# Computer Security Division




## 2008 Annual Report

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

# Table of Contents


| | |
|---|---|
| Welcome | 1 |
| Division Organization | 2 |
| The Computer Security Division Responds to the Federal Information Security Management Act of 2002 | 3 |
| Security Management and Assistance Group (SMA) | 4 |
| FISMA Implementation Project | 4 |
| Publications | 6 |
| Outreach and Awareness | 8 |
| Health Information Technology | 13 |
| Security Testing and Metrics Group (STM) | 14 |
| Validation Programs and Laboratory Accreditation | 14 |
| Security Technology Group (ST) | 19 |
| Cryptographic Standards Toolkit | 19 |
| Quantum Computing | 21 |
| Authentication | 22 |
| Security Aspects of Electronic Voting | 22 |
| Systems and Network Security Group (SNS) | 23 |
| Identity Management Systems | 23 |
| Biometric Standards and Conformity Assessment Activities | 30 |
| Research in Emerging Technologies | 34 |
| Technical Security Metrics | 38 |
| Automated Vulnerability Management and Measurement | 40 |
| Infrastructure Services, Protocols, and Applications | 42 |
| CSD's Role in National and International IT Security Standards Processes | 46 |
| Systems and Network Security Technical Guidelines | 49 |
| Honors and Awards | 52 |
| Computer Security Division Publications – FY 2008 | 53 |
| Ways to Engage Our Division and NIST | 55 |
| Acknowledgements | 56 |

# WELCOME

The Computer Security Division (CSD), a component of NIST's Information Technology Laboratory (ITL), provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services. During Fiscal Year 2008 (FY2008), CSD successfully responded to numerous challenges and opportunities in fulfilling its mission. CSD carried out a diverse research agenda and participated in many national priority initiatives, leading to the development and implementation of high-quality, cost-effective security and privacy mechanisms that improved information security across the federal government and throughout the national and international information security community.

In FY2008, CSD continued to develop standards, metrics, tests, and validation programs to promote, measure, and validate the security in information systems and services. Recognizing the potential benefits of more automation in technical security operations, CSD hosted the Information Security Automation Program (ISAP), which formalizes and advances efforts to enable the automation and standardization of technical security operations, including automated vulnerability management and policy compliance evaluations. The CSD also continued to work closely with federal agencies to improve their understanding and implementation of the Federal Information Security Management Act (FISMA) to protect their information and information systems. CSD supported a major intelligence community and national security community initiative to build a unified framework for information security across the federal government. This initiative is expected to result in greater standardization and more consistent and cost-effective security for all federal information systems.

As technology advances and security requirements evolve, CSD critically evaluates existing standards, guidelines, and technologies to ensure that they adequately reflect the current state of the art. In FY2008, CSD issued revisions of *The Keyed-Hash Message Authentication Code*, Federal Information Processing Standard (FIPS) 198-1 and *Secure Hash Standard*, FIPS 180-3, as well as a draft for public comment of the RSA Strong Primes - *Digital Signature Standard*, FIPS 186-3. The CSD also initiated an international competition for a next generation Secure Hash Algorithm (SHA-3).

During FY2008 CSD explored opportunities to apply its security research to national priorities and internal NIST initiatives. The CSD has played an active role in implementation planning for the Comprehensive National Cyber Security Initiative to protect our country's critical infrastructure. The CSD continued to expand its support for two key national initiatives, electronic voting and health information technology, by researching the security requirements of those areas and applying the results of that research, along with current technologies, to advance the stated goals of those initiatives. CSD also worked closely with the ITL management team to integrate security projects into ITL's research programs. These programs, which include Cyber Security, Pervasive Information Technologies, Identity Management, and Trustworthy Software, are designed to organize and build ITL core competencies in the most efficient manner, and to maximize the use of ITL resources to address emerging information technology challenges.

These are just some of the highlights of the CSD program during FY2008. You may obtain more information about CSD's program at *http://csrc.nist.gov* or by contacting any of the CSD experts noted in this report. If interested in participating in any CSD challenges – whether current or future – please contact any of the listed CSD experts.

William Curtis Barker
Chief Cybersecurity Advisor



# Division Organization



**William Curtis Barker**
***Chief Cybersecurity Advisor***



**Donna Dodson**
***Deputy Chief Cybersecurity Advisor***



**Matthew Scholl**
***Security Management & Assistance***



**Donna Dodson**
***Security Testing & Metrics (Acting)***



**William Burr**
***Security Technology***



**David Ferraiolo**
***Systems and Network Security***

# The Computer Security Division Responds to the Federal Information Security Management Act of 2002

The E-Government Act [Public Law 107-347], passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), included duties and responsibilities for the Computer Security Division (CSD) in Section 303 "National Institute of Standards and Technology." In 2008, CSD addressed its assignments through the following projects and activities:

- **Develop NIST guides for securing non-national security agency information systems** – Issued eighteen NIST Special Publications (SP) covering management, operational and technical security guidance. Collaborated with the Office of the Director of National Intelligence and the Department of Defense to transform the certification and accreditation process for information systems into a common framework for information security across the federal government.

- **Define minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category** – Issued revision 2 of SP 800-53, *Recommended Security Controls for Federal Information Systems*, in December 2007.

- **Identify methods for assessing effectiveness of security requirements** - Issued SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, in June 2008.

- **Establish performance measures for agency information security policies and practices** – Issued revision 1 of SP 800-55, *Performance Measurement Guide for Information Security*, in July 2008.

- **Provide assistance to agencies and private sector** – Conducted ongoing, substantial reimbursable and non-reimbursable assistance support, including many outreach efforts such as the Federal Information Systems Security Educators' Association (FISSEA), the Federal Computer Security Program Managers' Forum (FCSM Forum), the Small Business Corner, and the Program Review for Information Security Management Assistance (PRISMA).

- **Evaluate security policies and technologies from the private sector and national security systems for potential federal agency use** – Hosted a growing repository of federal agency security practices, public/private security practices, and security configuration checklists for IT products. In conjunction with the Government of Canada's Communications Security Establishment, CSD leads the Cryptographic Module Validation Program (CMVP). The Common Criteria Evaluation and Validation Scheme (CCEVS) and CMVP facilitate security testing of IT products usable by the federal government.

- **Solicit recommendations of the Information Security and Privacy Advisory Board on draft standards and guidelines** – Solicited recommendations of the Board regularly at quarterly meetings.

- **Provide outreach, workshops, and briefings** – Conducted ongoing awareness briefings and outreach to CSD's customer community and beyond to ensure comprehension of guidance and awareness of planned and future activities. CSD also held workshops to identify areas that the customer community wishes to be addressed, and to scope guidelines in a collaborative and open format.

- **Satisfy annual NIST reporting requirement** – Produced an annual report as a NIST Interagency Report (IR). The 2003-2007 Annual Reports are available via our Computer Security Resource Center (CSRC) website or upon request.

# Security Management and Assistance Group (SMA)

**STRATEGIC GOAL** ▸ *The Security Management and Assistance Group provides leadership, expertise, outreach, standards and guidelines in order to assist the federal IT community in protecting its information and information systems, which allows our federal customers to use these critical assets in accomplishing their missions.*

## Overview

Information security is an integral element of sound management. Information and information systems are critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or employees. However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed.

Ultimately, responsibility for the success of an organization lies with its senior management. They establish the organization's computer security program and its overall program goals, objectives, and priorities in order to support the mission of the organization. They are also responsible for ensuring that required resources are applied to the program.

Collaboration with a number of entities is critical for success. Federally, we collaborate with the United States Office of Management and Budget (OMB), the United States Government Accountability Office (GAO), the National Security Agency (NSA), the Chief Information Officers (CIO) Council, and all Executive Branch agencies. We also work closely with a number of information technology organizations and standards bodies, as well as public and private organizations.

Major initiatives in this area include the FISMA Implementation Project:

- Extended outreach initiatives to federal and nonfederal agencies;
- Information security training, awareness and education;
- Outreach to small and medium business;
- Standards development;
- Producing and updating NIST Special Publications (SP) on security management topics.

Key to the success of this area is our ability to interact with a broad constituency – federal and nonfederal--in order to ensure that our program is consistent with national objectives related to or impacted by information security.

## Federal Information Security Management Act (FISMA) Implementation Project

The Computer Security Division (CSD) continued to develop the security standards and guidelines required by federal legislation. Phase I of the FISMA Implementation Project included the development of the following publications—

- Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;
- NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective* (Targeted Completion February 2009);
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*;
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*;
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*; and
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The security standards and guidelines developed in Phase I will assist federal agencies in—

- Implementing the individual steps in the NIST Risk Management Framework as part of a well-defined and disciplined system development life cycle process;
- Demonstrating compliance to specific requirements contained within the legislation; and
- Establishing a level of security due diligence across the federal government.

In FY2008, the SMA group completed the following key publications:

- Initial public draft of a major revision to NIST SP 800-37, *Guide for Security Authorization of Federal Information Systems*, working in cooperation with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS), to develop a common process to authorize federal information systems for operation;
- Second public draft of NIST SP 800-39, which is the flagship document in the series of FISMA-related publications that provides a structured, yet flexible approach for managing that portion of risk resulting from the incorporation of information systems into the mission and business processes of organizations;
- Revision of NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, working with NIST's Intelligent Systems Division (Manufacturing Engineering Laboratory), in collaboration with the Department of Homeland Security and organizations within the federal government that own, operate, and maintain industrial control systems, to incorporate in NIST SP 800-53 guidance on appropriate safeguards and countermeasures for federal industrial control systems,
- Final publication of NIST SP 800-53A, which provides a new, streamlined, and flexible approach for developing security assessment plans containing assessment procedures to determine the effectiveness of security controls deployed in federal information systems. Also completed with NIST SP 800-53A, was an initial public draft of web-based assessment cases, which were developed by an interagency team to provide security assessors with online, worked examples identifying specific assessor action steps to accomplish for each of the assessment procedures in SP 800-53A;
- Revision of NIST SP 800-60, which updates the information types used by agencies to develop information system impact levels to help determine the criticality and sensitivity of federal information systems.

In addition to the above publications, the division collaborated with the Manufacturing Engineering Laboratory in developing a draft guide to industrial control system security, NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*.

Phase II of the FISMA Implementation Project, discussed in more detail in the next section of this annual report, focuses on several new initiatives to support the development of a program for credentialing public and private sector organizations to provide security assessment services for federal agencies.

---

http://csrc.nist.gov/sec-cert
Contact: Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

### Organizational Credentialing Program

Phase II of the FISMA Implementation Project is focusing on building a common understanding and capability for FISMA security control implementation and assessment in supporting development of a program for credentialing public and private sector organizations to provide security assessment services of information systems for federal agencies. These security services involve the comprehensive assessment of the management, operational, and technical security controls in federal information systems including the assessment of the information technology products and services used in security control implementation. The security assessment services will determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

This phase of the FISMA Implementation Project includes the following initiatives:

(1) *Training Initiative:* for development of training courses, Quick Start Guides (QSG's), and Frequently Asked Questions (FAQ's) to establish a common understanding of the NIST standards and guidelines supporting each of the steps in the NIST Risk Management Framework;

(2) *Support Tools Initiative:* for identifying common programs, reference materials, checklists, technical guides, tools and techniques supporting implementation and assessment of SP 800-53 security controls;

(3) *Product and Services Assurance Initiative:* for defining minimum criteria and guidelines for suppliers in specifying security functions and assurances (to include evidence of test results from SCAP tools and configu-

ration checklists, etc. where applicable) of products and services used in implementing SP 800-53 security controls;

(4) *Organizational Credentialing Initiative:* drawing upon material from the above initiatives and NIST standards and guidelines, define minimum capability and proficiency criteria for credentialing public and private sector organizations providing security assessment services for federal agencies; and

(5) *Harmonization Initiative:* for identifying common relationships and the mappings of FISMA standards, guidelines and requirements with: (i) ISO 27000 (International Organization for Standardization) series information security management standards; and (ii) ISO 9000 and 17000 series quality management, and laboratory testing, inspection and accreditation standards. This harmonization is important for minimizing duplication of effort for organizations that must demonstrate compliance to both FISMA and ISO requirements.

In FY2008, the CSD completed the initial public draft of NIST Interagency Report 7328, *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems*, which provides an initial set of requirements security assessment providers should satisfy to demonstrate the capability to conduct information system security control assessments in accordance with NIST standards and guidelines. The division also completed a set of Quick Start Guides (QSG's) and Frequently Asked Questions (FAQ's) to establish a common understanding of the NIST standards and guidelines supporting the categorization of systems step (i.e., first step) of the NIST Risk Management Framework.

---

http://csrc.nist.gov/sec-cert

Contacts: Mr. Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Ms. Pat Toth
(301) 975-5140
patricia.toth@nist.gov

## Publications

### Glossary of Key Information Security Terms

Over the years, the Computer Security Division (CSD) has produced many information security guidance documents with definitions of key terms used. The definition for any given term was not standardized; therefore, there were multiple definitions for a given term. In 2004, the CSD identified a need to increase consistency in definitions for key information security terms in our documents.

The first step was a review of NIST publications (NIST Interagency Reports, Special Publications, and Federal Information Processing Standards) to determine how key information security terms were defined in each document. This review was completed in 2005 and resulted in a listing of each term and all definitions for each term. Several rounds of internal and external reviews were completed, and comments and suggestions were incorporated into the document. The document was published in April 2006 as NISTIR 7298, *Glossary of Key Information Security Terms*.

In 2007, CSD initiated an update to the Glossary to reflect new terms and any different definitions used in our publications, as well as to incorporate information assurance terms from the Committee on National Security Systems Instruction No 4009 (CNSSI-4009). The glossary update was well underway when CSD was notified that CNSSI-4009 was being updated. NIST obtained a position on the CNSSI-4009 Glossary Working Group and has been working on that project since early 2008.

An updated NIST glossary is expected to be released in FY2009 and will include the updated CNSSI-4009.

---

Contact: Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

### Guide for Mapping Types of Information and Information Systems to Security Categories

In August 2008, NIST issued SP 800-60 Revision 1, Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*, and Volume 2, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*. SP 800-60, the companion guide to FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, was developed to assist federal agencies in categorizing information and information systems by facilitating provision of appropriate levels of information security according to a range of levels of impact or consequences that might result from the compromise of a security objective.

This revision of SP 800-60 further clarifies the system security categorization process; discusses the impact of security categorization results on other enterprise-wide activities such as capital planning, enterprise architecture, and disaster recovery planning; and provides recommendations and rationale for mission-based and management and support information types.

---

Contacts: Mr. Kevin Stine
(301) 975-4483
kevin.stine@nist.gov

Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

### Guide to NIST Computer Security Documents

Can't find the NIST CSD document you're looking for? Are you not sure which CSD documents you should be looking for?

Currently, there are over 300 NIST information security documents. This number includes Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, Information Technology Laboratory (ITL) Bulletins, and NIST Interagency Reports (NIST IRs). These documents are typically listed by publication type and number, or by month and year in the case of the ITL Bulletins. This can make finding a document difficult if the number or date is not known.

In order to make NIST information security documents more accessible, especially to those just entering the information security field or to those with needs for specific documents, CSD developed the *Guide to NIST Information Security Documents*. Publications are listed by type and number, and the guide presents three ways to search for documents: by topic cluster (general subject matters or topic areas used in information security), by family (the seventeen minimum security control family names in SP 800-53), and by legal requirement.

This guide is currently updated through the end of August of FY2008, and will be undergoing future updates to make access to CSD publications easier for our customers.

Contact: Ms. Pauline Bowen
(301) 975-2938
pbowen@nist.gov

### Performance Measures for Information Security

The requirement to measure information security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations, such as the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), and the Federal Information Security Management Act (FISMA), cite information performance measurement in general and information security measurement in particular as a requirement. Agencies are also using performance measures as management tools in their internal improvement efforts and linking implementation of their programs to agency-level strategic planning efforts.

In July 2008, NIST released SP 800-55, Revision 1, *Performance Measurement Guide for Information Security*. The document is a guide to assist in the development, selection, and implementation of measures to be used at the information system and program levels. These measures can help indicate the effectiveness of security controls applied to information systems and supporting information security programs.

Contacts: Ms. Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Mr. Kevin Stine
(301) 975-4483
kevin.stine@nist.gov

### Revision of the Guide to Information Technology Security Role-Based Training Requirements

In FY2007, CSD initiated an update to SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, for public review and comment. Originally published in April 1998, SP 800-16 contains a training methodology that federal departments and agencies, as well as private sector and academic institutions, can use to develop role-based information security training material.

During FY2008 we made significant changes to the document. We began meeting with stakeholders of other federally focused information security training and workforce development initiatives. The goal is to create a multi-agency task force to reduce the potential for confusion among our constituents by 1) developing a diagram that shows the interactions and relationships between the various initiatives, and 2) agreeing on a common training "standard" that can be used by various federal communities that currently own or manage the training and workforce development initiatives. SP 800-16, Rev. 1 is expected to be that common training "standard."

We expect the update of SP 800-16 to be completed during FY2009.

Contacts: Mr. Mark Wilson
(301) 975-3870
mark.wilson@nist.gov

Ms. Pauline Bowen
(301) 975-2938
pauline.bowen@nist.gov

### Security Considerations in the System Development Life Cycle

Consideration of security in the System Development Life Cycle (SDLC) is essential to implementing and integrating a comprehensive risk management strategy for all information systems. To be most effective, information security must be integrated into the SDLC from system inception. Early integration of security in the SDLC enables agencies to maximize return on investment in their security programs, through:

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;
- Awareness of potential engineering challenges caused by mandatory security controls;
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques;
- Facilitating informed executive decision making through comprehensive risk management in a timely manner.

In October 2008, NIST issued SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*. This publication addresses the FISMA direction to develop guidelines recommending security integration into the agency's established SDLC, and is intended to assist agencies in integrating essential information technology (IT) security steps into their established IT SDLC, resulting in more cost effective, risk appropriate security control identification, development, and testing.

Contacts: Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

Mr. Kevin Stine
(301) 975-4483
kevin.stine@nist.gov

## Outreach And Awareness

### Computer Security Resource Center

The Computer Security Resource Center (CSRC) is the Computer Security Division's Web site. CSRC is one of the four most visited Web sites at NIST. We use the CSRC to encourage broad sharing of information security tools and practices, to provide a resource for information security standards and guidelines, and to identify and link key security Web resources to support the industry. The CSRC is an integral component of all of the work that we conduct and produce. It is our repository for everyone, public or private sector, wanting access to our documents and other information security-related information. CSRC serves as a vital link to all our internal and external customers.

During FY2008, CSRC had more than 87.8 million requests, which included the additional traffic coming from the National Vulnerability Database (NVD) that became operational in late FY2005. Of the total 87.8 million requests, the CSRC received 38.2 million requests, while the NVD website received 49.6 million requests.

The CSRC web site is the primary source for gaining access to NIST computer security publications. Every draft document released for public comment or final document published through the Division has been posted to the CSRC website. Based on the web site's statistics, the five most requested CSD publications for FY2008 were:

(1) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*

(2) Federal Information Processing Standard (FIPS) 197, *Advanced Encryption Standard*

(3) SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*

(4) FIPS 140-2, *Security Requirements for Cryptographic Modules*

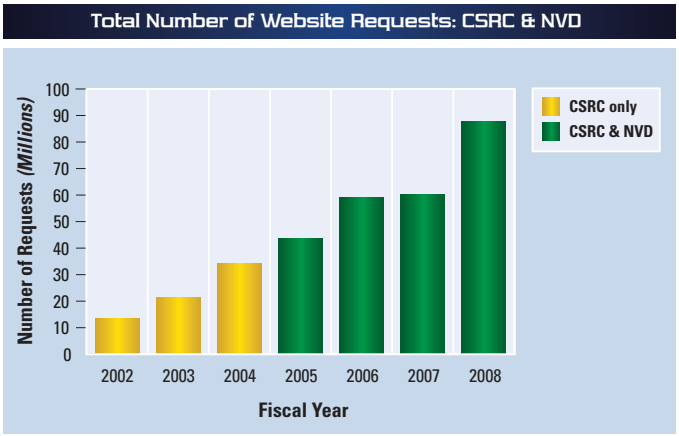
(5) SP 800-53 Revision 1 and, Revision 2, *Recommended Security Controls for Federal Information Systems*

During FY2008, the CSRC Web site was continuously updated with new information on all project pages along with the posting of new and updated publications. The new and improved CSRC Web site standardizes the CSRC Web pages and menus, and is easier to navigate. Some of the major highlights of the expanded CSRC website during FY2008 were:

- Creation of web pages for the 2008 Federal Information Systems Security Educators' Association (FISSEA) Conference;
- Improved Publications section that included the addition of the Archived Publications section for withdrawn FIPS and SPs (superseded);
- Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP) project;
- National Vulnerability Database (NVD) website – updated the Federal Desktop Core Configuration (FDCC) and Security Content Automation Protocol (SCAP) portion of website; and
- Addition of assessment cases for the FISMA project, to name a few of the major highlights.

In addition to the CSRC website, CSD maintains a publications announcement mailing list. This is a free email list that notifies subscribers about publications that have been released to the general public and that have been posted to the CSRC website. This email list is a valuable tool for the more than 7,600 subscribers who include federal government employees, private sector, educational institutions and individuals with a personal interest in IT security. This email list reaches people all over the world. Email is sent to the list only when the Computer Security Division releases a publication (Draft, FIPS PUB, Special Publication and NIST IR). Emails are only sent out by the list administrator – Pat O'Reilly (NIST, CSD). Individuals who are interested in learning more about this list or subscribing to this list should visit this webpage on CSRC for more information:

*http://csrc.nist.gov/publications/subscribe.html*



Questions on the Web site should be sent to the CSRC Webmaster at: *webmaster-csrc@nist.gov*.

CSRC will continue to grow and be updated in 2009. In addition, we will be integrating CSRC into a NIST-wide implementation of a content management system.

---

http://csrc.nist.gov/
Contact: Mr. Patrick O'Reilly
(301) 975-4751
patrick.oreilly@nist.gov

### Federal Computer Security Program Managers' Forum

The Federal Computer Security Program Managers' Forum (Forum) is an informal group of over 800 members sponsored by NIST to promote the sharing of security-related information among federal agencies. The Forum strives to provide an ongoing opportunity for managers of federal information security programs to exchange information security materials in a timely manner, to build upon the experiences of other programs, and to reduce possible duplication of effort. It provides an organizational mechanism for NIST to share information directly with federal agency information security program managers in fulfillment of NIST's leadership mandate under FISMA. It assists NIST in establishing and maintaining relationships with other individuals or organizations that are actively addressing information security issues within the federal government. Finally, it helps NIST and other federal agencies in developing and maintaining a strong, proactive stance in the identification and resolution of new strategic and tactical IT security issues as they emerge.

The Forum hosts the Federal Agency Security Practices (FASP) Web site, maintains an extensive e-mail list, and holds an annual off-site workshop and bimonthly meetings to discuss current issues and developments of interest to those responsible for protecting sensitive (unclassified) federal systems [except "Warner Amendment" systems, as defined in 44 USC 3502 (2)]. Ms. Marianne Swanson, NIST serves as the Chairperson of the Forum. NIST also serves as the secretariat of the Forum, providing necessary administrative and logistical support. Participation in Forum meetings is open to federal government employees who participate in the management of their organization's information security program. There are no membership dues.

Topics of discussion at Forum meetings in FY2008 included briefings on NIST SP 800-55, *Performance Measurement Guide for Information Security*, Internal Revenue Service certification and accreditation process, Department of Navy's SPAWAR (Space and Naval Warfare Systems Command) program, FISMA reporting experiences, General Services Administration's (GSA) Network program, NIST's FISMA Phase II activities, supply chain risk management and a briefing on the Cyber Counter Intelligence Plan. This year's two-day annual off-site meeting featured updates on the computer security activities of the United States Government Accountability Office, NIST, the United States Office of Management and Budget, and the Department of Homeland Security. Briefings were also provided on electronic authentication, secure telework, IPV6 implementation, HSPD-12 implementation, Federal Desktop Core Configuration (FDCC), the Security Content Automation Protocol (SCAP), Information System Security Line of Business on Phase II training, certification and accreditation transformation project, and revisions to NIST SP 800-16, *Information Technology Training Requirements: A Role- and Performance- Based Model* . Additionally, there was an Inspectors General panel briefing on FISMA implementation and a panel of Chief Information Security Officers discussing their experiences with the accreditation process.

---

http://csrc.nist.gov/organizations/cspmf.html
Contact: Ms. Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

### Federal Information Systems Security Educators' Association (FISSEA)

The Federal Information Systems Security Educators' Association (FISSEA), founded in 1987, is an organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, and education responsibilities. FISSEA strives to elevate the general level of information systems security knowledge for the federal government and the federally related workforce. FISSEA serves as a professional forum for the exchange of information and improvement of information systems security awareness, training, and education programs. It also seeks to provide for the professional development of its members.

FISSEA membership is open to information systems security professionals, professional trainers and educators, and managers responsible for information systems security training programs in federal agencies, as well as contractors of these agencies and faculty members of accredited educational institutions who are involved in information security training and education. There are no membership fees for FISSEA; all that is required is a willingness

to share products, information, and experiences. Business is administered by an 11-member Executive Board that meets monthly. Board members serve two-year terms, and elections are held during the annual conference. In March 2008, Emma Hochgesang-Noffsinger was elected to be the FISSEA Executive Board Chair.

Each year an award is presented to a candidate selected as Educator of the Year; this award honors distinguished accomplishments in information systems security training programs. The Educator of the Year for 2007, awarded in March 2008, was David Kurtz of the Department of Treasury's Bureau of the Public Debt. There is also a contest for information security posters, Web sites, and awareness tools with the winning entries listed on the FISSEA Web site. FISSEA has a semiannual newsletter, an actively maintained Web site, and a list serve as a means of communication for members. Members are encouraged to participate in the annual FISSEA Conference and to serve on the FISSEA ad hoc task groups. We assist FISSEA with its operations by providing staff support for several of its activities and by being FISSEA's host agency.

FISSEA membership in 2008 spanned federal agencies, industry, military, contractors, state governments, academia, the press, and foreign organizations to reach over 1,600 members in a total of 15 countries. The 800 federal agency members represent 89 agencies from the Executive and Legislative branches of government.

FISSEA conducted three free workshops during 2008. In July board members Susan Hansche and Mark Wilson, along with George Bieber, Tim Mucklow, Jeff Pound, and Jim Wrubel, conducted "What's Happening" in the information system security awareness and training field which was held at the Department of State. In April Susan Hansche and Louis Numkin presented "What's New in Cyber Security Training." In November the workshop featured a discussion of "Information Systems Security Qualifications Matrix: Complexities, Competencies, Experience, and Training." Workshop presentations are posted on the website and FISSEA will continue to offer free workshops in 2009.

The 2008 FISSEA conference was held at NIST on March 11-13 where 165 attendees heard presentations to enhance their awareness, training, and education programs. Conference attendees were given the opportunity to network, to tour NIST, and to participate in a vendor exhibition. The 2009 conference, which will be held on March 24-26, will have the theme "Awareness, Training, and Education – The Catalyst for Organizational Change." Further information regarding the conference is available on the FISSEA Web site.

FISSEA strives to improve federal information systems security through awareness, training, and education. Stay aware, trained, and educated with FISSEA.

---

http://csrc.nist.gov/fissea/

Contacts: Mr. Mark Wilson
(301) 975-3870
mark.wilson@nist.gov

Ms. Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

### The Information Security and Privacy Advisory Board

The Information Security and Privacy Advisory Board (ISPAB) is a federal advisory committee that brings together senior professionals from industry, government, and academia to help advise the National Institute of Standards and Technology (NIST), the United States Office of Management and Budget (OMB), the Secretary of Commerce, and appropriate committees of the United States Congress about information security and privacy issues pertaining to unclassified federal government information systems.

## The Information Security and Privacy Advisory Board Membership



*Pictured above, Left to Right:* **Back row:** *Jaren Doherty, Peter Weinberger, Joseph Guirreri, Howard Schmidt, Lisa Schlosser, Daniel Chenok, and Fred B. Schneider.* **Front row:** *Ari Schwartz, Alexander Popowycz, Rebecca Leng, Brian Gouker, Lynn McNulty and Pauline Bowen.*



*Pictured above, Left to Right: Philip Reitinger and Annie Sokol*

The membership of the Board consists of 12 individuals and a Chairperson. The Director of NIST approves membership appointments and appoints the Chairperson. Each Board member serves for a four-year term. The Board's membership draws from experience at all levels of information security and privacy work. The members' careers cover government, industry, and academia. Members have worked in the Executive and Legislative branches of the federal government, civil service, senior executive service, the military, some of the largest corporations worldwide, small and medium-size businesses, and some of the top universities in the nation. The members' experience, likewise, covers a broad spectrum of activities including many different engineering disciplines, computer programming, systems analysis, mathematics, management positions, information technology auditing, legal experience, an extensive history of professional publications, and professional journalism. Members have worked (and in many cases, continue to work in their full-time jobs) on the development and evolution of some of the most important pieces of information security and privacy legislation in the federal government, including the Privacy Act of 1974, the Computer Security Act of 1987, the E-Government Act (including FISMA), and numerous e-government services and initiatives.

This combination of experienced, dynamic, and knowledgeable professionals on an advisory board provides NIST and the federal government with a rich, varied pool of people conversant with an extraordinary range of topics. They bring great depth to a field that has an exceptional rate of change. In FY2008 the board lost two long time members, Leslie A. Reis and Susan Landau. They gained two more members, Ari Schwartz and Peter Weinberger.

ISPAB was originally created by the Computer Security Act of 1987 (Public Law 100-35) as the Computer System Security and Privacy Advisory Board. As a result of FISMA, the Board's name was changed and its mandate was amended. The scope and objectives of the Board are to—

- Identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;
- Advise NIST, the Secretary of Commerce, and the Director of OMB on information security and privacy issues pertaining to federal government information systems, including thorough review of proposed standards and guidelines developed by NIST; and
- Annually report the Board's findings to the Secretary of Commerce, the Director of OMB, the Director of the National Security Agency, and the appropriate committees of the Congress.

The Board meets quarterly and all meetings are open to the public. NIST provides the Board with its Secretariat. The Board has received numerous briefings from federal and private sector representatives on a wide range of privacy and security topics in the past year.

Areas of interest that the Board will be following in FY2009 include:

- Privacy technology,
- Essential Body of Knowledge,
- Industry Security Officers Best Practices,
- Federal Initiatives such as:
  - Trusted Internet Connection,
  - Federal Desktop Core Configuration,
  - Homeland Security Policy Directive 12,
  - IPv6,
  - Biometrics and ID management,
  - Security metrics,
  - Geospatial security and privacy issues,
  - FISMA reauthorization (and other legislative support),
  - Information Systems Security Line of Business – (ISS LOB),
  - National security community activities in areas relevant to civilian agency security (e.g., architectures),
  - Supervisory Control and Data Acquisition (SCADA) security,
  - Health care IT,
  - Telecommuting Security,
  - Senior Management's Role in FISMA Review,
  - Use and Implementation of Federal IT Security Products,
  - Social Networking and Security,
  - Einstein Program,
  - Role of chiefs (such as Chief Privacy Officer and Chief Security Officer),
  - NIST's outreach, research, and partnering approaches, and cyber security leadership in the Executive Branch.

---

http://csrc.nist.gov/ispab/
Contact: Ms. Pauline Bowen
(301) 975-2938
pauline.bowen@nist.gov

### Security Practices and Policies

Today's federal networks and systems are highly interconnected and interdependent with nonfederal systems. Protection of the nation's critical infrastructures is dependent upon effective information security solutions and practices that minimize vulnerabilities associated with a variety of threats. The broader sharing of such practices will enhance the overall security of the nation. Information security practices from the public and private sector can sometimes be applied to enhance the overall performance of federal information security programs. We are helping to facilitate a sharing of these practices and implementation guidelines in multiple ways.

The Federal Agency Security Practices (FASP) effort was initiated as a result of the success of the federal Chief Information Officers (CIO) Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection and security. We were asked to undertake the transition of this pilot effort to an operational program. As a result, we developed the FASP Web site. The FASP site contains agency policies, procedures and practices, the CIO Council's pilot BSPs, and a Frequently Asked Questions (FAQ) section. The FASP site differs from the BSP pilot in material provided and complexity.

The FASP area contains a list of categories found in many of the NIST Special Publications. Based on these categories, agencies are encouraged to submit their information security practices for posting on the FASP site so they may be shared with others. Any information on, or samples of, position descriptions for security positions and statements of work for contracting security-related activities are also encouraged. In the past year, a number of dated practices were removed from the site and new ones were added.

We also invite public and private organizations to submit their information security practices to be considered for inclusion on the list of practices maintained on the Web site. Policies and procedures may be submitted to us in any area of information security, including accreditation, audit trails, authorization of processing, budget planning and justification, certification, contingency planning, data integrity, disaster planning, documentation, hardware and system maintenance, identification and authentication, incident handling and response, life cycle, network security, personnel security, physical and environmental protection, production input/output controls, security policy, program management, review of security controls, risk management, security awareness training and education (including specific training course and awareness materials), and security planning.

In FY2009, we will continue the momentum to expand the number of sample practices and policies made available to federal agencies and the public. We are currently identifying robust sources for more samples to add to this growing repository. We plan to take advantage of the advances in communication technology and combine this outreach with other outreach areas for information security in order to reach many in the federal agencies and the public.

---

http://fasp.nist.gov/

Contacts: Ms. Pauline Bowen
(301) 975-2938
pauline.bowen@nist.gov

Mr. Mark Wilson
(301) 975-3870
mark.wilson@nist.gov

### Small and Medium-Size Business Outreach

What do a business's invoices have in common with e-mail? If both are done on the same computer, the business owner may want to think more about computer security. Information – payroll records, proprietary information, client, or employee data – is essential to a business's success. A computer failure or other system breach could cost a business anything from its reputation to damages and recovery costs. The small business owner who recognizes the threat of computer crime and takes steps to deter inappropriate activities is less likely to become a victim.

The vulnerability of any one small business may not seem significant to many, other than the owner and employees of that business. However, over 20 million United States businesses, comprising more than 95 percent of all United States businesses, are small and medium-size businesses (SMBs) of 500 employees or less. Therefore, a vulnerability common to a large percentage of all SMBs could pose a threat to the nation's economic base. In the special arena of information security, vulnerable SMBs also run the risk of being compromised for use in crimes against governmental or large industrial systems upon which everyone relies. SMBs frequently cannot justify an extensive security program or a full-time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs.

The difficulty for these businesses is to identify needed security mechanisms and training that are practical and cost-effective. Such businesses also need to become more educated in terms of security so that limited resources are well applied to meet the most obvious and serious threats. To address this need, NIST, the Small Business Administration (SBA), and the Federal Bureau of Investigation (FBI) agreed to cosponsor a series of training meetings on computer security for small businesses. The purpose of the meetings is to provide an overview of information security threats, vulnerabilities, and corresponding protective tools and techniques, with a special emphasis on providing useful information that small business personnel can apply directly or use to task contractor personnel.

In FY2008, the SMB outreach effort focused on expanding opportunities to reach more small businesses, and nine SMB workshops were held across the country. In July 2008, two half-day workshops were held in Buffalo, NY, and Houston, TX. Similar workshops were held in August 2008 in Kansas City, MO, Sacramento, CA and Honolulu, HI. Additional workshops were held in September in Milwaukee, WI, Springfield, IL, Chicago, IL, and St Louis, MO.

---

http://sbc.nist.gov/
Contact: Mr. Richard Kissel
(301) 975-5017
richard.kissel@nist.gov

## Health Information Technology

In April 2004, the President issued a plan for a healthcare system in the United States that puts the needs of the patient first, is more efficient, and is cost-effective. The President's plan is based on the following tenets:

- Medical information will follow consumers so that they are at the center of their own care.
- Consumers will be able to choose physicians and hospitals based on clinical performance results made available to them.
- Clinicians will have a patient's complete medical history, computerized ordering systems, and electronic reminders.
- Quality initiatives will measure performance and drive quality-based competition in the industry.
- Public health and bioterrorism surveillance will be seamlessly integrated into care.
- Clinical research will be accelerated and post-marketing surveillance will be expanded.

Together, these tenets are directed toward making healthcare more consumer-centric, and improving both the quality and the efficiency of healthcare in the United States. Critical components of these tenets is the assurance of privacy of health-related information, assuring the confidentiality and integrity of all health information technology (HIT) data and maintaining the availability to HIT whenever it is needed. The CSD is involved in assisting healthcare providers in this effort.

CSD participates with, and is consulted by, agencies, organizations, and standards panels that are shaping the HIT arena, including:

- American Health Information Community's (AHIC) Confidentiality, Privacy, and Security Workgroup;
- Nationwide Health Information Network (NHIN);
- Healthcare Information Technology Standards Panel (HITSP) ; and
- Certification Commission for Healthcare Information Technology (CCHIT).

In FY2008, CSD also issued a comprehensive update of NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. This SP discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule. The publication:

- Helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule;
- Directs readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule; and
- Aids readers in understanding the security concepts discussed in the HIPAA Security Rule. This publication does not supplement, replace, or supersede the HIPAA Security Rule itself.

To provide additional outreach and reinforce the security concepts in the Security Rule, NIST, in conjunction with the Centers for Medicare and Medicaid Services' (CMS) Office of E-Health Standards and Services (OESS), conducted a HIPAA Security Rule Implementation workshop in January 2008. This conference provided nearly 200 attendees with an opportunity to discuss challenges, tips, techniques, and issues surrounding implementing, adhering to, and auditing HIPAA Security Rule requirements, and to hear from various government and industry healthcare and health information technology organizations about their HIPAA Security Rule implementation strategies and experiences.

---

Contacts: Mr. Matthew Scholl
(301) 975-2941
mscholl@nist.gov

Mr. Kevin Stine
(301) 975-4483
kevin.stine@nist.gov

# SECURITY TESTING AND METRICS GROUP (STM)

**STRATEGIC GOAL** ▸ *Improve the security and technical quality of cryptographic products needed by federal agencies (in the United States, Canada, and the United Kingdom) and industry by developing standards, test methods and validation criteria, and the accreditation of independent third-party testing laboratories.*

## Overview

Federal agencies, industry, and the public rely on cryptography for the protection of information and communications used in electronic commerce, critical infrastructure, and other application areas. At the core of all products offering cryptographic services is the cryptographic module. Cryptographic modules, which contain cryptographic algorithms, are used in products and systems to provide security services such as confidentiality, integrity, and authentication. Although cryptography is used to provide security, weaknesses such as poor design or weak algorithms can render a product insecure and place highly sensitive information at risk. When protecting their sensitive data, federal government agencies require a minimum level of assurance that cryptographic products meet their security requirements. Also, federal agencies are required to use only tested and validated cryptographic modules. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

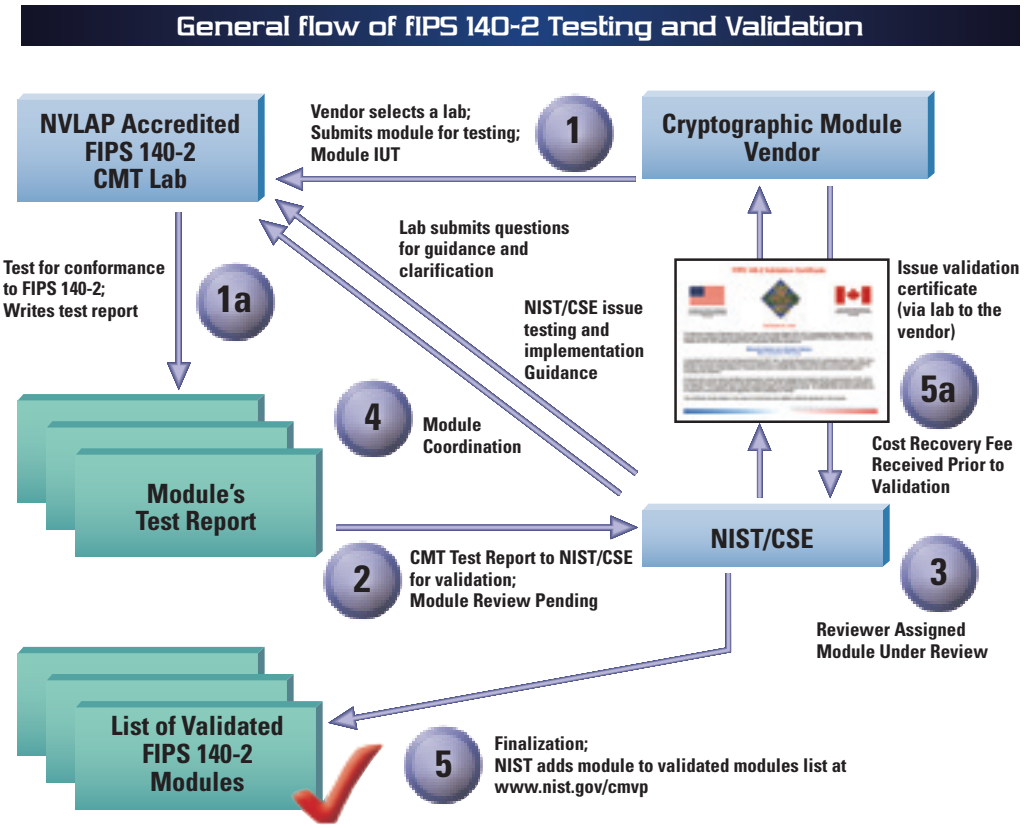
Our testing-focused activities include validating cryptographic modules and cryptographic algorithm implementations, developing test suites, providing technical support to industry forums, and conducting education, training, and outreach programs.

Activities in this area involve collaboration and the facilitation of relationships with other entities. Federal agencies that have collaborated recently with these activities are the Department of State, the Department of Commerce, the Department of Defense, the General Services Administration, the National Aeronautics and Space Administration, the National Security Agency, the Department of Energy, the United States Office of Management and Budget, the Social Security Administration, the United States Postal Service, the Department of Veterans Affairs, the Federal Aviation Administration, and NIST's National Voluntary Laboratory Accreditation Program. Industry entities that have worked with us in this area is long include the American National Standards Institute (ANSI), Oracle, Cisco Systems, Lucent Technologies, Microsoft Corporation, International Business Machines (IBM), VISA, MasterCard, Computer Associates, RSA Security, Research in Motion, Sun Microsystems, Network Associates, Entrust, and Fortress Technologies. The Division also has collaborated in this area at the international level with Canada, the United Kingdom, France, Germany, India, Japan, and Korea.

## Validation Programs And Laboratory Accreditation

The Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) were developed by NIST to support the needs of the user community for strong independently tested and commercially available cryptographic products. The programs work with the commercial sector and the cryptographic community to achieve security, interoperability, and assurance. The goal of these programs is to promote the use of validated products and provide federal agencies with a security metric to use in procuring cryptographic modules. The testing performed by accredited laboratories provides this metric. Federal agencies, industry, and the public can choose cryptographic modules and/or products containing cryptographic modules from the CMVP Validated Modules List and have confidence in the claimed level of security.

The CMVP provides a documented methodology for conformance testing through a defined set of security requirements in Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, and other cryptographic standards. Federal agencies are required to use modules that were validated as conforming to the provisions of FIPS 140-2. We developed the standard and an associated metric (the Derived Test Requirements) to ensure repeatability of tests and equivalency in results across the testing laboratories. The commercial Cryptographic and Security Testing (CST) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) provide vendors of cryptographic modules a choice of testing facilities and promote healthy competition. In the chart on the next page, the acronym IUT is known as Implementation Under Test.




### Laboratory Accreditation

Vendors of cryptographic modules and algorithms use independent, private sector testing laboratories accredited as CST laboratories by NVLAP to have their cryptographic modules validated by the CMVP and their cryptographic algorithms validated by the CAVP. As the worldwide growth and use of cryptographic modules has increased, demand to meet the testing needs for both algorithms and modules developed by vendors has also grown. There are currently 13 accredited laboratories in the United States, Canada, the United Kingdom and Germany. NVLAP has received several applications for the accreditation of CST Laboratories, both domestically and internationally. A complete list of accredited laboratories may be found at http://csrc.nist.gov/groups/STM/testing_labs/index.html.

---

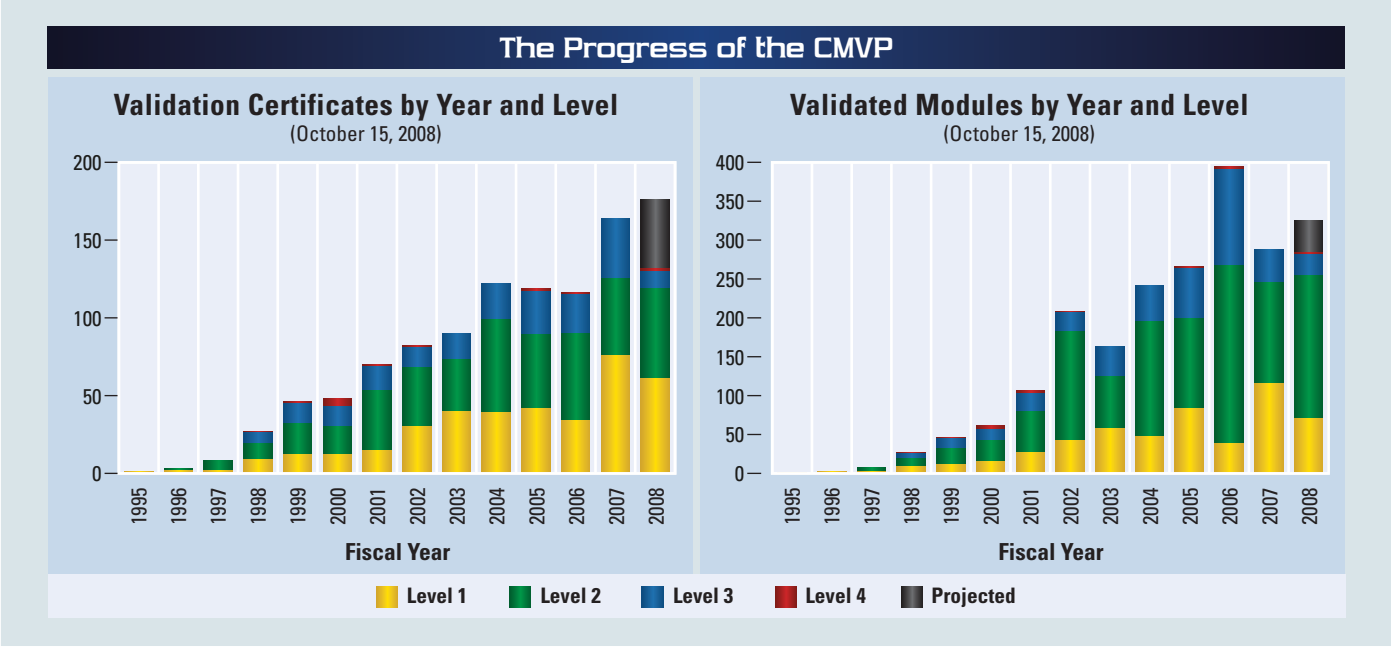
http://ts.nist.gov/standards/accreditation/index.cfm
Contact: Mr. Randall J. Easter
(301) 975-4641
randall.easter@nist.gov

### Cryptographic Module Validation Program and Cryptographic Algorithm Validation Program

The CMVP and the CAVP are separate, collaborative programs based on a partnership between NIST's CSD and the Communication Security Establishment Canada (CSEC). The programs provide federal agencies—in the United States, Canada, and the United Kingdom—with confidence that a validated cryptographic module meets a claimed level of security assurance and that a validated cryptographic algorithm has been implemented correctly. The CMVP/CAVP validate modules and algorithms used in a wide variety of products, including secure Internet browsers, secure radios, smart cards, space-based communications, munitions, security tokens, storage devices, and products supporting Public Key Infrastructure and electronic commerce. One module may be used in several products so that a small number of modules may account for hundreds of products. Likewise, the CAVP validates cryptographic algorithms that may be housed in one or more cryptographic modules.

The CMVP and the CAVP have stimulated improved quality of cryptographic modules. Statistics from the testing laboratories show that 48 percent of the cryptographic modules and 27 percent of the cryptographic algorithms brought in for voluntary testing had security flaws that were corrected during testing. Without this program, the federal government would have had only a 50-50 chance of buying correctly implemented cryptography. To date, over 1045 validation certificates have been issued, representing over 2,086 modules that were validated by the CMVP. These modules have been developed by more than 245 domestic and international vendors.

In FY 2008, the CMVP issued 182 module validation certificates. The number of modules submitted for validation continues to grow, representing significant growth in the number of validated products expected to be available in the future.




The CAVP issued 1127 algorithm validation certificates in FY2008. During the last two years the number of validation certificates issued has grown significantly. In FY 2006, 631 algorithm validation certificates were issued, and in FY2007, 1040 algorithm validation certificates were issued.

---

http://csrc.nist.gov/groups/STM

Contacts:

CMVP Contact: Mr. Randall J. Easter
(301) 975-4641
randall.easter@nist.gov

CAVP Contact: Ms. Sharon S. Keller
(301) 975-2910
sharon.keller@nist.gov

### Automated Security Testing and Test Suite Development

Each approved and recommended cryptographic algorithm is specified in a Federal Information Processing Standards (FIPS) publication or a NIST Special Publication (SP). The detailed instructions on how to implement the specific algorithm are found in these references. Based on these instructions, we design and develop validation test suites containing tests that verify that the detailed instructions of an algorithm are implemented correctly and completely. These tests exercise the mathematical formulas detailed in the algorithm to assure that they work properly for each possible scenario. If the implementer deviates from these instructions or excludes any part of the instructions, the validation test will fail, indicating that the algorithm implementation does not function properly.

The types of validation testing available for each approved cryptographic algorithm include, but are not limited to: Known Answer Tests, Monte Carlo Tests, and Multi-block Message Tests. The Known Answer Tests are designed to test the conformance of the implementation under test (IUT) to the various specifications in the reference. This involves testing the components of the algorithm to assure that they are implemented correctly. The Monte Carlo Test is designed to exercise the entire IUT. This test is designed to detect the presence of implementation flaws that are not detected with the controlled input of the Known Answer Tests. The types of implementation flaws detected by this validation test include pointer problems, insufficient allocation of space, improper error handling, and incorrect behavior of the IUT. The Multi-block Message Test (MMT) is designed to test the ability of the implementation to process multi-block messages, which require the chaining of information from one block to the next. Other types of validation testing exist to satisfy other testing requirements of cryptographic algorithms.

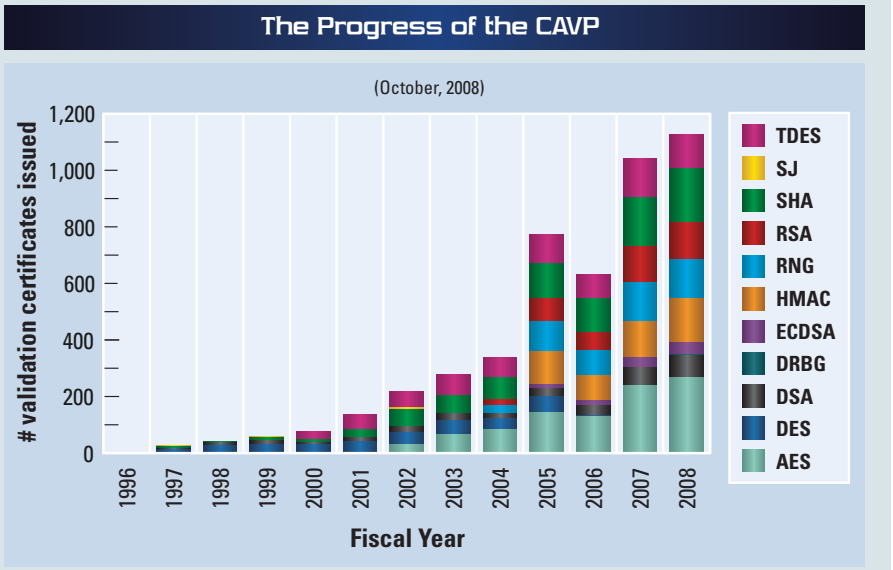
Automated security testing and test suite development are integral components of the Cryptographic Algorithm Validation Program (CAVP). The CAVP encompasses validation testing for FIPS-approved and NIST-recommended cryptographic algorithms. Cryptographic algorithm validation is a prerequisite to the Cryptographic Module Validation Program (CMVP). All of the tests under the CAVP are handled by the 13 third-party laboratories that are accredited as CMT laboratories by NVLAP. We develop and maintain a Cryptographic Algorithm Validation System (CAVS) tool which automates the validation testing. The CAVS currently has algorithm validation testing for the following cryptographic algorithms:

- The Triple Data Encryption Standard (TDES) algorithm (as specified in SP 800-67 *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher* and SP 800-38A *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*),
- The Advanced Encryption Standard (AES) algorithm (as specified in FIPS 197 *Advanced Encryption Standard* and SP 800-38A),

- The Digital Signature Standard (DSS) (as specified in FIPS 186-2 *Digital Signature Standard (DSS)* with change notice 1 dated October 5, 2001),
- Hashing algorithms SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 (as specified in FIPS 180-2 *Secure Hash Standard* (SHS) with change notice 1 dated February 25, 2004),
- Three random number generator (RNG) algorithms (as specified in Appendix 3.1 and 3.2 of FIPS 186-2, Appendix A.2.4 of ANSI X9.31, and Appendix A.4 of ANSI X9.62),
- The Deterministic Random Bit Generators (DRBG) (as specified in SP 800-90 *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*),
- The RSA algorithm (as specified in ANSI X9.31 and Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002),
- The Keyed-Hash Message Authentication Code (HMAC) (as specified in FIPS 198 *The Keyed-Hash Message Authentication Code (HMAC)*),
- The Counter with Cipher Block Chaining-Message Authentication Code (CCM) mode (as specified in SP 800-38C *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*),
- The Cipher-based Message Authentication Code (CMAC) Mode for Authentication (as specified in SP 800-38B *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*), and
- The Elliptic Curve Digital Signature Algorithm (ECDSA) (as specified in ANSI X9.62).

In FY2009, we expect to augment the CAVS tool to provide algorithm validation testing for:

- Key Agreement Schemes and Key Confirmation as specified in SP 800-56A *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, and
- The Galois/Counter Mode (GCM) GMAC Mode of Operation (as specified in SP 800-38D *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*).




| Fiscal Year | AES | DES | DSA | DRBG | ECDSA | HMAC | RNG | RSA | SHA | SJ | TDES | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FY 1996 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| FY 1997 | 0 | 11 | 6 | 0 | 0 | 0 | 0 | 0 | 7 | 2 | 0 | 26 |
| FY 1998 | 0 | 27 | 9 | 0 | 0 | 0 | 0 | 0 | 6 | 0 | 0 | 42 |
| FY 1999 | 0 | 30 | 14 | 0 | 0 | 0 | 0 | 0 | 12 | 1 | 0 | 57 |
| FY 2000 | 0 | 29 | 7 | 0 | 0 | 0 | 0 | 0 | 12 | 1 | 28 | 77 |
| FY 2001 | 0 | 41 | 15 | 0 | 0 | 0 | 0 | 0 | 28 | 0 | 51 | 135 |
| FY 2002 | 30 | 44 | 21 | 0 | 0 | 0 | 0 | 0 | 59 | 6 | 58 | 218 |
| FY 2003 | 66 | 49 | 24 | 0 | 0 | 0 | 0 | 0 | 63 | 3 | 73 | 278 |
| FY 2004 | 82 | 41 | 17 | 0 | 0 | 0 | 28 | 22 | 77 | 0 | 70 | 337 |
| FY 2005 | 145 | 54 | 31 | 0 | 14 | 115 | 108 | 80 | 122 | 2 | 102 | 773 |
| FY 2006 | 131 | 3 | 33 | 0 | 19 | 87 | 91 | 63 | 120 | 1 | 83 | 631 |
| FY 2007 | 240 | 0 | 63 | 0 | 35 | 127 | 137 | 130 | 171 | 1 | 136 | 1,040 |
| FY 2008 | 268 | 0 | 77 | 4 | 41 | 158 | 137 | 129 | 191 | 0 | 122 | 1,127 |

http://csrc.nist.gov/groups/STM/cavp
Contact: Ms. Sharon Keller
(301) 975-2910
sharon.keller@nist.gov

### ISO Standardization of Cryptographic Module Testing

CSD has contributed to the activities of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), which issued ISO/IEC 19790, *Security Requirements for Cryptographic Modules*, on March 1, 2006. With the publishing of ISO/IEC 19790, Subcommittee 27 (SC27) approved and began work on ISO/IEC 24759, *Test Requirements for*

*Cryptographic Modules*. This project was completed and ISO/IEC 24759, *Test Requirements for Cryptographic Modules*, was published on July 1, 2008. This effort will bring consistent testing of cryptographic modules in the global community.

At the spring 2008 ISO/IEC meeting, ISO/IEC JTC 1/SC 27 requested that its Secretariat circulate a call for contributions for the revision of ISO/IEC 19790, *Security Requirements for Cryptographic Modules*. An outline of planned NIST FIPS 140-3, *Security Requirements for Cryptographic Modules*, was submitted by the United States national standards body to be considered for this revision. At the fall 2008 ISO/IEC meeting the Secretariat approved the appointment of editors for this project, including Mr. Randall J. Easter from NIST.

---

http://csrc.nist.gov/cryptval/
Contact: Mr. Randall J. Easter
(301) 975-4641
randall.easter@nist.gov

### Development of Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules*

FIPS 140-2, *Security Requirements for Cryptographic Modules*, provides for four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. The standard provides users with a specification of security features that are required at each of four security levels; flexibility in choosing security requirements; a guide to ensuring that the cryptographic modules incorporate necessary security features; and the assurance that the modules are compliant with cryptography-based standards.

CSD continues to evaluate new technologies that impact cryptographic security, and examines cryptographic standards every five years for their security capabilities. We are developing FIPS 140-3 to meet the new and revised requirements of federal agencies for cryptographic systems, and to address technological and economic changes that have occurred since the issuance of FIPS 140-2. The development of FIPS 140-3 was started in 2005. In July 2007, the first draft of a future standard was released for public comment. This draft standard proposed increasing the number of security levels from four to five. Many other improvements were introduced, reflecting the developing industry trends and our analysis of public comments. The draft standard stipulated that the authentication requirements should be strengthened; that the software security should become a separate new topic; that at higher levels of security, the module should be protected against non-invasive attacks; and that there should be more flexibility in how the self-tests are performed. The comment period, which ended on October 11, 2007, was followed by a thorough review and analysis of all comments.

In March 2008, NIST held a one-day workshop to discuss the software security issues associated with FIPS 140-3. More than 70 people representing many software vendors participated in this event. The workshop participants contributed many new comments in addition to those collected after the first draft of FIPS 140-3 was published. The second draft of the standard is currently under development. It will be made available to the public for comments, with the final version of the standard expected to be announced in late FY2009. The FIPS 140-3 standard will take effect six months after the final version is approved by the Secretary of Commerce.

---

Contact: Dr. Allen Roginsky
(301) 975-3603
allen.roginsky@nist.gov

# SECURITY TECHNOLOGY GROUP (ST)

**STRATEGIC GOAL** ▸ *Develop and improve mechanisms to protect the integrity, confidentiality, and authenticity of Federal agency information by developing security mechanisms, standards, testing methods, and supporting infrastructure requirements and methods.*

## Overview

The CSD is continuing to make an impact in cryptography within and outside the Federal government. Strong cryptography can be used to improve the security of systems and the information that they process. Information technology users benefit from the availability of secure applications of cryptography in the marketplace. Our work in this area addresses such topics as hash functions, secret and public key cryptographic techniques, authentication, cryptographic protocols, public key certificate management, biometrics, and smart tokens. The impact of this work is demonstrated by the changes in the way that users authenticate their identities for on-line government services, and in the development of new standards for mobile wireless key derivation. This work also supports the CSD's Personal Identity Verification (PIV) project for Homeland Security Presidential Directive 12 (HSPD-12).

The CSD collaborates with national and international agencies and standards bodies to develop secure, interoperable security standards and guidelines. Federal agency collaborators include the Department of Energy, the Department of State, the National Security Agency (NSA), and the Communications Security Establishment of Canada. National and international standards bodies include the American Standards Committee (ASC) X9 (financial industry standards), the International Organization for Standardization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), the Liberty Alliance, and the Internet Engineering Task Force (IETF). Industry collaborators include Certicom, Entrust Technologies, InfoGard, Microsoft, NTRU, Orion Security, RSA Security, Voltage Security, Seagate, Cisco, and Wells Fargo.

## Cryptographic Standards Toolkit

### Hash Functions

A hash function processes a message, which can be very large, and produces a condensed representation, called the message digest. A cryptographic hash function is designed to achieve certain security properties and is typically used with other cryptographic algorithms, such as digital signature algorithms, key derivation algorithms, keyed-hash message authentication codes, or in the generation of random numbers. Cryptographic hash functions are frequently embedded in Internet protocols or in other applications; the two most commonly used cryptographic hash functions are MD5, which has been frequently broken but which was never approved for federal agency use, and the NIST-approved hash algorithm SHA-1.

In 2005, researchers found an attack method that threatens security of the SHA-1 hash algorithm. Since 2005 researchers at NIST and elsewhere have also discovered several generic limitations in the basic Merkle-Damgard construct, used by MD5, SHA-1 and most other existing hash functions. To address these threats, NIST held two cryptographic hash function workshops to assess the status of NIST's approved hash functions and to discuss the latest hash function research. NIST decided that it would be prudent to develop one or more additional hash functions through a public competition similar to the process used for the Advanced Encryption Standard (AES). We published draft minimum acceptability requirements, submission requirements, and evaluation criteria in the Federal Register on January 23, 2007 for public comment, and announced the cryptographic hash competition in the Federal Register on November 2, 2007. Submissions for new hash algorithms were requested by October 31, 2008. The competition is expected to take four years and we expect to complete an augmented Secure Hash Standard in 2012.

Two cryptographic standards were revised during 2008: FIPS 180-3, *Secure Hash Standard (SHS)*, and FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*. FIPS 180-3 specifies five cryptographic hash algorithms, and FIPS 198-1 specifies a method of using a hash algorithm from FIPS 180-3 to compute message authentication codes. In addition, two Draft NIST Special Publications (SPs) were posted for public review and comment: Draft SP 800-106, *Randomized Hashing for Digital Signatures,* and Draft SP 800-107, *Recommendation for Applications Using Approved Hash Algorithms*. The Draft SP 800-106 specifies a method to enhance the security of the cryptographic hash functions used in certain digital signature applications by randomizing the messages that are signed. The Draft SP

800-107 addresses security issues related to applications of approved hash algorithms and the use of HMAC as specified in FIPS 180-3 and FIPS 198-1 respectively; additional technical details for using these standards are also provided in the Draft SP 800-107.

### Digital Signatures

In FY2008, work continued on developing the draft of FIPS 186-3, a revision of the *Digital Signature Standard (DSS)*. This revision includes additional key sizes for the Digital Signature Algorithm (DSA) to provide higher security strengths, and guidance on the use of RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA) to promote interoperability. The draft DSS revision was issued for public comment in 2006. Subsequent work to address those comments has included analysis of the approved methods for RSA key pair generation and primality testing.

### Random Number Generation

Random numbers are needed by most cryptographic applications and algorithms. For example, random numbers are used to generate the keys needed for encryption and digital signature applications. NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs)*, specifies approved deterministic methods for random number generation. We have been working with Accredited Standards Committee X9 (ASC X9) to provide guidance on entropy sources and the construction of Random Bit Generators from entropy sources and DRBGs.

### Block Cipher Modes of Operation

The Galois/Counter Mode (GCM), a new mode of operation of the Advanced Encryption Standard (AES) algorithm specified in SP 800-38D *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, was approved in November 2007. GCM both encrypts and authenticates the data it protects. GCM is designed for high throughput in hardware applications, such as high-speed Internet routers.

In June 2008, we began a 90-day public comment period on a proposal to approve the XTS-AES mode of operation based on IEEE Standard 1619-2007. The XTS-AES mode is designed to encrypt data for storage applications, without expansion of the data; it was submitted to NIST by the Chair of the IEEE Security in Storage Working Group. The public comments on the mode were mixed; we are now reviewing the comments and we will decide whether to move forward with the approval in a NIST special publication.

We are also considering the Feistel Finite Set Encryption Mode (FFSEM), an AES mode designed to encrypt smaller blocks of data in a manner that preserves the format of the data. For example, the encrypted form of a social security number would itself appear to be a social security number. Consequently, in database applications, the fields of sensitive information could be encrypted, without disrupting the structure of the database; other fields of data could remain unencrypted to facilitate analysis.

### Recommendation for Key Management

The requirements for key management continue to expand as new types of devices and connectivity mechanisms become available (e.g., laptops, broadband access, smart cell phones). We continue to address the needs of the Federal government by defining the basic principles required for key management, including key establishment, wireless applications, and the Public Key Infrastructure (PKI).

SP 800-57, *Recommendation for Key Management* provides key management guidance. Parts 1 and 2 of SP 800-57 offer general guidance and best practices for the management of cryptographic keying material. Part 3 of SP 800-57 addresses application-specific guidance and will soon be available for public comment. It includes guidance on using a Public Key Infrastructure (PKI); protocols such as IPsec (Internet Protocol Security), TLS (Transport Layer Security), S/MIME (Secure/Multipart Internet Mail Extensions), Kerberos and OTAR (Over-the-Air Rekeying); and applications such as DNSSEC (Domain Name Systems Security Extensions) and Encrypted File Systems.

### Key Establishment using Public Key Cryptography

Key establishment is a process that results in shared secret keying material among different parties. NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, was completed in 2006. We expect to issue an additional publication, SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography* (e.g., RSA) for public review in FY2009.

### Key Management for Wireless Applications

Wireless Local Area Network (LAN) and Metropolitan Area Network (MAN) technologies are being widely adopted by government agencies. While wireless technologies can provide connections for mobile users, wireless devices and networks are also vulnerable to various attacks. The Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and other industry standards bodies have developed security protocols for wireless networks and communications.

A new feature for many wireless services is a fast "handoff" or transition between different access points. Fast handoff poses a new challenge for cryptographic key management. To make the handoff truly fast, cryptographic keys are derived and distributed among different access points so

that whenever a mobile station is roaming to a different access point, the keys are ready for a secure connection. A key hierarchy is derived from a master key for the fast handoff.

The primary security concerns relate to key establishment among multiple key holders. This is further complicated because, unlike a cellular system, a mobile LAN or MAN station determines when to make a transition from one access point to another. This makes it more difficult for the network to coordinate key establishment among multiple parties in a secure manner.

In 2008, we completed draft NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*, and requested public comments on the draft. The draft of SP 800-108 specifies three families of key derivation functions using pseudorandom functions. They incorporate the most commonly used key derivation functions in wireless applications. We expect to publish SP 800-108 in FY2009 after the public comments are resolved.

### Public Key Infrastructure

We continue to support the development and enhancement of key management standards for Public Key Infrastructure (PKI). Two significant milestones in NIST's Internet Engineering Task Force (IETF) standardization efforts were achieved in 2008. The *Server-based Certificate Validation Protocol (SCVP)* was published as RFC 5055. SCVP specifies a protocol that allows the work of validating certificates to be off-loaded to a delegated validation server. The third version of the *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* was published as RFC 5280. This document profiles the X.509 standard for Internet use, and is used as the basis for the development of most PKI products and the deployment of PKIs in both the public and private sectors. CSD led the editing teams for both of these documents. NIST has also contributed editors to three companion drafts for RFC 5280. These documents focus on encoding rules for public keys and digital signatures for some of the more advanced NIST-approved algorithms (e.g., elliptic curves and digital signatures with robust padding schemes). In addition to these documents, CSD will be organizing the interoperability report for RFC 5280, which is needed to progress this version to Draft Standard.

In addition to PKI standards, CSD has long assumed a leading role in the deployment of a robust and comprehensive Federal PKI (FPKI). Our efforts in 2008 focused on FPKI initiatives that support the deployment and management of Personal Identity Verification Cards (i.e., FIPS 201 *Personal Identity Verification (PIV) of Federal Employees and Contractors*). Since other aspects of the FPKI have entered a maintenance phase, we are taking a less active role. NIST remains a member of the FPKI Policy Authority, which manages the Federal Bridge Certification Authority (FBCA) and the Common Policy Root Certification Authority, and maintains the FPKI policies. NIST also maintains the FPKI certificate and CRL profiles that specify the contents of all FPKI X.509 certificates and CRLs used in the Federal PKI as a subset of the features in RFC 5280.

---

Contacts:

*Hash Functions* –
Ms. Shu-jen Chang
(301) 975-2940
shu-jen.chang@nist.gov

*Digital Signatures, RNG, Key Mgmt.*–
Ms. Elaine Barker
(301) 975-2911
ebarker@nist.gov

*Block Cipher Modes* –
Dr. Morris Dworkin
(301) 975-2354
moris.dworkin@nist.gov

Dr. David Cooper *(PKI)*
(301) 975-3194
david.cooper@nist.gov

*FIPS 180-3 & 198-1, SP 800-106 & 107* –
Mr. Quynh Dang
(301) 975-3610
qdang@nist.gov

*PKI* –
Mr. William Polk
(301) 975-3348
william.polk@nist.gov

*Wireless Key Mgmt.*–
Dr. Lily Chen
(301) 975-6974
lily.chen@nist.gov

## Quantum Computing

Quantum computing has the potential to become a major disruptive technology affecting cryptography and cryptanalysis. While a scalable quantum computing architecture has not been built, the physics and mathematics governing what can be done by a quantum computer are fairly well understood, and several algorithms have already been written for a quantum computing platform. Two of these algorithms are specifically applicable to cryptanalysis. Grover's quantum algorithm for database search potentially gives a quadratic speedup to brute force cryptanalysis of block ciphers and hash functions. Grover's algorithm may therefore have a long-term effect on the necessary key lengths and digest sizes required for the secure operation of cryptographic protocols. An even larger threat is presented by Shor's quantum algorithms for discrete logarithms and factorization. Given a quantum computer large enough to perform simple cryptographic operations, Shor's algorithm provides a practical computational mechanism for solving the two ostensibly hard problems that underlie all widely used public key cryptographic primitives. In particular, all the digital signature algorithms and public key-based key establishment schemes that are currently approved by NIST would be rendered insecure by the presence of even a fairly primitive quantum computer.

While practical quantum computers are not expected to be built in the next decade or so, it seems inevitable that they will eventually be built. CSD hopes to plan for this eventuality by adding primitives to the cryptographic toolkit for public key-based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. In the event that such algorithms

cannot be found, We intend to draft standards for computer security architectures that do not rely on public key cryptographic primitives. In addition, We will also examine new approaches, such as quantum key distribution.

During FY2008, we participated in a number of conferences and meetings on quantum computing and quantum key distribution: the Updating Quantum Cryptography conference in Japan; an ARO/NSA/DTO Quantum Computing/ Quantum Algorithms program review; and a meeting about possible standards for quantum key distribution systems. In addition, we are continuing to meet with members of the Advanced Network Technology Division to discuss the network layer implications of quantum key distribution.

During FY2009, we will continue to study security technologies that may be resistant to attack by quantum computers, especially those that have generated some degree of commercial impact. If any of these technologies emerges as both commercially viable and widely trusted within the cryptographic community, we hope to move towards standardization.

---

Contact: Mr. Ray Perlner
(301)975-3357
ray.perlner@nist.gov

## Authentication

In FY2008, we completed a draft update of SP 800-63, *Electronic Authentication Guideline*, and requested public comments. SP 800-63 supports the Office of Management and Budget (OMB) memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*. The OMB policy memorandum defines four levels of authentication in terms of assurance about the validity of an asserted identity. SP 800-63 gives technical requirements and example authentication technologies that work by making individuals demonstrate possession and control of a secret for each of the four levels. The draft publication updated SP 800-63 to address additional authentication mechanisms that are now available in the marketplace. Extensive comments were received that reflect the extent to which SP 800-63 has been adopted by many non-federal users and indicate a number of applications that were not anticipated in the original version of SP 800-63 or in the draft. The most difficult issues involve proposed new methods for reaching level 4, the highest authentication level, with current technologies. We expect to issue the final updated version of SP 800-63 in FY2009.

---

Contacts: Mr. William Burr
(301) 975-2934
william.burr@nist.gov

Mr. Ray Perlner
(301) 975-3357
ray.perlner@nist.gov

## Security Aspects of Electronic Voting

In 2002, Congress passed the Help America Vote Act (HAVA) to encourage the upgrade of voting equipment across the United States. HAVA established the Election Assistance Commission (EAC) and the Technical Guidelines Development Committee (TGDC), chaired by the Director of NIST. HAVA calls on NIST to provide technical support to the EAC and TGDC in efforts related to human factors, security, and laboratory accreditation. To explore and research issues related to the security and transparency of voting systems, the TGDC established the Security and Transparency Subcommittee (STS). As part of NIST's efforts led by the Software and Systems Division, CSD supports the activities of the EAC, TGDC, and STS related to voting equipment security.

From 2006 to 2007 we supported the TGDC in the final development of the *Voluntary Voting System Guidelines (VVSG)*. In the past year, we developed an initial draft of a test suite for the security requirements of the VVSG and initiated reviews of the draft test suite. At the request of the EAC, we investigated alternative means of achieving voting system auditability beyond the Software Independence approach, in order to encourage innovation in voting systems. We conducted research into the security ramifications of Ballot-on-Demand and Vote-By-Phone technologies. In addition, we supported the EAC's efforts to improve the voting process for citizens under the Uniformed and Overseas Citizens Voting Act (UOCAVA) by leveraging electronic technologies.

In FY2009 we will support the EAC with resolution of public comments on the VVSG recommendations. We will conduct an external review of the test suite for the security requirements in the VVSG recommendations. We plan to update the VVSG security requirements and the test suite based on the comments from these reviews. We will continue to assist the EAC on research efforts, such as UOCAVA voting, alternatives to Software Independence, and threats to voting systems. We will support the NIST National Voluntary Laboratory Accreditation Program (NVLAP) accreditation efforts of voting system test laboratories, host the TGDC plenary meetings, and support STS activities. We plan to engage voting system manufacturers, voting system test laboratories, state election officials, and the academic community to explore ways to increase voting system security and transparency.

---

http://vote.nist.gov/
Contacts: Dr. Nelson Hastings
(301) 975-5237
nelson.hastings@nist.gov

Mr. Andrew Regenscheid
(301) 975-5155
andrew.regenscheid@nist.gov

# SYSTEMS AND NETWORK SECURITY GROUP (SNS)

**STRATEGIC GOAL** ▸ *Devise advanced security methods, tools, and guidelines through conducting near-term and midterm security research.*

## Overview

In our security research, we focus on identifying emerging technologies and developing new security solutions that will have a high impact on the critical information infrastructure. We perform research and development on behalf of government and industry from the earliest stages of technology development through proof-of-concept, reference and prototype implementations, and demonstrations. We work to transfer new technologies to industry, to produce new standards, and to develop tests, test methodologies, and assurance methods.

To keep pace with the rate of change in emerging technologies, we conduct a large amount of research in existing and emerging technology areas. Some of the many topics we research include smart card infrastructure and security, wireless and mobile device security, Voice over Internet Protocol (IP) security issues, digital forensics tools and methods, access control and authorization management, IP security, intrusion detection systems, quantum information system security and quantum cryptography, and vulnerability analysis. Our research helps to fulfill specific needs by the federal government that would not be easily or reliably filled otherwise.

We collaborate extensively with government, academia, and private sector entities. In the past year, this included the National Security Agency, the Department of Defense, the Defense Advanced Research Projects Agency, the Department of Justice, the University of Maryland, George Mason University, Rutgers University, Purdue University, George Washington University, the University of Maryland-Baltimore County, Columbia University, Microsoft Corporation, Sun Microsystems, the Boeing Company, Intel Corporation, Lucent Technologies, Oracle Corporation, and MITRE.

## Identity Management Systems

### Personal Identity Verification

In response to Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, was developed and was approved by the Secretary of Commerce in February 2005. HSPD-12 calls for the creation of a new identity credential for Federal employees and contractors. FIPS 201 is the technical specification of the new identity credential and the PIV System that produces, manages, and uses the credential. The release of FIPS 201 marked the beginning of a learn-design-develop-test-validate phase for both HSPD-12 product suppliers and Federal departments and agencies. During this phase, over 300 standard-conformant products were developed, validated, and brought to market, and departments and agencies developed and refined their PIV issuance processes. By early 2008, production PIV issuance systems were operating, and the emphasis had shifted to high-volume enrollment of Federal employees and contractors in the PIV System. By October 2008, approximately 250,000 Federal employees have been sponsored to the General Services Administration PIV issuance system alone; several agencies have achieved issuance to 50% of employees; and some agencies are expected to reach 90-95% enrollment in the near future.

CSD activities in 2008 related to the FIPS 201 standard directly supported the increase in operational use of the identity credential. To achieve this level of use,

- Priority was given to requests for assistance from Federal departments and agencies and their suppliers;
- To maintain the stability of the technical standard, FIPS 201-1, the provisions of Change Notice 1 (in effect) were kept in effect.
- Modifications to the supporting Special Publications were limited to those committed and scheduled in previous years, a small number of necessary, backward-compatible process and technical improvements (detailed below), and editorial improvements for clarity;

- Effort was devoted to the application of issued PIV credentials, in particular, to Physical Access Control Systems (PACS), and downloadable software packages, useful as demonstrations of PIV and tutorials for product developers.

With the release of NIST Special Publication (SP) 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, in 2005, and continuing with the release of NIST SP 800-78-1 *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* in 2007, dates were established for discontinuing the use of certain cryptographic algorithms in the PIV System and PIV Cards (specifically, RSA 1024, SHA-1, and 2TDEA). This action was necessary to ensure adequate cryptographic strength for PIV applications. The use of higher strength cryptographic algorithms was enabled by SP 800-78-1, but since corresponding changes were needed in the PIV Card technical specification, a revision of NIST SP 800-73-2, *Interfaces for Personal Identity Verification*, was released in 2008. NIST SP 800-73-2 enabled the use of RSA 2048, SHA-256, and Elliptic Curve algorithms to replace those algorithms that were discontinued. SP 800-73-2 otherwise maintains strict backward compatibility with SP 800-73-1. Two optional features were added to the technical specification: an on-card Discovery Object and a middleware entry point "PIVMiddlewareVersion," to resolve specific implementation issues. SP 800-73-2 was also organized in four parts, for ease of use and maintenance, and incorporates many editorial improvements.

The public comment periods on NIST SP 800-73-2 elicited many valuable suggestions from Federal departments and agencies and industry for PIV System and PIV Card enhancements. Two of these, encryption key history management and biometric Match-On-Card, were strongly supported by Department of State, Department of Homeland Security, and Department of Defense. We are evaluating these issues for future PIV System enhancements and possible inclusion in future revisions of FIPS 201-1 and the relevant Special Publications.

NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)*, was released in 2008. While the original version, SP 800-79, was written before any operating PIV System had been accredited, SP 800-79-1 incorporates experience from multiple implementations and successful Certification & Accreditation activities by several agencies. Substantial improvements include: business models (in-house, leased, shared, etc.) for PIV Card Issuers (PCI); lessons learned from past accreditations; and the effect of recent OMB Memoranda. The most significant changes are the replacement of "Attributes" with an objective set of PCI controls, and an assessment and accreditation methodology that assesses the capability and reliability of a PCI based on these controls. Specifically the accreditation methodology consists of the following steps:



- Derivation of PCI controls based on requirements in FIPS 201-1 and supporting documents, OMB Memoranda, etc.;
- Providing a context for PCI controls by identifying a set of hierarchical concepts such as PCI Accreditation Topics and PCI Accreditation Focus Areas;
- Development of assessment methods appropriate for each PCI control that will assess conformance to those underlying requirements; and
- Guidance for evaluating the results of assessments in order to arrive at an accreditation decision.

Draft NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)* was released for a second public comment period, and is expected to be issued after we review and resolve the comments received. Draft SP 800-116 is an application note that explains how the FIPS 201-1 standard, and the PIV System and PIV Cards that it describes, should be used to perform subject authentication in Physical Access Control Systems (PACS). The publication explains the vision for PIV System implementation, the criteria for judging progress and completion, and the benefits that can be produced by a complete implementation. It explains a simple facility security model (first described in a widely-referenced Army physical security handbook), and recommends how PIV Card authentication mechanisms should be selected and implemented at perimeter and interior access points. CSD gratefully acknowledges the contributions to the development of the publication by twenty-two Federal employees with expertise across the disciplines required and the facilities being protected.

On 1 May 2008, during the first public comment period for Draft SP 800-116, a workshop was held at NIST in Gaithersburg on the integration of PIV credentials with Physical Access Control Systems. Seventy PACS suppliers and users participated in the workshop, and the lively discussion resulted

in important improvements and additions to Draft SP 800-116. The authors thank the workshop participants for their many contributions.

As with our experience in the development of NIST SP 800-73-2, comments on Draft SP 800-116 have stimulated R&D activities that could lead to future standards improvements. We have drafted a research paper, *Symmetric Key Injection onto Smart Cards*, describing new approaches to symmetric key management on smart cards, and four cryptographic protocols that could be used to implement them. NIST is a participant in the Physical Access Interagency Interoperability Working Group (PAIIWG) of the Government Smart Card-Interagency Advisory Board (GSC-IAB), where security engineering principles for symmetric key management in Physical Access Control Systems are under discussion.

NIST Interagency Report (IR) 7452, *Secure Biometric Match-On-Card Feasibility Report* was published in 2008. This study explores the technical feasibility of biometric fingerprint matching performed on a smart card. NIST specified the feasibility criteria and test conditions, invited industry participation, and reported on the successful test results. An especially challenging condition was the requirement that all communication of biometric data between the smart card and card reader be encrypted, and that all communication of smart card assertions to the card reader be authenticatable. At the conclusion of the study period, four companies had submitted seventeen test configurations resulting in successful tests. The performance criterion of match completion in less than 2.5 seconds was met by all seventeen configurations, an important milestone in the evolution of authentication technology. In parallel with the study underlying NISTIR 7452, the NIST Information Access Division completed NISTIR 7477, a companion study demonstrating that biometric Match-On-Card algorithms can meet the accuracy criteria established by the Minutiae Interoperability Exchange Test (MINEX) testing.

NIST published two software packages in 2008 that demonstrate PIV in action: *Partial CSP Software*, a partial implementation of a Windows 2000 Cryptographic Service Provider (CSP), that demonstrates the use of a PIV Card to logon to Windows 2000; and "PKCS #11 Software," an implementation of a Public Key Cryptography Standard #11 cryptographic module, that demonstrates the use of a PIV Card to authentication SSL/TLS sessions with Firefox, and to sign/verify and encrypt/decrypt email messages with Thunderbird, on Fedora Core Linux. These software packages can be downloaded without cost from the CSD web site, *http://csrc.nist.gov*. (Note: these packages are demonstrations, are limited in function, have not been tested and validated for use by Federal agencies or departments, and are provided without support; they are not suitable as alternatives to commercial software products.) A third demonstration package, featuring biometric enrollment and authentication, is currently under development.

NIST responds to many questions relating to HSPD-12, FIPS 201-1, and Personal Identity Verification each month. Questions originate from the OMB HSPD-12 Support Team, the Federal Identity & Credentialing Committee, the Government Smart Card-Interagency Advisory Board (GSC-IAB), Executive Branch departments and agencies, Legislative Branch offices, the media, the technology industry, and concerned citizens. Whenever possible, we try to answer questions immediately. Sometimes, the questions motivate new tasks with larger consequences. In 2008, for example, technical questions about the validation of PIV Cards motivated the description and initiation of a task entitled "PIV Card Trust Validation Procedure," to specify the exact technical procedure departments and agencies should use to validate the trustworthiness of a PIV Card. Occasionally, new questions are received concerning publications that are not currently under revision. These questions will be considered when the relevant publications are selected for revision.

NIST will review FIPS 201-1 by February 2010 to assess its adequacy and ability to adapt to advancements and innovations in science and technology.

---

http://csrc.nist.gov/groups/SNS/piv

Contacts: Mr. William I. MacGregor
(301) 975-8721
william.macgregor@nist.gov

Ms. Hildegard Ferraiolo
(301) 975-6972
hildegard.ferraiolo@nist.gov

### NIST Personal Identity Verification Program (NPIVP)

The objective of the NIST Personal Identity Verification Program (NPIVP) is to validate Personal Identity Verification (PIV) components as required by Federal Information Processing Standard (FIPS) 201 *Personal Identity Verification (PIV) of Federal Employees and Contractors* for conformance to specifications in the FIPS 201 companion document SP 800-73-1, *Interfaces for Personal Identity Verification*. The two PIV components that come under the scope of NPIVP are PIV Smart Card Application and PIV Middleware. All of the tests under NPIVP are conducted by third-party test facilities, which are accredited as Cryptographic Module Test (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). These laboratories have extended the scope of testing to include PIV Smart Card application and PIV Middleware test methods, and are called accredited NPIVP test facilities. As of September 2008, there were ten accredited NPIVP test facilities.

To facilitate development of PIV Smart Card Application and PIV Middleware for conformance to interface specifications in SP 800-73-1, NPIVP published SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines*. In addition to the tests, this document also provides an interpretation of SP 800-73-1 specifications through publication of C-language bindings for PIV Middleware interface commands as well as detailed mapping of PIV Card Command Interface return codes to PIV Middleware Interface return codes.

We also developed an integrated toolkit called "PIV Interface Test Runner" for conducting tests on both PIV Card Application and PIV Middleware products, and provided the toolkit to accredited NPIVP test facilities.

In FY2008, six PIV Card application products were validated and certificates issued, bringing the total number of NPIVP-validated PIV Card application products to 15. In addition, two PIV Card application products were revalidated after the vendors made changes to the products for efficiency reasons and for storage scalability. Nine NPIVP-validated PIV Card application products passed the FIPS 140-2 *Security Requirements for Cryptographic Modules* validation, bringing the total number of FIPS 140-2 and NPIVP-validated PIV Card application products to eleven. In addition to PIV Card application products validation, NPIVP validated three PIV Middleware products, bringing the total number of NPIVP-validated PIV Middleware products to ten.

To facilitate testing of credential data on PIV Cards for conformance to the data model specifications in Appendix A of SP 800-73-1, NPIVP published SP 800-85B, *PIV Data Model Test Guidelines*, and developed an associated toolkit, "PIV Data Model Test Runner." In order to enable the toolkit to be used for supporting the GSA's FIPS 201 Evaluation Program's Electronic Personalization Product certification, NPIVP made several enhancements to the PIV Data Model Test Runner, including reporting capabilities. NPIVP also enhanced the PIV Data Model Test Runner to include the functionality to generate multiple sample data sets in addition to the feature for populating a PIV Card with a data set. To facilitate development of conformant Personal Identity Verification (PIV) products by vendors, NPIVP also made the PIV Data Model Test Runner available for download from the NIST Web site. As of September 24, 2008, 163 vendors/system integrators had downloaded the PIV Data Model Test Runner.

In September 2008, we released SP 800-73-2, *Interfaces for Personal Identity Verification*. The four parts that comprise SP 800-73-2 supersede the single document SP 800-73-1, published in April 2006. While SP 800-73-2 was finalized, NPIVP identified the necessary updates for the PIV Interface Test Runner to align with SP 800-73-2 and SP 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. In the future, NPIVP Test Laboratory will use the updated PIV Interface Test Runner for evaluating new PIV Card application and PIV Middleware products.

---

http://csrc.nist.gov/groups/SNS/piv/npivp

Contacts: Dr. Ramaswamy Chandramouli
(301) 975-5013
chandramouli@nist.gov

Ms. Hildegard Ferraiolo
(301) 975-6972
hildegard.ferraiolo@nist.gov

## Conformance Tests for Transportation Worker Identification Credential (TWIC) Specifications

The TWIC Reader Hardware and Card Application Specification document was developed by the Transportation Worker Identification Credential (TWIC) Working Group (TWG) set up by the National Maritime Security Advisory Committee (NMSAC). This committee was set up under the provisions of the Maritime Transportation Security Act (MTSA), and is a joint initiative of Transportation Security Administration (TSA) and United States Coast Guard, both organizations under DHS. TWIC is a common identification credential for all personnel requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, and all mariners holding Coast Guard-issued credentials. TSA will issue workers a tamper-resistant "Smart Card" containing the worker's biometric (fingerprint template) to allow for a positive link between the card itself and the individual.

In order to facilitate commercial development of Smart Cards and Credential data for conformance to the TWIC Reader Hardware and Card Application Specification, the DHS Directorate of Science and Technology's (S&T) Office of Standards and Certification approached NIST to develop conformance tests. In FY2008, NIST completed the development of the "TWIC Interface and Data Model Test Runner" consisting of a suite of 102 tests under the following categories:

- TWIC Card Application Interface Conformance Tests
- TWIC Data Model Conformance Tests

The Data Model Conformance Tests validate conformance of data present in both the Smart Card chip as well as in the Magnetic Stripe. Following validation of the tests by running them against a sample TWIC card produced by TSA, NIST suggested enhancements to the test runner in the form of additional tests. Following approval of funding from the DHS S & T Directorate for this proposal, NIST has initiated development of these additional tests in the test runner. In addition, NIST also suggested improvements to the specifications to remove ambiguities in interpretation and to facilitate precise test outcomes.

---

Contact: Dr. Ramaswamy Chandramouli
(301) 975-5013
chandramouli@nist.gov

## Global eID

A very large number of large-scale identity management systems (IDMSs) are being developed and deployed worldwide. The technologies supporting these systems are also being developed globally. While many standards bodies, such as ISO (International Standards Organization), are covered by other areas of CSD, there are a number of non-standards bodies—such as the Porvoö Group, the International Telecommunication Union, the Asian Identification Card Forum, the Organisation for Economic Cooperation and Development, and the Global Collaboration Forum—meeting and moving forward with developments.

It is difficult to compare these large-scale IDMSs that are being developed and deployed, and to identify trends, locate potential interoperability issues, or develop metrics for them. Frequently, current information about large-scale IDMSs is presented in very inconsistent, often confusing formats. Particulars about the systems—technical, operational, policy-related—are haphazardly presented and discussed, leaving many unanswerable questions. To date, there has been no known attempt to fill in the gaps and to present the information about these systems in a consistent format that would enable research, trend analysis, and the development of metrics.

The principal long-term goal of the eID project is to help keep parts of NIST, as well as pertinent USG agencies, well informed of non-standards activities in the identity management realm outside of the United States borders.

Another goal is to assemble a large enough store of information about large-scale IDMSs so that several later projects will become more viable. This work will be a Landscape of IDMSs. One project that will benefit from this Landscape is the development of common models of IDMSs. Another is the development of metrics for IDMSs. Trend analyses and identification of barriers to interoperability of these systems will also be enabled by having this large amount of data on various systems in a consistent format.

The initial framework for this Landscape of IDMSs has been developed, and data collection has been started. This Landscape will only collect information that is publicly available, and will work closely with representatives world-wide to verify this information. The Landscape will also be included as collaborative work with the Permanent eID Status Observatory (PESO), which is also currently under development. A presentation on the Landscape work was given at the World eID 2008 Conference in Sophia-Antipolis, France, in September 2008.

---

http://www.itl.nist.gov/ITLPrograms/IDMS/external/Global_eID.html
Contact: Ms. Tanya Brewer
(301) 975-4534
tbrewer@nist.gov

## Identity Credential Smart Card Interoperability: ISO/IEC 24727 Identification Cards-Integrated Circuit Cards Programming Interfaces

With the emergence of Homeland Security Presidential Directive 12 (HSPD 12) and the respective mandate for a government wide standard for secure and reliable forms of identification for federal government employees and contractors, the use of smart cards will increase, both in private and public sectors, as will smart card-based transactions and applications.



According to recent reports, identity theft continues to be a growing problem and is considered the number one cyber threat by many experts. The use of solutions that provide secure and strongly authenticated identity credentials is increasingly important for safeguarding personal information and protecting the integrity of IT systems. Smart cards coupled with security protections provide the necessary elements of such a solution. They provide cryptographic mechanisms, store biometrics and keys, and, using certain techniques, address privacy considerations. Technological solutions for increased security of identity credentials improve the ability of the consumer to protect assets and informatics privacy.

Until recently, existing United States and international identification and smart card standards lacked standardized application interfaces and security mechanisms. Large-scale use of smart cards within the United States had lagged despite the potential benefits because of the interoperability limitations. The ISO/IEC 24727 suite of standards provides for the development of formal standards for smart card interoperability and security schemes.

During FY2008, we continued the development of ISO/IEC 24727, *Identification Cards – Integrated Circuit Cards Programming Interfaces*, the multipart standard resolving current voids and interoperability challenges found in existing standards.

This suite of standards established the architecture required to develop secure and interoperable frameworks for integrated circuit card technology and identity credentials. It enables interoperable and interchangeable smart card systems and eliminates consumer reliance on proprietary-based solutions that have been historically inherent in this industry. Existing standards provide the consumer with a solution, but these standards offer a plethora of options, making it very difficult, almost impossible, to ensure seamless interoperability. Furthering the development of formally recognized international standards through collaborative efforts with public and private sectors will support organizations in providing an interoperable and secure method for interagency use of smart card technology, in particular for identity management activities.

ISO/IEC 24727 provides a set of programming interfaces for interactions between integrated circuit cards (ICCs) and applications to include multi-sector use of generic services for identification, authentication, and signature. ISO/IEC 24727 is specifically relevant to identity management applications that require secure transactions and interoperability among diverse application domains. This standard defines interfaces such that independent implementations are interoperable. Card application and associated services are discoverable without reliance on proprietary information. This multi-part standard will allow conformant interfaces devices, such as reader devices, to read and interact with most if not all identity cards. It consists of the following parts :

- ISO/IEC 24727-1 – Identification cards – Integrated circuit card programming interfaces – Part 1: Architecture
  - ISO/IEC 24727-1 specifies the framework and supporting mechanisms and interfaces. It provides essential background information for the subsequent parts.
- ISO/IEC 24727-2 – Identification cards – Integrated circuit card programming interfaces – Part 2: Generic card interface
  - ISO/IEC 24727-2 details the functionality and related information structures available to the implementation of the application interface defined in ISO/IEC 24727-3. It provides a generic card interface.
- ISO/IEC 24727-3 – Identification cards – Integrated circuit card programming interfaces – Part 3: Application interface
  - ISO/IEC 24727-3 details service access mechanisms for use by any application to include authentication protocols that are in use by identity systems (e.g., personal identification number [PIN], biometric, symmetric key). It provides a common application programming interface (API) and interoperable authentication protocols, the first to be standardized by a standards-setting group.
- ISO/IEC 24727-4 – Identification cards – Integrated circuit card programming interfaces – Part 4: API administration
  - ISO/IEC 24727-4 details the security model and interface for secure messaging within the framework. It provides API administration between Part 2 and Part 3, and a standard API for interface devices (card readers).
- ISO/IEC CD 24727-5 – Identification cards – Integrated circuit card programming interfaces – Part 5: Testing
  - ISO/IEC 24727-5 contains conformance testing requirements.
- ISO/IEC CD 24727-6 – Identification cards – Integrated circuit card programming interfaces – Part 6: Registration procedures for the authentication protocols for interoperability
  - ISO/IEC 24727-6 outlines the registration process for ISO/IEC 24727 authentication protocols and for registering use of ISO/IEC 24727 using a registration authority. Using a registration authority prevents the need to amend the standard when new authentication protocols are introduced for ISO/IEC 24727-3. Standards Australia International has the contract with ISO for this registration authority.

As of September 30, 2008, ISO/IEC 24727-1, ISO/IEC 24727-2, and ISO/IEC 24727-4 were final and available for purchase. ISO/IEC 24727-3 was expected to be available in the near future. ISO/IEC 24727-5 is a committee draft, with an anticipated published date in late 2009. ISO/IEC 24727-6 is currently a final committee draft and final publication is anticipated in mid to late 2009. International support of these specifications will assure prescriptive APIs and interfaces for future years

Although not entirely finalized, this standard has been publicly adopted by the European community for the European Union Citizens Card, by Germany for the German health card, by Australia for their smart card framework, and by Queensland for the next generation driver's license. We continue to work with the United States national standards committee to ensure compatibility with federal credentials and to address the needs of nonfederal communities.

Contact: Ms. Teresa Schwarzhoff
(301) 975-5727
teresa.schwarzhoff@nist.gov

### IDMS Modeling and Metrics

Globally, there is emphasis on security for identity management (IDM) that is needed to support both logical and physical access control. Many different solutions are available and under development. For example, the public sector has deployed several identity management solutions such as Personal Identity Verification (PIV) for federal employees and contractors, Transportation Workers Identity Credential (TWIC) for transportation workers, First Responder Authentication Credential (FRAC) for first responders, passports for international travelers, and frequent flyer programs for registered travelers. Similarly, the private sector has its own identity management solutions to issue and manage identifiers deployed for various purposes, such as employee identification cards, customer loyalty cards, customer credit cards, amusement park season passes, and username/password combinations for web site access. All of these identity management systems (IDMSs) offer some level of security, but it is difficult for the owners of each system to evaluate these levels of security objectively. Objective evaluation would allow organizations to make an informed risk decision as to whether to trust identities presented from other organizations. Currently, there are no objective evaluation metrics to determine the level of the assurance in response to questions such as if the identity proofing process of IDMS A is as rigorous as the proofing process of IDMS B.

Determining a level or measure of assurance requires the development of objective, global IDMS metrics that measure the characteristics, protocols, and processes of an IDMS. The metrics will provide an objective basis for establishing trust among parties to an IDMS transaction. For example, the process of identity proofing could be used as a metric that affects the level of assurance in an identity.

The development of global IDMS metrics requires the creation of a generic IDMS model in order to establish a common frame of reference by which disparate implementations can be compared and contrasted against an established baseline at multiple levels of analysis. In FY2008, we developed the generic model for IDMS, which will provide the basis for the development of IDMS metrics. Additionally, we are beginning to collaborate with organizations actively engaged in the development of IDMS standards, such as ISO JTC 1/ SC27 and ITU-T. In the future, we will explore in-depth characteristics of IDMS to develop metrics that can be used to objectively evaluate IDMS implementations and can inform design decisions for new IDMS implementations.

The success of this project will:

- Provide a model and metrics to determine a level or measure of IDM assurance for the interoperation among parties.
- Provide design decisions for new IDMS implementations
- Assist understanding of identity assurance characteristics of various IDMS infrastructures and environments.
- Promote trust management for pervasive and community computing environments by providing a common understanding of risk among global entities.

Contacts:
Mr. Matthew Barrett
(301)975-3390
mbarrett@nist.gov

Ms. Donna Dodson
(301)975-3669
ddodson@nist.gov

Dr. Vincent Hu
(301) 975-4975
vhu@nist.gov

Ms. Erika McCallister
(301) 975-5144
erika.mccallister@nist.gov

Mr. Matthew Scholl
(301) 975-2941
matthew.scholl@nist.gov

Mr. Kevin Stine
(301) 975-4483
kevin.stine@nist.gov

## Biometric Standards and Conformity Assessment Activities

### Overview

Biometric technologies are used to establish or verify personal identity against previously enrolled individuals based upon recognition of a physiological or behavioral characteristic. Examples of biological characteristics include hand, finger, facial, and iris. Behavioral characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. Using biometrics for identifying human beings offers some unique advantages because only biometrics can identify you as you. Used alone, or together with other authentication technologies such as tokens, biometric technologies can provide higher degrees of security than other technologies employed alone and can also be used to overcome their weaknesses. For decades, biometric technologies were used primarily in law enforcement applications, and they are still a key component of these important applications.

Over the past several years, the marketplace for biometrics solutions has widened significantly and includes public and private sector applications worldwide. Biometric technologies are used in diverse applications such as border, aviation, maritime, and transportation security and physical / logical access control. Market opportunities for biometrics include financial institutions, the healthcare industry, and educational applications Consumer uses are also expected to significantly increase for personal security and convenience in home automation and security systems, and in retail, gaming and hospitality industries. Biometric technologies are also used in cell phones, mobile computing devices and portable memory storage.

### Meeting Government and Other Customers' Needs

Many government and private sector applications require biometric-based, high-performance, interoperable, information systems. In the absence of the timely availability of open systems standards, users may need to use proprietary solutions. Migration from these proprietary systems to standards-based open-system solutions is usually difficult and expensive.

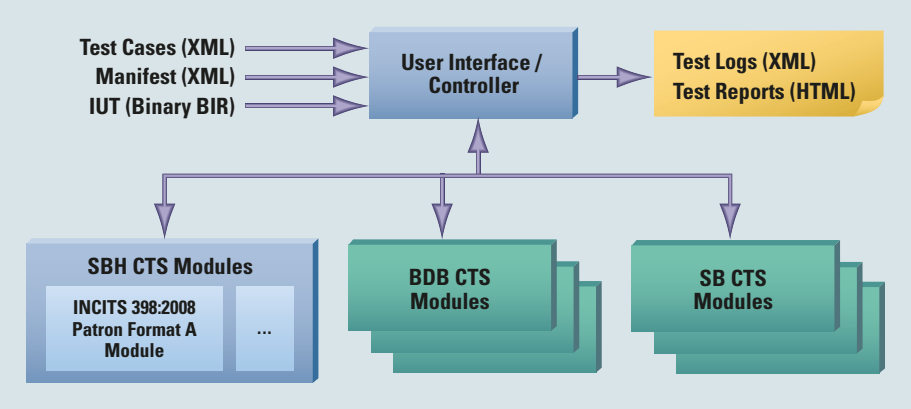
Our program supports the development of open standards for biometrics and promotes United States innovation and industrial competitiveness by advancing measurement science, standards and technology. We are responding to government, industry and market requirements for open-systems standards by

- accelerating development of formal national and international biometric standards and associated conformity assessment



- educating users on the capability of standards-based open-systems solutions
- promoting standards adoption
- developing conformance testing architectures and testing tools to test implementations of these standards
- supporting harmonization of biometric, tokens and security standards
- addressing the use of biometric-based solutions for ID Management applications

In FY2008, we continued to work in close partnership with other United States Government agencies, United States industry and academic institutions developing formal national and international biometric standards. We actively participate in NSTC's Subcommittee on Biometrics and Identity Management. CSD staff members and other NIST/ITL experts participate in its Standards and Conformity Assessment Working Group (SCA WG) and have collaborated within this group in the development of the initial version of the *Registry of United States Government Recommended Biometric Standards* which outlines those standards recommended for USG use in its operational systems. Updates of the Registry are planned. We are also participating in the Department of Homeland Security Biometrics Working Group and the Department of Defense Biometrics Task Force's Biometric Standards Working Group and other groups.. Our program experts work in close collaboration with ITL's Information Access Division's biometric experts to advance the adoption of biometric standards. Our program has gained national and international recognition for its achievements.




## National Biometric Standards Development

In late 2001, we helped to establish Technical Committee M1 – Biometrics under the InterNational Committee for Information Technology Standards (INCITS). Biometric standards are considered to be critical for United States needs, such as homeland defense, ID management, the prevention of identity theft, and for other government and commercial biometric-based personal verification or identification applications. CSD provides the Chair of INCITS M1, as well the Chair for one of the five INCITS M1 Task Groups, and actively participates in the development of its standards. During 2008 NIST/ITL/IAD provided the staff that served as the chair of one of the other INCITS M1 Task Groups.

Since its inception, twenty-four biometric standards developed by INCITS M1 have been published as American National Standards. They include data interchange formats for a number of biometric modalities, biometric technical interface standards, conformance testing methodology standards, biometric profiles, and biometric performance testing and reporting standards. INCITS M1 currently has sixteen ongoing standards development projects. During the last year, seven standards developed by INCITS M1, including two standards that were co-sponsored by CSD in INCITS M1:

- ANSI INCITS 429-2008, American National Standard for Information Technology - Conformance Testing Methodology for ANSI INCITS 358-2002, BioAPI Specification, May 2008
- ANSI INCITS 398-2008, American National Standard for Information Technology – Common Biometric Exchange Formats Framework (CBEFF), January 2008

## International Biometric Standards Development

In 2002, we successfully supported the establishment of Subcommittee 37 - Biometrics under the ISO/IEC Joint Technical Committee 1 (ISO/IEC JTC 1). CSD provides the Chair of SC37, NIST/ITL provides a member of the staff to serve as the Chair of one of its six Working Groups, and NIST/ITL/IAD provides technical editors supporting the development of some of the JTC 1/SC 37 projects. JTC 1/SC 37 has completed the first generation of biometric data interchange format and interface standards.

To date twenty-four standards developed by this Subcommittee have been published as International standards. They include data interchange formats for a number of biometric modalities, biometric technical interface standards, biometric performance testing and reporting standards and biometrics profiles. Three technical reports have been published as well.

JTC 1/SC 37's ongoing program of work of fifty standard projects includes a biometric vocabulary, interface-related standards, data interchange formats, and testing and performance specifications.

## Conformity Assessment to Biometric Standards

Base standards, such as biometric data interchange and technical interface standards, do not contain the conditions to demonstrate that products meet the technical requirements specified in the standards. Conformance testing captures the technical description of a specification and measures whether an implementation faithfully implements the specification. A conformance test suite implementation is test software that is used to ascertain conformance to a testing methodology described in a specification or standard. We support the development of biometric conformance testing methodology standards and other conformity assessment efforts through active technical participation in the development of these standards, sponsorship of specific biometric conformance testing methodology standards (e.g., conformance testing methodologies for biometric technical interfaces and biometric data interchange formats), and the development of associated conformance testing architectures. We develop these architectures and Conformance Test Suites (CTSs) to support users that require conformance to selected biometric standards and to support product developers interested in conforming to biometric standards by using the same testing tools available to users. These

testing tools support the possible establishment of conformity assessment programs to validate conformance to biometric standards.

### BioAPI Conformance Test Suite

In 2006 we released a BioAPI CTS developed to test implementations of ANSI INCITS 358-2002, the BioAPI specification. This software tool was developed to help users verify the conformance of Biometric Service Providers to ANSI INCITS 358-2002, the BioAPI Specification 1.1. The BioAPI CTS and associated documentation can be found at NIST's Biometric Resource Center web site (*http://www.nist.gov/biometrics*) We also co-sponsored with other members of INCITS M1 a conformance testing methodology standard for BioAPI. The BioAPI CTS implementation was developed using concepts and principles specified in this conformance testing methodology standard. The CTS was thoroughly tested with a number of commercially available vendor biometric subsystems for different modalities (e.g., face, iris and fingerprint recognition) claiming conformance to the BioAPI standard. The test results were successfully cross-validated with another similar CTS independently developed by DoD's Biometric Task Force.

### Conformance Testing Architectures for Biometric Data Interchange Formats and CBEFF Biometric Information Records

In August 2008 we released a conformance testing architecture that supports CTSs to test implementations of biometric data interchange formats and the three components of CBEFF Biometric Information Records (metadata, biometric data and security blocks). We also released a CTS to test implementations of Patron Format A data structures specified in ANSI INCITS 398-2008, Information technology - Common Biometric Exchange Formats Framework. The software and documentation can also be found at NIST's Biometric Resource Center . The CTS for Patron Format A supported by this conformance testing architecture was developed to help users determine whether binary file implementations of Biometric Information Records (BIRs) based on this Patron Format conform or not to the standard. NIST/ITL CSD sponsored in INCITS M1 development of a conformance testing methodology standard for CBEFF data structures specified in ANSI INCITS 398-2008 and has submitted to INCITS M1 the test assertions and related test cases developed for the Patron Format A Conformance Test Suite as well as test assertions and test cases for other Patron Formats specified in the ANSI INCITS 398-2008 standard. This standard is under development.

### Ongoing work

An advanced conformance testing architecture is currently being developed. Some of the key improvements being researched and /or implemented include:

- Module Dynamic Discovery – Similar to well-known programs that support "add-ins" or "plug-ins", this implementation loads CTS modules at runtime. There are two main benefits of this architecture: the modules can be developed without modifying the GUI source code, and new or updated modules are easily distributed and installed.
- Web Services – Modules can be called either on the local computer or on a web services computer anywhere on the internet or an intranet.
- Test Case Enhancement – Test Cases are greatly improved, allowing far fewer Test Cases to test more success and failure conditions.
- Testing Flexibility – Any module can be tested by itself (e.g., conformance testing to a standard biometric data interchange format).

### Impact of Biometric Standards and Related Conformity Assessment

Some of the "first generation" of biometric standards are now required by customers of personal authentication applications. Large organizations such as the International Civil Aviation Organization (ICAO) (for Machine Readable Travel Documents), the International Labour Office of the United Nations (for the Seafarers Identification Credential program) as well as the European Union (EU) have published requirements that include the use of international biometric standards developed by JTC 1/SC 37. The EU password specification working document, for example, describes solutions for chip-enabled EU passports, based on EU's Council Regulation on standards for security features and biometrics in passports and travel documents issued by member states. The specification relies on international standards, especially ISO standards and ICAO recommendations on Machine Readable Travel Documents, and includes specifications for biometric face and fingerprint identifiers; thus, the specifications are underpinned by ISO standards resulting from the work of JTC 1/SC 37. Several countries represented in JTC 1/SC 37 are also adopting the JTC1/SC 37 standards. For example, in Spain two official documents store biometric data using JTC 1/SC 37 standards. The electronic national identity card (DNIe) includes personal information of the citizen, details of electronic certificates and the biometric information. The image of the face is stored following the JTC 1/SC 37 face image format and ICAO standards. Finger minutiae are stored using the JTC 1/SC 37 standard. The biometric data included in Spanish e-Passports is the image of the face based on the JTC 1/SC 37 standard as well as the ICAO standard for MRTDs.

In the United States, several organizations require selected biometric data interchange standards developed by JTC 1/SC 37. Examples include applications and tests performed by government organizations, private industry, and consortia. The Transportation Security Administration (TSA) of the Department of Homeland Security (DHS) has issued guidance for use of biometric

technology in airport access control systems and is performing tests to establish a qualified products list of biometric technologies that meet standards set forth in the aforementioned guidance. Products tested in TSA Qualified Product List (QPL) Testing include enrollment stations and biometric sensors/readers that can be deployed at access points to secure airport areas. The test requirements reference two parts of the multi-part standard developed by JTC 1/SC 37 on biometric performance testing and reporting. NIST used a part of this multi-part standard for the "Minutiae Interoperability Exchange Test (MINEX)" tests. The Registered Traveler Interoperability Consortium (RTIC) uses some of the JTC 1/SC 37 standards as well.

INCITS M1 biometric standards are also required in major United States Government programs. Transportation Worker Identification Credential (TWIC) - Phase III - Prototype Phase - (DHS/TSA) required INCITS biometric standards such as the application profile - Interoperability and Data Interchange - Biometric Based Verification and Identification of Transportation Workers. DoD IT Standards Registry includes a number of the biometric data interchange format standards developed by INCITS M1. The Personal Identity Verification (PIV) specification (NIST SP 800-76-1) includes conformance requirements to several data interchange format standards including the finger minutiae template, the finger image and the face image data format standards as well as an instantiation of a BIR conforming to the CBEFF standard published in 2005 (INCITS 398-2005). The Registered Traveler Technical Interoperability specification requires conformance to a modified CBEFF BIR specified by the PIV specification as well as the finger and face image data interchange formats developed by INCITS M1. The *"Registry of USG Recommended Biometric Standards"* recommends a number of biometric standards developed by INCITS M1 and JTC 1/SC 37. A Working Group established by the Customer Service Department of the Reserve Bank of India to suggest suitable standards for raw images of fingerprints recommended the finger image standard developed by JTC1/SC 37.

We expect that the adoption of standards developed by INCITS M1 and JTC1/SC 37 will significantly increase in the near future. There are still a number of national and international standards under development that should reap big payoffs. CSD staff is instrumental in promoting ongoing biometrics standards work and the adoption of these standards. The work on national and international biometric standards and our related technical work have been presented by CSD staff at national and international conferences and publications.

### The Biometric Consortium

The Biometric Consortium (BC) serves as a focal point for research, development, testing, evaluation, and application of biometric-based personal identification/verification technology. The BC maintains a web-based Bulletin Board (BCBB).[1] The BC promoted government and industry specifications under the umbrella of NIST/BC *"Biometric Interoperability, Performance and Assurance Working Group"*. This Working Group developed the first specification of CBEFF published as NISTIR 6529 and the biometric template protection specification, now a standard project under development in ISO/IEC JTC 1/SC 27. Today, the BC's primary function is to organize and host an annual conference, which enables U.S. government participants to . engage in exchanges with national and international participants. CSD staff co-chairs the Consortium and helps to plan its conferences with the NSA co-chair.

The 2008 conference, held September 23-25 addressed the important role that biometrics can play in the identification and verification of individuals in government and commercial applications worldwide. Topics included technology innovations, biometric standards and the latest trends in biometrics research, development and applications of biometric technologies as well as current government initiatives and commercial applications in the United States and abroad. The Biometrics Symposium, a special session on research was held as one of the conference sessions. The Symposium was sponsored by the Biometric Knowledge Center of the National Science Foundation Center for Identification Technology Research (CITeR) and co-sponsored by IEEE, the IEEE Computer Society and IEEE Pattern Analysis and Machine Intelligence Technical Committee.

One of the largest conferences dedicated to biometrics worldwide, the conference as well as the co-located Technology Expo attracted more than 1,500 participants from United States and foreign governments, commercial organizations, industry, and academia. Over 120 internationally recognized experts in biometric technology, system application and standards developers, IT strategists, government and commercial executives and university researchers participated in the program. The conference was co-sponsored by NIST/ITL, National Security Agency (NSA), Department of Homeland Security (DHS), DoD Biometrics Task Force, National Institute of Justice (NIJ), General Services Administration - Office of Technology Strategy (GSA), Volpe National Transportation Systems Center, United States Department of Transportation and the Armed Forces Communications and Electronics Association (AFCEA). Five Keynote speakers from government and industry participated in the program. In addition to the three concurrent conference tracks, a series of special sessions and workshops were held.

NIST/ITL's biometric programs were represented at the NIST/ITL Booth, including ongoing activities of the Information Systems and the Computer Security Divisions. The biometric conformance testing architecture released in August 2008 and an existing CTS module, as well as a pre-released version of the advance architecture that supports CTSs for biometric data inter-

[1] *http://www.nist.gov/bc2008*

change formats and CBEFF Biometric Information Records, both developed by CSD staff, were demonstrated at this booth.

---

http://www.nist.gov/biometrics
Contact: Mr. Fernando Podio
(301) 975-2947
fernando.podio@nist.gov

## Research in Emerging Technologies

### Automated Combinatorial Testing for Software

NIST research suggests that software faults are triggered by only a few interacting variables. These results have important implications for testing. If all faults in a system can be triggered by a combination of n or fewer parameters (where n is the number of parameters), then testing all n-way combinations of parameters can provide high confidence that nearly all faults have been discovered. For example, if we know from historical failure data that failures for a particular application never involved more than four parameters, then testing all 4-way or 5-way combinations of parameters gives strong confidence that flaws will be found in testing.

We are working with the University of Texas, Arlington on a project that was initiated in 2006 to take advantage of this empirical observation by developing software test methods and tools that can test all n-way combinations of parameter values. The methods have been demonstrated in a proof-of-concept study that was presented at a NASA conference and are being further developed through application to real-world projects at NIST and elsewhere.

This work uses two relatively recent advances in software engineering—algorithms for efficiently generating covering arrays and automated generation of test oracles using model checking. Covering arrays are test data sets that cover all n-way combinations of parameter values. Pairwise (all pairs of values) testing has been popular for some time, but our research indicates that pairwise testing is not sufficient for high assurance software. Model checking technology enables the construction of the results expected from a test case by exploring all states of a mathematical model of the system being tested. Tools developed in this project will have applications in high assurance software, safety and security, and combinatorial testing.

Our focus is on empirical results and real-world problems. Accomplishments for FY2008 include the following:

- The project team released software implementing a new covering array algorithm that outperforms other known algorithms, in some cases by several orders of magnitude. The new tool has been acquired by over 100 beta users, including most of the major software and hardware developers and a number of universities. Several users have expressed interest in cooperating on joint projects to analyze the effectiveness of combinatorial testing on their real-world projects. In FY2008 the software was improved based on feedback from beta users. Several news articles on the software tools and the project appeared in IT trade publications.

- Research in FY2008 included a large study comparing combinatorial and random testing for a grid computer network simulation, a joint project initiated with North Carolina State University on combinatorial testing for analyzing access control systems, and improvements on a parallel covering array algorithm developed previously. Joint work with NIST/MEL (Manufacturing Engineering Laboratory) and Chalmers University (Sweden) was also initiated on applying these methods to manufacturing simulation.

- A repository for covering arrays, the first of its kind, was established in FY2007 on the NIST Mathematical and Computational Sciences Division server. The repository has now been populated with a large set of covering arrays for use by researchers in a variety of fields, including biotechnology, statistics, and software testing.

Plans for FY2009 include measuring the effectiveness of combinatorial testing for XML validation and Web application testing, access control policy and firewall testing, and working with industry researchers and practitioners to transition the tools and methods into practical application. We are working with researchers from several major universities, other NIST divisions and labs, and private industry.

---

http://csrc.nist.gov/acts
Contacts: Mr. Rick Kuhn
(301) 975-3337
kuhn@nist.gov

Dr. Raghu Kacker
Mathematical and Computational Sciences Division
(301) 975-2109
raghu.kacker@nist.gov

### Conformance Verification for Access Control Policies

Access control (AC) systems are among the most critical of network security components. Faulty policies, misconfigurations, or flaws in software implementation can result in serious vulnerabilities. The specification of access control policies is often a challenging problem. It is common that a system's privacy and security are compromised due to the misconfiguration of access

control policies instead of the failure of cryptographic primitives or protocols. This problem becomes increasingly severe as software systems become more and more complex, and are deployed to manage a large amount of sensitive information and resources that are organized into sophisticated structures. Identifying discrepancies between policy specifications and their properties (intended function) are crucial because correct implementation and enforcement of policies by applications is based on the premise that the policy specifications are correct. As a result, policy specifications must undergo rigorous verification and validation through systematic testing to ensure that the policy specifications truly encapsulate the desires of the policy authors.

To formally and precisely capture the security properties that access control should adhere to, AC models are usually written, bridging the rather wide gap in abstraction between policy and mechanism: users see an access control model as an unambiguous and precise expression of requirements; vendors and system developers see access control models as design and implementation requirements. Thus, techniques are required for verifying whether an AC model is correctly expressed in the AC policies and whether the properties are satisfied in the model. In practice, the same access control policies may express multiple access control models or express a single model in addition to extra access control constraints outside of the model. Ensuring the conformance of access control models and policies is a non-trivial and critical task.

During the past year, we developed a general approach of property verification for access control models by combining model checking and combinatorial testing. To demonstrate the proof of concept, we also devised prototype AC models for the application of various testing tools such as NuSMV model checker and Fireeyes combinatorial array generator. Our reports were published at some major related symposiums and conferences. In the coming year, we will extend our prototype system to a practical system that can be applied to generic AC models. We will also investigate in-depth issues such as code assertion verification, limitation, and none-model applications.

This project is expected to:

- Provide generic paradigm and framework of access control model/property conformance testing;
- Provide tools or services for checking the security and safety of access control implementation;
- Promote (or accelerate) the adoption of combinatorial testing for large system testing; and
- Assist system architects, security administrators, and security managers whose expertise is related to access control in managing their systems, and to learn the limitations and practical approaches for their applications.

Contacts: Dr. Vincent Hu
(301) 975-4975
vhu@nist.gov

Mr. Rick Kuhn
(301) 975-3337
kuhn@nist.gov

### Forensics for Web Services

Web services are becoming a popular way to design and implement a Service Oriented Architecture (SOA) in areas such as financial, government and military applications. Web services enable a seamless integration of different systems over the Internet using choreographies, orchestrations and dynamic invocations. Web services based on the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and related open standards, and deployed in SOA allow data and applications to interact without human intervention through dynamic and ad hoc connections.

The security challenges presented by the Web services approach are formidable. Many of the features that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are at odds with traditional security models and controls. The complexity in web services arises due to composing new services. These compositions create service inter-dependencies that can be misused for monetary or other gains. When a misuse is reported, investigators have to navigate through a collection of logs to recreate the attack. In order to facilitate that task, we are investigating techniques for forensics on web services (FWS), a specialized web service that when used would securely maintain transactional records between other web services. These secure records can be re-linked to reproduce the transactional history by an independent agency. In FY2008 as part of this project, we showed the necessary components of a forensic framework for web services and published a paper in a conference. In FY2009 we plan to do a proof of concept implementation to validate our results and publish the results as a NIST Internal Report.

Contact: Dr. Anoop Singhal
(301) 975-4432
Anoop.singhal@nist.gov

### Mobile Handheld Device Security and Forensics

Cell phones and other mobile handheld devices are ubiquitous today, used by individuals for both personal and professional purposes. Mobile devices can allow users to place calls, perform text, multimedia, and instant



messaging, exchange electronic mail, browse the Web, manage personal information (e.g., address book, task list, and calendar schedule), capture photos and videos, and also read, edit, and create digital documents. Over time, a significant amount of information tends to accumulate on them that may need to be protected from intruders or to be recovered as evidence for a security incident or crime investigation. Because of their pervasiveness and capabilities, mobile handheld devices are an emerging but rapidly growing area of computer security and forensics.

Although mobile handheld devices are approaching the functionally of desktop computers, their organization and operation are quite different in certain areas. For example, most cell phones do not contain a hard drive and rely instead on flash memory for persistent storage. They also are generally treated more as fixed appliances with a limited set of functions than as general-purpose systems with the capability for expansion, and no single operating system dominates cell phones. Such differences make the application of classical computer security and forensic techniques difficult.

The focus of the project is twofold: to improve the security of handheld devices develop and to improve the state-of-the-art of mobile device forensics. Past work in handheld device security included several proof-of-concept implementations of security mechanisms suitable for the capabilities and limitations of such devices. They are documented on the project Web site. This past year, we produced Special Publication (SP) 800-124, *Guidelines on Handheld Device Security*. The publication provides an overview of cell phone and Personal Digital Assistant (PDA) devices in use today and offers insights into making informed information technology security decisions on their treatment. The content covers details about the threats and technology risks associated with the use of these devices and the available safeguards to mitigate them. Users of cell phones, PDAs, and other business-oriented handheld devices, as well as security professionals and officials in the organization who are responsible for information technology security throughout the system lifecycle, should find the information beneficial.

Prior work at NIST in the mobile device forensics area examined the quality and use of forensic tools. During FY2008, our work has progressed to identifying and removing impediments to the practice of cell phone forensics. The first development is a forensically sound method to address the problems forensic tools have with latency in coverage for newly available phone models coming onto the market. The approach, called phone manager protocol filtering, augments the functionality of off-the-shelf phone managers, available from device manufacturers, to block unsafe commands. NIST recently issued Interagency Report (NISTIR) 7516, *Forensic Filtering of Cell Phone Protocols*, which documents the technique as applied to two popular phone managers.

The second development in mobile device forensics in FY2008 is a means to validate the correct functioning of forensic tools quickly and accurately. The approach, called identity module programming, automatically populates the identity modules of certain classes of cell phones with reference test data that serve as a baseline for validating the correct functioning of related forensic tools. A conference paper on the technique, *Reference Material for Assessing Forensic SIM Tools*, has been published and is available on the project Web site. A more in-depth NISTIR is expected to follow soon. The intended audience for publications in mobile device forensics ranges broadly from response team members handling a computer security incident, to organizational security officials investigating an employee-related situation, to forensic examiners involved in criminal investigations.

---

http://csrc.nist.gov/groups/SNS/mobile_security/

Contact: Mr. Wayne Jansen
(301) 975-5148
wjansen@nist.gov

## Policy Machine

As a major component of any operating system or application, access control mechanisms come in a wide variety of forms, each with their individual attributes, functions, methods for configuring policy, and a tight coupling to a class of policies. A natural consequence of the deployment of many heterogeneous systems is a lack of interoperability. A lack of interoperability may not be a problem for systems that can adequately operate independently of one another, but access control mechanisms require interoperability to function efficiently. Users with vastly different credentials have a need to access resources protected under different mechanisms, and resources that are protected under different mechanisms differ vastly in their sensitivity and therefore accessibility. This lack of interoperability introduces significant privilege and identity management issues.

Interoperation is one problem associated with today's access control operations. Another problem pertains to policy enforcement. Since the early days of shared computing, research programs have focused on creating access control models that support specific organization and resource sensitivity requirements. Of the numerous recognized access control policies, today's operating systems (Oss) are limited to the enforcement of instances of Discretionary Access Control (DAC) and simple variations of Role-Based Access Control (RBAC) policies, and to a far lesser extent, instances of Mandatory Access Control (MAC) policies. As a consequence, there are a number of important policies (orphan policies) that lack a commercially viable OS mechanism for their enforcement. Among these orphan policies is the need to combine arbitrary policies.

To fill policy voids, policies are routinely accommodated through the implementation of access control mechanisms at the application level. Essentially, any application that requires a user's authentication implements some form of access control. Not only do applications aggravate interoperation, identity and privilege management problems, but applications can also undermine policy enforcement objectives. For instance, although a file management system may narrowly restrict access to a specific file, chances are the contents of that file can be attached to or copied to a message and mailed to anyone in the organization or the world.

To solve the interoperability and policy enforcement problems of today's access control paradigm, NIST (in part under sponsorship of the Department of Homeland Security) has designed and developed a reference implementation for a standard access control mechanism referred to as the Policy Machine (PM). The PM is not an extension of any existing access control model or mechanism, but instead is an attempt to fundamentally redefine access control in general from its basic abstractions and principles. In doing so, we believe that the PM as currently specified and implemented represents a paradigm shift not only in the way we can specify and enforce policy, but also in the way we can develop applications, interact with, and approach our computer systems. The PM requires changes only in its configuration in the enforcement of arbitrary and organization-specific, attribute-based access control policies. Included among the PM's enforceable policies are combinations of policy instances (e.g., Role-Based Access Control and Multi-Level Security). In its protection of objects under one or more policy instances, the PM categorizes users and resources and their attributes into policy classes and transparently enforces these policies through a series of fixed PM functions that are invoked in response to user or subject (process) access requests.

In FY2008, we developed a simpler PM specification and revised our reference implementation to reflect those changes. Although simpler, the PM preserves its expressive capabilities (in terms of policies that could be configured and enforced). This includes support for database records as composite PM objects. Through composite objects, we are able to provide protection at the granularity of a field within a record or a form. In addition we managed to configure new policies used to confine and track the dissemination of sensitive data. This includes the protection of copies and extracts of sensitive data under the same policies as the original. In addition we are currently in the process of developing new architectural and functional specifications for the PM, which, we believe, will further enhance its efficiency and scalability.

If successful, we believe that the PM can benefit organizations in a number of ways, including—

- Policy flexibility – Virtually any collection of attribute-based access control policies can be configured and enforced.
- Policy combinations – Resources (objects) could be selectively protected under any combination of currently configured policies (e.g., DAC only, or DAC and RBAC).
- Single scope of control – Policies implemented at the file management and application levels today can be configured and enforced and as such are included in the PM's scope of control. Demonstrated application services include internal email, workflow management, and database management.
- Enterprise wide scope of protection – One administrative domain vs. administration on an OS-by-OS basis, access control policies are uniformly enforced over resources that are physically stored under different operating systems.
- Comprehensive enforcement – All user and process access requests, and all exchange of data to and from and among applications, between processes and access sessions, all exportation of data outside the



bounds of the PM are uniformly controlled under the protection policies of the objects of concern.

- Assurance – Configuration strategies could render malicious application code harmless, all enforcement could be implemented at the kernel level, and attributes could be automatically and minimally assigned to sessions (least privilege) to fit a user's access requests (as opposed to a user's attribute selection).

- True single-sign on – By virtue of the PM's single scope of control and a personal object system (POS) that includes the potential to view and open all user accessible resources, the need for a user to authenticate to multiple applications and systems is effectively eliminated.

Contacts: Mr. David Ferraiolo
(301) 975-3046
david.ferraiolo@nist.gov

Dr. Vincent Hu
(301) 975-4975
vhu@nist.gov

### Security for Grid and Pervasive Systems

While grid and pervasive computing have become closer to reality due to the maturity of the current computing technologies, these technologies present greater challenges compared to static network systems with infrastructure security issues such as authorization, directory services, and firewalls. The research available on grid and pervasive security-related topics is targeted to one specific system, is incomplete by making assumptions, or is ambiguous regarding the critical elements in their works. Because of the complexities of architecture and applications of the grid, a practical and conceptual guidance for their security is needed.

During FY2008, we 1) identified access control requirements and issues that are specific to grid and pervasive computing, 2) developed a trust management protocol for multi-grid environments, and 3) investigated solutions for composing access control policies for resource federation networks using emerging pervasive computing technologies such as Semantic Web and Resource Description Framework (RDF). Our findings were presented at some major related symposiums and conferences. In FY2009, we will extend our investigation from grid computing only to include trust management frameworks, functional stacks, protocols, and APIs for the pervasive systems' security functions that have either been embedded or recommended by commercial or standards organizations. In the future, we will focus on analyzing the capabilities and limitations of authorization management infrastructures that the selected grid or pervasive systems of previous research are capable of providing. We will also develop guide documentations or reference implementations using already-developed tools (such as Globus and Access Control languages) to demonstrate how to configure a grid or pervasive system to satisfy the security requirements.

We expect that this project will:

- Promote (or accelerate) the adoption of community computing that utilizes the power of shared resources and computing time of grid and pervasive infrastructure;

- Provide prototype security standards for the authorization management of community computing environments;

- Increase security and safety of static (connected) distributed systems by applying the trust domain concept of grid and pervasive computing; and

- Assist system architects, security administrators, and security managers whose expertise is related to community computing in managing their systems, and to learn the limitations and practical approaches for their applications.

Contact: Dr. Vincent Hu
(301) 975-4975
vhu@nist.gov

## Technical Security Metrics

Measurement is the key to making major advancements in any scientific field, and computer security is no exception. Measures give us a standardized way of expressing security characteristics. Because of the ever-increasing complexity of threats, vulnerabilities, and mitigation strategies, there is a particularly strong need for additional research on attack, vulnerability,

and security control measurement. Improved measurement capabilities in these areas would allow organizations to make scientifically sound decisions when planning, implementing, and configuring security controls. This would improve the effectiveness of security controls, while reducing cost by eliminating unnecessary, ineffective controls.

In FY2008, CSD began a long-term project on technical security metrics, focused primarily on attack, vulnerability, and security control measurement. A paper detailing the technical concepts behind the project was presented at the 1st International IEEE Conference on Information Technology in Gdansk, Poland in May 2008. The first stage of this work involves developing specifications for measuring and scoring individual vulnerabilities, and researching how vulnerabilities from multiple hosts can be used in sequence to compromise particular targets. A summary of these efforts from the past year is presented below.

### Vulnerability Measurement and Scoring

The Common Vulnerability Scoring System (CVSS) is an industry standard that enables the security community to calculate the relative severity of software flaw vulnerabilities within information technology systems through sets of security metrics and formulas. The CVSS version 2 standard is being promoted by a special interest group within the international Forum of Incident Response and Security Teams (FIRST). During the past year, NIST security staff provided technical leadership in determining how CVSS could be adapted for use with other types of vulnerabilities besides software flaws. This work resulted in the development of the following publications:

- Draft NIST Interagency Report (NISTIR) 7502, *The Common Configuration Scoring System (CCSS)*, published in May 2008. CCSS is based on CVSS but has been customized for use with software configuration-related vulnerabilities.
- Paper on the research efforts behind CCSS's development, presented at the 4th Workshop on Quality of Protection (QoP 2008) in October 2008.
- Draft NISTIR on the Common Misuse Scoring System (CMSS), to be published in FY2009. CMSS adapts CVSS for use with feature misuse and trust relationship misuse vulnerabilities.

NIST has also been analyzing CVSS version 2 scores calculated for the National Vulnerability Database (NVD) to identify possible shortcomings of CVSS version 2 and the existing scoring documentation. During FY2009, we plan to recommend changes and additions to the CVSS version 2 specification to clarify how scoring should be performed so as to improve the consistency of CVSS scores across organizations. We also plan on finalizing the CCSS specification and publishing a draft of the CMSS specification next year.

---

http://nvd.nist.gov/cvss.cfm?version=2

Contacts: Ms. Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

Mr. Peter Mell
(301) 975-5572
mell@nist.gov

### Network Security Analysis Using Attack Graphs

At present, computer networks constitute the core component of information technology infrastructures in areas such as power grids, financial data systems and emergency communication systems. Protection of these networks from malicious intrusions is critical to the economy and security of our nation. To improve the security of these network systems, it is necessary to measure the amount of security provided by different network configurations. The objective of our research is to develop a standard model for measuring security of computer networks. A standard model will enable us to answer questions such as "are we more secure than yesterday" or "how does the security of one network configuration compare with another one". Also, having a standard model to measure network security will bring together users, vendors and researchers to evaluate methodologies and products for network security.

Good metrics should be measured consistently, are inexpensive to collect, are expressed numerically, have units of measure, and have specific context [1]. We meet this challenge by capturing vulnerability interdependencies and measuring security in the exact way that real attackers penetrate the network. Our methodology for security risk analysis is based on the model of attack graphs. We analyze all attack paths through a network, providing a probabilistic metric of the overall system risk. Through this metric, we analyze tradeoffs between security costs and security benefits. Decision makers can therefore avoid over investing in security measures that do not pay off, or under investing and risk devastating consequences. Our metric is consistent, unambiguous, and provides context for understanding security risk of computer networks.

In FY 2008 we developed models that combined attack graphs and CVSS scores to determine the security risk of enterprise networks. Several papers were published in conferences and workshops based on this work]. In FY2009 we plan to do a proof of concept implementation to validate our results and publish our results in conferences.

---

Contact: Dr. Anoop Singhal
(301) 975-4432
Anoop.singhal@nist.gov

## Automated Vulnerability Management

### National Vulnerability Database (NVD)

The National Vulnerability Database (NVD) is the United States Government repository of standards-based vulnerability management reference data. The NVD makes available information on vulnerabilities, impact measurements, detection techniques, and remediation assistance. It provides the necessary reference data that enables the Security Content Automation Protocol (SCAP) security automation capabilities. As of September 2008, NVD contained the following resources:

- Over 32,000 vulnerability advisories with an average of 11 new vulnerabilities added daily;
- 22 SCAP checklists containing thousands of low-level security configuration checks that can be automatically processed by commercial tools;
- 129 non-SCAP capable checklists (i.e., English prose guidance and configuration scripts);
- 151 US-CERT (U.S. Computer Emergency Readiness Team) alerts, 2262 US-CERT vulnerability summaries, and 2097 SCAP machine-readable software-flaw checks;
- the emerging industry standard product dictionary with 15,558 entries; and
- 17,022 vulnerability advisories translated into Spanish.

NVD is sponsored by the Department of Homeland Security's National Cyber Security Division and the National Security Agency.

NVD is the second most popular web site at NIST, only behind the NIST atomic clock web site. The NVD receives approximately 69 million hits per year. NVD's effective reach is extended by its security data being incorporated into many commercial security products (e.g., McAfee and Symantec). Just one of these products is used by an estimated 75,000 organizations worldwide. The scope of vendor adoption is shown by NVD XML feeds, which power NVD-based products, being downloaded an average of 2900 times a day.

NVD also plays a pivotal role in the Payment Card Industry (PCI) in their efforts to mitigate vulnerabilities in credit card systems. PCI has mandated that NVD's vulnerability severity scores be used for measuring the risk to payment card servers world-wide and for determining which vulnerabilities must be fixed. PCI's use of NVD increases the security of credit card transactions and protects consumers' personal information.

Further, NVD is a core and critical element in the strategy to secure the Department of Defense (DOD) in their Computer Network Defense (CND) initiative. DOD vulnerability management services are integrating with NVD and NVD is being mirrored on classified networks.

In FY2008, NVD maintained its widely used vulnerability reference data while expanding its support of security checklists, SCAP, and the Department of Defense CND initiative. Accomplishments under the NVD program included authoring the emerging industry standard product dictionary, moving the National Checklist Program under NVD, creating NVD web services, offering new vulnerability data feeds, and migrating to a faster, more robust server architecture and code base.

NVD data is a fundamental component of modern security infrastructure and is substantially increasing the security of networks worldwide. The Computer Security Division plans to expand and improve the NVD in FY2009.

---

http://nvd.nist.gov
Contact: Mr. Peter Mell
(301) 975-5572
peter.mell@nist.gov

### Security Configuration Checklists for Commercial IT Products

There are many threats to users' computers, ranging from remotely launched network service exploits to malicious code spread through emails, malicious websites, and downloads of infected files. Vulnerabilities in information technology (IT) products are discovered daily, and many ready-to-use exploitation techniques are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security configuration controls are usually not enabled by default, so many out-of-the-box IT products are immediately vulnerable. In addition, identifying a reasonable set of security settings for many IT products is a complicated, arduous, and time-consuming task, even for experienced system administrators.

Although the solutions to IT security are complex, one basic but effective tool is a security configuration checklist. A security checklist is a document that contains instructions for securely configuring an IT product for an operational environment or verifying that an IT product has already been securely configured. Whenever feasible, organizations should apply checklists to operating systems and applications to reduce the number of vulnerabilities that attackers can attempt to exploit and to lessen the impact of successful attacks. The use of checklists improves the consistency and predictability of system security. There is no checklist that can make a system or product 100% secure, and using checklists does not eliminate the need for ongoing security maintenance, such as patch installation. However, organizations can reduce the number of ways in which their systems can be attacked and



achieve greater levels of product security and protection from future threats by using checklists that emphasize hardening of systems against software flaws (e.g., by applying patches and eliminating unnecessary functionality) and configuring systems securely.

A central checklist repository can help organizations find security checklists that provide the appropriate level of security to determine if the checklist is current and obtain information about how the checklist should be implemented.

To facilitate development of security configuration checklists for IT products and to make checklists more organized and usable, NIST established the National Checklist Program. The goals of the NCP are to—

- Facilitate development and sharing of checklists by providing a formal framework for vendors and other checklist developers to submit checklists to NIST
- Provide guidance to developers to help them create standardized, high-quality checklists that conform to common operational environments
- Help developers and users by providing guidelines for making checklists better documented and more usable
- Encourage software vendors and other parties to develop checklists
- Provide a managed process for the review, update, and maintenance of checklists
- Provide an easy-to-use repository of checklists
- Provide checklist content in a standardized format
- Encourage the use of automation technologies for checklist application such as the Security Content Automation Protocol (SCAP).

Checklists can take many forms, including files that can automatically set or verify security configurations. Having such automated methods has become increasingly important for several reasons, including the complexity of achieving compliance with various laws, Executive Orders, directives, policies, regulations, standards, and guidance; the increasing number of vulnerabilities in information systems; and the growing sophistication of threats against those vulnerabilities. Automation is also needed to ensure that the security controls and configuration settings are applied consistently within an information system, and that the controls and settings can be effectively verified.

The SCAP program addresses these needs by enabling standards based security tools to automatically perform configuration checking using NCP checklists. Working closely with government, industry, and academia, CSD encourages the development of automated checklists, particularly those that are compliant or compatible with XCCDF (Extensible Configuration Checklist Description Format) and/or OVAL (Open Vulnerability and Assessment Language). These are widely used for automated checklists—XCCDF primarily for mapping policies and other sets of requirements to high-level technical checks, and OVAL primarily for mapping high-level technical checks to the low-level details of executing those checks on the operating systems or applications being assessed.

There are 130 checklists posted on the website; 25 of the checklists are SCAP-expressed and can be used by SCAP-validated software tools. This allows organizations to use checklists obtained from the CSD web site (checklists.nist.gov) for automated security configuration and patching without vendor interaction. Some vendors, including Microsoft Corporation and RedHat provide SCAP checklists content to the NCP, while most of the checklists come from government organizations, not-for-profit, and Federally Funded Research and Development Centers (FFRDCs). NCP currently has SCAP checklists for Windows Vista, Windows 2003 Server, Windows XP, Windows

2000, Office 2007, Internet Explorer 7.0, RedHat Linux, AIX, HPUX, Symantec AntiVirus, McAfee AntiVirus, and other products.

Federal agencies are required to use security configuration checklists from the NCP. In February 2008, revised Part 39 of the Federal Acquisition Regulation (FAR) was published. Paragraph (d) of section 39.101 states, "In acquiring information technology, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations available from the NIST website at http://checklists.nist.gov." Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated."

In FY2008 NIST announced the completion of SCAP version 1.0; developed the Federal Desktop Core Configuration (FDCC) checklists; hosted the 4th Annual Security Automation Conference, drawing nearly 800 attendees, and an FDCC workshop drawing over 700 attendees; and further integrated the NCP website with the NIST National Vulnerability Database (NVD). NIST personnel also both visited and hosted a number of software vendors to encourage participation in the checklist program.

In fiscal year 2009, CSD will complete activities to evolve the NVD to production readiness for SCAP version 2.0; we plan to announce the readiness of the NVD to support SCAP version 2.0 and associated standards. CSD will also communicate SCAP standards and guidelines through a combination of NISTIRs and SPs, and continue education and awareness activities. We also plan to continue beta test and production support and to provide an automated web-based feed from the NCP website.

---

http://checklists.nist.gov
Contact: Mr. Stephen Quinn
(301) 975-6967
stephen.quinn@nist.gov

### Security Content Automation Protocol (SCAP) Validation Program

The Security Content Automation Protocol (SCAP) Validation Program performs conformance testing to ensure that products correctly implement SCAP. Conformance testing is necessary because SCAP is a complex specification consisting of six vulnerability management specifications. A single error in product implementation could result in undetected vulnerabilities within agency and industry networks.

The SCAP Validation Program was created on request by the Office of Management and Budget (OMB) to support the Federal Desktop Core Configuration (FDCC). The SCAP program works with the NIST National Voluntary Laboratory Accreditation Program (NVLAP) to set up independent conformance testing laboratories. Due to the need to support FDCC quickly, the SCAP validation program was created in just six months and was deployed February 2008. Within the first eight months of operation, the program accredited nine testing laboratories and validated 17 products from 11 vendors.

While FDCC SCAP testing is an important part of the program, it is only one of seven different SCAP capabilities which vendors can apply to test their products. The others cover product capabilities such as configuration scanning, vulnerability scanning, patch checking, remediation capabilities, and vulnerability databases. In addition, product vendors can test the conformance of their products to each of the six specifications that make up SCAP, independent of the products' overall SCAP validation. This program has been popular, resulting in the award of 70 capability validations to the 17 validated products (an average of 4 capabilities per product).

Use of SCAP validation has already expanded beyond FDCC. The General Services Administration (GSA) SmartBUY program is conducting enterprise wide blanket purchase agreements for vulnerability and configuration scanners. This procurement mandates SCAP validation for participating products. The DOD Computer Network Defense (CND) initiative also relies on SCAP validation for the future DOD cyber security strategy.

SCAP has been designed to be inexpensive, yet effective. The SCAP conformance tests are either easily human verifiable or automated through NIST provided reference tools.

The SCAP Validation Program will continue to operate in FY2009. It will expand to include additional capabilities, will provide enhanced testing support, and will evolve to include new technologies as SCAP itself matures.

---

http://nvd.nist.gov/validation.cfm
Contact: Mr. Peter Mell
(301) 975-5572
peter.mell@nist.gov

## Infrastructure Services, Protocols, And Applications

### Border Gateway Protocol

The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISPs).

The BGP project was initiated in February 2004. The project aims to help industry to understand the potential risks to inter-domain routing and the

design and implementation trade-offs of the various BGP security mechanisms currently proposed in the Internet Engineering Task Force (IETF) community. Previously, there was a lack of awareness and knowledge in the information technology (IT) sector of the potential threats, risks, mitigation techniques, and their costs. The project also seeks to expedite convergence towards standardized, implemented, and deployed BGP security solutions.

Our project efforts continue to focus on characterizing the problem and design space for BGP security technologies. Our subsequent work has focused primarily on two activities – large-scale simulation modeling of focused BGP attacks and analytical models of threat versus countermeasure effectiveness. We are working with industry and government network operators and security experts to—

- Identify the threats and vulnerabilities of BGP/inter-domain routing;
- Document best common practices in securing the current BGP deployments; and
- Provide deployment and policy guidance for emerging BGP security technologies.

In June 2007, we issued NIST Special Publication (SP) 800-54, *Border Gateway Protocol Security*, to provide a guideline of best practices for securing BGP. Work on updating and extending this publication was initiated in FY2008 and will be completed with a new release in FY2009.

---

http://www.antd.nist.gov/iipp.shtml

Contacts: Mr. Rick Kuhn
(301) 975-3337
kuhn@nist.gov

Mr. Douglas Montgomery (ANTD)
(301) 975-3630
dougm@nist.gov

### Guide to Secure Sockets Layer (SSL) Virtual Private Networks (VPNs)

Secure Sockets Layer (SSL) virtual private networks (VPNs) provide users with secure remote access to an organization's resources. An SSL VPN consists of one or more VPN devices to which users connect using their Web browsers. The traffic between the Web browser and SSL VPN device is encrypted with the SSL protocol. SSL VPNs can provide remote users with access to Web applications and client/server applications, as well as connectivity to internal networks. They offer versatility and ease of use because they use the SSL protocol, which is included with all standard Web browsers, so special client configuration or installation is often not required. In planning VPN deployment, many organizations are faced with a choice between an Internet Protocol Security (IPSec) based VPN and an SSL-based VPN. In 2005, we published NIST SP 800-77, *Guide to IPSec VPNs*.

A complementary document, SP 800-113, *Guide to SSL VPNs*, was published in July 2008. It seeks to assist organizations in understanding SSL VPN technologies. The publication also makes recommendations for designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions. SP 800-113 provides a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also includes a comparison with other similar technologies such as IPSec VPNs and other VPN solutions.

---

Contact: Ms. Sheila Frankel
(301) 975-3297
sheila.frankel@nist.gov

### Internet Protocol Version 6 (IPv6) and Internet Protocol Security (IPsec)

The Internet Protocol Version 6 (IPv6) is an updated version of the current Internet Protocol, IPv4. It has been, and continues to be, developed and defined by the Internet Engineering Task Force (IETF) in a series of consensus-based standards documents—Requests for Comment (RFCs), which are approved standards documents, and Internet Drafts (IDs), which are works-in-progress that may progress to become standards. These documents define the contents and behavior of network communications at every level of the networking stack, from applications down to the physical layer.

The primary motivations for the development of IPv6 were to increase the number of unique IP addresses and to handle the needs of new Internet applications and devices. In addition, IPv6 was designed with the following goals: increased ease of network management and configuration, expandable IP headers, improved mobility and security, and quality of service controls.

The United States Office of Management and Budget (OMB) mandated that government agencies should incorporate IPv6 capability into their backbones (routers, gateways, etc.) by 2008. NIST personnel actively participated in the federal IPv6 Working Group, formed to help government agencies plan and execute the transition in an interoperable and secure manner. We also developed an IPv6 profile to define which pieces and features of IPv6 are mandatory for government agencies, which are optional, and where these elements are definitively defined. A test and conformity assessment program is also in the planning stage.

Internet Protocol Security (IPsec) is a framework of open standards for ensuring private communications over IP networks, which has become the most popular network layer security control. It can provide several types of data protection—confidentiality; integrity; data origin authentication; prevention of packet replay and traffic analysis; and access control. IPsec

typically uses the Internet Key Exchange (IKE) protocol to negotiate IPsec connection settings, exchange keys, authenticate endpoints to each other, and establish security associations, which define the security of IPsec-protected connections. IPsec and IKE were added to IPv4 after the fact, but are now integrated into all of the major operating systems. For IPv6, IPsec and IKE are planned to be an integral part of the network protocols.

IPsec has several uses, with the most common being a virtual private network (VPN). This is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks. Although VPNs can reduce the risks of networking, they cannot totally eliminate them. For example, a VPN implementation may have flaws in algorithms or software, or insecure configuration settings and values that attackers can exploit.

Special Publication (SP) 500-267, *A Profile for IPv6 in the United States Government - Version 1.0*, was published in July 2008. This document is a profile to assist federal agencies in developing plans to acquire and deploy products that implement Internet Protocol version 6 (IPv6). The profile recommends IPv6 capabilities for common network devices, including hosts, routers, intrusion detection systems, and firewalls, and includes a selection of IPv6 standards and specifications needed to meet the minimum operational requirements of most federal agencies. It was developed to help ensure that IPv6-enabled federal information systems are interoperable and secure and addresses how such systems can interoperate and coexist with the current IPv4 systems. Agencies with unique information technology requirements are expected to use the NIST profile as a basis for further refined specifications and policies.

A guidance document on IPv6 and IPsec, SP 800-119, *Guidance for the Secure Adoption of IPv6*, is planned for FY2009. This document will describe IPv6's new and expanded protocols, services, and capabilities. It will characterize new security threats posed by the transition to IPv6. It will issue guidance on IPv6 deployment, including transition, integration, configuration, and testing. It will also include several practical IPv6 transition scenarios. In addition, our personnel are conducting research on the challenges posed to intrusion detection systems (IDSs) and firewalls by adding IPv6 to networks.

Contacts: Ms. Sheila Frankel
(301) 975-3297
sheila.frankel@nist.gov

Mr. Douglas Montgomery (ANTD)
(301) 975-3630
dougm@nist.gov

### Securing the Domain Name System (DNS)

The Domain Name System (DNS) is the method by which Internet addresses in mnemonic form such as **http://csrc.nist.gov** are converted into the equivalent numeric IP (Internet Protocol) addresses such as **129.6.13.39**. Certain servers throughout the world maintain the databases needed, as well as perform the translations. A DNS server that is performing a translation may communicate with other Internet DNS servers if it does not have the data needed to translate the address itself.

As are other Internet-based systems, DNS is subject to several threats. To counter these threats, the Internet Engineering Task Force (IETF)—an international standards body—developed a set of specifications for securing DNS called DNS Security Extensions (DNSSEC). In partnership with the Department of Homeland Security, we have been actively involved in promoting the deployment of DNSSEC since 2004.



As part of this continuing effort, we published guidelines for DNSSEC deployment in Special Publication (SP) 800-81, *Secure Domain Name System (DNS)* Deployment Guide, in May 2006. This guidance document formed the core material for a series of workshops held at NIST for USG DNS administrators to demonstrate basic DNSSEC deployment steps and explain how DNSSEC changes the way an agency maintains its DNS.

NIST also expanded the Secure Naming Infrastructure Pilot (SNIP) in FY2008 to meet the following goals, which were established when the SNIP domain was first deployed:

- To enable United States government DNS stakeholders to become familiar with DNSSEC and to understand its impact on current DNS operations.
- To deploy and test new DNSSEC tools, implementations and applications as they become available. Vendors are encouraged to work with the SNIP testbed as a means to demonstrate and evaluate DNSSEC enabled software in a signed infrastructure.
- To be used as a persistent, signed infrastructure for use with NIST sponsored DNSSEC workshops for USG DNS administrators.

In FY2008, tools from Sparta Inc and Secure64 were deployed on the SNIP as new DNSSEC enabled software and hardware. In addition, in FY 2008, we also published a new white paper on deploying new cryptographic algorithms in DNSSEC and made it available on the NIST DNSSEC project webpage (*http://www-x.antd.nist.gov/dnssec*). This document lays out the roadmap of cryptographic guidelines within the United States Federal Government and the expected impact on DNSSEC, and it provides a list of steps for DNS administrators to use when deploying new cryptographic algorithms to a signed zone. We expect to integrate this work into a revision of NIST SP 800-81 in FY2009.

NIST continued efforts with the United States General Services Administration (GSA) to set in motion the process for securing the top-most DNS domain of the United States Government (i.e., .gov). NIST is tracking the progress of DNSSEC implementations in several DNS servers/ products and is planning to update the SP 800-81 document to cover these technologies. The update will include guidelines for secure configuration and deployment of new security features specified with DNSSEC such as the new Hashed Next Secure (NSEC3) RR and deployment of new digital signing algorithms. NIST is also working with standards organizations to ensure that the DNSSEC specifications keep up with current best security practices with regards to cryptographic algorithm deployment options and cryptographic key sizes. These new cryptographic algorithm, key lifetime and key size parameters will be included in Part 3 of NIST SP 800-57, *Recommendation for Key Management*, which will be issued for public comments in FY2009. We worked with the editors team for Part 3 during FY2008 to provide a set of recommendations for key management in DNSSEC based on the key management foundations published in Part 1 of SP 800-57. The recommendations in SP 800-57 Part 3 differ from the recommendations of SP 800-81 and we plan to revise SP 800-81 to bring its recommendations in line with what is described in SP 800-57 Parts 1 and 3.

Contacts: Dr. Ramaswamy Chandramouli
(301) 975-5013
mouli@nist.gov

Mr. Scott Rose (ANTD)
(301) 975-8439
scott.rose@nist.gov

### Voice over Internet Protocol Security Issues

Voice over IP (VoIP)—the transmission of voice over packet-switched IP networks—is one of the most important trends in telecommunications. VoIP provides a cheaper, clearer, and more flexible alternative to traditional Public Switched Telephone Network (PSTN) telephone lines. In addition to telephone handsets and other end-user equipment, VoIP systems include call processors/call managers, gateways, routers, and firewalls. Most of these components have counterparts used in data networks, but the performance demands of VoIP and the need to support critical services, such as Emergency 911, mean that ordinary software and hardware must be supplemented with special VoIP components.

Those new to VoIP might assume that because digitized voice travels in packets just like other data, existing network architectures and tools can be used without change. However, VoIP adds a number of complications to existing network technology, and these problems are magnified by security considerations. Quality of Service (QoS) is fundamental to the operation of a VoIP network that meets users' quality expectations. However, the implementation of security measures can cause a marked deterioration in QoS unless VoIP-specific equipment and architectures are used. These complications range from firewalls delaying or blocking call setups to encryption-produced latency and delay variation (jitter). Because of the time-critical nature of VoIP and its low tolerance for disruption and packet loss, many security measures implemented in traditional data networks must be specialized for VoIP.

Another important security consideration for VoIP is that voice communications must be protected. In a conventional office telephone system, intercepting conversations requires physical access to telephone lines or compromise of the office private branch exchange (PBX); as a result, only particularly security-sensitive organizations encrypt voice traffic over traditional telephone lines. The same cannot be said for Internet-based VoIP connections—such a connection may pass through more than a dozen systems that are under third-party control, any one of which could monitor a conversation. When a

person visits a retailer on the Internet and provides a credit card number and other sensitive information, it is protected; likewise, sensitive VoIP communications on the Internet should be similarly protected.

During FY2008, CSD continued to update SP 800-58, *Security Considerations for Voice Over IP Systems*, which had been published in January 2005. This publication investigates the attacks and defenses relevant to VoIP and explores ways to provide appropriate levels of security for VoIP networks at reasonable cost. The updated publication will reflect changes in technology, potential interactions between protocol features that could result in security weaknesses, revisions of standards, and new applications of VoIP and related technologies, such as video over Internet. The new version of SP 800-58 is expected to be released for public comment in FY2009.

Contacts: Ms. Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

Mr. Rick Kuhn
(301) 975-3337
kuhn@nist.gov

### Wireless Security Standards

Wireless communications and devices are convenient, flexible, and easy to use. Users of wireless local area network (WLAN) devices have the flexibility to move from one place to another while maintaining connectivity with the network. The most widely used WLAN devices today are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. Wireless personal area networks (WPANs) allow users to share data and applications between devices without using cables or other physical connections. WPANs are used for cell phones, PDAs, keyboards, mice, printers, and other types of devices.

While wireless networks are exposed to many of the same risks as wired networks, they are vulnerable to additional risks as well. Wireless networks transmit data through radio frequencies and are open to intruders unless protected. Intruders have exploited this openness to access systems and services, destroy and steal data, and launch attacks that tie up network bandwidth and deny service to authorized users.

This past year, we completed two Special Publications dealing with wireless security issues. The first, SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, was published in July 2008. It describes the inherent flaws in legacy IEEE 802.11 WLAN technologies. It provides recommendations for applying compensating controls to mitigate these flaws, and it discusses the value of migrating to newer IEEE 802.11 technologies that are based on versions of the IEEE 802.11 standard and that offer much stronger security capabilities. SP 800-48 Revision 1 is an update to the original version of SP 800-48, which was published in 2002.

The second publication on wireless security issued in FY2008 is SP 800-121, *Guide to Bluetooth Security*. It discusses the security capabilities and shortcomings of the most recent versions of the Bluetooth specification for WPANs, and it describes several common vulnerabilities of Bluetooth-enabled devices. SP 800-121 recommends how organizations employing Bluetooth technologies can secure them effectively against common attacks. SP 800-121, which was published in September 2008, replaces the Bluetooth section of the original SP 800-48 issued in 2002.

CSD has also recently begun work on a publication on wireless metropolitan area network (WLAN) security, specifically considerations for Worldwide Interoperability for Microwave Access (WiMAX) technologies. We expect to release a NIST SP on WiMAX security during FY2009.

Contact: Ms. Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

## CSD's Part in National and International IT Security Standards Processes

The International Organization for Standardization (ISO) is a network of the national standards institutes of 148 countries, with the representation of one member per country. The scope of ISO covers standardization in all fields except electrical and electronic engineering standards, which are the responsibility of IEC, the International Electrotechnical Commission.

The IEC prepares and publishes international standards for all electrical, electronic, and related technologies, including electronics, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines such as terminology and symbols, electromagnetic compatibility, measurement and performance, dependability, design and development, safety, and the environment.

Joint Technical Committee 1 (JTC1) was formed by ISO and IEC to be responsible for international standardization in the field of Information Technology. It develops, maintains, promotes, and facilitates IT standards required by global markets meeting business and user requirements concerning—

- design and development of IT systems and tools
- performance and quality of IT products and systems
- security of IT systems and information
- portability of application programs

- interoperability of IT products and systems
- unified tools and environments
- harmonized IT vocabulary
- user-friendly and ergonomically designed user interfaces.

JTC1 consists of a number of subcommittees (SCs) and working groups that address specific technologies. SCs that produce standards relating to IT security include:

- SC 06 - Telecommunications and Information Exchange Between Systems
- SC 17 - Cards and Personal Identification
- SC 27 - IT Security Techniques
- SC 37 - Biometrics

JTC1 also has—

- Technical Committee 68 – Financial Services
- SC 2 - Operations and Procedures including Security
- SC 4 - Securities
- SC 6 - Financial Transaction Cards, Related Media and Operations
- SC 7 - Core Banking

American National Standards Institute (ANSI) is a private, nonprofit organization (501(c)(3)) that administers and coordinates the United States voluntary standardization and conformity assessment system.

### National Standardization

ANSI facilitates the development of American National Standards (ANSs) by accrediting the procedures of standards-developing organizations (SDOs). The InterNational Committee for Information Technology Standards (INCITS) is accredited by ANSI.

### International Standardization

ANSI promotes the use of United States standards internationally, advocates United States policy and technical positions in international and regional standards organizations, and encourages the adoption of international standards as national standards where they meet the needs of the user community.

ANSI is the sole United States representative and dues-paying member of the two major non-treaty international standards organizations, ISO and, via the United States National Committee (USNC), the IEC.

INCITS serves as the ANSI Technical Advisory Group (TAG) for ISO/IEC Joint Technical Committee 1. INCITS is sponsored by the Information Technology Industry (ITI) Council, a trade association representing the leading United States providers of information technology products and services. INCITS currently has more than 750 published standards.

INCITS is organized into Technical Committees that focus on the creation of standards for different technology areas. Technical committees that focus on IT security and IT security-related technologies include:

- B10 – Identification Cards and Related Devices
- CS1 – Cyber Security
- E22 – Item Authentication
- M1 – Biometrics
- T3 – Open Distributed Processing (ODP)
- T6 – Radio Frequency Identification (RFID) Technology

As a technical committee of INCITS, CS1 develops United States national, ANSI-accredited standards in the area of cyber security. Its scope encompasses—

- Management of information security and systems
- Management of third-party information security service providers
- Intrusion detection
- Network security
- Incident handling
- IT security evaluation and assurance
- Security assessment of operational systems
- Security requirements for cryptographic modules
- Protection profiles
- Role-based access control
- Security checklists
- Security metrics

- Cryptographic and non-cryptographic techniques and mechanisms including:
  - confidentiality
  - entity authentication
  - non-repudiation
  - key management
  - data integrity
  - message authentication
  - hash functions
  - digital signatures
- Future service and applications standards supporting the implementation of control objectives and controls as defined in ISO 27001, in the areas of—
  - business continuity
  - outsourcing
- Identity management, including:
  - identity management framework
  - role-based access control
  - single sign-on
- Privacy technologies, including:
  - privacy framework
  - privacy reference architecture
  - privacy infrastructure
  - anonymity and credentials
  - specific privacy enhancing technologies.

The scope of CS1 explicitly excludes the areas of work on cyber security standardization presently underway in INCITS B10, M1, T3, T10 and T11; as well as other standard groups, such as the Alliance for Telecommunications Industry Solutions, the Institute of Electrical and Electronics Engineers, Inc., the Internet Engineering Task Force, the Travel Industry Association of America, and Accredited Standards Committee (ASC) X9. The CS1 scope of work includes standardization in most of the same cyber security areas as are covered in the NIST Computer Security Division.

As the United States TAG to ISO/IEC JTC 1/SC 27, CS1 contributes to the SC 27 program of work on IT Security Techniques in terms, comments, and contributions on SC 27 standards projects; votes on SC 27 standards documents at various stages of development; and identifying United States experts to work on various SC 27 projects or to serve in various SC 27 leadership positions. Currently 10 CS1 members are SC 27 document editors or coeditors on various standards projects, including Randy Easter of NIST for ISO/IEC 24759, Test Requirements for Cryptographic Modules, and Allen Roginsky of NIST, Co-Editor on 29150, Signcryption. All input from CS1 goes through INCITS to ANSI, then to SC 27. It is also a conduit for getting United States-based new work item proposals and United States-developed national standards into the international SC 27 standards development process. CS1 is making contributions on several new areas of work in SC 27, including study periods and/or new work item proposals on Secret sharing mechanisms, Key establishment mechanisms for multiple entities, Categorization and Classification of Information Security Incidents, Light-weight cryptographic mechanisms, OID and ASN.1, Information security governance, Evidence acquisition procedure for digital forensics, and information security for critical infrastructure – Sector-specific guidance.

Through its membership on CS1, where Dan Benigni serves as the nonvoting chair, and Richard Kissel is the NIST Primary with vote, NIST contributes to all CS1 national and international IT security standards efforts. NIST can also initiate IT security-related projects for national or international standardization through its membership on CS1. As an example, CSD staffer David Ferraiolo has asked CS1 to consider a new family of national standards concerning an access control mechanism that can be embedded into operating systems, called the Policy Machine.

Dan Benigni also serves as CS1 Liaison to the INCITS Study Group on Security Best Practices, whose charter is to study the security needs and requirements of the financial and insurance services industries, assess what is missing in current standards and practices, and make recommendations on an approach to create deployable best practices and frameworks for security in these industries. This group has produced a new project proposal for SC 27 to consider, a sector-specific ISMS guideline for the Financial Services and Insurance industries. This standard is intended to provide guidance to the Financial Services and Insurance Industries on how to adapt 27002 controls and processes to specific regulatory and industry-mandated services and legally binding procedures. CS1 has voted to bring it to SC 27 for approval as a new standards project.

Dan was also a Liaison to the recently completed joint study effort organized by the American National Standards Institute's (ANSI) Homeland Security Standards Panel (HSSP) and the Internet Security Alliance (ISA), where the output is a soon to be published Action Guide. This Guide, titled *The Financial Impact of Cyber Risk -- 50 Questions Every CFO Should Ask*, provides private sector enterprises the means to assess and address the financial exposure of cyber security from all angles. It is a tool the CFO (and often other executives) can use to build a framework for analyzing, managing and transferring the Net Financial Risk of cyber security. As opposed to focusing on technological standards or even best practices, this guide is presented to further advance the understanding of financial management.

CS1 has created a task group called CS1.1 RBAC, with a national standards project called *Requirements for the Implementation of Role-Based Access Control (RBAC)* INCITS Project 1794. This standard will provide implementation requirements for RBAC systems, which use RBAC components defined in INCITS 359-2004. RBAC was originally developed at NIST. The implementation requirements in this standard are intended to ensure the interchange of RBAC data (e.g., roles, permissions, users) and promote functional interoperability among RBAC services and applications. In Q2 of FY2009, this work will be ready for its first public review. CS1 has also approved a new project to revise RBAC 359-2004, and has sent it to the INCITS Executive Board for Approval. The revision will cover refinements of the standard that may include the following items: Role-role constraints: extend beyond dynamic and static separation of duty; Reflect distinction between structural roles and functional roles; and Reflect session-less role activation.

In addition, CS1 has recently created another national standards project, entitled *Small Organization Baseline Information Security Handbook*. This standard will provide minimum guidance, leveraging the existing body of knowledge, and provide sufficient detail that small organizations can identify and address their most important security issues. In addition, the standard will provide pointers to key domestic and international security standards and references. The goal is to make information security accessible to small businesses. By enhancing the general level of information security, it is a contribution to the overall stability of national critical infrastructure.

In its international efforts, CS1 has consistently, efficiently, and in a timely manner responded to all calls for contributions on all international security standards projects in ISO/IEC JTC1 SC 27. Contributions from CS1 members have also included many NIST publications. For instance, FIPS 140-3, when published, will become the basis for the Revision of ISO/IEC 19790: 2006-03-01 (1st edition), Security requirements for cryptographic modules.

---

Contact: Mr. Daniel Benigni
(301) 975-3279
benigni@nist.gov

## Systems and Network Security Technical Guidelines

The items below provide brief summaries of system and network security technical guidelines released for public comment or as final during FY2008.

### Securing Cell Phones and PDAs

Special Publication (SP) 800-124, *Guidelines on Cell Phone and PDA Security,* provides an overview of cell phone and personal digital assistant (PDA) devices in use today. These devices can perform many functions done at a desktop computer, may also have specialized built-in hardware such as cameras and Global Positioning System (GPS) receivers, and offer a range of wireless network interfaces, including infrared, wireless local area network, Bluetooth, and one or more cellular interfaces. The publication offers insights for making informed information technology security decisions on their treatment, and it gives details about the threats, technology risks, and safeguards for these devices. SP 800-124 was released for public comment in July 2008.

### Server Security

SP 800-123, *Guide to General Server Security*, assists organizations in understanding the fundamental activities performed as part of securing and maintaining the security of servers. The publication, which was published as final in July 2008, discusses the need to secure servers and provides recommendations for selecting, implementing, and maintaining the necessary security controls. Other NIST publications provide recommendations for particular types of servers. The recommendations in SP 800-123 are a foundation for other server-related publications and do not override more specific recommendations made in such publications.

### Security for Bluetooth Devices

SP 800-121, *Guide to Bluetooth Security*, provides information to organizations on the security capabilities of Bluetooth, which is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area networks (WPANs) used by cell phones, personal digital assistants (PDAs), laptops, printers, and other types of devices to share information and services. SP 800-121, which was published as final in September 2008, recommends how organizations that employ Bluetooth technologies can secure them effectively. It supersedes the Bluetooth recommendations in the original SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*.

### Information Security Testing and Assessment

SP 800-115, *Technical Guide to Information Security Testing and Assessment*, was published as final in September 2008. It provides guidelines to organizations on planning and conducting technical information security testing and assessments. It includes practical recommendations for designing, implementing, and maintaining technical information relating to security test and assessment processes and procedures. SP 800-115 presents an overview of the key elements of technical security testing and assessment with an emphasis on specific techniques, their benefits and limitations, and recommendations for their use. It replaces SP 800-42, *Guideline on Network Security Testing*, which was released in 2003.



### Securing External Telework Devices

SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, helps teleworkers secure the external devices that they use for telework, such as personally owned desktop and laptop computers, cell phones, and personal digital assistants (PDAs). The publication, which was published as final in November 2007, focuses on security for telework involving remote access to an organization's nonpublic computing resources. It provides practical, real-world advice on securing telework computers' operating systems and applications, as well as teleworkers' home networks, cell phones, PDAs, and other consumer devices. The publication also provides tips on considering the security of a device owned by a third party before deciding whether it should be used for telework.

### SSL VPNs

SP 800-113, *Guide to SSL VPNs*, was published as final in July 2008. It assists organizations in understanding Secure Sockets Layer (SSL) Virtual Private Network (VPN) technologies. The publication makes recommendations for designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions. SP 800-113 provides a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also includes a comparison with other similar technologies such as Internet Protocol Security (IPSec) VPNs and other VPN solutions.

### Storage Encryption for End User Devices

SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, assists organizations in understanding storage encryption technologies for end user devices, such as laptops, PDAs, smart phones, and removable media, and in planning, implementing, and maintaining storage encryption solutions. The publication provides practical, real-world recommendations for three classes of storage encryption techniques: full disk encryption, volume and virtual disk encryption, and file/folder encryption. It also discusses important security elements of a storage encryption deployment, including cryptographic key management and authentication. SP 800-111 was published as final in November 2007.

### National Checklist Program

SP 800-70 Revision 1, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, was released for public comment in September 2008. It describes security configuration checklists and their benefits, and it explains how to use the NIST National Checklist Program (NCP) to find and retrieve checklists. It also describes the policies, procedures, and general requirements for participation in the NCP. SP 800-70 Revision 1 updates the original publication, which was released in 2005.

### Windows XP Professional Security

SP 800-68 Revision 1, *Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, was released for public comment in July 2008. It assists IT professionals in securing Windows XP Professional systems running Service Pack 2 or 3. The guide provides detailed information about the security features of Windows XP and security configuration guidelines. SP 800-68 Revision 1 updates the original publication, which was released in 2005.

### Computer Security Incident Handling Guide

SP 800-61 Revision 1, *Computer Security Incident Handling Guide*, helps organizations in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. Published as final in March 2008, it includes guidelines on estab-

lishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents. SP 800-61 Revision 1 updates the original publication, which was released in 2004.

### Security for Legacy Wireless Local Area Networks

SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, was published as final in July 2008. The publication provides advice to organizations in securing their legacy wireless local area networks (WLANs) that are based on early versions of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. The publication assists organizations in reducing the risks associated with legacy WLANs by selecting appropriate compensating controls. SP 800-48 Revision 1 updates the original version of SP 800-48, which was released in November 2002. SP 800-48 Revision 1 complements, and does not replace, SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*. People seeking information on IEEE 802.11i should consult SP 800-97.

### Firewalls and Firewall Policy

SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy*, helps organizations understand the capabilities of firewall technologies and firewall policies. It provides practical recommendations for developing firewall policies and for selecting, configuring, testing, deploying, and managing firewalls. It also discusses factors to consider when selecting firewall solutions. This publication, which was released for public comment in July 2008, replaces the original version of SP 800-41, which was released in 2002.

### Active Content and Mobile Code

SP 800-28 Version 2, *Guidelines on Active Content and Mobile Code*, was published as final in March 2008. It provides an overview of active content and mobile code technologies in use today and offers insights for making informed information technology (IT) security decisions on their application and treatment. SP 800-28 Version 2 gives details about the threats, technology risks, and safeguards for end user systems related to active content and mobile code. This publication replaces the original version of SP 800-28, which was released in 2001.

### Security Content Automation Protocol (SCAP) Test Requirements

NIST Interagency Report (NISTIR) 7511, *Security Content Automation Protocol (SCAP) Validation Program Test Requirements Version 1.1*, describes the requirements that must be met by products to achieve SCAP validation. Validation is awarded by independent laboratories that have been accredited for SCAP testing. This report, which was released for public comment in August 2008, was written primarily for accredited laboratories and for vendors interested in receiving SCAP validation for their products.

### Common Configuration Scoring System (CCSS)

NISTIR 7502, *The Common Configuration Scoring System (CCSS)*, was released for public comment in May 2008. CCSS is an open specification for measuring and communicating the characteristics and relative severity of software security configuration issues. This publication defines and describes the CCSS standard, provides advice on performing scoring, and demonstrates the use of CCSS through a set of examples. Once the CCSS specification has been finalized, CCSS data is expected to assist organizations in making sound decisions on how configuration issues should be addressed, and how the data could be used as part of quantitative assessments of host security.

### Extensible Configuration Checklist Description Format (XCCDF)

NISTIR 7275 Revision 3, *Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4*, was published as final in February 2008. The publication describes XCCDF, which is a standardized XML format that can be used to hold structured collections of security configuration rules for a set of target systems. The XCCDF specification is designed to provide automated testing and scoring that can support FISMA compliance and other efforts. NISTIR 7275 specifies the data model and Extensible Markup Language (XML) representation for version 1.1.4 of XCCDF; the previous revision of NISTIR 7275 addressed version 1.1.3 of XCCDF.

---

Contact: Ms. Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

# HONORS AND AWARDS

## Department of Commerce Gold Medal Award

The group is recognized for their achievement in developing standards and guidelines that enable a new generation of voting equipment to be more usable, accessible, reliable and secure. The new standards are a comprehensive set of rigorous, scientifically based requirements that balance competing interests. The standards provide the ability to test voting equipment to ensure their integrity. These standards have been adopted by at least 39 states, each of which is using them to transform the way elections occur in areas such as usability, security, and accessibility.



*Pictured Left to Right: William Burr, (CSD); Sharon Laskowski, (Information Access Division, ITL); John Wack (Software & Systems Division, ITL); Nelson Hastings, (CSD); Mark Skall, (Software & Systems Division, ITL); Barbara Guttman, (Software & Systems Division, ITL); John Kelsey, (CSD); Alan Goldfine (Software & Systems Division, ITL); and Dave Flater, (Software & Systems Division, ITL).*

## Department of Commerce Gold Medal Award

Stephen is recognized for the development of a test tool which has been used by industry to accelerate the development of a Public Safety interoperability interface, the Project 25 Inter-Rf SubSystem Interface. The tool is being used by industry to verify whether or not communication interfaces between first responder radio systems are working. Components within the test tool have also been leveraged in commercial product developments within the public safety communications industry.



*Left to Right: Stephen Quirolgico, (CSD); Mudumbai Ranganathan, (Advanced Network Technologies Division, ITL)*

## Department of Commerce Bronze Medal Award

Dr. Cooper is recognized for significant achievements in public key infrastructure (PKI) standardization, testing and evaluation methodologies, and deployment to address a fundamental security problem-secure distribution of cryptographic keys—within the federal government and in the global Internet community. His technical contributions include critical standards, widely used testing specifications, and technical analysis that have enhanced the interoperability and security of PKI products as well as the security of the federal PKI. His contributions have helped to create a secure and robust foundation for the deployment of the Personal Identity Verification (PIV) card and satisfy the requirements imposed on NIST.



*David Cooper*

## FED 100 Award

Stephen Quinn, a computer scientist in the Computer Security Division, received the 2008 Federal 100 Award from Federal Computer Week. Quinn was honored for his work as co-originator of the Security Content Automation Protocol (SCAP), a technical framework that supports the automation of security operations in information systems.



*Stephen Quinn*

# COMPUTER SECURITY DIVISION PUBLICATIONS – FY2008

**Key to Publications:**

FIPS = Federal Information Processing Standards
SP = Special Publication
NIST IR = NIST Interagency Report
ITL / CSD = Information Technology Laboratory / Computer Security Division Security Bulletins

**Draft Publications**

| Number | Title | Date |
|---|---|---|
| SP 800-73-2 | Interfaces for Personal Identity Verification | October 2007 |
| SP 800-39 | Managing Risk from Information Systems: An Organizational Perspective | October 2007 |
| SP 800-60, Rev. 1 Vol. 1 & 2 | Guide for Mapping Types of Information and Information Systems to Security Categories and Appendices | November 2007 |
| SP 800-115 | Technical Guide to Information Security Testing | November 2007 |
| SP 800-53 Rev. 2 | Recommended Security Controls for Federal Information Systems | November 2007 |
| SP 800-53 A(final draft) | Guide for Assessing the Security Controls in Federal Information Systems | December 2007 |
| SP 800-79-1 | Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations | February 2008 |
| SP 800-63 Rev. 1 | E-Authentication Guideline | February 2008 |
| SP 800-73-2 (2nd draft) | Interfaces for Personal Identity Verification | March 2008 |
| SP 800-64 Rev. 2 | Security Considerations in the System Development Life Cycle | March 2008 |
| SP 800-116 | A Recommendation for the Use of PIV Credentials in Physical Access Control Systems | April 2008 |
| SP 800-39 (2nd draft) | Managing Risk from Information Systems: An Organizational Perspective | April 2008 |
| SP 800-108 | Recommendation for Key Derivation Using Pseudorandom Functions | May 2008 |
| SP 800-66 Rev. 1 | An Introductory Resource Guide to Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule | May 2008 |
| SP 800-123 | Guide to General Server Security | May 2008 |
| NIST IR 7502 | The Common Configuration Scoring System (CCSS) | May 2008 |
| SP 800-124 | Guidelines on Cell Phone and PDA Security | July 2008 |
| SP 800-121 | Guide to Bluetooth Security | July 2008 |
| SP 800-107 (2nd draft) | Recommendation for Applications Using Approved Hash Algorithms | July 2008 |
| SP 800-41 Rev. 1 | Guidelines on Firewalls and Firewall Policy | July 2008 |
| SP 800-68 Rev. 1 | Guide to Securing Microsoft Windows XP Systems for IT Professionals | July 2008 |
| SP 800-106 | Randomized Hashing for Digital Signatures | August 2008 |
| NIST IR 7511 Ver. 1.1 | Security Content Automation Protocol (SCAP) Validation Program Test Requirements | August 2008 |
| SP 800-37 Rev. 1 | Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach | August 2008 |
| SP 800-116 (2nd draft) | A Recommendation for the Use of PIV Credentials in Physical Access Control Systems | September 2008 |
| SP 800-70 Rev. 1 | National Checklist Program for IT Products--Guidelines for Checklist Users and Developers | September 2008 |
| SP 800-82 (final draft) | Guide to Industrial Control Systems (ICS) Security | September 2008 |

| Federal Information Processing Standards (FIPS) | | |
|---|---|---|
| **Date** | **Title** | **Date** |
| FIPS 198-1 | The Keyed-Hash Message Authentication Code (HMAC) | July 2008 |

| NIST Special Publications | | |
|---|---|---|
| **Number** | **Title** | **Date** |
| SP 800-114 | User's Guide to Securing External Devices for Telework and Remote Access | November 2007 |
| SP 800-111 | Guide to Storage Encryption Technologies for End User Devices | November 2007 |
| SP 800-38 D | Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC | November 2007 |
| SP 800-53 Rev. 2 | Recommended Security Controls for Federal Information Systems | December 2007 |
| SP 800-28 Ver. 2 | Guidelines on Active Content and Mobile Code | March 2008 |
| SP 800-61 Rev. 1 | Computer Security Incident Handling Guide | March 2008 |
| SP 800-87 Rev. 1 | Codes for the Identification of Federal and Federally-Assisted Organizations | April 2008 |
| SP 800-53 A | Guide for Assessing the Security Controls in Federal Information Systems | June 2008 |
| SP 800-67 Rev. 1.1 | Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher | June 2008 |
| SP 800-79-1 | Guidelines for the Accreditation of Personal Identity Verification Card Issuers | June 2008 |
| SP 800-113 | Guide to SSL VPNs | July 2008 |
| SP 800-55 Rev. 1 | Performance Measurement Guide for Information Security | July 2008 |
| SP 800-48 Rev. 1 | Guide to Securing Legacy IEEE 802.11 Wireless Networks | July 2008 |
| SP 800-123 | Guide to General Server Security | July 2008 |
| SP 800-60, Rev. 1 Vol. 1 & 2 | Guide for Mapping Types of Information and Information Systems to Security Categories and Appendices | August 2008 |
| SP 800-73-2 | Interfaces for Personal Identity Verification | September 2008 |
| SP 800-121 | Guide to Bluetooth Security | September 2008 |
| SP 800-115 | Technical Guide to Information Security Testing and Assessment | September 2008 |

| NIST Interagency Reports | | |
|---|---|---|
| **Number** | **Title** | **Date** |
| IR 7442 | Computer Security Division - 2007 Annual Report | April 2008 |
| IR 7516 | Forensic Filtering of Cell Phone Protocols | August 2008 |

| ITL-CSD Security Bulletins | |
|---|---|
| **Number** | **Title** |
| October 2007 | The Common Vulnerability Scoring System (CVSS) |
| November 2007 | Using Storage Encryption Technologies to Protect End User Devices |
| December 2007 | Securing External Computers And Other Devices Used by Teleworkers |
| January 2008 | Secure Web Servers Protecting Web Sites That Are Accessed By The Public |
| February 2008 | Federal Desktop Core Configuration (FDCC): Improving Security For Windows Desktop Operating Systems |
| March 2008 | Handling Computer Security Incidents: NIST Issues Updated Guidelines |
| April 2008 | Using Active Content And Mobile Code And Safeguarding The Security Of Information Technology Systems |
| May 2008 | New Cryptographic Hash Algorithm Family: NIST Holds A Public Competition To Find New Algorithms |
| July 2008 | Guidelines On Implementing A Secure Sockets Layer (SSL) Virtual Private Network (VPN) |
| August 2008 | Security Assessments: Tools For Measuring The Effectiveness Of Security Controls |
| September 2008 | Using Performance Measurements To Evaluate And Strengthen Information System Security |

# WAYS TO ENGAGE OUR DIVISION AND NIST

## Guest Research Internships at NIST

Opportunities are available at NIST for 6- to 24-month internships within CSD. Qualified individuals should contact CSD, provide a statement of qualifications, and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring institution; however, in some cases, these guest research internships carry a small monthly stipend paid by NIST. For further information, contact Mr. Curt Barker, (301) 975-8443, william.barker@nist.gov or Ms. Donna Dodson, (301) 975-3669, donna.dodson@nist.gov.

## Details at NIST for Government or Military Personnel

Opportunities are available at NIST for 6- to 24-month details at NIST in CSD. Qualified individuals should contact CSD, provide a statement of qualifications, and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring agency; however, in some cases, agency salary costs may be reimbursed by NIST. For further information, contact Mr. Curt Barker, (301) 975-8443, william.barker@nist.gov or Ms. Donna Dodson, (301) 975-3669, donna.dodson@nist.gov.

## Federal Computer Security Program Managers' Forum

The FCSPM Forum is covered in detail in the Outreach section of this report. Membership is free and open to federal employees. For further information, contact Ms. Marianne Swanson, (301) 975-3293, marianne.swanson@nist.gov.

## Security Research

NIST occasionally undertakes security work, primarily in the area of research, funded by other agencies. Such sponsored work is accepted by NIST when it can cost-effectively further the goals of NIST and the sponsoring institution. For further information, contact Mr. Tim Grance, (301) 975-3359, tim.grance@nist.gov.

## Funding Opportunities at NIST

NIST funds industrial and academic research in a variety of ways. Our Technology Innovation Program provides cost-shared awards to industry, universities, and consortia for research on potentially revolutionary technologies that address critical national and societal needs in NIST's areas of technical competence. The Small Business Innovation Research Program funds R&D proposals from small businesses. We also offer other grants to encourage work in specific fields: precision measurement, fire research, and materials science. Grants/awards supporting research at industry, academia, and other institutions are available on a competitive basis through several different Institute offices. For general information on NIST grants programs, contact Ms. Melinda Chukran, (301) 975-5266, melinda.chukran@nist.gov.

## Summer Undergraduate Research Fellowship (SURF)

Curious about physics, electronics, manufacturing, chemistry, materials science, or structural engineering? Intrigued by nanotechnology, fire research, information technology, or robotics? Tickled by biotechnology or biometrics? Have an intellectual fancy for superconductors or perhaps semiconductors?

Here's your chance to satisfy that curiosity, by spending part of your summer working elbow-to-elbow with researchers at NIST, one of the world's leading research organizations and home to three Nobel Prize winners. Gain valuable hands-on experience, work with cutting-edge technology, meet peers from across the nation (from San Francisco to Puerto Rico, New York to New Mexico), and sample the Washington, D.C., area. And get paid while you're learning. For further information, see *http://www.surf.nist.gov* or contact NIST SURF Program, 100 Bureau Dr., Stop 8400, Gaithersburg, MD 20899-8499, (301) 975-4200, NIST_SURF_program@nist.gov

## Acknowledgements

The editor, Patrick O'Reilly of the National Institute of Standards and Technology (NIST), wishes to thank his colleagues in the Computer Security Division, who provided write-ups on their 2008 project highlights for this document. The editor would also like to acknowledge Kevin Stine (NIST) for his support and help with this annual report. The editor would also like to acknowledge Tanya Brewer (NIST) for her guidance with this annual report. The editor would also like to acknowledge Karen Scarfone (NIST), Shirley Radack (NIST) and Nipa Shah (State Department) for reviewing and providing feedback for this annual report.




**U.S. Department of Commerce**
Otto J. Wolff, *Acting Secretary*

**National Institute of Standards and Technology**
Patrick Gallagher, *Deputy Director*

NISTIR 7536

# Computer Security Division 2008 Annual Report

Patrick O'Reilly, *Editor*

**Computer Security Division**
Information Technology Laboratory
National Institute of Standards and Technology

Michael James, *Art Director*
The DesignPond

**Disclaimer:** Any mention of commercial products is for information only; it does not imply NIST recommendation or endorsement, nor does it imply that the products mentioned are necessarily the best available for the purpose.


WWW