bartol, Jonathan Smith, and Aderonke Adeniji

Global Importance of Standardization

During the past ten years, Information Assurance (IA) standardization has gained increasing international recognition as a critical issue. As government, industry, and citizens in the US and abroad rapidly increase their reliance on computers, they face corresponding increases in the cost and difficulty of assuring the protection of information that their computer systems transmit, process, and store.

IA professionals face an extraordinarily dynamic threat environment in which foreign nations, terrorist organizations, crime syndicates, and individuals have all recognized and exploited opportunities to attack government, industrial, and individual computer resources at an ever-increasing pace. In 2004, the average time between the announcement of a vulnerability and the first known exploitation was 5.8 days; [1] exploits of the recent Zotob worm were disrupting major enterprises within 24 hours of the announcement. [2] These challenges are being met with standards that address a broad range of issues from identifying baseline practices for information security management systems to standardizing specific IA technologies for product implementation.

To make matters worse, national infrastructures become more dependent on Information Technology (IT) every day. Electrical power systems rely on automated controls; banks rely on IT for processing business transactions; an entire IT business sector has formed around computers and the Internet and is responsible for tens of thousands of jobs—municipalities have begun implementing electronic voting tools—threats to which can be described, with no exaggeration, as threats to our democracy.

Much of the challenge to the above-mentioned IT infrastructure is the rapid development of functionality without consideration of security. The electrical power industry rapidly automated power-generation and power-transmission facilities and are only now developing standards to protect their information and infrastructure. The North American Electric Reliability Council is a coalition of electric-power companies that has been developing a series of voluntary "cyber security standards" intended to "reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets (computers, software and communication networks) that support those systems." [3] The Energy Policy Act of 2005 established those standards as mandatory for all US electric-power utilities. [4]

Security trails behind functionality in industry after industry because functionality sells—governments see opportunities to provide better services to citizens, businesses see opportunities for new revenue or increased efficiency, and individuals buy based on utility. Security has always been an afterthought. Even in the critical function of electronic voting, the United States Election Assistance Commission concluded in September 2005 that current electronic voting testing procedures mistakenly focus on voting functionality, not system security. [5]

In Germany, approximately 60% of the critical infrastructure is privately owned. This leaves the German government in the precarious position of attempting to support assurance for information and information systems that are not fully under its control. The situation is even more difficult in the US, where approximately 85% of critical infrastructure is owned by the private sector. [6] In all such situations, elected officials recognize the costs and unpopularity of increased regulations on privately held infrastructure and are reluctant to impose such rules.

Governments do have non-regulatory opportunities to influence the private sector. For example, the US government is increasingly using contracts and federal acquisition regulations to impose standards on companies that provide products to, or perform direct services for, federal departments and agencies. For this approach to be effective, contracting and IA personnel must work closely together to ensure compliance with government-specified IA requirements and applicable laws and regulations. The subject becomes much more complex with government purchases of products that turn out to be developed

Standards development is a global effort, focused on market needs and facilitated by full and open cooperation and collaboration among industry participants worldwide.

overseas or contracts with companies who outsource portions of work to other countries. The farther work gets from the prime contract, the more difficult it is for the government to ensure and enforce applicable IA requirements.

A prime example of how international standards help increase economic efficiencies is the ISO 9000 series of quality management standards. Over the past 50 years, most large businesses have embraced the concept of a quality management system. With the growth of modern industrial production driven by the military demands of World War II, business leaders found themselves managing processes of unprecedented complexity without the tools to fully control or improve those processes. They knew they needed to find ways to improve production and enhance the bottom line. In time, experts came to identify, collect, and document a common set of best practices that supported quality, and thus the ISO 9000 series was born. These standards, born of necessity, are among the most widely known of all international standards and are used by about 760,900 organizations in 154 countries because they are proven tools for increasing productivity. [7]

Engaging in standards development is a less direct approach to influencing private-sector behavior then is increasing regulation. The US government has a clear stake in the outcome of standards activities, including IA. Standards provide a common IA language that can be used by all parties to facilitate contracting for products and services and can provide a shorthand that can be used to define expected levels of performance. Businesses are likely to adopt standards when it is clear that purchasers are looking for compliance as a requirement for participation. A common language and common approaches are also critical for public–private coordination.

The US is committed to the view that "standards development is a global effort, focused on market needs and facilitated by full and open cooperation and collaboration among industry participants worldwide." [8] Establishing and using international standards is essential for facilitating trade, ensuring interoperability among trade partners, and facilitating increased efficiencies in the global economy. Confusion would quickly ensue if nations could not agree on how much oil should be contained in a "barrel" or if different suppliers did not consistently grade their products using common oil nomenclature (crude, sweet, very light, etc.). Establishing common standards also reduces confusion in the marketplace—a classic example is the incompatible VHS vs. Betamax video-recording formats. When the video-recording industry didn't agree to a common standard for recording media, they expended significant resources battling over who had the better format rather than innovating and improving on an accepted format. Standardization also provides a baseline for communicating requirements to product vendors, which leads to improved interoperability among devices and a general lowering of development costs. [9] Finally, governments often take advantage of international standards, using them as a basis for legislation and regulation.

Standards Bodies and Organizations

How then are these problems being addressed? Many standards organizations address IA-related topics with areas of influence ranging from the truly global to the highly technology-specific. Most influential are the three consensus-driven standards organizations whose outputs

have been written into international trade treaties. The World Trade Organization (WTO) often cites standards from these organizations in its rules for international commerce—referred to as the Code of Good Practice in the WTO's Technical Barriers to Trade agreement:

- **The International Organization for Standardization (ISO)**—The ISO is the world's largest developer of standards and is a non-governmental, consensus-building network of the national standards institutes of 156 countries. Those institutes do not directly represent the governments of their respective countries but commonly have close ties to both governments and industries.
- **The International Electrotechnical Commission (IEC)**—The IEC develops international standards and conformity assessments for government, business, and society for all electrical, electronic, and related technologies. Their standards are relied on to create national standards and for international commercial contracts and agreements. [10]
- **The International Telecommunications Union (ITU)**—The ITU has its roots in the treaties of the late 1800s, when it addressed international telegraph interconnections. The ITU is now an international organization within the United Nations System of Organizations through which governments and the private sector coordinate global telecom networks and services. [11]

Examples of other standards bodies whose standards are widely used on a more voluntary basis include:

- **The Institute of Electrical and Electronics Engineers (IEEE)**—The IEEE establishes standards for electronic and information technologies. As is true of other standards, these support broader commercialization, interoperability, efficient design and implementation, and protection of users and the environment. [12]
- **The Internet Engineering Task Force (IETF)**—The IETF develops Internet-related standards, especially those relating to the Transmission Control Protocol/Internet Protocol (TCP/IP). Its membership is open to the general public and although it meets three times a year, most of its work is conducted via e-mail.

Users of international IA standards range from international treaty organizations to local municipalities and from multinational corporations to local vendors. WTO political and trade agreements are based on standards-driven technical agreements that define common terms and measures. Multinational corporations do business worldwide because they can express requirements and specifications in a common language.

Each international standards organization has its own way of conducting its business. Most organizations accomplish their work through an array of technical committees, subcommittees, working groups, and similar bodies. The most widely accepted standards organizations leverage formal organizational structures and rules of operation to develop and maintain standards. One such organization that creates many of the most significant and far-reaching IT standards today exists under the auspices of an ISO and IEC partnership: the ISO/IEC Joint Technical Committee 1 (JTC1). (See Figure 1)

JTC1 is chartered to develop IT standards. Among its numerous components, Subcommittee 27 (SC27) has the primary charter to develop information security standards. SC27 accomplishes its work through three working groups with broad functional perspectives. Working Group 1 establishes standards for the general management and operation of IA. Working Group 2 focuses on cryptography. Working group 3 focuses on IA assessment and evaluation. Two other subcommittees have ties to IA. Subcommittee 7 (SC7) focuses on software and system engineering principles, including a working group on system and software assurance issues. The domain of Subcommittee 37 (SC37) is biometrics, which, although it is an IA technology, is handled independently.

The international activities of JTC1 and its Subcommittees are directed and supported by associated national standards bodies. The US is represented by the InterNational Committee for Information Technology Standards (INCITS), which is the US counterpart to JTC1. Similarly, INCITS has established Cyber Security 1 (CS1) as the US counterpart to SC27. (See Figure 2) In addition to national standards bodies, other standards committees,

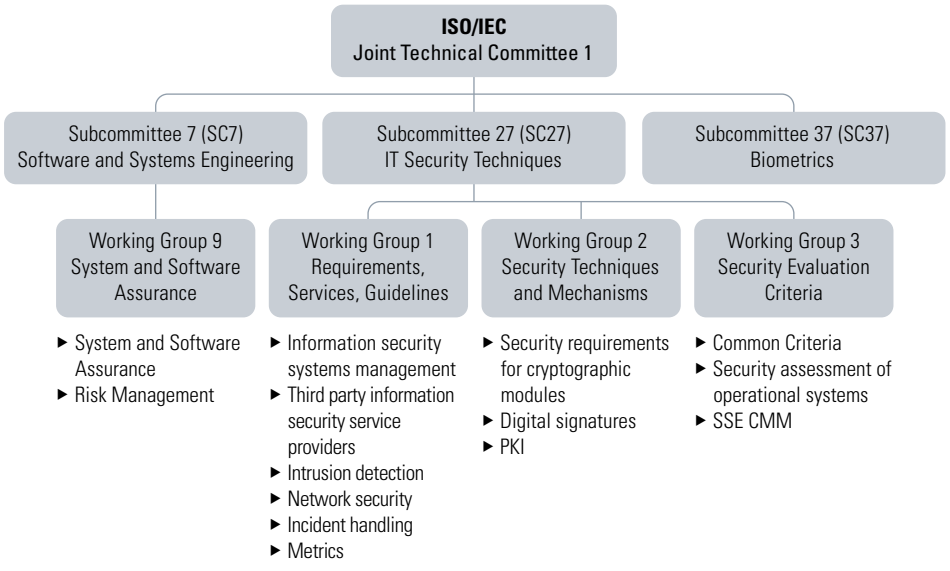


Figure 1 JTC1 Subcommittees and Working Groups Related to IA

subcommittees, working groups, and industry associations can participate in these international bodies as liaison members. Since they don't represent national standards bodies, liaison members do not vote; however, they can participate in standards development by contributing materials and expertise.

While the aforementioned standards activities are all fairly generic, there are also numerous industry-specific efforts. The American National Standards Institute (ANSI) hosts such wide-ranging activities as the Healthcare Informatics Standards Board, the Homeland Security Standards Panel, and even a technical committee on Fasteners (mechanical properties, dimensions, tolerances, *etc.*). "X9" is the standards organization for the US financial industry, while "N14" addresses the packaging and transport of radioactive and non-nuclear hazardous materials.

Standards Development Process and Participants

The process of creating most international standards can be very complex and formalized. Well-documented and transparent processes are necessary to build a standards document that will be voluntarily accepted by a significant majority of national representatives. It takes a substantial effort to gain international consensus on any issue, but standardization organizations accomplish this every day.

Developing each ISO standard is expected to take two to five years from inception to publication. Typically, standards begin with an established marketplace requirement. An industry that requests a standard must communicate its need trough its national standards body, which then proposes this request to a corresponding subcommittee. The subcommittee presents the proposal for a discussion and a vote, and, if accepted, the subcommittee begins working on the standard. When the proposal is presented to the national standards bodies for a vote, these bodies are asked whether they are willing to provide an editor—an expert who will actively participate in the standard's development and contribute content that could advance the new standard. This process facilitates active participation in developing technically sound standards by technical experts in each individual standard.

During standard development the relevant subcommittee reviews multiple drafts and requests comments from national standards bodies to advance drafts to the next formal stage of development. Advancing the standard from one formal stage to another requires an international ballot, voted on by each standards body. With their votes, the national standards bodies submit comments on content, suggestions for improvement, and explanations for no votes. When a standard successfully advances through all required stages, it is published as an international standard. [13]

Individual participants in SC27 activities are either delegates selected by corresponding national standards bodies to represent their national interests or liaison organization representatives contributing their technical expertise. Within the US, CS1's membership consists of individuals appointed by their respective employers to represent specific US industry and government interests. In turn, CS1 sends delegates to bi-annual SC27 meetings to represent consensus US positions and priorities. The individual level of participation in both SC27 and CS1 is driven by the willingness of individuals to commit time to standards development. Any participation at the level of a national standards body also requires some financial commitment, depending on the type of organization (government, academia, not for profit, or industry) and the level of engagement (from basic organizational membership to INCITS Board membership). Current US government members of the INCITS Board include the Department of Homeland Security (DHS), the Department of Defense (DoD), and the National Institute of Standards and Technology (NIST). Other board members include a wide range of business, not-for-profit, and academic concerns. [14]

It is important to note that, while US government organizations participate in many ANSI and INCITS activities, the US government does not control US national standards positions. That said, the US government has made a clear commitment to using international standards. The White House has mandated that agencies "use voluntary consensus standards in lieu of government-unique standards except where inconsistent with law or otherwise impractical." [15] To support this, the government has provided "guidance for agencies participating in voluntary consensus standards bodies." [16]

Figure 2 Relationships Between International and US Standards Bodies

NIST is an active participant in international IA standards development. This complements its role as the primary standards developer for US government agencies and its mission to "develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life." [17] The Federal Information Security Management Act (FISMA) authorized NIST to develop information security standards and guidance for all US government systems, except for national security systems. These standards and guidance documents are widely recognized as best practices and have been adopted worldwide by private-sector organizations.

DoD is committed to developing and deploying standards. This is in

part a response to its own needs and in part a response to numerous broader federal legal and regulatory requirements promoting security and interoperability. An example of the latter is that DoD Chief Information Officers are obliged under law to "ensure that information technology and national security systems are interoperable with other relevant information technology and national security systems of the Government and the Department of Defense." [18] This can only be accomplished through developing, adopting, and deploying relevant standards. To support standard adoption, DoD operates an IT standards governance process that provides executives, experts, and stakeholders with the opportunity to vet a particular international standard before it is adopted by the enterprise. Individual DoD representatives also participate in relevant standards-development activities where deemed appropriate by their respective organizations.

The Defense Information Systems Agency (DISA) is tasked as the executive agent for coordinating IT standardization activities within DoD. DISA is committed to developing and maintaining a spectrum of standards from interoperability standards for the warfighter to secure configuration standards for systems. [19] DoD Directive 5101.7, *Executive Agent for Information Technology Standards*, instructs DISA to maintain the DoD IT Standards Registry (DISR) and to establish processes and procedures for life-cycle configuration management of IT standards contained in the DISR. The DISR provides DoD community with access to applicable and available standards. [20]

The US government has established standards-development activities that target national-security systems within the Committee on National Security Systems (CNSS). Established by executive order, the CNSS "provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems." [21]

IA Standards Topics

One of the most significant recent efforts of JTC1 and SC27 was establishing the new ISO/IEC 27000 series. The 27000 series addresses managing information security and includes topics such as requirements for information security management systems and guidance, metrics, and measurements for information security management. The 27000 series groups and addresses the issues of information security management similarly to the manner in which the ISO 9000 series groups and addresses quality management. When completed, the 27000 series is expected to include all topics pertinent to managing information security programs. Myriad other IA standards have been published or are under development, ranging in subjects from

Topic	ISO Standards	NIST Standards	DoD Policy
Product Evaluation Criteria	ISO/IEC 15408	Special Publication (SP) 800-36 National Information Assurance Partnership (NIAP)	NIAP
Maturity Models	ISO/IEC 21827	N/A	Common Criteria
Information Security Management System	ISO/IEC 17799:2005, ISO/IEC 13335-1, ISO/IEC 27001	SP 800-12, SP 800-64, SP 800-18	DoDI 8500.1, Director of Central Intelligence Directives (DCID) 6/3
Risk Management	ISO/IEC 13335-2	SP 800-30	DoDI 5200.40, Department of Defense Directive (DoDD) 5160.54
Management	ISO/IEC 13335-3	SP 800-12, SP 800-64	DoDI 8500.1, DoDD 8570.1, DCID 6/3
Selection of Controls	ISO/IEC 17799:2005, ISO/IEC 13335-4	Federal Information Processing Standard (FIPS) 200, SP 800-53, SP 800-53A	DoDI 5200.40, DoDI 8500.1, DoDD 8570.1
Network Security	ISO/IEC 13335-5, ISO/IEC 18028	SP 800-31, SP 800-70	DoDI 8530.1, DoDI 8530.2, National Security Agency (NSA) Red Team Certification & Accreditation (C&A), Public Key Infrastructure (PKI) Road Map
Intrusion Detection Systems	ISO/IEC 18043	SP 800-31	Chairman, Joint Chiefs of Staff Instruction CJSCI 6510.01C
Incident Management	ISO/IEC 18044	SP 800-61	
Cryptography	ISO/IEC 18033, ISO/IEC 9798	FIPS 197, FIPS 196	Various NSA, PKI Road Map
Metrics and Measures	ISO/IEC 27004	SP 800-55	CJCSI 3401.03

Table 1 IA Topics Mapped Across ISO Standards, NIST Standards, and DoD Policy

hash functions to network security to IT disaster recovery.

The topics of many SC27 standards are similar to the topics of NIST standards and guidance and those of DoD Directives and Instructions. Table 1 provides a sample cross-comparison of several IA topics among the standards, guidance documents, directives, and instructions developed by SC27, NIST, and DoD. (See Table 1)

Summary

International IA standardization efforts are producing valuable resources at a rapidly accelerating pace. US government IA practitioners should take advantage of these best practices to complement existing internal guidance. The importance of international standards within US government space will continue to grow as it becomes increasingly more difficult to identify where the boundaries of a government system or infrastructure end and the boundaries of a private system or infrastructure begin. By participating in the process of developing international IA standards, US government experts can promote better security practices among domestic and international private-sector organizations and thereby facilitate adopting globally accepted IA practices by product suppliers and service providers. These voluntary consensus standards provide a ready-to-use tool for improving the IA posture of US critical infrastructure. The increased deployment of international IA standards and engagement in standards development by US government IA practitioners will provide a strong technical base for industry-wide standardization and assist in promoting best practices supportive of US economic and national security interests. ■

References

[1] "Symantec Internet Security Threat Report Identifies More Attacks Now Targetinge-Commerce, Web Applications," 20 September 2004. *http://www.symantec.com/press/2004/n040920b.html.*

[2] Brenner, Bill. "Time Shrinks for Patch Management." Information Security. September 2005.

[3] "Northern American Electric Reliability Council—Standards Authorization Requests Approved for Posting, " 27 September 2005 *http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html*

[4] Lipowicz, Alice, "Power grid makes moves to bolster cyber security," Washington Technology, 15 August 2005. *http://www.washingtontechnology.com/news/1_1/daily_news/26797-1.html*

[5] "E-voting experts call for revised security guidelines," 3 October 2005. *http://www.securityfocus.org/news/11336*

[6] "DHS Organization—Information Analysis & Infrastructure Protection," 18 October 2005. *http://www.dhs.gov/dhspublic/display?theme=52&content=207*

[7] "ISO 9000 and ISO 14000—In Brief," 27 September 2005. *http://www.iso.ch/iso/en/iso9000-14000/understand/inbrief.html*

[8] "Guide for U.S. Delegates to Meetings of the IEC and ISO." American National Standards Institute, Washington DC. July 2002.

[9] "INCITS: Why Participate," 6 October 2005. *http://www.incits.org/purpose.htm*

[10] "About the IEC," 3 October 2005. *http://www.iec.ch/about/mission-e.htm*

[11] "ITU Overview," 3 October 2005. *http://www.itu.int/aboutitu/overview/history.html*

[12] "Standards Development At The IEEE Standards Association," 3 October 2005. *http://standards.ieee.org/announcements/bkgnd_stdsprocess.html*

[13] "Overview of the ISO System," 20 September 2005. *http://www.iso.org/iso/en/aboutiso/introduction/index.html.*

[14] "InterNational Committee for Information Technology Standards Executive Board," 6 October 2005. *http://www.incits.org/ebmem.htm*

[15] Office of Management and Budget Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, February 1998.

[16] Ibid.

[17] "NIST—General Information," 27 Sept. 2005. *http://www.nist.gov/public_affairs/general2.htm.*

[18] United States Code Title 10, Section 2223, Information Technology: Additional Responsibilities of Chief Information Officers, July 2005.

[19] "DISA Core Mission Areas,"18 October 2005. *http://www.disa.mil/main/about/coremission.html*

[20] DoD Directive 5101.7, "DoD Executive Agent for Information Technology Standards," 21 May 2004.

[21] "The Committee on National Security Systems: History," 6 October 2005. *http://www.cnss.gov/history.html*

About the Authors

Nadya Bartol CISSP | has led implementation of security program measurement and improvement efforts for multiple government and commercial organizations, ranging from the CIO level to security engineering service providers. She has co-authored several National Institute of Standards and Technology (NIST) guidance documents, including Special Publication (SP) 800-55, Security Metrics Guide for IT Systems, NIST SP 800-65, and Integration of IT Security into Capital Planning and Investment Control (CPIC) Process Guide. Ms. Bartol serves as the US delegate to ISO/IEC JTC1 SC27, where she is one of the experts working on the ISO/IEC 27000 series standards. She also serves as chair of the International System Security Engineering Association (ISSEA) Metrics Working Group.

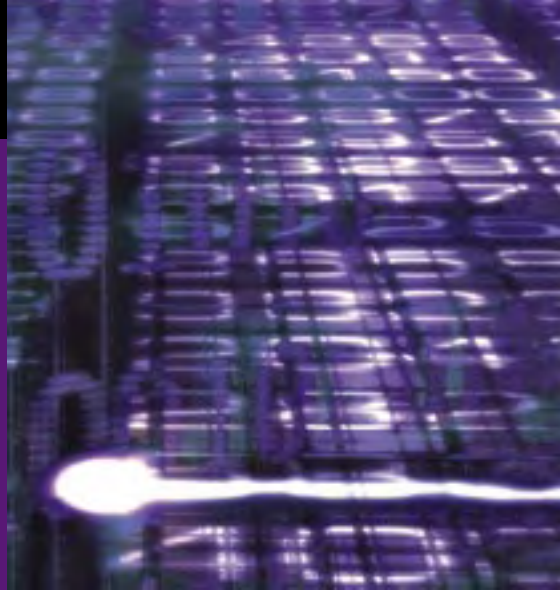
Jonathan Smith CISSP | supports OCIOs at a wide range of DoD and civilian agencies. He specializes in the governance of IA programs, including the development of IA strategies, policies, and performance measurements (strategic, operational, and compliance-oriented). Mr. Smith is co-author of NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems. His background also includes technology training, federal government service, and network engineering.

Aderonke Adeniji | supports Information Security Compliance efforts within the federal government arena. She assists civil agencies perform C&A of systems and helps fulfill FISMA submission requirements. Her interest lies in both strategic information management in the public sector and quantitative performance management. Ms. Adeniji has previous experience within the telecommunication and records management environments. Her background includes an undergraduate degree in Management Science & Statistics and a graduate degree in Information Management from the University of Maryland at College Park.

All of these authors can be contacted at iatac@dtic.mil.

When Writing Software, Security Counts

by Matthew Fisher



The life of the average Information Technology (IT) security engineer is becoming more difficult every day. The tools an engineer uses are becoming more complicated and varied, as are the threats, and he or she must fight a growing tide of hacks against the one thing that can't be controlled: the application itself.

The majority of IT vulnerabilities existing today stem from the initial stages of software development: its design, coding, or implementation. In the case of Web-application software, hacking the application can be extremely simple and effective for someone looking to steal sensitive information. Since the application is typically the only service exposed over the network and the least secured, it becomes an easy target for hackers. While hackers can and certainly do perform attacks against the daemon itself, these often have a limited life span, since disclosed vulnerabilities in the daemon are subject to patching. There are certainly many undisclosed vulnerabilities against popular Web servers, but these are typically not widely circulated beyond the founding hacker groups. By exploiting flaws in the actual application itself, a entirely new realm of possibilities exist, many with few defenses that can be used aside from actually securing the code itself. Fortunately for the mischievous hacker, most software developers aren't aware of the multitude of attack techniques deployed against their software. This is largely caused by a lack of education, process, and appropriate tools required to secure their code.

For people who understand application security, this is a bit of a shock, as software vulnerabilities have existed for a long time. Take for instance the "buffer overflow" that was first popularized in the classic Morris Worm of 1988.

> Despite firewalls, intrusion detection, and other technologies, Web vulnerabilities such as SQL Injection are exploited on a daily basis.

Despite being well known and easily prevented, buffer overflows are still extremely common more than 17 years later. Structured Query Language (SQL) Injection, which is remarkably easy to fix, was first documented by Rain Forest Puppy in 1998. Yet SQL Injection still lives and thrives on Web sites across the Internet. Despite firewalls, intrusion detection, and other technologies, Web vulnerabilities such as SQL Injection are exploited on a daily basis. Of course, there's much more to secure coding than preventing SQL Injection and buffer overflows. Both types of attacks are input validation issues, and there are several other input validation attacks as well as many other complete categories of existing attacks that are not so well known. Learning the complete threat model takes time but is essential to defending against these threats, which show no sign of subsiding.

A common mistake that organizations make about application security is fixating on the security portion and treating it as a matter to be dealt with purely by the security department. In fact, the security department is often the one least able to do anything about these vulnerabilities since they aren't likely to be modifying custom code. Typically, by the time a security department finds them, these vulnerabilities are likely to be well beyond the point at which the application can be quickly and easily remediated.

In reality, application vulnerabilities need to be treated like any other software defect: early and often. The security department will always perform oversight assessments and check for application vulnerabilities as part of any certification measures, but the most effective measures are those that take place throughout the entire life cycle of an application. Years of metrics have proven that finding and

fixing functional and performance bugs is easiest, cheapest, and generally most effective the earlier they are discovered. The same is true with security bugs. A developer that has the awareness, education, and tools to conduct unit tests for security is considerably more likely to produce more secure code than one that does not. Likewise, Quality Assurance (QA) groups should be taught to test for security and given the appropriate tools to do so. Personally, I find QA a very efficient place for security testing for a variety of reasons, not the least of which is that they "carry the hammer." Development staff are well aware that their work is not complete until it passes QA testing. QA groups are also highly effective at finding bugs and getting them fixed. With the right security testing technology, they can easily begin checking for security related defects, along with functional and performance defects, without changing their work process.

Ultimately, though, it's awareness that begins the entire process. All too often, developers believe that the security department handles all aspects of security, and that developers don't play a role. Until the full scope of the many ways of attacking software is presented, it's easy for developers to be blissfully unaware of potential security issues in their code. Once someone shows them all the ways they can create vulnerabilities in their code—often just by using what are generally accepted (yet poor) coding techniques—they tend to become impassioned about writing secure software, especially if their security is going to be tested by others. After all, no one wants his or her code to be the chunk that got hacked. But overall, writing secure code is about quality. As Michael Howard explains in his book, Writing Secure Code, "secure software is a subset of quality software and reliable software." Nothing could be truer. As the paradigm of writing secure software spreads, everyone will benefit from the side effects of mature, secure code.

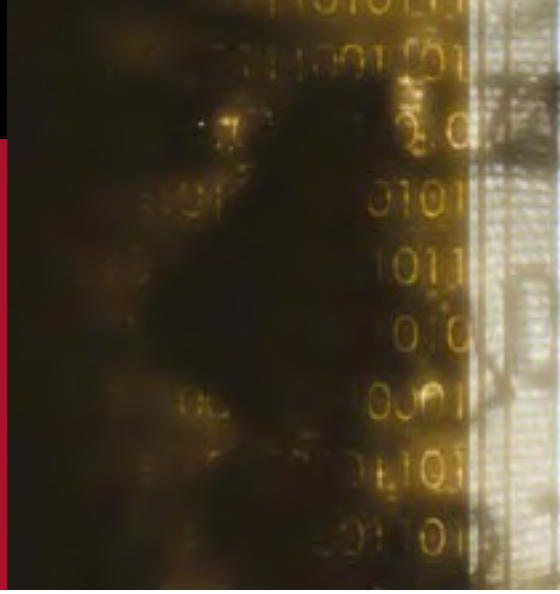
In the end, of course, it's the decision of the organization. Companies can wait to get hacked or caught off guard by an unflattering security assessment, or they can proactively implement a secure coding program throughout their development environment. As SQL Injection enters its eight year, I highly recommend the latter. ■

About the Author

Matthew Fisher | is a Senior Security Engineer for SPI Dynamics, a Web application security assessment and testing firm and acts as a subject matter expert for the DISA IATAC. He has performed hundreds of web assessments throughout the DoD and is a frequent speaker at security and development conferences. Mr. Fisher was also a contributing author to the book, Google Hacking for Penetration Testers and is currently working on his own book, Web Application Security : A Guide for Developers and Penetration Testers. Prior to beginning his computer career, Mr. Fisher spent six years in a reserve Infantry battalion.

Viruses, Worms, and Trojan Horses Welcome Here!

by Rusty Baldwin



The Center for Information Security Education and Research (CISER) at the Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, OH, will soon unveil a powerful network-emulation facility. This facility, the Cyber OpeRations Emulator (CORE), is a global-scale network-emulation test bed that provides DoD, researchers, and students a unified, efficient, and flexible framework for studying malicious code and DoD network operations.

The CORE architecture is based on the proven and fielded Emulab (*http://www.emulab.net*) and PlanetLab (*http://www.planet-lab.org*) emulation environments which enables CORE to configure and control hundreds of rack-mounted PCs and network devices. The CORE's users can precisely specify a network configuration to emulate, including network-topology and packet-transmission characteristics such as line speed, packet loss, and latency. Application software can also be installed on the CORE's nodes and tested under realistic conditions.

The CORE's Unique Capabilities

When fully operational, the CORE will possess unique capabilities that make it particularly valuable for defense research. For instance, the CORE was specifically designed to research malicious activities such as the introduction of viruses, worms, and Trojan horses into networks and network nodes. This alone makes the CORE an invaluable asset, since most networks do not the intrusion of such malicious software for fear of its spreading beyond the confines of the network. Since the CORE can be disconnected from other networks, there is no danger of malicious software spreading beyond the confines of the network environment. Furthermore, after experiments are completed, all persistent storage elements in the CORE are scrubbed and replaced with known clean images, removing any traces of malicious code.

Another unique capability is the CORE's operating modes. The CORE can simultaneously operate in two distinct modes:

- A research mode, such as that described above, for high-fidelity study of networks.
- A "network-simulator" mode for realistic network-operations training.

In its "network-simulator" mode, one or more operator consoles (OPERATOR) are populated with network-operation tools, while a "network simulation" controller console (CONTROLLER) monitors and directs the training session. The CONTROLLER can submit automated scenarios to the CORE or inject specific network events or attacks into the network at will to which OPERATOR(s) respond in real time. The CORE's "network simulation" mode brings an exceptional level of realism into network training and can also be easily used for human-factor studies.

Finally, the CORE's Graphical User Interface (GUI) makes it easy to quickly and efficiently specify a network topology, workload, and operating characteristics. The CORE uses a commercial network simulator as a graphical front end to specify network configurations and scenarios. This has many advantages. By using GUI software, network topology, traffic, and "users" can be quickly specified by using built-in objects or by creating custom objects. These are then exported as an eXtensible Markup Language (XML) file that is automatically mapped to the CORE's hardware for emulation. While being emulated by the CORE, this same network could, if desired, be simulated to compare with emulation results. The GUI software can also be used to specify a network for the network-simulator mode by including a CONTROLLER node and the appropriate number of OPERATOR consoles in the network. Thus, the CORE provides a remarkable level of flexibility and opportunity for both research and realistic training.

The CORE's Concept of Operations (CONOPS)

Figure 1 shows the essential steps in the CORE Concept of Operations (CONOPS).

- In the Step 1, a CORE user specifies the network using the GUI software.

Although a relatively small-sized network is shown in Figure 1, for purposes of illustration, an enterprise-wide network, including a global network with hundreds of nodes, could be specified and emulated.

- In Step 2, an XML description of the network is submitted to the CORE Configuration Manager (CCM) for mapping to the CORE's hardware.
- In Step 3, the CORE switches are configured, PC disk images loaded, and experimental scenarios are readied for execution.
- During execution, metrics and logs file entries (Step 4) are recorded. After the emulation is complete, metrics and logs are transferred to specified locations for later analysis. If the CORE is in network-simulator mode, OPERATOR(s) and CONTROLLER interact with the CORE in real time.

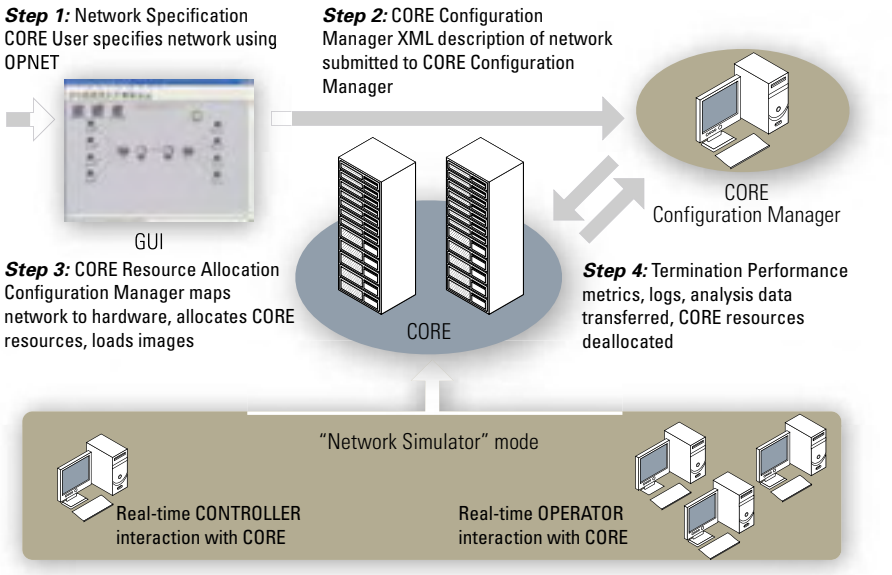


Figure 1 The CORE's Concept of Operations

Current Status and Configuration

The CORE is operational and currently supporting multiple research efforts. However, in its current state of development, it must be manually configured. We have one person working full-time on integration and software development. We expect to achieve the operating capability described above within the next year.

The CORE consists of four equipment racks with almost 100 rack-mounted PCs; four switches and four routers that support GB Ethernet, access-control lists, multicast management, Internet Protocol (IP) routing, and traditional Local Area Network (LAN) switching; and other hardware that provides limited, remote-access capability and power control of the CORE. Network traffic generation and collection of performance data is currently performed using host-based software. We plan to purchase a router switch, 36 additional rack-mounted PC's, and hardware-based traffic generators this year.

The CORE's Impact on Education

The CORE provides an invaluable platform for research-related education in a wide range of areas. Each year, approximately 90 students take our courses in Distributed Software Systems, Introduction to Computer Networking, and Computer Communications Networks. In these courses, the most effective learning takes place by observing and interacting with real systems in operation. Using the CORE as a virtual laboratory will significantly enhance the learning experience in these courses. Each student will be able to simultaneously implement and change the configuration of actual networks and distributed systems, observing the results of their changes in real time. Students performing simulation-based projects

can use the CORE as a validation platform for their simulations.

The CORE will also make a unique contribution to the research-related educational areas of secure software design, computer security, analysis of malicious code, and computer attack tools and techniques. For obvious reasons, many research facilities do not permit malicious software applications or code such as worms and viruses on their sites—malicious software could damage or destroy equipment or operations. However, such code and applications must be studied in a controlled environment to understand how they operate, to determine their attack profiles, and to devise effective and efficient detection and prevention countermeasures. The CORE provides the ideal environment for such education and research. When viruses and other malicious code are released into the CORE, they can be studied "in action" by using the CORE's instrumentation at the same time yet are restricted to the CORE environment. The effects of the malicious code can also be transferred to a benign environment for further study in support of our computer forensics courses. Clean images for network devices and nodes replace the infected images, and the CORE nodes and devices used in the study are then released back into the common resource pool.

The CORE's Impact on Research

The most significant impact the CORE will have on current research efforts is the unified, efficient, and easily reconfigurable environment it provides. These capabilities enable multiple researchers to focus on the research problem at hand rather than on unique instrumentation for a particular effort. Selected CISER research efforts are presented below and include a description of how the CORE might be used in each.

- **Security Metrics**—Security metrics are an indispensable tool to measure the effectiveness of various components of a network, the services and processes it provides, and the ability of an organization to defend the network against attack. However, a set of generally accepted security metrics has not yet been developed. Our research in security metrics is focused on developing strategic, tactical, and operational security metrics for weapon systems. A methodology and framework for measuring, testing, and logging the security and performance of deployed systems and supporting networks will provide command staff with enhanced decision-making capabilities. Furthermore, operational metrics provide valuable feedback to design teams on the effectiveness of security technologies and protocols in different theaters of engagement. The CORE can be used in this effort by organizing nodes in a strategic, tactical, or operational configuration and measuring traces of actual traffic as it flows through the network. From an analysis of this data, effective metrics can be proposed and their effectiveness evaluated.
- **Insider Threats in Computer Networks**—Insiders represent a significant security challenge because they are trusted. We have two active research thrusts on insider threats. First, individual communication patterns are being assessed to identify behavioral anomalies indicative of a malicious activity. Second, we are developing an insider-threat ontology to build specific measures for detecting and stopping activities that circumvent or undermine the protection state of a secure network. Using the CORE network-simulator mode, a human-factors analysis of volunteer-network user actions can be recorded and studied to discover identifiable behaviors that may suggest an insider threat.
- **The Global Information Grid (GIG)**—The CORE will become a basic research tool in our support of the National Security Agency's (NSA's) Information Assurance research for the Global Information Grid (GIG). Although the CORE's architectural concept was developed independently of the NSA, it incorporates many of the same elements of the NSA's Information Assurance Modeling and Simulation Plan. [1] Both the NSA and the CORE use the same GUI simulation software as a simulation engine. The CORE also uses GUI software to specify network topologies to be mapped to the CORE hardware for high-fidelity network emulation. In this area, we add additional value and capabilities to NSA efforts by validating simulations and providing an even higher-fidelity emulation capability for critical design decisions or performance analyses in the GIG. Although not currently part of the CORE, the NSA also envisions using different software to capture operational and system views of the GIG. This software can easily be incorporated into the CORE operation as an architectural front end to the GUI software. ■

References

[1] National Security Agency, Information Assurance (IA) Modeling and Simulation Plan Version 1.0, Information Assurance Architecture and Technical Framework Office (I11), 30 June, 2004.

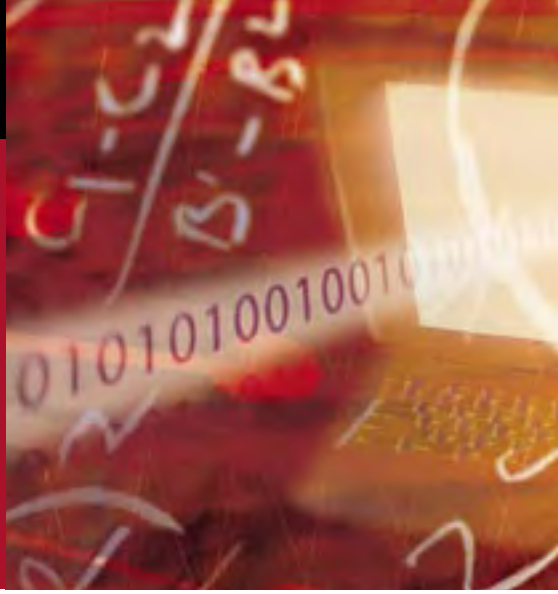
About the Author

Dr. Rusty Baldwin | is an Associate Professor of Computer Engineering at the AFIT. He earned a Bachelor of Science, Electrical Engineering (BSEE) degree with Honors from New Mexico State University in 1987, a Master of Science (MS) degree in Computer Engineering in 1992 from AFIT, and a PhD degree in Electrical Engineering from The Virginia Polytechnic Institute and State University in 1999. Dr. Baldwin's research interests include computer-communications protocols, software engineering, information warfare, computer architecture, and wireless networks. He is a senior member of the Institute of Electrical & Electronics Engineers (IEEE) and a member of Eta Kappa Nu. Dr. Baldwin may be reached for more information on the CISER or the CORE at 937/255-6565, ext 4445, or by e-mail at rusty.baldwin@afit.edu.

Dr. Rayford Vaughn, Head of Computer Security

Mississippi State University

by Pius Uzamere II



IATAC Spotlight on Research

This article is the fourth in a series of profiles of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) program. Information Assurance (IA) and Information Operations (IO) experts from many different organizations volunteer to be IATAC SMEs and to provide information on their areas of expertise, education and training, professional certifications, inventions, and patents. When DoD or other government personnel contact IATAC with questions regarding IA or IO, IATAC can leverage its SME database to identify those who are particularly well suited to answering those questions. SMEs are also encouraged to contribute papers and other materials to IATAC's collection of Scientific, Technical, and Operational Support Information (STOSI). The work of the SMEs furthers understanding and capabilities in IA.

The IATAC SME profiled in this article is **Dr. Rayford Vaughn**, head of the Center for Computer Security Research (CCSR) [1] at Mississippi State University (MSU) [2]. His primary areas of research include Software Engineering and Information Security. Dr. Vaughn received a PhD in Computer Science from Kansas State and spent 26 years in the military, retiring as a colonel.

One area of research Dr. Vaughn pursues is Intrusion Detection (ID) within high-performance computer clusters. This research abstracts the concept of the computer cluster in a manner that deals with both macroscopic clusters such as labs with hundreds of workstations and microscopic clusters such as those located in the cone of an aircraft or missile, for example. This problem is interesting not only because of the high value associated with such clusters but because of design constraints inherent in the solution to the problem; namely, any ID scheme must not slow down the performance of the cluster. Ongoing research at the CCSR has made novel use of hidden Markov models to quickly identify anomalous behaviors or patterns. These algorithms facilitate the rapid combination and analysis of disparate sensor data, a concept called "sensor fusion."

Dr. Vaughn and his students have also helped pioneer new methods of threat modeling using exploitation graphs. Exploitation graphs are built from the results of vulnerability scanners, known system-vulnerability data, and system-configuration data to provide a specific profile of how an attacker may exploit a given system. Graphs created by Dr. Vaughn's team can be used to systematically and precisely describe the minimum set of vulnerabilities that must be mitigated to prevent an attack or predict how attack strategies are likely to change as a function of changing network topology and the ongoing mitigation of vulnerabilities. These approaches are very useful for characterizing Return On Investment (ROI) from various Information Technology (IT) strategies. As most IA practitioners can attest, providing hard numbers on ROI can be a difficult problem. The threat-modeling approaches developed at MSU's CCSR can provide a powerful new tool in the arsenal of any IA professional confronted with the need to justify the cost of vulnerability mitigation

Questions for Dr. Vaughn or other IATAC SMEs may be sent to *iatac@dtic.mil.* The IATAC staff will assist you in reaching the SME best suited to helping you solve the challenge at hand. If you have any questions about the SME program or are interested in joining the SME database and providing STOSI to others in your domains of expertise, contact *iatac@dtic.mil* and the URL for the SME application will be sent to you.

Reference

[1] *http://www.security.cse.msstate.edu/*

[2] *http://www.msstate.edu*

▷▷ *Authors Bio page 32*

DOWN with Trusted Devices

by Mahalingam Ramkumar

There is an ever-growing need for "trusted" devices and assurances from the technology industry of tamper resistance and read proofing of secrets stored in such devices. We discuss a simple security policy—Decrypt Only When Necessary (DOWN)—and its implications for the security of secrets stored in trusted computers. The DOWN policy, used in conjunction with the emerging paradigm of Physical Unclonable Functions (PUFs), can be a promising approach for realizing trusted computers.

Introduction

In many emerging applications that will rely on extensive mutual co-operation among a highly interconnected network of computers, an important requirement is the ability to *trust* the devices. Trusted devices [4] are expected to possess "unflinching" morals. They will *not* trust the owners or controllers of devices (the human operators) and cannot be directed to do something that violates the rules they are entrusted to obey. Practical realization of trusted devices calls for two fundamental assurances—*tamper resistance and read proofing.* [5] Tamper resistance is necessary to ensure that the software controlling the devices (which govern the morality of a device) cannot be changed. Read proofing is necessary to ensure that secrets from a trusted device (which will be used for authenticating the device) cannot be transferred to untrusted devices.

DOWN, a simple security policy, can substantially improve the ability of trusted computers to protect their secrets. The emerging paradigm of PUF [6], used in conjunction with the DOWN policy, can further improve trustworthiness of computers. The need for the DOWN policy stems from the realization that, while it may be possible to protect the secrets stored in a trusted computer when the computer is *in use* and when the computer is *at rest,* the *transition* period—when the computer goes from in-use to rest state—is perhaps the most vulnerable period. The DOWN policy seeks to *avoid explicit transitions.*

Trusted Computers

Trusted computers can function at two fundamental states—in use or at rest. Obviously, secrets must be protected during both states. While the computer is in use, it is possible to use many sensors that actively monitor for intrusions and delete secrets when tampering attempts are suspected. Attackers could monitor electromagnetic radiations from chips to gain clues about the secrets stored inside. But using proper shielding could prevent this. [8] Some attacks are also based on inducing faults in memory [9] and using differential power analysis [10], [11]. Another approach for attackers is to use sophisticated Focused Ion Beams (FIB) [12] to drill fine holes and establish a connection with the computer buses, thereby monitoring the bits that traverse the buses. In Ref. [13], the manufacturers claim to protect against FIB attacks by employing "active shields."

While rest encryption [14] is commonly used to protect databases at rest, the problem of rest encryption for trusted devices is very different. For the former, the secret used for encrypting the contents of the database is typically stored *outside* the database. For the latter, as trusted computers *will not trust anyone else with their secrets,* the secret used for encrypting the contents should be stored inside the trusted computer. Obviously, the secret should be protected at rest, which calls for a continuous power supply to the devices, even when they are at rest, to monitor for potential intrusions and erase the secret when an intrusion is sensed.

Rest Encryption With PUFs

The evolving paradigm of PUFs [6,15] provides a very satisfactory solution for rest encryption. To provide an unclonable, unique, Physical One-Way Function (POWF) or a "random oracle," Silicon PUFs exploit uncontrollable statistical delay variations of connections and transistors etched on substrates in each manufactured chip. The response of the random oracle (PUF) to some randomly chosen query could be used to encrypt

the secrets at rest. The challenge (or query) itself could be safely stored in Non-Volatile Memory (NVM). When the device is at rest, there is no way for an attacker to query the PUF to determine the key used for encrypting the secrets.

One practical problem associated with PUFs is that the random oracle may drift with temperature and aging. Gassend, *et al.* [6] argue that it is possible to employ error-correction codes to compensate for the drift.

Protecting Secrets During State Transition

The transition from in use to rest will typically involve (1) encrypting all keys for storage with a key and (2) *clean erasure* of all secrets stored in volatile memory. While the second step may at first sound redundant, it is, in fact, required to ensure that the secrets temporarily stored in volatile memory do not leave a "footprint." Such footprints left behind in magnetic and solid-state memories [18] could be used to decipher the previous contents of the memory, especially if the footprints had been stored in a memory location for long periods. Safe erasure [19] of contents in magnetic and solid-state memory (or removing all traces of their footprints) may require many *repeated* overwriting operations.

To render an attack more worthwhile, the attacker's strategy may be to induce a "glitch" attack that causes the computer to "hang." Even if some sensors, which work independently of the Central Processing Unit (CPU), detect intrusion attempts, they may not be able to perform the repeated overwriting operation needed for safe erasure. Thus immediate cooling following a glitch attack can be very productive for an attacker, who may be able to extract all secrets from footprints in Random Access Memory (RAM). The ability of an attacker to scavenge bits is also significantly enhanced by cooling the device.

In general, using hardware-protection mechanisms for protecting a *single* secret could be easier than protecting multiple secrets. For example, such a secret—say K_v—can be stored in a special CPU register, hidden even from the Operating System (OS) kernel. [1] Various techniques could be used to ensure that K_v does not leave a deep footprint in memory such as periodic *ones complementing* (perhaps every few milliseconds). However, this should be performed in hardware to ensure that this process continues to occur even if the CPU hangs. While the device is powered on, it may also be possible to protect some limited areas of volatile RAM by not providing clear-line-of-sight access; however, it may not be practical to use ones-complementing techniques for contents of RAM (to avoid footprints).

If multiple secrets must be protected, K_v secrets can be encrypted with . However, the process of encryption of all secrets with K_v has to be performed *without* transferring K_v to the RAM, where it cannot be protected from scavenging attacks, or encryption must be done in hardware. This could be easily achieved if the CPU has exclusive access to a hardware block cipher. In other words, secrets can be well protected as long as they must not be transferred to RAM. Secrets that are stored in RAM, especially for extended periods, are more susceptible to tampering attacks involving "abnormal state transitions," as it may not be possible to perform a "clean erasure" of the RAM's contents.

When the device is at rest, there is no way for an attacker to query the PUF to determine the key used for encrypting the secrets.

The DOWN Policy

If the RAM's contents cannot be well protected following abnormal state transi-

IATAC New Addres
Continued S

ss, New Look, Service

By the time you receive this issue of the *IAnewsletter*, the Information Assurance Technology Analysis Center (IATAC) will have relocated to its new, larger home in Herndon, Virginia, an outer suburb of Washington, DC. Our new mailing address and telephone number will be:

IATAC
13200 Woodland Park Road, Suite 6031
Herndon, Virginia 20171
Phone 703/984-0775
Fax 703/984-0773

Only our physical location and phone number will be affected by this move—there will be no interruption to your *IAnewsletter* subscription, or to the many IATAC services you have come to expect and rely on.

You may also notice that this issue of the *IAnewsletter* introduces a new look. From its debut in 1997 as a 6-page, office-style publication to its present 32-page, 4-color format, the *IAnewsletter* has evolved with IATAC to continuously provide information assurance (IA) professionals throughout the Department of Defense, government, research and development (R&D), industry, and academia with a trusted forum in which to share ideas.

If you have a previously unpublished article that you would like to share with our over 7,200-member audience—whether a technical paper, overview, discussion of lessons learned, or warfighter perspective "from the trenches"—please see *http://www.iatac.org/IA_newsletter.html* for submission guidelines.

Our focus has been—and remains—to bridge these diverse organizations while helping synchronize the IA community Your involvement is the key to IATAC's continuing success. ■

tions that may be induced by an attacker, one solution is to ensure that the RAM has very minimal information *at any time*. The DOWN policy recognizes that most cryptographic operations have some inherent *atomicity*. At any time, only one or even a small part of a secret may be necessary for cryptographic computations.

For instance, if the secret to be protected is a Rivest-Shamir-Adleman (RSA) private exponent *r,* and *n* represents the RSA modulus, decryption of some cipher text *C* involves modular exponentiation of *C* with *r.* Or $P = C^r \bmod n$. However, to perform the exponentiation, only *one bit* of *r* is needed at any time (*e.g.,* exponentiation using the square-and-multiply algorithm). We could thus keep *r* encrypted at all times and decrypt each bit *as and when necessary.*

Without the DOWN policy, abnormal state transitions induced by an attacker may imply compromise of the *entire* private key *r. With* DOWN, however, if proper care is taken—if, for instance, the decrypted bits are always stored in the same memory location in the special cache memory (and therefore overwrite each other—an attacker can discover at most *1 bit of the RSA private key.* The main advantages of the DOWN policy are as follows:

- It provides a guarantee that *not more than a small fraction* of secrets stored in trusted devices can be compromised by the attacker.
- NVM, where the secrets are stored, *does not need any* protection.

Trusted Computer Architecture with DOWN

DOWN-enabled trusted computers will host a hidden CPU register for storing K_v and a hardware block cipher or a hash function *h()*, also hidden from the OS kernel. The secret K_v could be generated at random using various inputs. DOWN-enabled CPUs will support a few additional CPU instructions.

(1) *GenerateSecret(),* which, seeded by various random inputs, generates a secret K_v and stores it in a hidden register.
(2) *EncryptSecret(K_i, i),* which will return for example, $E_i = h(K_v, i) XOR K_i$.
(3) *DecryptSecret(E_i, i),* which returns $K_i = h(K_v, i) XOR E_i$.

Each cryptographic operation (*e.g.,* decryption using the private key) is broken down into many elementary *DOWN operations.* Each DOWN operation will involve the following:

(1) Fetching the i^{th} encrypted secret E_i from NVM
(2) Calling *DecryptSecret(E_i, i)* to get K_i
(3) Using K_i in a cryptographic algorithm
(4) Flushing traces of K_i from RAM
(5) Storing intermediate results in RAM

In the example of RSA, if each bit is encrypted separately, the decryption process would involve 1024 DOWN operations. On the other hand, if 128 bits are decrypted at a time, the process would involve only eight DOWN operations.

For rest encryption, CPUs with a PUF (or a random oracle) *H()* and a hardware hash function (or block cipher) *h()* will support two additional instructions:

(1) *EncryptMasterKey(C,R_N),* which returns $K_E = K_v XOR H(h(C \| R_N))$, and
(2) *DecryptMasterKey(C,R_N,K_E)*

Before a device goes to the rest state,

(1) A random challenge, *C,* and a random nonce, R_N, are generated and stored in NVM.
(2) *EncryptMasterKey(C,R_N)* is called to get K_E.
(3) K_E is stored in NVM.
(4) K_V is erased from the hidden register.

When the CPU boots up, it fetches K_E and *C* from NVM, and the call *DecryptMasterKey(C,R_N,K_E)* is made. When this call is finished, K_V is restored in the hidden register.

"DOWN-Friendly" Key-Distribution Schemes

It is not intuitive [2] that *how well secrets are protected* could depend on the *nature* of secrets to be protected. However, the realization of the DOWN policy is intricately tied to the Key Distribution Scheme (KDS) that is used. Some KDSs "lend themselves better" to DOWN implementation. For example, it is easy to ensure DOWN policy for RSA for decryption and digital signatures. However, extending the DOWN policy for other public-key schemes not based on modular exponentiation are not obvious and may not even be possible.

Even for RSA, strictly implementing the DOWN policy may not be feasible unless it is possible to ensure DOWN even for the process of *generating* the public-private key pair. However, schemes based on symmetric-key cryptography can be more easily extended to accommodate imposing the DOWN policy.

Another class of key-distribution schemes that benefit substantially from the DOWN policy are Key Pre-distribution Schemes (KPS) [20]. KPS schemes use only symmetric-key cryptography. Unlike Kerberos-like schemes, KPSs do not require the ongoing involvement of a trusted server for mutual authentication, which is a very important requirement in many emerging application scenarios involving *ad hoc* networks.

However, while KPSs cater to *ad hoc* authentication without using expensive asymmetric-cryptographic primitives, the secrets provided to each device are interdependent. By compromising secrets from a finite number of devices, an attacker can compromise the entire KPS. There is thus a concept of *n*-secure KPS. An *n*-secure KPS can resist compromise of

all secrets from n devices. Typically, n can be increased arbitrarily by increasing the number of keys, k (the size of the key-ring), assigned to each device. [3]

The DOWN policy can increase the security of KPSs *dramatically* for the following two reasons:

(1) The policy can ensure that an attacker can expose no more than one secret by tampering with a device, which renders an n-secure KPS nk-secure.

(2) As the secrets are stored in NVM, which does not need any protection, external flash memory can be used for storing the secrets. (New flash-based SD/xD cards on the market have up to 8Gb of storage). Thus it is possible to increase k to further increase security.

Even among KPSs, some [19,20,21] are more "DOWN friendly." While for most KPSs, increasing the key-ring size k directly translates to increased computational complexity, for a certain class of KPSs, called random KPSs, it is possible to increase k-and therefore the security: nk, the attacker coalition size that can be resisted—*without* increasing the computational complexity. In other words, to improve security, some KPSs can take full advantage of the "practically unlimited" insecure storage complexity that could be provided by inexpensive flash-based storage. Some of our ongoing research focuses on:

(1) Extending DOWN policy to asymmetric ciphers that do not employ modular exponentiation;

(2) Investigating KDSs in light of DOWN complexity;

(3) Searching for novel, DOWN-friendly KDSs; and

(4) Investigating a new "dimension" in security-complexity trade-offs; *i.e.*, improving security by leveraging insecure storage complexity. ■

References

[1] Hiding a secret from the kernel ensures that attackers cannot tamper with the software and thereby direct the CPU to "spit out" the secret K_V.

[2] How does the ability to protect a secret depend on whether the secret is an RSA private key or a Kerberos password?

[3] For efficient KSPs, k is linear in n.

[4] A. Pfitzmann, B. Pfitzmann, M. Schunter, and M. Waidner, *Mobile User Devices and Security Modules: Design for Trustworthiness.* IBM Research Report RZ 2784 #89262 02/05/96, IBM Research Division, Zurich, Feb. 1996.

[5] R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali, T. Rabin, *Tamper Proof Security: Theoretical Foundations for Security Against Hardware Tampering.* Theory of Cryptography Conference, Cambridge, MA, February 2004.

[6] B. Gassend, D. Clarke, M. van Dijk, S. Devadas, *Silicon Physical Random Functions.* Proceedings of the 9th ACM conference on Computer and communications security, pp 148–160, 2002.

[7] J.P. McGregor, R. B. Lee, *Protecting Cryptographic Keys and Computations via Virtual Secure Coprocessing.* ACM SIGARCH Computer Architecture News archive, 33(1), March 2005.

[8] R. Anderson, M. Kuhn, *Low Cost Attacks on Tamper Resistant Devices.* IWSP: International Workshop on Security Protocols, Paris, April 1997.

[9] S. Skorobogatov, R. Anderson, *Optical Fault Induction Attacks.* Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), LNCS 2523, Springer-Verlag, ISBN 3-540-00409-2, pp 2–12.

[10] P. Kocher, *Differential Power Analysis.* Advances in Cryptology, CRYPTO 1999, Springer LNCS series, Vol 1666, pp 388–397.

[11] M.G Karpovsky, K. Kulikowski, A. Taubin, *Robust Protection Against Fault-Injection Attacks of Smart Cards Implementing the Advanced Encryption Standard.* The Proceedings of Int. Conference on Dependable Systems and Networks (DNS 2004), July, 2004.

[12] O. Kommerling, M. Kuhn, *Design principles for tamper-resistant smart-card processors.* Proceedings of the Usenix Workshop on Smartcard Technology, pp. 9–20, 1999.

[13] P. Laackmann, B. Meier, H. Nguyen, Infineon Technologies, *Revolution In The Smart Card Security. http://www.epn-online.com/page/11955/revolution-in-the-smart-card-security-physical-attacks.html*

[14] IEEE P1619—Standard Architecture for Encrypted Shared Storage Media. *http://siswg.org/docs/*

[15] D. Lim, *Extracting Secret Keys from Integrated Circuits.* Masters Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May 2004.

[16] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems.* John Wiley and Sons, 2001.

[17] P. Gutman, *Secure Deletion of Data from Magnetic and Solid-State Memory.* Sixth USENIX Security Symposium, San Jose, CA, July 1996.

[18] R. Blom, *An Optimal Class of Symmetric Key Generation Systems.* Advances in Cryptology: Proc. of Eurocrypt 84, Lecture Notes in Computer Science, 209, Springer-Verlag, Berlin, pp. 335–338, 1984.

[19] M. Ramkumar, *Safe Renewal of a Random Key Pre-distribution Scheme for Trusted Devices,* 6th IEEE Information Assurance Workshop (The West Point Workshop), United States Military Academy, West Point, NY, June 2005.

[20] M. Ramkumar, N. Memon, *An Efficient Random Key Pre-distribution Scheme for MANET Security.* IEEE Journal on Selected Areas of Communication, March 2005.

[21] M. Ramkumar, *I-HARPS: An Efficient Key Pre-distribution Scheme.* Cryptology ePrint Archive, 2005/138, May 2005, *http://eprint.iacr.org/2005/138.pdf*

About the Author

Mahalingam Ramkumar | has been an Assistant Professor in the Department of Computer Science and Engineering at Mississippi State University since August 2003. He was a Research Professor at Polytechnic University, Brooklyn, NY, from September 2002 to July 2003 and Co-founder and Chief Technology Officer of PixWave.com Inc. from March 2000 to August 2002. His research interests include security under resource constraints, ad hoc and sensor networks, and data hiding. He has published over 50 conference papers, seven journal articles, and one book.

Network Security Monitoring: Beyond Intrusion Detection

by Richard Bejtlich

It is fashionable in the security community to consider so-called Intrusion Prevention Systems (IPSs) as replacements for Intrusion Detection Systems (IDSs). The logic seems to be that stopping an attack ("prevention") is better than just telling someone about it ("detection"). This reasoning seems sound, but it is flawed. This article argues that the IPS is not a superior replacement for the IDS. Both technologies have flaws as well as benefits. However, proven methods exist to address the shortcomings of both, while retaining the value each system delivers to the enterprise.

Three problems hamper IPS technology. First, most vendors assume their products can accurately and consistently identify attacks. Unfortunately, no combination of signatures, anomaly detection, or other heuristics has yielded a system that reliably identifies a wide range of malicious activity. Achieving highly accurate detection usually involves decreasing the number of rules applied to a packet or traffic flow. Certain vendors commendably recognize this situation in an explicit manner by assigning probabilities to their alerts. Some vendors are also applying greater degrees of network context to the process that creates alerts, but these efforts do not alter the underlying problem of identifying attacks.

Even systems that do not employ signatures (so-called "behavioral anomaly" systems) cannot reliably identify attacks. These products seek to find events that stand out when compared to a baseline of "normal" activity. Unfortunately, baselines can be difficult to establish in operational networks. When the anomaly detection system reports, it can also be frustrating to understand how and why the product made its determination.

Second, intrusion prevention, as currently fielded in commercial products, completely inverts the traditional access control security model. An IPS is supposed to recognize "bad" traffic and prevent it from attacking the enterprise. All other traffic not identified by the IPS as being malicious is allowed to pass. This contradicts the "allow what's good, deny all else" security model used in most effective access control policies. For example, a proper access control policy might allow port 80 Transmission Control Protocol (TCP) to the Web server and port 25 TCP to the mail server while rejecting all other traffic. An IPS is a "deny what's bad, allow all else" appliance. Denying the bad only works when "bad" can be recognized in all its forms—and that cannot be achieved.

Finally, IPSs build on the same technology and research that hampered IDSs, and thereby IPSs inherit IDSs' inherent weaknesses. This article's first point mentioned the inability to recognize all attacks, and the second explained problems caused by inverting the access control model. This third problem unites IPSs with IDSs, as both are alert-centric security devices. In the vendor's mind, the job of each product is to identify an attack or intrusion and then take some action. An IDS generates an alert, and an IPS drops the evil traffic. Those actions are the end goal for each system. What happens when the system fails to notice an attack or intrusion? In each case, the malicious traffic sails by, with no record of its existence.

This article proposes an alternative way forward, beyond intrusion detection. This path does not lead to intrusion prevention. It is important to realize that an IPS is just the latest evolution of the network firewall. The original stateful packet filter made its pass or block decision by using Open System Interconnection (OSI) Layer 3 Internet Protocol (IP) address and OSI Layer 4 (port) information. The IPS now makes its access control choices using OSI Layer 7 (application content) data as well. Some vendors even call their solutions "intrusion-prevention firewalls," while others use the term "deep packet inspection." In all cases, a convergence between the layer 3–4 firewall and the layer 7 IPS will result in a single appliance making access control decisions by inspecting traffic. Marketing departments are responsible for the similarity in names between the IDS and IPS, but the former is a transaction logging device, and the latter is an access control device.

This article's proposed path does not lead to enhanced access control, although it agrees that the IPS' granular blocking ability is a powerful defensive tool. Rather,

this article's recommendation relies on realizing the importance of network transaction logging and appropriate data collection. IPS proponents need to think more as their firewall brethren do, who understand the role of access control in network architectures.

Prevention is not always possible or even preferred when security is at stake. In some situations, it may not be technically or politically feasible to enforce a restrictive security policy. In other cases, it may not be possible to strictly define malicious activity before it appears, or it may be too expensive or intrusive to do so. Anywhere prevention cannot be implemented, detection and transaction logging must be applied instead. In fact, everywhere prevention is active, detection and transaction logging must also be applied. Without detection and transaction logging, how can one be sure the prevention system is performing its job?

This appreciation for the importance of network-centric detection and transaction logging is codified in a framework called Network Security Monitoring (NSM). NSM is defined as the collection, analysis, and escalation of indications and warning to detect and respond to intrusions. NSM is an operational model inspired by the US Air Force's Signals Intelligence (SIGINT) collection methods and by Todd Heberlein's "Network Security Monitor" software, which became the Automated Security Incident Measurement (ASIM) sensor that watches all Air Force bases.

SIGINT is the collection of information on communications and the transformation of that information into intelligence products. Similarly, NSM collects and analyzes network traffic to identify and validate intrusions. NSM uses full content, statistical, session, and alert data to help analysts make decisions. Whereas intrusion detection and prevention cares more about identifying and/or blocking attacks, NSM provides evidence to scope the extent of an intrusion, assess its impact, and guide effective remediation steps. In this sense, NSM is related to pure network forensics in which keeping track of all traffic for purposes of remediation, prosecution, or pursuit is the goal.

NSM is effective against "unstructured threats," such as script kiddies and worms, but the framework is more concerned with more sophisticated intruders. These structured threats employ stealth, encryption, zero-day exploits, and advanced back doors for which no IDS or IPS strategy has been devised. To meet these challenges, the NSM philosophy follows three principles:

- Some intruders are smarter than you.
- Intruders are unpredictable.
- Prevention eventually fails.

The consequences of believing these principles means traditional alert-centric intrusion detection and prevention must be supplemented by methods that are more content neutral. By using content-neutral techniques and tools, analysts have a chance of gathering the right data to identify, contain, and remove intruders operating beyond the field of view of the IDS or IPS.

NSM's key insight is the need to collect data that describes the network environment to the greatest extent possible. By keeping a record of the maximum amount of network activity allowed by policy and collection mechanisms, analysts buy themselves the greatest likelihood of understanding the extent of intrusions. The four NSM data forms are as follows:

- Full content data
- Session data
- Statistical data
- Alert data

Not all NSM operations will be able to collect all this information for technical or legal means. However, the greater the variety of data one collects, the better off he or she will be. The following paragraphs briefly explain the four types of NSM data and their uses.

Full Content Data

Full content data is the header and application layer information contained in packets traversing the network. Full content data offers two compelling features that make collecting it worthwhile: granularity and application relevance. Granularity refers to the capture of every nuanced bit in a packet. If an intruder uses a covert channel that depends on the value of an arbitrary bit in a TCP header or layer 7 field, collecting full content data will preserve that evidence for inspection. Application relevance refers to saving the information passed above the transport layer. The process of differentiating among normal, suspicious, and malicious traffic often requires seeing the data passed between parties on the Internet. Even visually confirming encrypted payloads can be valuable, if an analyst realizes that encrypted traffic is abnormal within the context of the investigation at hand.

Full content data is the most expensive form of network-based evidence one can collect. It can be difficult to engineer and deploy hardware and software sufficiently robust to capture significant traffic on a busy network. Software and hardware have not scaled their performance to match increases in network bandwidth usage. Network processors and packet-oriented hardware are overcoming some limitations of commodity PCs, but bandwidth and Packets Per Second (PPS) counts still test vendors' best efforts. Still, it can be invaluable to have the infrastructure in place to collect whatever subset of full content data one's hardware and software permits. Something is always better than nothing in a security scenario, and often that "something" is enough to tip the case in a positive direction.

Session Data

Session data, also known as flows, streams, or conversations, is a summary of a packet exchange between two systems. Session data collected completely independently of full content data is preferred. The basic elements of session data include the following:

- Source IP
- Source port
- Destination IP
- Destination port
- IP Protocol—*e.g.,* TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP)
- Time stamp—generally when the session began
- Measure of the amount of information exchanged during the session

Although the concept of a "port" most frequently applies to TCP and UDP traffic, session data is not limited to those protocols. NSM analysts collect session data for ICMP, Encapsulating Security Protocol (ESP), and so on.

> No IDS or IPS can be as effective as a human analyst, sufficiently trained and equipped and working with the most relevant data available.

From the standpoint of a network investigation, full content data is more valuable than session data. Full content data can be sliced and diced in any number of ways by multiple tools. Because collecting full content data can be nearly impossible on high-traffic links, one turns to session data as the next-best approximation of conversations between parties. Session data is relatively cheap to collect, and many enterprise-grade networking devices can export session data (*e.g.,* in the form of NetFlow records) if configured appropriately.

Statistical Data

Statistical data is a description of activity designed to highlight deviations from norms. Full content data offers the ultimate level of granularity. Session data moves one step above by omitting content and collapsing packets into flows or conversations. Statistical data jumps even higher by summarizing broad categories of network traffic. Monitoring network load, or percentage of bandwidth occupied by peer-to-peer clients, or the frequency of attempts to connect to a certain port are examples of collecting statistical data.

Observe that collecting full content data, session data, and statistical data is a content neutral affair. One does not base the traffic-capture decision on any individual aspect of any of these forms of data. Filters might be used to reduce the amount of packets logged to disk, but one should not consciously filter traffic expected to offer evidence of intrusion.

The fact that NSM advocates collecting traffic, regardless of a predetermination of security value, shows how the framework handles smart, unpredictable intruders. If an analyst can't be sure what piece of data will help her detect and respond to an intruder, she should grab as much data as her legal and technical means allow. Once one or more forms of NSM data have provided a pointer for additional investigation, she can turn to other NSM data already saved or begin augmented collection to improve her incident response and remediation efforts.

Alert Data

Alert data is different when compared with full content, session, or statistical data. Alert data is a judgment made by a software product concerning the nature of an observed network event. Alert data is not content neutral, because the decision to generate it is based on a product's decision that something is "bad" about the traffic causing the alert. Traditional IDSs produce

alert data to notify operators that something suspicious or malicious is happening on the network. Generating accurate alerts is typically the *raison d'etre* for IDS vendors. Unfortunately, if these traditional systems fail to identify suspicious or malicious activity, they usually record no other data of use to a security analyst. IPSs operate in a similar manner, except their purpose is blocking.

Alert data is important because it helps direct human analysts to investigate events of interest. Because it is difficult for most humans to manually inspect network traffic, it is beneficial to encapsulate the experience of security engineers into code and algorithms that notice odd network activity. If the primary purpose of an IDS is to raise the red flag but provide no supporting data to justify its decision, then the analyst will find the IDS opaque, frustrating, and often worthless. The IPS is no different. Consider these two scenarios, one implementing NSM, the other not:

Scenario 1
An analyst's IDS device reports a suspicious event. He has no way to independently validate the incident and isn't sure he can even trust the alert. He opens a trouble ticket and forwards it to the point of contact responsible for administering the target machine. If he is worried enough, he calls the client to ask him to investigate a potential compromise. He knows little about the circumstances of the incident. He resumes working and doesn't realize his IPS completely ignored traffic related to the suspicious event, because it didn't recognize what it was seeing. By default the IPS lets unrecognized traffic pass.

Scenario 2
At another site, a second analyst's IDS reports a suspicious event. She consults her alert, session, and full content data. She trusts her IDS because she can validate its findings using multiple, independently collected NSM data. With no further alerts from the IDS, she determines an intruder exploited a vulnerable Microsoft SQL server, causing it to retrieve three files via File Transfer Protocol (FTP). Her session data shows the FTP server is active, and she verifies the nature of the intrusion by examining the files transmitted during the FTP session.

Searching backwards through her session logs, she finds the initial exploitation of the vulnerability and learns exactly how the intruder compromised the victim. Armed with this information, the analyst calls the local system administrator. She explains the situation and offers suggestions for remediation, since she knows almost everything that has happened to the victim machine. Once the administrator is satisfied, the analyst classifies the relevant alerts on her display and appends her username, taking responsibility for her actions.

The analyst applies new rules to her IDS and IPS that alert and block appropriately, based on new information retrieved during her investigation. She resumes working, ready to provide network forensics should the client decide to pursue the intruder in court.

Implementing an NSM operation does not typically involve purchasing thousands of dollars of new hardware or software. Collecting full content data can easily be done with free tools such as Tethereal (*http://www.ethereal.com*), the command-line version of Ethereal that simplifies capturing traffic in a hard drive ring buffer. Session data can be obtained from routers that export flow data, and open source tools such as Argus (*http://www.qosient.com/argus*), the Security Analyst Connection Profiler (SANCP, *http://www.metre.net/sancp.html*), and Flow-Tools (*http://www.splintered.net/sw/flow-tools/)* offer cheap yet powerful session-data alternatives. Free tools such as Ntop (*http://www.ntop.org*) and the Multi Router Traffic Grapher (MRTG, *http://www.mrtg.org*) with the Round Robin Database (RRD) Tool offer network trending statistics. Supplemental alert data is available in the Snort open source IDS /IPS (*http://www.snort.org*).

If an analyst is looking for a fairly complete open source NSM implementation, Sguil (*http://www.sguil.net*) is a compelling option. Sguil provides alert data from Snort, session data from SANCP, and full content data from Tcpdump or a second instance of Snort. Sguil packages all of this information in a user-friendly, non-Web-based interface. Security analysts have been running Sguil in production environments for over three years, as well as several Fortune 500 companies that also have Sguil in production.

When considering NSM, the idea is not to replace existing infrastructure. Rather, security architects should determine what NSM data is missing and then begin collecting it. Putting NSM data in the hands of network analysts gives them the best chance to identify, contain, and remediate intrusions—especially when confronting clever attackers using novel tools and techniques. No IDS or IPS can be as effective as a human analyst, sufficiently trained and equipped and working with the most relevant data available. ■

About the Author

Richard Bejtlich | is founder of TaoSecurity *(http://www.taosecurity.com),* a NSM consulting and training company, and the TaoSecurity Blog *(http://taosecurity.blogspot.com).* He wrote *The Tao of Network Security Monitoring: Beyond Intrusion Detection* (Addison-Wesley, 2005), *Extrusion Detection: Security Monitoring for Internal Intrusions* (Addison-Wesley, 2006), and co-authored *Real Digital Forensics* (Addison-Wesley, 2006). He began his security career as a captain in the Air Force Computer Emergency Response Team in 1998.

Air Force Enterprise Defense (AFED)—A Lightweight, Adaptable Security Information Manager (SIM)

by Brian Spink, Martin Sheppard, and Richard Wood

The Air Force Research Laboratory (AFRL) developed Air Force Enterprise Defense (AFED) to provide an extensible, highly configurable system to integrate and manage diverse security information assets, including sensors, firewalls, databases, and decision-support tools. The system's modular components are available at no cost to Government users.

The Challenge

A Security Information Management (SIM) system is able to detect, protect, assess, and react to intrusion attempts and network anomalies. Flexible information integration is a key to meeting this requirement for several reasons:

- Integrating diverse sensors and analysis tools is key to robust detection of and response to information security events. As sensors and other tools evolve, the SIM must be able to take advantage of new technology.
- A SIM installation needs to integrate site-specific data sources such as data related to mission(s), network topology, and asset management.
- A SIM must provide flexibility to address site-specific Concept of Operations (CONOPS).
- A SIM must be able to report high-priority and/or aggregated data to higher-level SIMs.

AFED Overview

Figure 1 illustrates how AFED provides these integration capabilities through an open, modular, highly configurable, and extensible architecture that is not available in most SIM systems. AFED reduces the workload of network operation and security analysts by combining data sources and reducing the number of events and alerts, while providing access to in-depth information for investigation, analysis, and response. AFED provides a number of benefits for network security personnel:

- It accepts, correlates and aggregates, stores, and displays data from multiple sources—Intrusion Detection (ID) sensors, firewalls, vulnerability-assessment tools, network mappers, System Log (Syslog) servers, wireless ID sensors, and external databases.
- It provides fast access to critical analysis data, including correlated alerts, raw events, host vulnerabilities, host Operating Systems (OSs), host services, Points of Contact (POCs), locations, and missions.

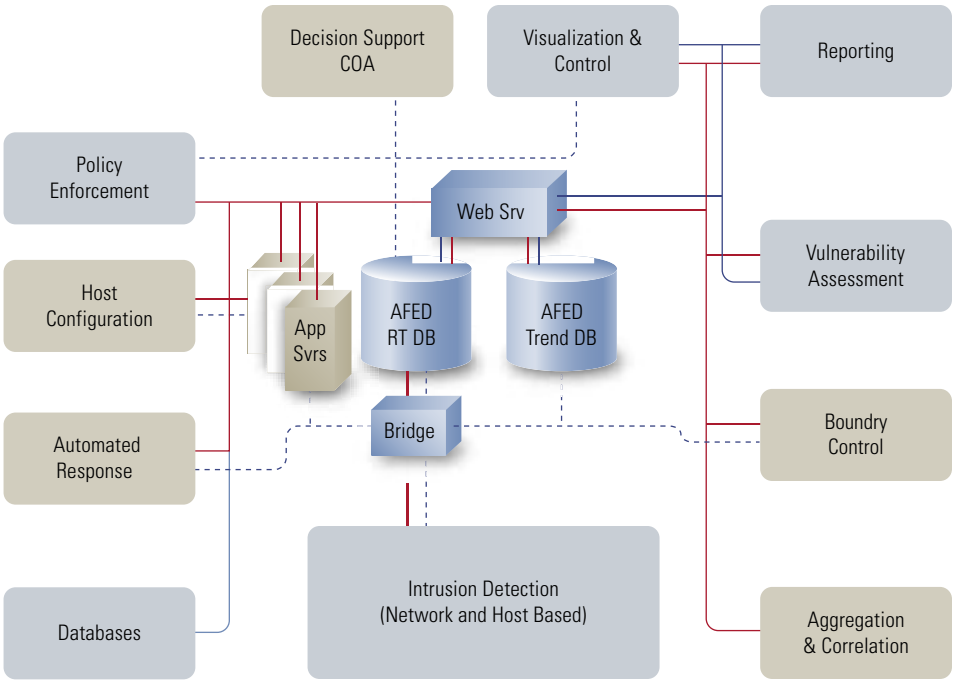


Figure 1 AFED Architecture

- Through aggregation, correlation, and filtering, it reduces the volume of raw events that must be analyzed. Reductions of two to three orders of magnitude are typical.
- It permits analysts to define multiple data views with aggregation, filtering, and color codes to help identify specific types of events.
- It integrates external applications in a single console and user interface.

AFED Functions and Components

AFED comprises a suite of open, configurable components that can be deployed on a wide range of hardware. These components are modular and can be deployed separately or in combination. A complete AFED system consists of the following.

Sensors and Data Acquisition

AFED supports a wide range of sensors, including the following:

- Wired and wireless Network-Based IDs (NIDS) and Host-Based IDs (HIDS)
- Vulnerability scanners
- System and audit loggers
- Boundary devices (firewalls, routers)
- Network discovery tools

AFED integrates sensors using the *Data Extraction Utility* (DEU), a highly configurable data-collection module, shown schematically in Figure 2.

The DEU extracts data from a text file or database, such as Syslogs, firewall logs, eXtensible Markup Language (XML) documents, and sensor specific databases, and from the output of processes such as Operating System (OS) utilities. It maps the extracted data values to configurable data elements, transmits the data securely across the network, and delivers it to AFED's database or to another data consumer. Customized data filtering, aggregation, and transformation are supported through a "plug-in" interface. DEU can implement automated event reporting and/or response through its ability to launch external processes based on data content.

The DEU assures robust, reliable data transmission through features including the following:

- Automatic start, re-start, and recovery
- Data-rate control

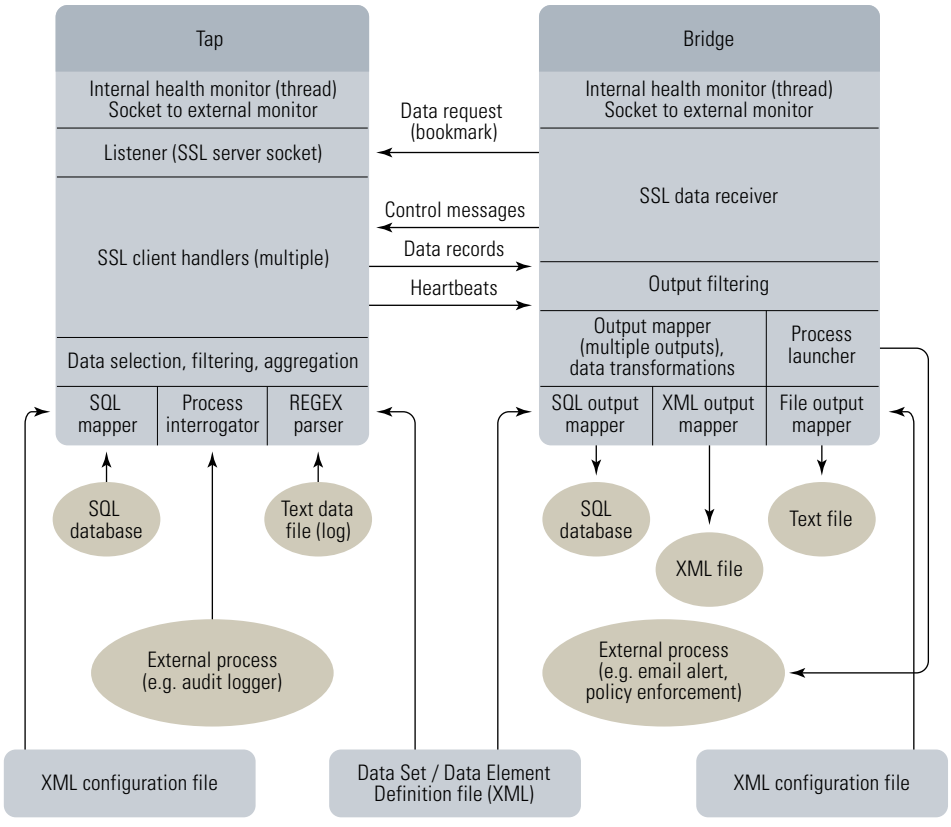


Figure 2 Data Extraction Utility (DEU)

- Data bookmarking—A "bookmark" of successfully transmitted data assures that data is not lost or duplicated if network connectivity is lost or a platform re-boots.
- Multiple data paths—Data from a single source can be transmitted to multiple recipients.
- Secure Socket Layer (SSL) data transmission
- Sensor-health monitoring

The DEU has been used to acquire data from the sensors shown in Table 1.

AFED System Server and Database

A central server provides the core SIM functions and database. Solaris-, Linux/Intel-, and Windows-based servers are supported. To demonstrate this, self-contained AFED systems have been deployed on Windows laptops.

Multiple servers are also supported for either hierarchical systems or distributed processing.

AFED's real-time database manages data including the following:

- High-level (correlated) alerts
- Events generated by NIDS, HIDS, and other sensors
- Vulnerabilities
- Asset management
- Event status and reporting

AFED's reference database is Oracle 9i. AFED supports central database implementation on other database platforms that are compliant with Java Database Connectivity (JDBC) such as Postgres or MySQL. Moreover, because of AFED's highly configurable architecture, a wide range of database schemas can be accommodated, including existing databases (*e.g.*, existing asset-management and personnel databases). Also supported are multiple databases hosted on multiple database systems and multiple platforms.

Source/Sensor	Supplier/Type	Data Type
Snort	SourceFire/Network intrusion detection system (IDS)	MySql database
Antura	System Detection/Network IDS anomaly detection system	Postgres database
Daiwatch	Lockheed Orincon/Host-based IDS/anomaly detection	Oracle database
Pix Firewall	Cisco Systems/Firewall	Syslog
TCP wrappers	Hot-based IDS	Syslog
DSIM	Air Force Information Warfare Center/ Hot-based IDS (firewall)	XML
WIDS	Air Force Research Laboratory/Wireless IDS	Text (Syslog)
Windows Event Logs	Microsoft/Open Source Event forwarder	Syslog
Iptables	Linux Open Source	Syslog

Table 1 Sensors Integrated Using DEU

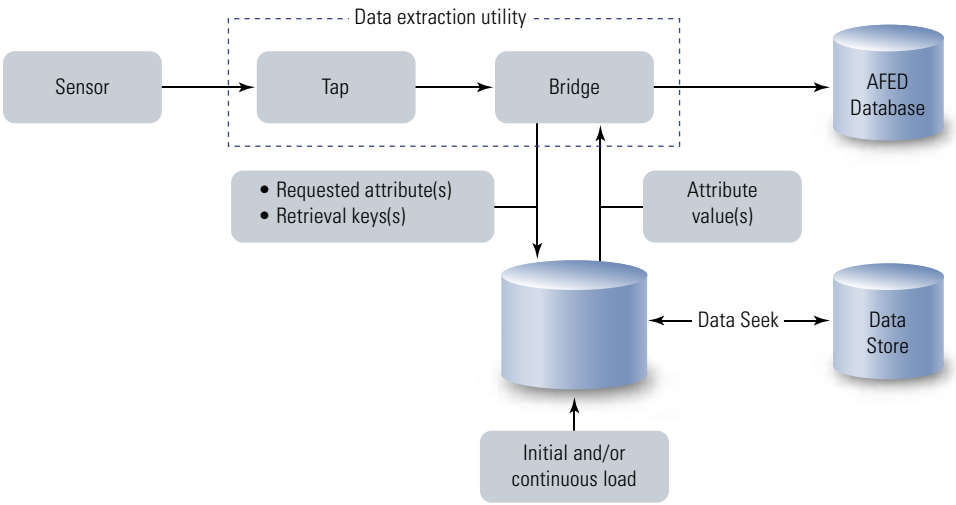


Figure 3 Caching Correlator

Trending/Archive Database

AFED provides a *Trend Database* for data trending, long-term analysis, and archiving, which is hosted on a separate server platform. The Trend Database is also used for data backup and archiving.

Data Normalization

Data normalization is the process of associating similar or related events from disparate sensors, usually through standardized naming and/or categorization. AFED accomplishes normalization by using a *Caching Correlator*, operated in conjunction with the DEU, shown in Figure 3.

The Correlator is pre-loaded with normalized event types and associated retrieval keys such as sensor and signature names. As event records pass through the DEU, key value(s) are used to retrieve an event's normalized type.

Data Fusion

The process used for data normalization can also be used to fuse other, related data to incoming events:

- Event categorization and prioritization
- Host-related data such as mission, location in enterprise network topology, OS, and accreditation data
- Host vulnerability to event
- Compliance with site-security policy
- Internet Protocol (IP) address-range registration data (owner, country, POC) and internal *vs.* external IP address ranges

Data Correlation

AFED is designed to integrate a variety of third-party correlators, including advanced correlators under development by AFRL.

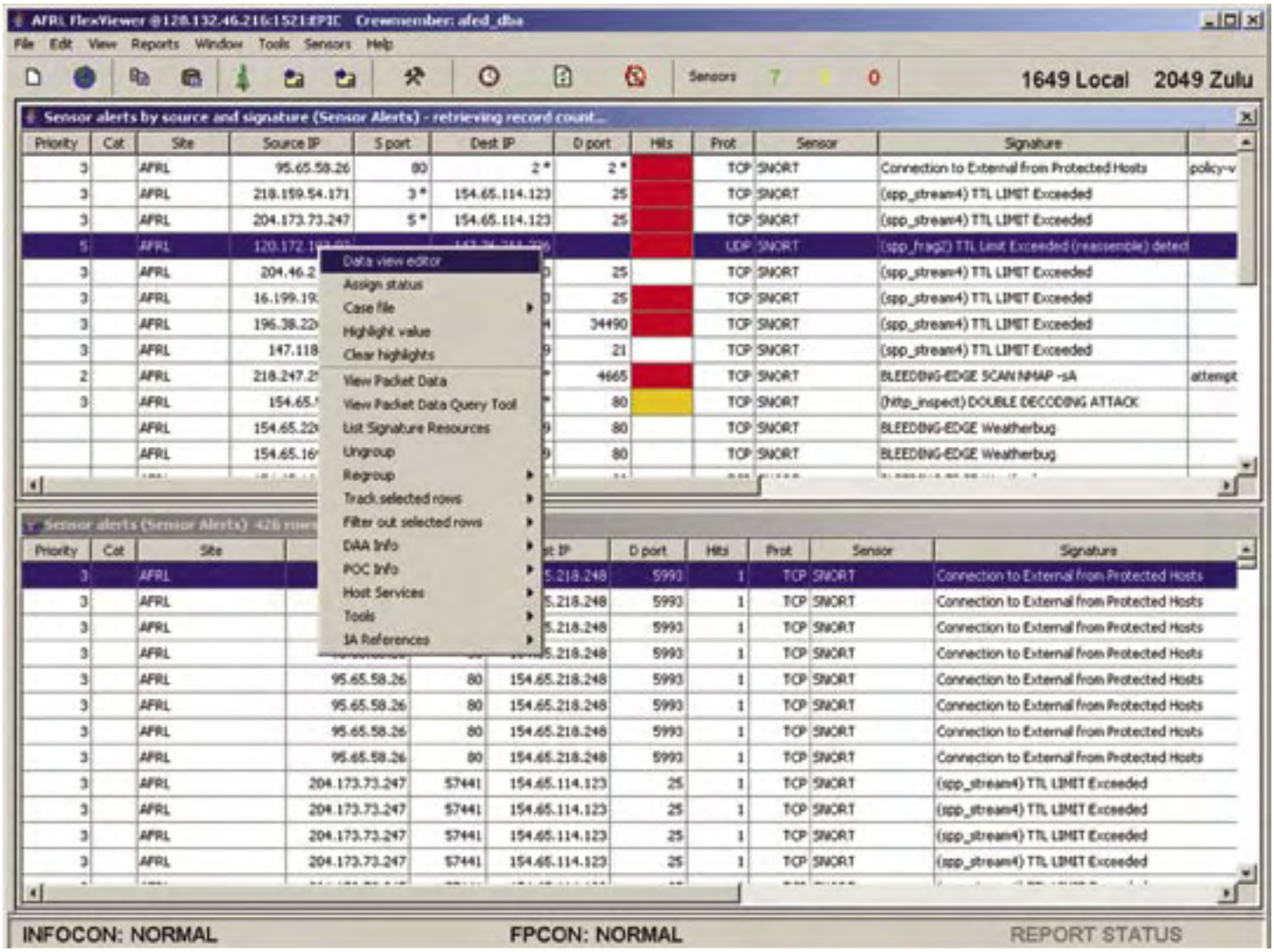


Figure 4 Sample FlexViewer Display

AFED provides an *SQLCorrelator* that supports correlation rules defined by an analyst using a graphical editor. The rules are implemented as SQL database queries. The Correlator polls an event database and generates "correlated events," which represent groups of events that satisfying these rules. The Correlator is able to implement rules that represent combinations of event types, such as signatures, and thresholds on event frequency.

Visualization and Control

AFRL's *FlexViewer* provides AFED's data visualization. FlexViewer is an extensible, highly configurable data-visualization and manipulation environment that provides an analyst with extensive analytical tools and a high degree of control over data presentation. Figure 4 shows a typical FlexViewer display.

FlexViewer's principal features include the following:

- **Configurable data definition**—FlexViewer can be configureWd to present virtually any data from any JDBC-compliant database. This is accomplished through an XML metadata file that defines the data to be presented. This feature supports site-specific tailoring of data sources, use of existing databases (without modification or import and export), and addition and modification of presented data over time.
- **Multiple Data Sets**—FlexViewer displays are constructed from *Data Sets*, packages of data defined in the configuration metadata. The Data Set defines columns, associated data fields, and data types to be displayed. An unlimited number of Data Sets can be defined and presented in independent windows, giving an analyst immediate access to these data sources. For example, high-priority alerts could be displayed in one presentation, vulnerabilities in a second, and asset-management data in a third. Each Data Set definition specifies its database source and connectivity, thereby permitting data from multiple databases to be seamlessly presented.
- **User defined data views**—A FlexViewer display is defined by a *Data View*, which applies user-

specified data grouping (aggregation), sorting, filtering, color coding, and other parameters to a Data Set. Filtering and color coding are based on rule-like logical expressions that can be constructed using any column(s) in the Data Set. Data Views are created using a graphical *Data View Editor*, are saved by user, and can be shared. Analysts have reported that constructing data views that reflect their own thought processes, viewing different aggregations of the same data, and highlighting patterns using color codes greatly aids in recognizing attack patterns.

- **Configurable drilldowns**—An Analyst's task often involves locating and analyzing data related to one or more alerts and answering questions such as "What is the OS of the affected host?" "What activity has been seen previously from a potential attacker?" FlexViewer provides drilldowns to support these tasks.

  FlexViewer drilldowns allow an analyst to select one or more events and records of interest and to "drill down" into other data sets (or the same data set) to create a view of related data. For example, an analyst might drill down from selected events in a view of IDS alerts to asset-management information for the affected hosts.

  Drilldown relationships are defined in FlexViewer's configuration metadata, making these relationships completely configurable. The definition specifies cross-data-set relationships (*e.g.*, "Show asset data for hosts that are target IP addresses of the selected alerts."), filtering and grouping operations, and the pop-up menu caption by which the drilldown option is displayed and invoked.
- **Integrate tools and third-party applications**—FlexViewer's drilldown engine is used to seamlessly integrate external tools by launching them using data selected in an AFED display. Examples include:
  - Network discovery and vulnerability scanners,
  - "Who-is" utilities such as McAfee Neotrace Pro, and
  - Web sites such as Common Vulnerabilities and Exposures (CVE), Intelligence Collection Analysis Team (ICAT), and the Internet Storm Center.

A Java XML scripting engine allows AFED's functionality to be extended without coding. XML scripts can implement specialized tasks and/or define extended graphical interfaces. This resource has been used to retrieve and display raw packet data from a sensor, to provide a sensor-configuration interface, and to generate custom reports. Tool integration is configured in the same manner as are drilldowns, thereby providing great extensibility.

Applications

A representative application of AFED's components could include the following capabilities:

Sensor Integration and Normalization
The DEU is used to securely deliver data to AFED's central database from multiple NIDS, dispersed on subnets across the enterprise, and from HIDS. These sensors can include open-source Snort, proprietary, and/or Research & Development (R&D) sensors, because the DEU can be configured to map their native data to the appropriate AFED data elements and to normalize the various sensor signatures to standardized names.

The DEU extracts, parses, and generates alerts from relevant Syslog data on selected hosts. This data may include unsuccessful logons, excessive repeated logons, and execution of suspect applications.

Data Fusion
The Correlator, operating in conjunction with the DEU, identifies IP addresses involved in alerts as inside or outside the enterprise and fuses the country of origin, domain owner, and threat level to incoming IDS events.

Multiple Database Integration
Existing asset-management and vulnerability-tracking databases on separate corporate database platforms are integrated by defining FlexViewer Data Sets for these sources. Drilldowns permit viewing asset data (*e.g.*, mission, criticality, location) for selected alerts or viewing the thread level (*e.g.*, alert count) for selected critical assets. NIDS and HIDS events are color coded red when the target asset is mission critical.

Third-Party Tool Integration
FlexViewer's drilldowns provide tools for event analysis, including retrieval of raw packet data, vulnerabilities associated with the event type, and IP address-identification tools.

Correlated High-Level Alerts
The SQL Correlator creates high-level cyberalerts. Correlation rules can be defined based on the site's experience and concept of operations. The following are examples of detected conditions that could generate a cyberalert:

- X or more distinct outside IP addresses generate alerts for a single inside host in an eight-hour period.
- An outside IP address generates alerts involving Y or more critical inside assets in a four-hour period.
- Z or more distinct event signatures are generated for any inside asset in a 12-hour period.

AFED has also been applied to:

- Computer system mis-use detection
- Managing and visualizing audit-log data
- Loading data from static sources and files or across database platforms
- IP address anonymization
- Control of wireless access points to enforce security policies

Conclusion

Integrating data and tools is key to an effective, sustainable SIM system in today's rapidly evolving security environment. AFED provides this integration capability through a modular, configurable, non-

proprietary suite of tools that is available at no cost to Government users.

AFED was developed as an in-house program of AFRL's Information Grid Division, with major contributions from a contractor team including Booz Allen Hamilton, Dolphin Technology, ITT Industries Advanced Engineering & Sciences, and Northrop Grumman Information Technology. For further information, AFRL's Brian Spink may be contacted at brian.spink@rl.af.mil. ■

About the Authors

Brian Spink | is a Senior Electronics Engineer at the United States Air Force, Air Force Research Laboratory Rome Research Site, working in the Distributed Computing Branch on Network and Security Enabling Technology. He began his career with Rome Air Development Center in 1980 in the Satellite Communications Branch. He has a Bachelor of Science Degree in Electrical Engineering from Clarkson University and a Master of Science Degree from Syracuse University. He has been working in the Computer Network Security area for the last 12 years with the formation of the Information Warfare Team at Rome Laboratory.

Martin Sheppard | is a Senior Security Engineer in Rome, NY, where he provides on-site support for Dolphin Technology with the Air Force Research Laboratory (AFRL) Rome Research Site. Martin holds a Bachelor of Science Degree in Computer Science from the State University of New York Institute of Technology. Martin has been working in the Computer Security area since 1991 with Multi-Level Secure Routers, Security Guards, and Multi-Level Distributed Operating Systems. Martin is currently one of the Lead System Engineers for AFRL's Security Management Systems research. Martin served as a Network Security Analyst in a number of Air Force experiments including the Expeditionary Force Experiments (EFX) and Joint Expeditionary Force Experiments (JEFX). Martin also participated in a number of security exercises while working for The MITRE Corporation. Sheppard functions as a key interface between the AFRL Defensive Information Warfare (DIW) Laboratory and the AFRL Rome Research Site Network Operations Center (NOC). Martin is working to transition Advanced Technology sensors and management tools from research into operational use. Martin supplements NOC personnel by monitoring the Rome Research Site with various sensors and security management systems and has assisted in the investigation of various security incidents in support of daily operations.

Richard Wood | PE, CISSP, is a Principal Engineer for ITT Industies-AES in Rome, NY. He is currently working on data collection, transport and visualization software applications for the Defensive Information Warfare Branch of the Air Force Research Laboratory Information Directorate. He holds a BS degree in Electrical Engineering from Brown University, and has done graduate study in Public Administration and in Solid State Science. From 1993 through 1995 he directed the Knowledge Based Technology Applications Center sponsored by the Electric Power Research Institute.

Letter to the Editor

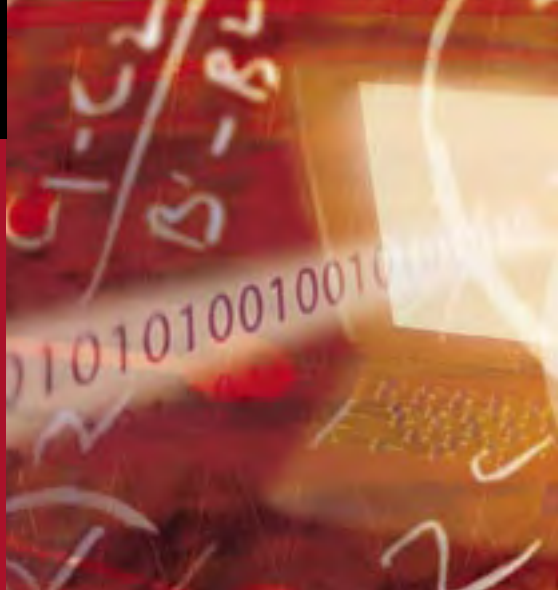
Q ***While attending the 2006 DoD Cyber Crime Conference in Tampa FL, there was talk about Directive 8570.1, Information Assurance Training, Certification, and Workforce Management, and the new Manual implementing this Directive. Could you please tell me a bit more about 8570.1?***

A DoD Directive 8570.1, signed 15 August 2004, lays the framework to train, certify, and manage the DoD Information Assurance (IA) workforce. This Directive requires every IA technical personnel technician and IA management personnel manager to be trained and certified to a DoD baseline requirement. This requirement policy applies to every full-time and part-time DoD IA workforce member, including military personnel, civilians, foreign and local nationals, and contractors—regardless of occupational specialty or job series, or whether the IA functions are performed on a full-time, primary-duty basis or as an embedded duty. The Directive's vision and goal is to have a sustained, professional IA workforce with the knowledge and skills to effectively protect against and prevent and respond to attacks against DoD information, information systems, and information infrastructures. Ultimately, DoD wants this effort to put the right people with the right skills in the right place.

The DoD Manual 8570.1M, signed 19 December 2005, implements the corresponding Directive. The Manual 8570.1-M provides guidance for the identifying and categorizing positions and for certifying personnel who conduct Information Assurance (IA) functions throughout the DoD Global Information Grid (GIG). The Manual identifies two categories of IA workforce: Technical and Management. These categories are further subdivided into three levels (I, II, III), based on skill and environment. These various categories and skill levels provide determine specific training and certification requirements, which are provided in the Manual.

To permit planning, budgeting, and identification requirements, DoD will use a phased approach to implement the 8570.1. The first year allots time to fulfill the above requirements and to certify the first 10% of the IA workforce to be trained and certified. In the subsequent three-year period, at least 30% of the IA workforce must be brought into compliance.

For additional information, please contact IATAC at 703/984-0775 or on its Web site at iatac@dtic.mil. An electronic copy of these documents may be found at *http://www.dtic.mil/whs/directives.* ■



Mississippi State University

by Pius Uzamere II

IATAC Spotlight on Education
This article is the second in a series that spotlights important activities in Information Assurance (IA) education and research and describes the latest projects in some of the nation's best IA academic centers.

The program profiled in this article is the Center for Computer Security Research (CCSR) [1] at Mississippi State University (MSU) [2]. One of Mississippi State's most prestigious programs, CCSR is lead by Dr. Rayford Vaughn, Director.

MSU has the distinction of offering a top-notch cybersecurity program within its CCSR and of also being the nation's first public institution to offer bachelor's degree in Software Engineering accredited by the Accreditation Board for Engineering and Technology (ABET). This program recognizes the importance of applying strong engineering and design methodologies to developing software, rather than to focusing solely on pure computer-science principles. Combining a strong theoretical foundation with practical experience gained by working with real industry clients, MSU's Computer Science and Engineering Department prepares its software engineering graduates for real-world issues surrounding product life cycles and their IA implications.

Since its inception in 2001, CCSR has grown to 13 faculty members, with five PhD students expected to graduate this year. CCSR offers a wide array of graduate-level IA courses, enabling graduate students to continue their research on a variety of topics. Examples of topics addressed by graduate research students include industrial espionage, steganography, phishing, distributed operating systems, computer forensics, biometrics, cyberdefense, cryptography, and embedded software protection.

CCSR offers opportunities to students through its robust Cybercorps Scholarship Program. The program includes both the Scholarship for Service, funded by the Office of Personnel Management (OPM) and the National Science Foundation (NSA), and the Information Assurance Scholarship Program funded by the NSA. This program benefits over 20 students, some of whom are fully funded by the scholarships that include even housing assistance. During summer breaks, students typically accept internships with government agencies, providing both extra financial support and an important link to real-world implementations of IA principles.

Perhaps the greatest impact of CCSR is its extensive partnership with law-enforcement agencies, in which agents and officers learn how to investigate computer crimes ranging from phishing attacks to cyberterrorism against national infrastructure systems. Most law-enforcement officials, especially on the local level, are not taught the unique rules of evidence regarding electronic systems or the investigative skills necessary to properly discover evidence in the first place. CCSR is bridging a major gap through programs like the Cyber Crime Fusion Center. This center, led by Dr. David Dampier, marks an unprecedented partnership with the State Attorney General, the Secret Service, local law-enforcement officials, and other entities to ensure that law-enforcement officers are well prepared for the unique challenges inherent in responding to cyber crime. Recently, CCSR was given $2.5M in Department of Justice (DOJ) grants for these programs. ■

Reference

[1] *http://www.security.cse.msstate.edu/*
[2] *http://www.msstate.edu*

About the Author

Pius Uzamere II | does privacy and security consulting, primarily in the Federal sector. Mr. Uzamere is the primary author of the Bluetooth security chapter in the textbook RFID: Applications, Security and Privacy (Addison Wesley, 2005). In addition, he assisted the National Institute of Standards and Technology (NIST) in developing the privacy section of the new Federal identification system standard document, Federal Information Processing Standard 201 (FIPS 201). Mr. Uzamere holds a Bachelor's degree in computer science and engineering from the Massachusetts Institute of Technology.

IATAC Attended Conferences

American Computer Machinery (ACM) Computer and Communication Security

IATAC attended the 12th Annual American Computer Machinery (ACM) Computer and Communication Security (CCS) conference in Alexandria, VA. ACM is an international scientific and educational organization dedicated to advancing the arts, sciences, and applications of information technology. The Special Interest Group on Security, Audit, and Control (SIGSAC), a subgroup of ACM, sponsored the conference, which was held 7–11 November 2005 at the Hilton Alexandria Mark Center. Doug Maughan from Cyber Security Research & Development (R&D), Department of Homeland Security (DHS), delivered the keynote address. Forty–one academic papers were presented on topics including privacy and anonymity, trust management, authentication, cryptography, intrusion detection and prevention, and key management. These papers provided insight into the future of computer and communication security by outlining many technologies years before they may be available to the commercial market. Along with academic papers was an industry track, including *EGAD–A Unique Anomaly Detection Framework for Protecting Critical Infrastructure Against Cyber Attacks* by Robert Ross and James Reynolds and full–day workshops such as *Digital Identity Management, Rapid Malcode*, and *Secure Web Services*. Lastly, there were several tutorials, *Common Ways Cryptography is Mis-used and How to Get It Right* by John Black, University of Colorado at Boulder; and *Designing Deception Operations for Computer Security: Processes, Principles, and Techniques*, by Fred Feer, Professional Consultant, and Jim Yuill, North Carolina State University. The Defense Advanced Research Projects Agency (DARPA), the US Army Research Office, Microsoft Research, IBM Research, and mobile communications company NTT Do Co Mo of Japan sponsored this event. More information, including this year's conference proceedings and information about next year's conference, may be found at *http://www.acm.org/sigs/sigsac/ccs.html*.

Computer Security Applications Conference (ACSAC)

The 21th Annual Computer Security Applications Conference (ACSAC), sponsored by the Institute for Electronic and Electrical Engineers (IEEE), was held 5–9 December 2005 in Tucson, AZ. Daily conference began with a distinguished speaker, including Brian Snow of the National Security Agency (NSA), who discussed the ways in which assurance factors could be improved in operating systems, applications, and hardware by developing better environments, requirements definitions, systems engineering, quality certification, and legal and regulatory constraints. Next, Mary Ellen Zurko of IBM Corporation delivered an address on roadblocks at social, technical, and pragmatic levels that must be overcome by user–centered security. The remainder of the conference included tracks on several topics during which academic papers were presented and critiqued by peers. Tracks included Software Security, Network Intrusion Detection, Security Designs, Protocol Analysis, Vulnerability Assessment, Security Analysis, Data Integrity, and Malware. The best paper award was given to six individuals from the University of California, Berkley, for *Model Checking an Entire Linux Distribution for Security Violations*. The authors have created a tool that views the source code of a Linux distribution for bugs, even before the code is installed. At the time the paper was published, their tool had found 108 exploitable bugs in Red Hat 9. IATAC was also directly involved in the conference. Our Chief Scientist, Ron Ritchey, chaired a session on Vulnerability Assessment and also presented a paper from his recent research results entitled, *A Host-based Approach to Network Attack Chaining Analysis*. More information about this conference and future ACSAC conferences may be found at *http://www.acsa–admin.org*. ■

IATAC Conference and Event Planning

IATAC

Experienced Assistance for Your Classified or Unclassified Event

Are you a government client in need of planning and hosting assistance for an upcoming conference? Look no further… IATAC's conference and event planners provide the assistance you need.
Since 1998, we have offered a full range of services to support classified and unclassified conferences, meetings, and other gatherings for groups ranging from 20 to 300+ participants. From site selection and registration to catering and security requirements coordination, we can plan and execute an event that complies with government conference regulations and provides a high level of customer satisfaction. All members of our staff hold active security clearances ranging from Secret to Top Secret/SCI.

Services are available to all government clients regardless of whether or not they are currently affiliated with the IATAC contract. Support can be arranged through Technical Area Tasks (TATs) subscription accounts with payments *via* Military Interdepartmental Purchase Requests (MIPRs), if applicable.

Our experienced planners offer service and support for all phases of your event.

Before the event
- Site selection
- Budget oversight
- Contract negotiation
- Secure online registration and payment
- Graphics support
- Audio/visual coordination
- Agenda development
- Sponsorship/exhibitor solicitation
- Marketing and promotion
- Security requirements coordination (classified events)

During the event
- Check-in and registration
- Note-taking (session minutes)
- Speaker assistance
- Problem resolution
- Catering coordination

After the event
- After-action report
- Conference surveys and evaluations
- Distribution of conference proceedings
- Reconciliation of invoices

Want more information?
To find out more about IATAC's conference and event planners and what they can do for you, please contact:

April Perera
Director, Conference and Event Planning
703/984-0769

Avery-Lynn Dickey
Conference and Event Planner
703/984-0766
iatac@dtic.mil

Examples of recent events
- Federal PKI Deployment Workshop, March 2003
- Federal PKI Deployment Workshop 2: Federal Credentialing and Beyond, May 2004
- Intel Support to CND Conference, August 2003
- Second Intel Support to CND Conference, February 2004
- Fourth Intel Support to CND Conference, March 2005
- The Political/Military Dimensions of Cyber Security, March 2004
- Treasury IT Security Conference 2004
- Making the Grade, June 2004
  DoD Defense Continuity Conference, September 2004
- Joint Task Force for Global Network Operations (JTF-GNO) Component Commanders Conference, January 2005
- JTF–GNO Reporting Working Group, February 2005
- GO/FO/SES Global NetOps Conference, July 2005

FREE Products Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not 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/registration*. The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ☐ USA ☐ USMC ☐ USN ☐ USAF ☐ DoD
☐ Industry ☐ Academia ☐ Government ☐ Other

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

_____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)
☐ Firewalls ☐ Intrusion Detection ☐ Vulnerability Analysis

Critical Review and Technology Assessment (CR/TA) Reports
☐ Biometrics (soft copy only) ☐ Configuration Management ☐ Defense in Depth (soft copy only)
☐ Data Mining (soft copy only) ☐ IA Metrics (soft copy only) ☐ Network Centric Warfare
☐ Wireless Wide Area Network (WWAN) Security ☐ Exploring Biotechnology (soft copy only)
☐ Computer Forensics* (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)

State-of-the-Art Reports (SOARs)
☐ Data Embedding for IA (soft copy only) ☐ IO/IA Visualization Technologies (soft copy only)
☐ Modeling & Simulation for IA ☐ Malicious Code (soft copy only)
☐ A Comprehensive Review of Common Needs and Capability Gaps

UNLIMITED DISTRIBUTION

IAnewsletters Hardcopies are available to order. The list below represents current stock.
Softcopy back issues are available for download at http://www.iatac.org/IA_newsletter.html

Volumes 4		☐ No. 2	☐ No. 3	☐ No. 4
Volumes 5	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 6	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 7	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 8	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4

Fax completed form to IATAC at 703/984-0773

Calendar

March

Milspace 2006—Challenges and Changes
8–9 March 2006
Royal Windsor Hotel
Brussels, Belgium
http://www.smi-online.co.uk/events/overview.asp?is=1&ref=2317

Military Technologies Conference
14–15 March 2006
Boston, MA
http://mtc06.events.pennnet.com/

ICIW 2006: International Conference on i-Warfare and Security
15–16 March 2006
http://academic-conferences.org/iciw/iciw2006/iciw06-home.htm

2006 Controlling Authority and EKMS Conference
28–30 March 2006
Marriott Waikiki Resort & Spa
Honolulu, HI
http://www.fbcinc.com/event.asp?eventid=Q6UJ9A009U7E

UAV Summit 2006
29–30 March 2006
Hilton Hotel
Silver Spring, MD
http://idga.org/cgi-bin/templates/singlecell.html?topic=221&event=9237

April

DTIC Annual Conference
3–5 April 2006
Hilton Alexandria
Old Town Alexandria, VA
http://www.dtic.mil/dtic/annualconf/

InfoSec World Conference & Expo 2006
3–5 April 2005
Orlando, FL
http://www.misti.com/default.asp?page=65&Return=70&ProductID=4983

IPCCC 2006
The 25th IEEE International Performance Computing and Communications Conference
10–12 April 2006
Phoenix, AZ
http://ipccc.org/

Fiesta Informacion 2006
24–27 April 2006
San Antonio, TX
http://www.fiestainformacion.com/confinfo/info.htm

GovSec 2006
26–27 April 2006
Washington Convention Center
Washington, DC
http://www.govsecinfo.com

May

REDTEAM 2006 Conference
2–4 May 2006
Sandia National Laboratories,
Kirtland AFB, Albuquerque, NM
http://www.sandia.gov/redteam2006/

IATAC
Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

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: 703/984-0775, fax us at: 703/984-0773, or send us a message at: iatac@dtic.mil