Computer Security Division

2009 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 Implements the Federal Information Security Management Act of 2002 3

Security Management and Assurance Group 4

Federal Information Security Management Act Implementation Project 4
- FISMA Implementation Project – Phase I 4
- FISMA Implementation Project – Phase II 5

Outreach and Awareness 6
- Computer Security Resource Center 6
- Federal Computer Security Program Managers' Forum 8
- Federal Information Systems Security Educators' Association 8
- Information Security and Privacy Advisory Board 9
- Security Practices and Policies 11
- Small and Medium Size Business Outreach 11

Health Information Technology Security 12

Smart Grid Cyber Security 13

Supply Chain Risk Management 13

Cryptographic Validation Programs and Laboratory Accreditation 14
- Laboratory Accreditation 14
- Cryptographic Module Validation Program and Cryptographic Algorithm Validation Program 15
- Automated Security Testing and Test Suite Development 16
- ISO Standardization of Cryptographic Module Testing 18

Guidelines and Documents 18

Cryptographic Technology Group 21

Cryptographic Standards Toolkit 21
- Hash Algorithms 21
- Security Guidelines of Using Approved Hash Algorithms 21
- Digital Signatures 22
- Random Number Generation 22
- Key Establishment Using Public Key Cryptography 22
- Block Cipher Modes of Operation 22

Key Management 23

Authentication and Key Management for Wireless Applications 23

Internet Security 23

Quantum Computing 24

Authentication 24

Security Aspects of Electronic Voting 24

Development of FIPS 140-3, Security Requirements for Cryptographic Modules 25

Systems and Emerging Technologies Security Research Group 27

Identity Management Systems 27
- Personal Identity Verification 27
- NIST Personal Identity Verification Program 28
- Conformance Tests for Transportation Workers Identification Credential Specifications 29
- Identity Credential Smart Card Interoperability ISO/IEC 24727 Identification Cards Integrated Circuit Cards Programming Interfaces 29

Biometric Standards and Conformity Assessment Activities 31

Research in Emerging Technologies 33
- Access Control - Information Sharing Environment 33
- Automated Combinatorial Testing for Software 33
- Conformance Verification for Access Control Policies 34
- Forensics for Web Services 35
- Mobile Handheld Device Security and Forensics 35
- NIST Cloud Computing Project 36
- Policy Machine 36
- Security for Grid and Pervasive Systems 38
- Security Ontologies: Modeling Quantitative Risk Analysis of Enterprise Systems 38

Automated Vulnerability Management 39
- National Vulnerability Database 39
- Security Content Automation Protocol 39
- National Checklist Program 41
- Security Content Automation Protocol Validation Program 43

Technical Security Metrics 44
- Vulnerability Measurement and Scoring 44
- Network Security Analysis Using Attach Graphs 44

Infrastructure Services, Protocols, and Applications 45
- Internet Protocol Version 6 and Internet Protocol Security 45
- Securing the Domain Name System 46
- Wireless Security Standards 47

CSD's Part in National and International IT Security Standards Processes 47

Systems and Network Security Technical Guidelines 51

Honors and Awards 54

Computer Security Division Publications - FY2009 56

Ways to Engage Our Division and NIST 59

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 2009 (FY2009), CSD continued its standards development and cybersecurity outreach activities and carried out an expanded research agenda designed to develop and implement high-quality, cost-effective mechanisms needed to improve information security and privacy across the federal government and throughout the national and international information security community. CSD worked with federal partners to establish a unified framework for information security across the federal government. This initiative is resulting in greater standardization and more consistent and cost-effective security for all federal information systems.

NIST continues to develop automated security tools to improve efficiency and reduce dependence on labor-intensive compliance documentation efforts. This includes efforts to standardize technical security operations, including automated vulnerability management. In parallel with its automation development and support activities, CSD also continues 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.

In FY2009, CSD continued to develop cybersecurity standards, security metrics, and product assurance programs to promote, measure, and validate the security attributes of information systems and services. 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 FY2009, CSD published revisions of *The Digital Signature Standard*, Federal Information Processing Standard (FIPS) 198-1 and *Secure Hash Standard*, FIPS 180-3, published twelve final and twelve draft security guidelines in the form of NIST Special Publications, and drafted ten Interagency Reports on cybersecurity topics. During FY2009 CSD continued its national and international consensus standards activities, particularly in the areas of cryptographic functions, cryptographic product assurance, and identity credentials. Also during FY2009, CSD continued its international competition for a next generation Secure Hash Algorithm (SHA-3) and continued to expand its support for sector-specific national initiatives: electronic voting, Smart Grid, and health information technology.

To better assist the Nation in meeting its ever-increasing cybersecurity needs, in FY2009 CSD became more tightly integrated into both ITL and Department of Commerce cybersecurity activities. CSD provided a Chief Cybersecurity Advisor to the Director of ITL and a cybersecurity coordinator for the Department of Commerce Cybersecurity and Privacy Task Force. These new roles were necessary to better coordinate NIST and Commerce participation in inter-departmental cybersecurity planning and to more effectively leverage the resources necessary to make significant contributions to Departmental and National initiatives. CSD also led ITL's transition from planning for Comprehensive National Cybersecurity Initiative (CNCI) activities to initiation of CNCI research programs and implementation of recommendations of the President's 2009 Cyberspace Policy Review.

These are just some of the highlights of the CSD program during FY2009. 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

William Curtis Barker
Chief Cybersecurity Advisor

Donna Dodson
Deputy Chief Cybersecurity Advisor

William Burr
Cryptographic Technology

David Ferraiolo
Systems and Emerging Technologies Security Research

Matthew Scholl
Security Management and Assurance

The Computer Security Division Implements 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 (U.S.). 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 (NIST)." In Fiscal Year (FY) 2009, CSD addressed its assignments through the following projects and activities:

- Issued sixteen NIST Special Publications (SP) covering management, operational, and technical security guidance, as well as four NIST Interagency Reports (NISTIRs) on technical topics, and one revised Federal Information Processing Standard (FIPS);

- Collaborated with the Office of the Director of National Intelligence, Committee on National Security Systems, and the Department of Defense to establish a common foundation for information security across the federal government, including a consistent process for selecting and specifying safeguards and countermeasures (i.e., security controls) for federal information systems;

- Provided 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 (FCSPM Forum), and the Small Business Corner;

    - Drafted NISTIR 7621, *Small Business Information Security: The Fundamentals*, which was released in August 2009. NISTIR 7621 helps small businesses and other small organizations implement the fundamental components of an effective information security program;

    - Initiated the development of an outreach video for the Small Business Outreach to help promote Information Technology (IT) security awareness for small to medium sized businesses. This video is expected to be publicly available in October 2009 on the CSRC website;

- Evaluated security policies and technologies from the private sector and national security systems for potential federal agency use. Assembled 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;

- Solicited recommendations of the Information Security and Privacy Advisory Board (ISPAB) on draft standards and guidelines: solicited recommendations of the Board on information security and privacy issues regularly at quarterly meetings;

- Drafted NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP)*. The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures that the broadest possible range of use cases is reflected in SCAP functionality;

- Provided outreach, workshops, and briefings: Conducted ongoing awareness briefings and outreach to CSD's customer community and beyond to advance the implementation 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; and

- Produced an annual report as a NISTIR. The 2003-2008 Annual Reports are available via our Computer Security Resource Center (CSRC) website or upon request.

Security Management and Assurance Group

STRATEGIC GOAL

The Security Management and Assurance (SMA) Group provides leadership, expertise, outreach, validation, standards and guidelines in order to assist the federal IT community in protecting its information and information systems, which allows our federal custom ers 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 U.S. Office of Management and Budget (OMB), the U.S. 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. Internationally we work jointly with the governments of our allies to include Canada, Japan and several European and Asian countries to standardize and validate the correct implementation of cryptography.

Major initiatives in this area include:

- The Federal Information Security Management Act (FISMA) Implementation project;
- The Cryptographic Module Validation Program;
- The Cryptographic Algorithm Validation Program;
- Extended outreach initiatives to federal and nonfederal agencies, state and local governments and international organizations;
- Information security training, awareness and education;
- Outreach to small and medium business;
- Standards development; and
- 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

Federal Information Security Management Act (FISMA) Implementation Project – Phase I

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 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;
- NIST SP 800-39, *Integrated Enterprise-wide Risk Management: Organization, Mission and Information Systems View*;
- NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*;

- 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 FY2009, the SMA group completed or updated the following key publications:

- Major revision of NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, 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 set (catalog) of security controls for all federal information systems;

- Initial public draft of a major revision to NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, working in cooperation with the ODNI, DOD, and the CNSS, to develop a common process to authorize federal information systems for operation; and

- 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.

In addition to the above publications, the division collaborated with the Manufacturing Engineering Laboratory in reviewing comments received and updating the 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 initiatives to support security control assessment capability for public and private sector organizations providing security assessment services for federal agencies.

For FY2010, CSD intends to continue collaboration with the ODNI, the DOD, and the CNSS, in expanding the series of NIST SPs for a unified information security framework for the federal government. Updates to the following draft publications will be completed in FY2010: NIST SP 800-37 Revision 1, 39 and 53A.

---

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

Federal Information Security Management Act (FISMA) Implementation Project – Phase II

Phase II of the FISMA Implementation Project is focusing on building common understanding and reference guides for organizations applying the NIST suite of publications that support the Risk Management Framework (RMF), and for public and private sector organizations that 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:

(i) ***Training Initiative***: for development of training courses, NIST publication of Quick Start Guides (QSGs), and development of Frequently Asked Questions (FAQs) for establishing common understanding of the NIST standards and guidelines supporting the NIST RMF;

(ii) ***Support Tools Initiative***: for defining criteria for common reference programs, materials, checklists, technical guides,

automated tools and techniques supporting implementation and assessment of SP 800-53-based security controls;

(iii) ***Product and Services Assurance Initiative***: for defining minimum criteria and guidelines for security assurances (to include test results from SCAP tools and configuration checklists, etc. where applicable) in products and services supporting implementation and assessment of SP 800-53-based security controls in information system operational environments;

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

(v) ***Organizational Security Assessment Capability Initiative***: drawing upon material from the above initiatives, define minimum capability and proficiency criteria for public and private sector organizations providing security assessment services for federal agencies.

In FY2009 CSD completed the following activities:

(i) ***Training Initiative:*** completed QSGs and FAQs supporting the categorization and monitor step of the 6-step NIST RMF; and prototyped 2 training courses on the RMF;

(ii) ***Support Tools Initiative:*** developed an SP 800-53 Revision 3 Reference Database Application that enables users to display and search the SP 800-53 security control catalog in a variety of views, and to export those views in many different file formats for incorporating into automated support tools;

(iii) ***Product and Services Assurance Initiative:*** held meetings with several security product and service providers and federal agencies seeking their views on common types of artifacts that are readily available for assurances that SP 800-53 based security control product and service claims are continuously being meet in organization specific information system operational environments;

(iv) ***ISO Harmonization Initiative:*** developed mapping tables of SP 800-53 Revision 3 security controls to ISO/IEC 27001 (Annex A) controls to aid organizations that need to demonstrate compliance to both sets of security controls; and

(v) ***Organizational Security Assessment Capability Initiative:*** updated the initial public draft of NIST Interagency Report 7328, *Security Assessment Provider Requirements and Customer Responsibilities*, which defines capabilities security assessment providers should satisfy to demonstrate proficiencies in conducting information system security control assessments in accordance with NIST standards and guidelines.

For FY2010, CSD intends to develop QSGs and FAQs for the select, implement, assess and authorize steps of the 6-step RMF, and prototype a web-based training module for the RMF; draft a guide defining criteria for common support tools and techniques supporting implementation and assessment of SP 800-53-based security controls; outline a guide for submission of supplier claims for product and service assurances; develop additional mappings of NIST standards and guidelines supporting the RMF to ISO/IEC 27001 information security management system (ISMS) framework; and complete update of NISTIR 7328, *Security Assessment Provider Requirements and Customer Responsibilities*.

---

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

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

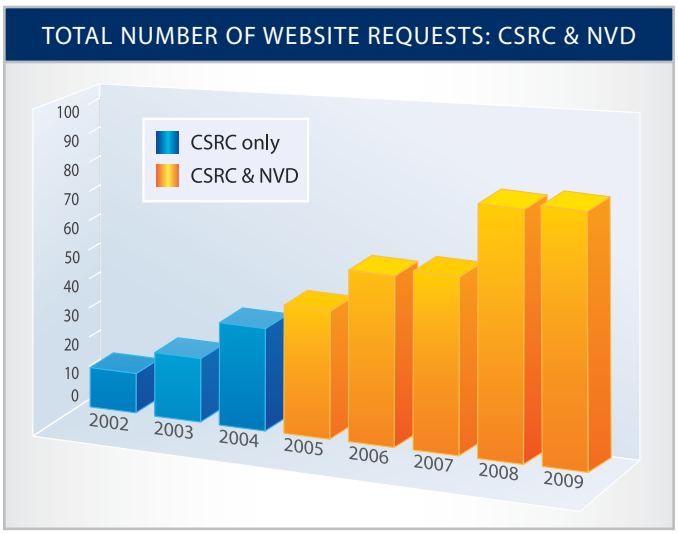
Ms. Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Outreach and Awareness

Computer Security Resource Center (CSRC)

The Computer Security Resource Center (CSRC) is the Computer Security Division's website. CSRC is one of the most visited websites 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 valuable information security-related information. CSRC serves as a vital link to all our internal and external customers.

During FY2009, CSRC had more than 91.4 million requests. Of these, the National Vulnerability Database (NVD) website within CSRC received 48.4 million requests, with the rest of the CSRC receiving 43.0 million requests.



The CSRC website is the primary source for gaining access to NIST computer security publications. We post the following publications: Drafts, Federal Information Processing Standards (FIPS), Special Publications (SPs), NIST Interagency Reports (NISTIRs), and ITL Security Bulletins. Every draft document released for public comment or final document published through the Division has been posted to the CSRC website.

The URL for the Publications homepage is: http://csrc.nist.gov/publications . This URL provides links to the publications listed above. We also have organized the publications by Topic clusters, by Family categories, and by Legal Requirements to help users locate various documents under these topics.

The top 10 CSD publications (Drafts, FIPS, SPs, NISTIRs, and ITL Security Bulletins) that were downloaded in FY2009 (October 1, 2008 to September 30, 2009) were:

1) SP 800-53 Revision 2 and Revision 3,*Recommended Security Controls for Federal Information Systems and Organizations*;

2) SP 800-53 A,*Guide for Assessing the Security Controls in Federal Information Systems*;

3) SP 800-30, *Risk Management Guide for Information Technology Systems*;

4) SP 800-34,*Contingency Planning Guide for Information Technology Systems*;

5) SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*;

6) SP 800-77, *Guide to IPsec VPNs*;

7) FIPS 140-2,*Security Requirements for Cryptographic Modules*;

8) SP 800-100,*Information Security Handbook: A Guide for Managers*;

9) FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; and

10) NISTIR 7298, *Glossary of Key Information Security Terms*.

During FY2009, the CSRC website was continuously updated with new information on various project pages. Some of the major highlights of the expanded CSRC website during FY2009 were:

- Created web pages for the 2009 Federal Information Systems Security Educators' Association (FISSEA) Conference;
- Updated and created new validated products and algorithms web pages for the Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP) project;
- Updated the Small Business Community website with new information and workshops that took place in FY2009;
- Redesigned and updated the National Vulnerability Database (NVD) website – the Federal Desktop Core Configuration (FDCC) and Security Content Automation Protocol (SCAP) portion of website; and
- Created web pages that included assessment cases for the FISMA project.

In addition to the CSRC website, CSD maintains a publication announcement mailing list. This is a free e-mail list that notifies subscribers about publications that have been posted to the CSRC website and are available to the general public. This e-mail list is a valuable tool for more than 7,700 subscribers who include federal government employees, the private sector, educational institutions, and individuals with a personal interest in IT security. This e-mail list reaches people all over the world. E-mail is sent to the list only when the CSD releases a publication, posts an announcement on the CSRC website, and when the CSD is hosting a security event. E-mails are only sent out by the list administrator – Pat O'Reilly (NIST, CSD).

During FY2009 we have offered more services and technical support for our list. We now offer multiple lists under one main list. We have expanded our publications list into multiple topic lists: Drafts, FIPS, SPs, NISTIRs, ITL Security Bulletins, CSRC News, and CSD sponsored events. Our subscribers have full control of which lists they would like to belong to. Once subscribed to the list, subscribers have an option to join other topics from the list mentioned above. Each subscriber has an individual user preference (profile). We plan to expand the topics offered in FY2010.

Individuals who are interested in learning more about this list or subscribing to it should visit this web page on CSRC for more information:

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

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

---

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 900 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) website, maintains an extensive e-mail list, and holds an annual off-site conference 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 from 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 FY2009 included briefings on Trusted Internet Connection, NIST's Health Information Technology Security Program, cloud computing, virtual machine monitor security, Networx Trusted Internet Connection/Managed Trusted IP Services, and domain name security. This year's two-day annual off-site meeting featured updates on the computer security activities of the U.S. Government Accountability Office, NIST, the U.S. Office of Management and Budget, General Services Administration, and the Department of Homeland Security. Briefings were also provided on protecting the confidentiality of personally identifiable information, social media and the Government, training initiatives, Information System Security Line of Business for Certification and Accreditation Shared Service Providers, effectively and securely using cloud computing, integrated enterprise-wide risk management, and contingency planning.

The number of members on the e-mail list steadily grows and continues to provide a valuable resource for federal security program managers. Timely topics such as social media, enterprise security architecture, and personally identifiable information are discussed; policies, procedures, and plans are exchanged; and resources are shared. This year the topic of certification and accreditation cost estimation was explored on the mailing list. The discussion was followed by a half day workshop where members shared their approaches and strategies for determining the cost of conducting an assessment for information systems of various sizes and complexities.

---

http://csrc.nist.gov/groups/SMA/forum/
Contact: Ms. Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov
sec-forum@nist.gov

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.

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

FISSEA membership is open to information systems security professionals, professional trainers and educators, 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 to join FISSEA; all that is required is a willingness to share products, information, and experiences. Business is administered by a 13-member Executive Board that meets monthly. Board members are elected to serve two-year terms. In March 2009, Susan Hansche was elected to be the FISSEA Executive Board Chair.

Each year an award is presented to a candidate selected as FISSEA Educator of the Year; this award honors distinguished accomplishments in information systems security training programs. The Educator of the Year for 2008, awarded in March 2009, is Luke Andersen of Global Knowledge. Louis Numkin received the first FISSEA Life Member Award in appreciation of his leadership, outreach, and dedication to the FISSEA mission. Board member, Gretchen Morris coordinated a contest for the awareness, training, and/or education items used as a part of one's security program. Terri Cinnamon of the Department of Veterans Affairs won the motivational item contest. Susan Farrand of the Department of Energy won the security newsletter contest. Jane Moser of Service Canada had the winning poster entry. David Kurtz of the Bureau of the Public Debt was selected as having the best security website. DISA, SAIC, and Carney won the training exercise contest. The winning entries are posted to the FISSEA website.

FISSEA maintains a website, an interactive list serve, and a semi-annual newsletter as a means of communication for its members. Members are encouraged to participate in the annual FISSEA conference and to serve on the FISSEA ad hoc task groups. NIST assists FISSEA with its operations by providing staff support for several of its activities and by being FISSEA's host agency.

FISSEA membership in 2009 spanned federal agencies, industry, military, contractors, state governments, academia, the press, and foreign organizations to reach over 1,250 members in a total of 15 countries. The 700 federal agency members represent 89 agencies from the Executive and Legislative branches of government.

FISSEA conducted two free workshops during FY2009. On November 13, 2008, board member Susan Hansche, along with Janet Barnes, Dagne Fulcher, David Ascione, and Ruth Kao presented "Information Systems Security Qualifications Matrix: Complexities, Competencies, Experience, and Training" held at NIH. On March 11, board members Mark Wilson, Susan Hansche, Louis Numkin, and John Ippolito presented "FISSEA: Tips for Educating and Training the Cyber Workforce of Today and Tomorrow". Workshop presentations are posted on the website and FISSEA will continue to offer free workshops in 2010.

The 2009 FISSEA conference was held at NIST on March 24-26, 2009. Approximately 170 information systems security professionals and trainers attended, primarily from federal agencies, but including college and university faculty and staff, and industry representatives from firms that support federal information systems and security programs. The theme was "Awareness, Training, and Education – The Catalyst for Organizational Change." Conference attendees were given the opportunity to tour NIST and participate in a vendor exhibition. FISSEA conferences provide a great networking opportunity for attendees. The 2010 conference will be held at the National Institutes of Health on March 23-25 and the theme is "Unraveling the Enigma of Role-Based Training". The first two days of the 3-day conference include one track devoted to role-based training and a second track focusing on awareness, training, education, and certification topics. The third day features a special emphasis on Cyber Security Initiatives. Captain Cheryl Seaman is the Conference Director and Daniel Benjamin is the Program Director. Further information regarding the conference is available on the FISSEA website.

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
fisseamembership@nist.gov

Contacts: Mr. Mark Wilson	Ms. Peggy Himes
(301) 975-3870	(301) 975-2489
mark.wilson@nist.gov	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 NIST, the U.S. Office of Management and Budget (OMB), the Secretary of Commerce, and appropriate committees of the U.S. Congress about information security and privacy issues pertaining to unclassified federal government information systems.

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.

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, 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 other 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 three times per year 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 followed in FY2009 were:

- Privacy technology;
- Essential Body of Knowledge;
- Industry Security Officers Best Practices; and
- 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); and

- NIST's outreach, research, strategies, 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 website. 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 website. 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 FY2010, 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 U.S. businesses, comprising more than 95 percent of all U.S. 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. 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) are cosponsoring 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 FY2009, the SMB outreach effort focused on expanding opportunities to reach more small businesses, and five SMB workshops were held across the country. In October 2008, two half-day workshops were held in Dallas, TX and New Orleans, LA. Similar workshops were held in January 2009 in Guam and in February 2009 in Maui, HI and Hilo, HI.

In addition to the workshops, NIST has also published a small business information security guide, NISTIR 7621, *Small Business Information Security: The Fundamentals*. This short document contains common sense information security advice for small businesses.

As an additional outreach tool, NIST has also recorded a video covering the content of the small business information security workshops. This tool will be used in many ways to reach out and educate small business owners and principals.

---

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

Health Information Technology Security

The widespread adoption and use of health information technology (HIT) have the potential to enable comprehensive management of medical information and its secure exchange between health care consumers and providers, leading to improvements in healthcare quality, reduced medical errors, increased efficiencies in care delivery and administration, and improved population health. Central to reaching these goals is the assurance of the confidentiality, integrity, and availability of health information. The CSD works actively with federal, state, and local government agencies, industry consortia, and others to provide security tools, technologies, and methodologies that provide for the security and privacy of health information.

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

- The Department of Health and Human Services' (HHS) Office of the National Coordinator for Health IT (ONC) and Office for Civil Rights (OCR);
- The Centers for Medicare and Medicaid Services' (CMS) Office of E-Health Standards and Services (OESS);
- The Healthcare Information Technology Standards Panel (HITSP); and
- The Certification Commission for Healthcare Information Technology (CCHIT).

In FY2009, CSD issued two publications related to health IT security. The first, an update of NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, was issued as a final publication in October 2008. This publication discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule, and helps to educate readers about information security concepts and terms used in the HIPAA Security Rule. The revision reflects current NIST resources and publications; discusses the latest threats, vulnerabilities, and exposures, as well as the technologies used to combat those exposures; proposes methodologies for addressing specific Security Rule implementation challenges such as conducting risk assessments and developing contingency plans; and sets the stage, through security control mappings, for security automation of the technical safeguards.

The second publication, issued in draft form in January 2009, was NISTIR 7497, *Security Architecture Design Process for Health Information Exchanges (HIEs)*. The purpose of this draft publication is to provide a systematic approach to designing a technical security architecture for the exchange of health information that leverages common government and commercial practices and that applies them specifically to the HIE domain. It seeks to assist organizations in ensuring that data protection is adequately addressed throughout the system development life cycle, and that these data protection mechanisms are applied when the organization develops technologies that enable the exchange of health information. Final publication is planned for early 2010.

To provide additional outreach and reinforce the security concepts in the HIPAA Security Rule, NIST, in conjunction with CMS' OESS, conducted a second annual HIPAA Security Rule conference, "Safeguarding Health Information: Building Assurance through HIPAA Security", in May 2009. This conference provided nearly 200 attendees with an opportunity to discuss challenges, tips, techniques, and issues surrounding implementing the HIPAA Security Rule. Presentations and panel sessions discussed a variety of HIPAA and HIT security topics including CMS' security compliance review activities, assessments from the assessor and organization perspectives, ePrescribing, FISMA's applicability to

health information, the role of the HIPAA Privacy Rule, and the HIT security and privacy provisions of the American Recovery and Reinvestment Act (ARRA) of 2009.

In FY2010, NIST plans to continue to work closely with health IT and HIPAA authoritative agencies, standards panels, and industry organizations, and to collaborate in areas including standards harmonization, testing infrastructure, and security technologies and methodologies, among others, to advance secure health information technology.

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

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

Smart Grid Cyber Security

Recognizing the benefit of focusing NIST's technical expertise and industry-oriented mission on what is one of the Nation's most pressing issues, Congress, in the Energy Independence and Security Act of 2007 (EISA) called on NIST to take a leadership role in ensuring an interoperable, secure, and open energy infrastructure that will enable all electric resources, including demand-side resources, to contribute to an efficient, reliable electricity network.

The issue of cyber security is specifically called out in the EISA legislation. This is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Existing vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.

To help ensure that the cyber security requirements of the Smart Grid are addressed as part of the NIST Smart Grid Interoperability Framework, NIST has established a Smart Grid Cyber Security Coordination Task Group (CSCTG), which now has more than 250 volunteer members from the public and private sectors, academia, regulatory organizations, federal agencies, and representatives from five countries. The CSCTG is led by CSD. This group and its work are open to the public.

To complete the work, there are several working groups that focus on specific components of the cyber security strategy, e.g., vulnerability analysis, bottom-up security issues, security architecture, high level requirements, and standards assessment. Cyber security is being addressed in a complementary and integral process that will result in a comprehensive set of cyber security requirements. These requirements are being developed using a high-level risk assessment process that is defined in the cyber security strategy for the Smart Grid.

Although still a work in progress, NIST has published a preliminary report, Draft NISTIR 7628, *Smart Grid Cyber Security Strategy and Requirements*, which describes the CSCTG's overall cyber security strategy for the Smart Grid. The preliminary report identifies security-relevant use cases, logical interface diagrams and interface categories, vulnerability classes abstracted from other relevant cyber security documents, specific issues applicable to the Smart Grid, privacy concerns, security requirements applicable to the advanced metering infrastructure, a cross-reference matrix of applicable security requirements from various standards documents. The next draft of NISTIR 7628 is scheduled to be issued at the end of December 2009. The additional content will be high level requirements for the entire Smart Grid and a functional architecture. The final document is scheduled to be published in spring 2010.

---

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG
Contact: Ms. Annabelle Lee
(301) 975-8897
annabelle.lee@nist.gov

Supply Chain Risk Management

The ever broadening reliance upon globally sourced information system equipment exposes federal information systems and networks to an enlarging risk of exploitation through counterfeit materials, malicious code, or untrustworthy products. NIST participation in the President's Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, *Develop Multi-Pronged Approach for Global Supply Chain Risk Management*, which is co-chaired by the Department of Defense (DoD) and Department of Homeland Security (DHS), will provide federal agencies with a standard, well-understood toolkit of acquisition, technical, and intelligence resources to manage supply chain risk to a level commensurate with the criticality of information systems or networks. This integrated approach is based on the work of subject matter experts operating across the government.

NIST, in coordination with DoD, DHS, and Department of State will be issuing for public review draft NISTIR 7622, *Supply Chain Risk Management Practices for Federal Information Systems*. This document discusses the following topics:

- Determining procurements that are vulnerable to supply chain risk;
- Understanding procurement strategies and working with the procurement office to help mitigate supply chain risk;
- Mitigating residual supply chain risk by requiring either the contractor or the organization to implement additional ap-

plicable practices contained in the planned document and augmenting the baseline of security controls (NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government) defined for the information system; and

- Describing the roles and responsibilities within the organization as it relates to supply chain risk management.

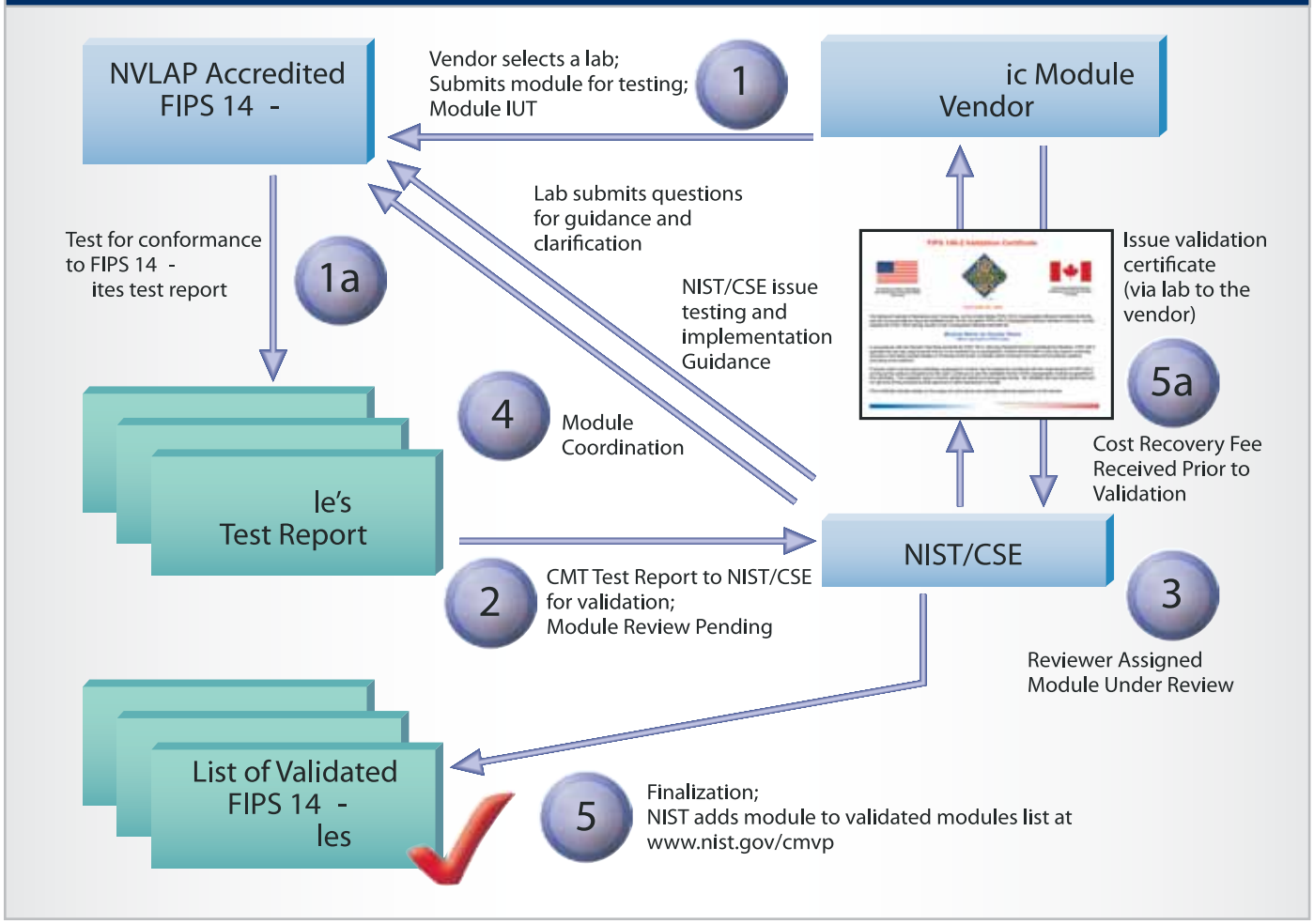
NIST intends to expand this document into a NIST SP after many of the practices and organizational structure and methodologies have been piloted under the auspice of the CNCI Initiative.

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

Cryptographic 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. Through these programs, NIST works 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.

GENERAL FLOW OF FIPS 140 2 TESTING AND VALIDATION CHART



The CMVP provides a documented methodology for conformance testing through a defined set of security requirements in 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 previous page, the acronym IUT stands for 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 18 accredited laboratories in the United States, Canada, the United Kingdom, Germany, Spain, Japan, and Taiwan R.O.C. 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/.

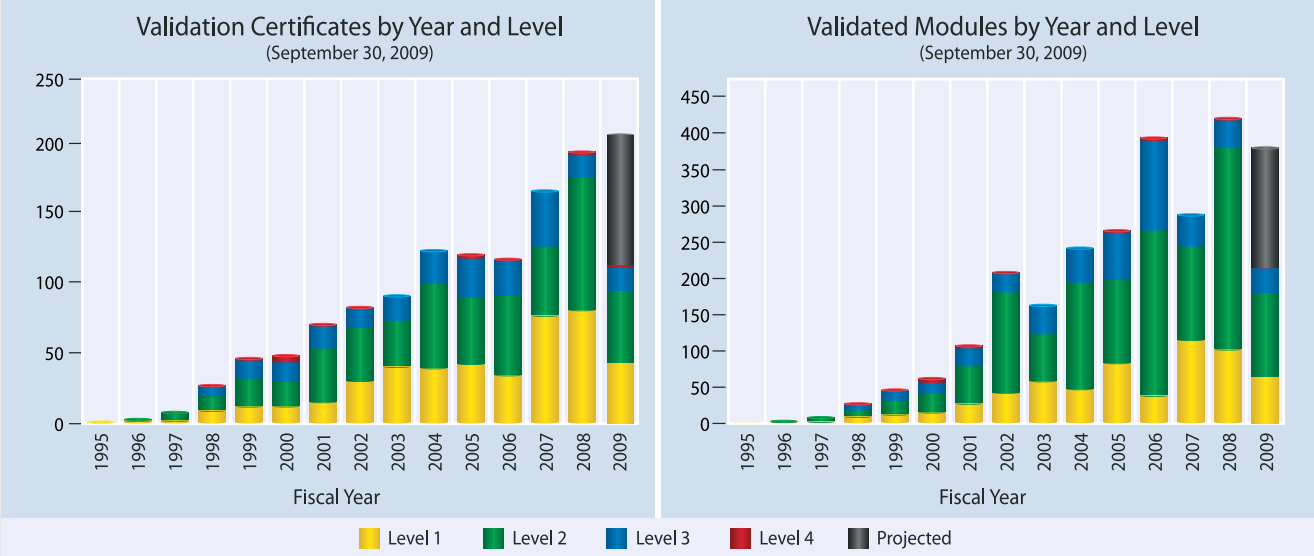
http://ts.nist.gov/standards/accreditation/index.cfm
Contact: Mr. Randall J. Easter
(301) 975-4641
randall.easter@nist.gov

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 and Canada—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 and the 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 a small number of modules may account for hundreds of products. Likewise, the CAVP validates cryptographic algorithms that may be integrated in one or more cryptographic modules.

The CMVP and the CAVP have stimulated improved quality and security assurance of cryptographic modules. Statistics from the testing laboratories show that 60 percent of the cryptographic modules and 9 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 less than a 50 percent chance of buying correctly implemented cryptography. To date,

THE PROGRESS OF THE CMVP



over 1,185 validation certificates have been issued, representing over 2,420 modules that were validated by the CMVP. These modules have been developed by more than 280 domestic and international vendors.

In FY2009, the CMVP issued 166 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 1,345 algorithm validations in FY2009. This is an increase of approximately 220 algorithm validations since FY2008. During the last three years the number of validation certificates issued has grown significantly. In FY2006, 631 algorithm validation certificates were issued, and in FY2007, 1,040 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 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 18 third-party laboratories that are accredited as CMT laboratories by NVLAP. We develop and maintain a Cryptographic Algorithm Validation System (CAVS) tool that 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);
- The Digital Signature Standard (DSS2) (as specified in FIPS 186-3, *Digital Signature Standard (DSS)*, dated June 2009);
- Hashing algorithms SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 (as specified in FIPS 180-3, *Secure Hash Standard (SHS)*, dated October 2008);
- 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, *Recom-*

mendation 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*);

- The Elliptic Curve Digital Signature Algorithm (ECDSA) (as specified in ANSI X9.62);

- Key Agreement Schemes and Key Confirmation (as specified in SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, dated March 2007); 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*, dated November 2007).

In FY2010, we expect to augment the CAVS tool to provide algorithm validation testing for:

- The Elliptic Curve Digital Signature Standard (ECDSA2) (as specified in FIPS 186-3, *Digital Signature Standard (DSS)*, dated June 2009);

- RSA2 (as specified in FIPS 186-3, *Digital Signature Standard (DSS)*, dated June 2009);

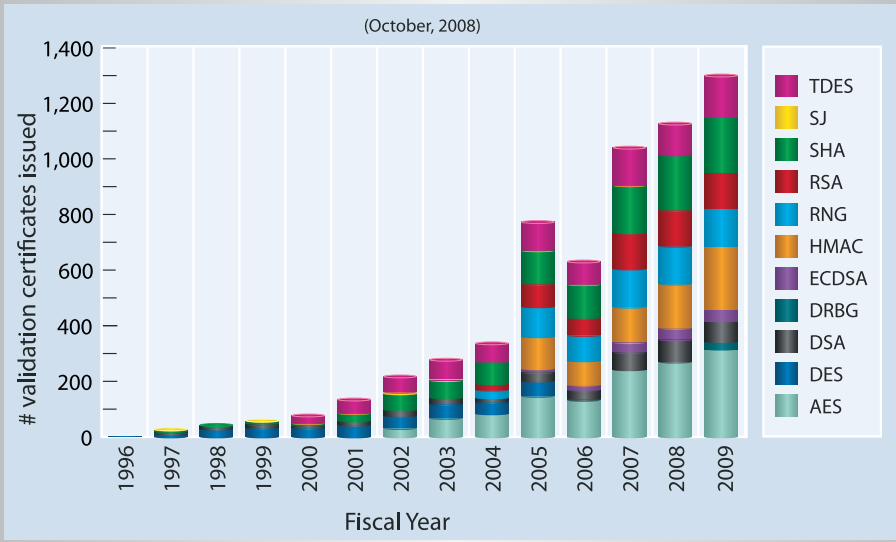
- SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*, dated November 2008;

- SP800-106, *Randomized Hashing for Digital Signatures*, dated February 2009;

- SP800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, dated August 2009; and

- Draft SP800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*.

THE PROGRESS OF THE CAVP



Fiscal Year	AES	DES	DSA	DRBG	ECDSA	HMAC	KAS	RNG	RSA	SHA	SJ	TDES	Total
FY 1996	0	2	0	0	0	0	0	0	0	0	0	0	**2**
FY 1997	0	11	6	0	0	0	0	0	0	7	2	0	**26**
FY 1998	0	27	9	0	0	0	0	0	0	6	0	0	**42**
FY 1999	0	30	14	0	0	0	0	0	0	12	1	0	**57**
FY 2000	0	29	7	0	0	0	0	0	0	12	1	28	**77**
FY 2001	0	41	15	0	0	0	0	0	0	28	0	51	**135**
FY 2002	30	44	21	0	0	0	0	0	0	59	6	58	**218**
FY 2003	66	49	24	0	0	0	0	0	0	63	3	73	**278**
FY 2004	82	41	17	0	0	0	0	28	22	77	0	70	**337**
FY 2005	145	54	31	0	14	115	0	108	80	122	2	102	**773**
FY 2006	131	3	33	0	19	87	0	91	63	120	1	83	**631**
FY 2007	240	0	63	0	35	127	0	137	130	171	1	136	**1,040**
FY 2008	269	0	77	4	41	158	0	137	129	191	0	122	**1,127**
FY 2009	376	0	71	23	33	193	3	142	143	224	1	138	**1,347**
Total	**1,339**	**331**	**388**	**27**	**142**	**680**	**3**	**643**	**567**	**1,092**	**18**	**861**	**6,091**

---

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, and ISO/IEC 24759, *Test requirements for cryptographic modules*, on July 1, 2008. These efforts bring consistent testing of cryptographic modules in the global community.

ISO/IEC JTC 1/SC 27 has addressed plans for the revision of ISO/IEC 19790, Security requirements for cryptographic modules. At its fall 2008 ISO/IEC meeting, the Secretariat approved the appointment of editors for this project, including Mr. Randall J. Easter from NIST. Due to the delay in the release of the NIST 2nd draft of FIPS 140-3, there was no further progress in addressing the revision of ISO/IEC 19790 in FY2009.

---

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

Guidelines and Documents

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 (NISTIRs). 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*. This guide can be found on our CSRC website, under the Publications section. 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 FY2009, 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

Draft Special Publication 800-16, Revision 1, Information Security Training Requirements: A Role- and Performance-Based Model

During FY2008, CSD made significant changes to SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. 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 FY2009, we completed changes to the draft document and announced a three-month public review and comment period. Comments were received and analyzed, and changes made to the document.

Related to this guideline, we continued to work with stakeholders of other federally focused information security training and workforce development initiatives. The goal is to create a multi-agency task force to assist 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 Revision 1 to be completed during FY2010.

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

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

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

SP 800-64 Revision 2, 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 compre-

hensive 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; and
- 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 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

SP 800-65 Revision 1, Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process

In December 2008, CSD started to review and update SP 800-65, and to develop Revision 1 of the publication. SP 800-65 was approaching five years of age and was in need of updating to reflect recent laws, regulations, and guidance.

This document discusses how information security considerations, including continuous monitoring, Plans of Action and Milestones (POA&M), external evaluations, new mandates, evolving threats, and system life cycle considerations, impact capital planning considerations. This document also discusses considerations and frameworks agencies can use to prioritize security investments and help ensure that security concerns are incorporated into the capital planning process to deliver maximum security and mission value to the agency.

The process presented in this guidance document is intended to serve as a model methodology. Agencies should work within their investment planning environments to adapt and incorporate the pieces of this process into their own unique processes to develop workable approaches for CPIC. If incorporated into an agency's processes, the methodology can help ensure that IT security is appropriately planned for and funded throughout the investment's life cycle, thus strengthening the agency's overall security posture.

SP 800-65 Revision 1 was published in draft form for public comment in August 2009. It is expected to be released in final form in the first quarter of FY2010.

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

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

NISTIR 7298, Glossary of Key Information Security Terms

Over the years, 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, 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 (NISTIRs, SPs, and FIPS) 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 those 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.

The updated draft NIST glossary was released for public comment in the forth quarter of FY2009 and includes all terms and definitions in the updated CNSSI-4009.

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

NISTIR 7621, Small Business Information Security: The Fundamentals

NIST, in partnership with the Small Business Administration and the Federal Bureau of Investigation has had educational outreach to the small business community since 2002. With full participation from our partners, we schedule, promote, and conduct information security workshops for small businesses throughout the United States.

The core information in the workshops has been collected in NISTIR 7621, *Small Business Information Security: The Fundamentals*. This document covers the fundamentals of information security for small business. The intent was to publish a short, easy to read document that small business owners could use to protect the information, computers, and networks used in their small businesses.

The draft of NISTIR 7621 was released for public comment in September 2009 and is planned for release as a final document in the first quarter of FY2010.

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

Cryptographic Technology Group

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 procedures.

Overview

The Cryptographic Technology (CT) Group continues 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 they process. IT users enjoy the enhanced availability of secure applications in the marketplace that is made possible by the appropriate use of cryptography. Our main work in this area addresses topics such as hash algorithms, symmetric and asymmetric cryptography techniques, key management and transport, authentication, cryptographic protocols, Internet security services, security applications, biometrics, and smart tokens. A few examples of the impact of our work are changes to how users authenticate their identities for online government services and new methods for authentication and key management of wireless applications. This work also supports the NIST's Personal Identity Verification (PIV) project in response to the Homeland Security Presidential Directive 12 (HSPD-12).

The CT Group collaborates with national and international agencies, academic and research organizations, and standards bodies to develop interoperable security standards and guidelines. Federal agency collaborators include the Department of Energy, the Department of State, the National Security Agency (NSA), the Election Assistance Commission (EAC), and the Communications Security Establishment of Canada, while 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, the Internet Engineering Task Force (IETF), and the Organization for the Advancement of Structured Information Standards (OASIS). Industry collaborators include Booz Allen Hamilton, Certicom, Entrust Technologies, Microsoft, Orion Security, RSA Security, Voltage Security, and Cisco. Academic and research organizations include the Computer Security and Industrial Cryptography-Katholieke University Leuven, the University of Malaga, the International Association for Cryptologic Research (IACR), the European Network of Excellence in Cryptology (ECRYPT) II, and the Japanese Cryptography Research and Evaluation Committees (CRYPTREC).

Cryptographic Standards Toolkit

Hash Algorithms

A hash algorithm processes a message, which can be very large, and produces a condensed representation, called the message digest. A cryptographic hash algorithm is designed to achieve certain security properties and is typically used with other cryptographic algorithms, such as digital signature algorithms, key derivation functions, and keyed-hash message authentication codes, or in the generation of random numbers. Cryptographic hash algorithms are frequently used in Internet protocols or in other applications.

In 2005, researchers developed an attack that threatens the security of the NIST-approved, government hash algorithm standard SHA-1. Since 2005 researchers at NIST and elsewhere have also discovered several generic limitations in the basic Merkle-Damgard construct that is used by SHA-1 and most other existing hash algorithms. To address these threats, NIST initiated a public competition in November 2007 for a SHA-3 hash algorithm. 64 entries were received by the submission deadline of October 31, 2008, of which 51 first round candidates were announced on December 9, 2008 as meeting the minimum submission requirements.

Submitters of the first round candidates were invited to present their algorithms at the First SHA-3 Candidate Conference in Leuven, Belgium in February 2009. Cryptanalysis and public feedback on these candidates were requested by June 1, 2009. NIST announced 14 second round candidates on July 24, 2009. A year is allocated for the public review of the second round candidates, and NIST plans to host the Second SHA-3 Candidate Conference on August 23-24, 2010 at the University of California, Santa Barbara. The competition is expected to be completed in 2012.

Security Guidelines of Using Approved Hash Algorithms

Two NIST SPs were completed during FY2009: SP 800-106, *Randomized Hashing for Digital Signatures*, and SP 800-107, *Recom-*

mendation for Applications Using Approved Hash Algorithms. SP 800-106 specifies a method to enhance the security of the cryptographic hash algorithms used in certain digital signature applications by randomizing the messages that are signed. SP 800-107 addresses security issues related to applications of approved hash algorithms as specified in FIPS 180-3, *The Secure Hash Standard (SHS)*, including the use of HMAC as specified in FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*. Additional technical details for using FIPS 180-3 and 198-1 are also provided in SP 800-107.

Digital Signatures

The completion of FIPS 186-3, *Digital Signature Standard (DSS)*, was announced in June 2009. This revision includes additional key sizes for the Digital Signature Algorithm (DSA) to provide higher security strengths, and guidance on the use of Rivest-Shamir-Adelman (RSA) and the Elliptic Curve Digital Signature Algorithm (ECDSA) to promote interoperability when using digital signatures. An additional publication on the use of digital signatures, SP 800-102, *Recommendation for Digital Signature Timeliness*, was completed in September 2009.

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) on the development of Draft American National Standard (DANS) X9.82, *Random Number Generation*, which will include guidance on entropy sources and the construction of random bit generators from entropy sources and DRBGs.

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, and contains specifications for Diffie-Hellman and MQV key agreement schemes. In August 2009, SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, (e.g., RSA) was completed. It contains specifications for key transport and key agreement schemes using RSA, and is based on American National Standard (ANS) X9.44, *Key Establishment Using Integer Factorization Cryptography*.

Block Cipher Modes of Operation

The XTS-AES mode was submitted to NIST by the Chair of the IEEE P1619 Task Group. The XTS-AES mode is designed to encrypt data for storage applications, without expansion of the data, to avoid disrupting existing data pathways. Although this requirement precludes the incorporation of a tag-based authentication method, XTS-AES is designed to mitigate the resulting vulnerability to manipulation of the encrypted data. Last year NIST proposed to approve XTS-AES by reference to IEEE Std 1619-2007. This year, after considering the public comments on the proposal and follow-up comments from the submitters, we decided to proceed with the proposal. Draft SP 800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*, is the vehicle for the approval; the document underwent a period of public comment in August and September 2009 and is nearly finalized.

A proposed specification of the AES Key Wrap mode has been available for many years on our website. This mode provides an option for authenticated encryption, intended for applications that need to segregate the protection of cryptographic keys from the protection of other data. The mode can be considered as a kind of "meta" block cipher, in that each bit of output data depends, in a nontrivial manner, on each bit of input data, at the cost of relatively slow performance. This year we expect to specify and approve an extension of that specification that supports the padding method specified in Request for Comments (RFC) 5649.

We also will continue to consider two submissions for format-preserving encryption, where the format of the data might be a credit card number or a social security number. Such a mode could facilitate the analysis of databases by concealing personally-identifiable information without disrupting existing data structures and any applications that rely on those structures. The two submissions are the Feistel Finite Set Encryption Mode, whose submitter has indicated that a revision is forthcoming, and the Format Controlling Encryption Mode.

Contacts:
Ms. Shu-jen Chang (Hash Algorithms)
(301) 975-2940
shu-jen.chang@nist.gov

Mr. Quynh Dang (FIPSs 180-3 & 198-1, SPs 800-106 & 107)
(301) 975-3610
qdang@nist.gov

Ms. Elaine Barker (Digital signatures, RNG, Key Establishment)
(301) 975-2911
ebarker@nist.gov

Dr. Morris Dworkin (Block cipher modes of operation)
(301) 975-2354
moris.dworkin@nist.gov

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).

In 2009, public comments were requested on Draft SP 800-57, *Recommendation for Key Management - Part 3: Application-Specific Key Management Guidance*. This document addresses application-specific guidance that includes guidance on using a PKI; protocols such as Internet Protocol Security (IPsec), Transport Layer Security (TLS), Secure/Multipart Internet Mail Extensions (S/MIME), Kerberos, and Over-the-Air Rekeying (OTAR); and applications such as Domain Name Systems Security Extensions (DNSSEC), and Encrypted File Systems. This Recommendation is expected to be published in the first quarter of FY2010.

In June 2009, a Cryptographic Key Management (CKM) workshop was conducted by CSD to identify and develop technologies that would allow organizations to leap ahead of normal development lifecycles to vastly improve the security of future sensitive and valuable computer applications. The workshop was the first step in developing a CKM framework. Draft NISTIR 7609, *Cryptographic Key Management Workshop Summary*, is a draft report of the workshop. This draft report is available on our CSRC website under the NISTIR publications section. This draft should become final during Q1 FY2010. This summary provides the highlights of the presentations, organized by both topic and by presenter. A draft of a general CKM framework is expected to be available for comment during Q2 FY2010. Further information about this project is available on the CSRC website.

---

http://csrc.nist.gov/groups/ST/key_mgmt/

Contacts: Mr. Quynh Dang
(301) 975-3610
qdang@nist.gov

Ms. Elaine Barker
(301) 975-2911
ebarker@nist.gov

Authentication and Key Management for Wireless Applications

An access authentication with key establishment protocol allows a mobile device to be securely connected to the network. The Extensible Authentication Protocol (EAP), specified by the Internet Engineering Task Force (IETF), is commonly employed as a framework for authentication and key establishment in well-launched wireless technologies, such as the wireless local area network (WLAN) specified by the Institute of Electrical and Electronics Engineers in IEEE 802.11.

In FY2009, we published NIST SP 800-120, *Recommendation for EAP Methods Used in Wireless Network Access Authentication*. The Recommendation formalizes a set of core security requirements for EAP methods when employed by the U.S. Government for wireless access authentication and key establishment.

In FY2009, we also published NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*. SP 800-108 specifies three families of key derivation functions using pseudorandom functions. They incorporate the most commonly used key derivation functions in wireless and mobility applications.

Contact: Dr. Lily Chen
(301) 975-6974
lily.chen@nist.gov

Internet Security

We continue to support the development and enhancement of key management standards for Public Key Infrastructure (PKI). NIST has led the development of an interoperability report for RFC 5280, *The Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280 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. The development of the interoperability report will demonstrate the maturity of Internet Engineering Task Force (IETF) PKI standards, identify implementation gaps, and will ultimately result in promoting RFC 5280 from proposed standard to draft standard. 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). One of these documents, *Elliptic Curve Cryptography Subject Public Key Information*, was published as RFC 5480 in March 2009.

The CSD has been collaborating with the Advanced Network Technologies Division of ITL to support the development of security enhancements for routing protocols. The goal of this work is to develop protocols that allow for the validation of Internet routing information in order to prevent attacks against the infrastructure which are intended to misroute Internet traffic or cause denial of service conditions. Other ongoing activities are focused on key

management and cryptographic agility to support the authentication of routing components (e.g., to support the Border Gateway Protocol).

Contacts: Mr. William Polk
(301) 975-3348
william.polk@nist.gov

Dr. David Cooper
(301) 975-3194
david.cooper@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. NIST plans to respond to this eventuality by identifying and 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, NIST intends to draft standards for computer security architectures that do not rely on public key cryptographic primitives. In addition, NIST will examine new approaches, such as quantum key distribution.

In FY2009, we published two research papers related to quantum computing and quantum information. Alan Mink, Sheila Frankel, and Ray Perlner published a journal article on the integration of quantum key distribution with the popular commodity security protocols, TLS and IPSec. Ray Perlner and David Cooper also published a survey paper on public key cryptographic algorithms that resist quantum attacks, and Ray Perlner presented the paper at the 8th Symposium on Identity and Trust (IDTrust2009).

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 December 2008, we completed a second draft update of SP 800-63, *Electronic Authentication Guideline*, and requested public comments. This followed a similar first draft and a public comment request period early in 2008. SP 800-63 supports the Office of Management and Budget (OMB) Memorandum 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 first draft 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. Comments on the second draft, along with additional comments from the OpenID Consortium and the Federal CIO Council's Citizen Outreach Focus Group, raised concerns with the password entropy and identity proofing requirements in the first two drafts. These concerns have been addressed. A third draft is expected late in 2009, leading to final publication in 2010.

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. As part of NIST's efforts led by the Software and Systems Division of ITL, CSD supports the activities of the EAC and the TGDC related to voting equipment security.

In the past year, we assisted the EAC in updating the i by incorporating security requirements found in the draft of the next version of these guidelines, the VVSG 2.0. Updated security requirements included software verification techniques, cryptographic modules, securing electronic records, voter verifiable paper audit trails (VVPAT), and security documentation. As part of this effort, we supported the EAC with resolutions to public comments on the incorporated security requirements. Associated test suites were also developed for the updated requirements. 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. This work included the development of NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems*, which identified threats to systems which electronically transmit election materials. In addition, the test suites for the security requirements found in the VVSG 2.0 were updated based on public comments received.

In FY2010, we will investigate how to incorporate open-ended vulnerability testing (OEVT) into the voting system conformance testing process and plan to revise the security test suites for the updated VVSG based on public comments. We will provide technical support to the EAC on their UOCAVA efforts and continue to conduct research on threats to voting systems and innovative voting system architectures. NIST will be holding an end-to-end (E2E) voting system workshop to investigate the viability of using these novel voting systems for large-scale elections. In addition, we will support the NIST National Voluntary Laboratory Accreditation Program (NVLAP) efforts to accredit voting system test laboratories and host the TGDC plenary meetings. We plan to engage voting system manufacturers, voting system test laboratories, state election officials, and the academic community in exploring 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

Development of FIPS 140 3, Security Requirements for Cryptographic Modules

FIPS 140-3 (draft), *Security Requirements for Cryptographic Modules*, provides four increasing qualitative levels of security that are 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 physical ports and logical interfaces; roles, authentication, and services; software security; operational environment; physical security; physical security – non-invasive attacks; sensitive security parameter management; self-tests; life-cycle 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.

The FIPS 140-3 draft is a result of the reexamination and reaffirmation of the current standard, FIPS 140-2. The draft standard adds new security requirements imposed on cryptographic modules to reflect the latest advances in technology and security, and to mirror other new or updated standards published by NIST in the area of cryptography and key management. Additionally, software and firmware requirements are addressed in a new area dedicated to software and firmware security, while another new area specifying requirements to protect against non-invasive attacks is also provided.

The development of FIPS 140-3 started in 2005 and relied on the preliminary inputs provided by users, laboratories, and vendors during the September 2004 NIST-CSE Cryptographic Module Validation Symposium and the September 2005 NIST-CSE Physical Security Workshop. In 2007, the first draft of the standard was released for public comment, and NIST received over 1,200 comments, which were sorted by sections and subsections and centralized in a dedicated database.

During the past year, the comments were thoroughly reviewed and discussed, and the working group's resolutions were implemented in the second draft of the standard. As a result of this process, the working group revisited the five security levels introduced in the previous draft and decided to provide only four increasing security levels, to introduce the notion of a trusted channel and define the associated requirements, to keep the firmware concept that was removed in the first draft of the revised standard, to dedicate a separate section for the software and firmware security requirements, and to introduce a new section specifying requirements to address non-invasive attack methods that will be listed in a new, dedicated annex.

The second draft of FIPS 140-3 was submitted for internal review to NIST specialists and partners. The feedback of this review process was analyzed, and the draft was updated to include the provided comments. Prior to the submission of this proposed revised standard (i.e., FIPS 140-3) to the Secretary of Commerce for review and approval, NIST considered it essential that consideration be given

to the needs and views of the public, users, the information technology industry, and federal, state and local government organizations; therefore, in September 2009 a revised draft of FIPS 140-3 was prepared for a second public review. The Federal Register Notice announcing the revised draft standard for public review and comment is being reviewed prior to publication.

Contact: Dr. Michaela Iorga
(301) 975-8431
michaela.iorga@nist.gov

Systems and Emerging Technologies Security Research Group

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 (PIV)

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 450 standard-conformant products were developed, validated, and brought to market. 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. According to the Office of Management and Budget (OMB), as of June 2009 approximately 2.7 million federal employees (60 percent of the federal workforce) have completed background investigations, and 2.6 million of them (59 percent of the federal workforce) have been issued their PIV cards.

CSD activities in FY2009 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 (SP) were limited to those committed to and scheduled in previous years, a small number of necessary, backward-compatible process and technical improvements (detailed below), and editorial improvements for clarity.

In 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. Further PIV Card enhancements were introduced in September 2009 with the third edition of SP 800-73 (draft SP 800-73-3, *Interfaces for Personal*

Identity Verification). This draft features technical improvements and clarifications for PIV cards and related PIV systems such as:

(1) Encryption Key History Management - to enable on-card retention of retired Key Management keys and corresponding X.509 certificates for the purpose of deriving or decrypting data encryption keys with the help of retired Key Management key(s);

(2) Key Establishment – to clarify the use of the Elliptic Curve Diffie-Hellman (ECDH) key establishment scheme with the Key Management key, as specified in SP 800-78-1; and

(3) Non-Federal Issuer (NFI) provisions – to enable the use of PIV Compatible (PIV-C) and PIV Interoperable (PIV-I) cards for NFI credentials, in accordance with the Federal CIO Council's NFI card specifications.

The public comment periods on NIST SP 800-73-3 elicited many valuable suggestions from federal departments, agencies and industry. Two of these, (1) encryption key history management and (2) NFI provisions, were strongly supported by the industry and governmental agencies alike.

NIST responds to many questions relating to HSPD-12, FIPS 201-1, and Personal Identity Verification each month. Questions originate from the OMB, 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. 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 Gerraiolo
(301) 975-6972
hildegard.ferraiolo@nist.gov

NIST Personal Identity Verification Program (NPIVP)

Program Objectives & Organization: The objective of the NIST Personal Identity Verification Program (NPIVP) is to validate Personal Identity Verification (PIV) components as required by FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, for conformance to specifications in FIPS 201 and its companion documents. The two PIV components that come under the scope of NPIVP are PIV Smart Card Application and PIV Middleware. All of the tests under NPVIP are handled by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP) and are called accredited NPIVP test facilities. As of September 2009, there are ten such facilities.

Specifications and Conformance Testing Toolkit Updates: 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, *Interfaces for Personal Identity Verification*, 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.

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 single data set. To facilitate development of conformant PIV products by vendors, NPIVP also made the PIV Data Model Test Runner available for download from the NIST website.

In FY2008, the second edition of SP 800-73 (SP 800-73-2), *Interfaces for Personal Identity Verification*, was published. After SP 800-73-2 was finalized, we updated SP 800-85A-1, *PIV Card Application and Middleware Interface Test Guidelines*, to provide test guidelines that align with the second edition of SP 800-73 (SP800-73-2). After a public comment period and resolution of received comments, the final publication of SP 800-85A-1 was released in April 2009.

Similarly, to facilitate testing of credential data on PIV Cards for conformance to the data model specifications in the second edition of SP 800-73 (SP 800-73-2) Appendix A, we updated and published SP 800-85B-1, *PIV Data Model Test Guidelines*.

After SP 800-73-2 was published, NPIVP identified the necessary updates for the PIV Interface Test Runner to align with SP 800-73-2 and the revised PIV card interface test guidelines in SP 800-85A-1. The PIV Interface Test Runner was updated to perform additional

tests needed for SP 800-73-2 compliance and made available to accredited NPIVP test facilities in FY2009. The NPIVP test facilities were also provided the directive that all future evaluations of PIV Card application and PIV Middleware products should only be performed for SP 800-73-2 compliance.

With the release of NIST 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, the Rivest-Shamir-Adelman (RSA) 1024 cryptographic algorithm on the PIV card for Digital Signatures and Key Management). This action was necessary to ensure adequate cryptographic strength for PIV applications. The use of higher strength cryptographic algorithms specified in SP 800-78-1 caused the discontinuation of use of the RSA 1024 cryptographic algorithm for Digital Signature and Key Management functionality of validated PIV card application products at the end of 2008. Instead of RSA 1024, SP 800-78-1 specifies alternative cryptographic algorithms that provide a minimum of 112 bits of security strength for digital signature and key management functionality on the PIV card. In advance of the sunset date, we coordinated the upgrade to 112 bit security strength and provided re-validation guidelines for the affected client products. Sixteen PIV Card Application products were affected by the discontinuation of RSA 1024. Three vendors re-submitted their PIV Card application products to support the higher strength security for their digital signature key and Key Management functionality.

Additions to Validated Product List: In FY2009, four more PIV Card application products were validated and certificates issued, bringing the total number of NPIVP-validated PIV Card application products to 19. Two more PIV Middleware products were validated and issued certificates, bringing the total number of NPIVP-validated PIV Middleware products to 11.

---

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 the Transportation Security Administration (TSA) and the U.S. Coast Guard, both organizations under the Department of Homeland Security (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 must hold 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; and
- 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.

In FY2009, NIST performed enhancements to the TWIC Testing toolkit to reflect some updates to "The TWIC Reader Hardware and Card Application Specification" document as well as to incorporate tests for all Authentication Use Cases.

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

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

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, support interoperability, and address privacy considerations. Technological solutions chosen for identity credentials should serve to increase the reliability of information, improve consumer/user trust and protect privacy, and do so while enabling interoperable government-wide applications. An example of such a credential is the U.S. Government HSPD-12 PIV smart card based token.

The United States led effort to address interoperability limitations and the lack of normative identity related services resulted in a new standard, International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 24727, *Identification Cards – Integrated Circuit Cards Programming Interfaces*. This multi-part standard strives to resolve existing ambiguities in current standards that challenge interoperability and introduces much needed application programming interfaces and normative processes for identification, authentication, and signature services (IAS).

ISO/IEC 24727 established the architecture required to develop secure and interoperable frameworks for integrated circuit card technology based identity credentials. It enables interoperable and interchangeable smart card systems, eliminating consumer reliance on proprietary-based solutions historically provided by industry. Existing standards provide the consumer a great degree of flexibility, which can introduce challenges to achieving interoperable solutions for identity credentials, card readers, and card applications. ISO/IEC 24727 builds on these standards, fine-tuning them to improve interoperability and addressing areas that were lacking, such as a normative set of authentication protocols and IAS services.

ISO/IEC 24727 provides a set of programming interfaces for interactions between integrated circuit cards 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 conformant identity credentials. The parts consist of:

- 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. and
- 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, 2009, ISO/IEC 24727-1, ISO/IEC 24727-2, ISO/IEC 24727-3, and ISO/IEC 24727-4 are finalized and available for purchase. ISO/IEC 24727-5 is at final committee draft stage, with an anticipated publication date in late calendar year 2009. ISO/IEC 24727-6 is nearing completion and is expected to be published by the end of calendar year 2009. NIST also published NISTIR 7611, *Use of ISO/IEC 24727, Service Access Layer Interface for Identity (SALII):*

Support for Development and use of Interoperable Identity Credentials, which describes the use of the standard for the development and use of interoperable identity credentials.

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.

This standard (ISO/IEC 24727) 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 U.S. 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

Biometric Standards and Conformity Assessment Activities

For decades, biometric technologies were used primarily in law enforcement 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 control, 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.

Biometric Standards Activities

The NIST biometrics program supports the development of open standards for biometrics, and responds 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 test architectures and test tools to test implementations of these standards;
- Supporting harmonization of biometric, tokens and security standards; and
- Addressing the use of biometric-based solutions for ID Management applications.

In FY2009, NIST continued to work in close partnership with government agencies, industry and academic institutions to develop formal national and international biometric standards. NIST actively participated in the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management. NIST participated in the Standards and Conformity Assessment Working Group (SCA WG) and collaborated within this group in the development of an updated version of the *Registry of U.S. Government Recommended Biometric Standards*, which outlines those standards recommended for U.S. Government (USG) use in its operational systems (Registry of USG Recommended Biometric Standards, Version 2.0, August 10, 2009, NSTC Subcommittee on Biometrics and Identity Management http://www.biometrics.gov/Standards/Biometric_Standards_Registry_v2.pdf.)

NIST participates in the Department of Homeland Security Biometrics Working Group, the Department of Defense Biometrics Task Force's Biometric Standards Working Group and other government groups. Our program experts work in close collaboration with the ITL's Information Access Division (IAD) biometric experts to advance the adoption of biometric standards. Our program has gained national and international recognition for its achievements.

NIST provides the chair of Technical Committee M1 – Biometrics under the InterNational Committee for Information Technology Standards (INCITS), and actively participates in the development of its standards. NIST also provides the chair of Subcommittee 37 (SC 37) - Biometrics under the ISO/IEC Joint Technical Committee 1 (ISO/IEC JTC 1). Additionally, NIST chairs one of its six Working Groups, and provides technical editors to JTC 1/SC 37 projects.

Conformity Assessment to Biometric Standards

At the present time, biometric base standards (e.g., 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. NIST actively contributes to the development of biometric conformance testing methodology standards and other conformity assessment efforts, and to the development of associated conformance test architectures and Conformance Test Suites (CTSs). These activities support users who require conformance to selected biometric standards, as well as product developers who are interested in conforming to biometric standards by using the same testing tools available to users.

Conformance Test Architectures for Biometric Data Interchange Formats

In August 2009, NIST completed the development of an advanced Conformance Test Architecture (CTA) that supports CTSs for biometric data interchange formats. Four CTSs designed to test implementations of finger minutiae and finger image data records were completed as well. They include CTSs to test implementations of: (a) ANSI INCITS 378-2004 (referred to in the Registry of USG Recommended Biometric Standards); (b) ANSI INCITS 381-2004 (referred to in the Registry of USG Recommended Biometric Standards – PIV program); (c) ANSI INCITS 378-2009; and (d) ANSI INCITS 381-2009. The advanced CTA and the four CTSs are at pre-release final test status. The advanced CTA incorporates features such as strong test cases for data, structure and full testing of the CTSs, independent component development (each can be independently developed and tested), and dynamically-loaded CTS modules (modules automatically loaded at runtime).

Ongoing and Planned work

Beta 3 of the advanced conformance test architecture is planned for the fourth Quarter of FY2010. Some of the features that are being researched and/or implemented are providing for full web services support and the development of a CTS developer's kit to promote third-party development of CTS modules that can be incorporated into our architecture. Sample data (conformant/non-conformant) to the biometric data interchange formats that can be tested with our existing CTSs is under development. NIST has initiated the development of CTSs for selected international versions of biometric data interchange formats. The associated sample data will also be generated. Research is planned on the need for the development of additional CTSs to test implementations of new biometric technical interface standards being developed. NIST will also research the adaptation of existing modules to our architecture. The detailed analysis of the base standards that are the target of our CTS development has already led to a number of technical contributions towards the development of national and international biometric standards taking place in INCITS and JTC 1/SC37 (e.g., finger minutiae and finger image standards, conformance testing methodology standards).

The Biometric Consortium

The Biometric Consortium (BC), co-chaired by NIST and NSA, serves as a focal point for research, development, testing, evaluation, and application of biometric-based personal identification/verification technology. The BC's primary function is to organize and host an annual conference, which enables federal government participants to engage in exchanges with national and international participants on topics such as biometric technologies for defense, homeland security, identity management, border crossing and electronic commerce.

The 2009 conference, co-sponsored by NIST, NSA, DHS, DoD Biometrics Task Force, the National Institute of Justice (NIJ), GSA, the Volpe National Transportation Systems Center, and the Armed Forces Communications and Electronics Association (AFCEA), was held September 22-24. It 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. One of the largest conferences dedicated to biometrics worldwide, the conference attracted over 1,500 participants from the 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 pro-

gram. Presentations are available at the conference website: http://www.nist.gov/bc2009.

---

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

Research in Emerging Technologies

Access Control – Information Sharing Environment

Information flow within an organization may be controlled mostly by operational and management procedures. Organizations may avoid sharing information when they aren't sure what access rules should be applied when information is requested from another organization and, as a result, they may not fully share information. This project explores more protections, privacy and accountability, and provides a means to give the right information to authorized users at the right time while complying with and enforcing federal, state, local, or tribal security and privacy policies.

This project involves applying electronic security and privacy policy access controls in an information sharing environment such as the Privilege Management project for Fusion Centers. This project will develop the supporting standards and guidance for reference implementations. A pilot will be built upon the multi-year Global Federated Identity and Privilege Management (GFIPM) work to help the National Information Exchange Model (NIEM) leap forward in supporting institutionalized secure information sharing, and to provide critical support for Identity and Authorization Management challenges within the Information Sharing Environment (ISE).

During the past year, we worked on the Director of National Intelligence (DNI) Privilege Management Pilot project, which will address the concerns of law enforcement officials, fusion center analysts, and privacy advocates by enabling sharing of more information in a timely manner with enforceable and auditable access policies. The tasks included the following:

- Wrote proposal, work statements, and design documents;
- Developed architecture and functional specification for the design of the Pilot system;
- Extended Access Control Protocol Testing (ACPT) tool for access control (AC) model and property composing and verification; and
- Developed privacy AC control framework, which supports sharing of data from fusion center.

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

Dr. Stephen Quirolgico
(301) 975-8246
stephn.quirolgico@nist.gov

Dr. Tom Karygiannis
(301) 975-4782
tom.karygiannis@nist.gov

Automated Combinatorial Testing for Software (ACTS)

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 National Aeronautics and Space Administration (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 FY2009 include the following:

- Release of a new version of the ACTS covering array generator that includes constraint handling, a critical requirement for many real-world software projects; development of new methods and software tools for measuring several different forms of combinatorial coverage; completion of software in a joint project with North Carolina State University on combinatorial testing for analyzing access control systems; and distribution of over 230 copies of a beta version of the testing tool. The team won the Excellence in Technology Transfer Award from the Federal Laboratory Consortium, Mid-Atlantic Region, for the ACTS tool. and

- The team also initiated research on applying combinatorial methods to domains beyond software testing, including analysis of gene expression data in microarrays, evolutionary programming, and modeling and simulation.

Plans for FY2010 include working with another national laboratory on measurements of combinatorial coverage in spacecraft software and correlation with fault detection; methods and tools for identification of failure-causing combination (fault localization); combinatorial test sequence generation; combinatorial security testing; design for testability; and a generic interface to integrate ACTS in existing hardware-software testing infrastructures. A planned addition is 'robustness testing' to check and reject invalid inputs. We also plan to work with industry researchers and practitioners to transition the tools and methods into practical application. Tansuo is the prototype tool to build navigation graphs for dynamic web applications and generate combinatorial tests for the applications. We are working with researchers from several major universities, other NIST divisions and labs, and private industry to gather data on fault detection effectiveness of combinatorial test methods.

---

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) is 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 to bridge 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 extended our prototype system to a practical system that can be applied to generic AC models with limited capability. We investigated in-depth issues such as code assertion verification, limitation, and none-model applications. Our reports were published in an international journal and at some conferences. In the coming year, we will add more model templates and eXtensible Access Control Markup Language (XACML) generating capability in the Access Control Property Testing (ACPT) tool. We will also perform testing of the tool in a testbed environment, as well as continue investigating different testing methods for access control properties.

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 man-

aging 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, and related open standards, and deployed in SOA allow data and applications to interact without human intervention through dynamic 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 interdependencies 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 FY2009, we did a proof of concept implementation to validate our results. In FY2010, we plan to enhance our techniques for different kinds of attacks on web services and publish our results in conferences and workshops.

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, used by individuals for both personal and professional purposes. Mobile devices allow users to place calls; perform text, multimedia, and instant messaging; exchange electronic mail (e-mail); browse the Web; manage personal information, such as address book, task list, and calendar entries; capture photos and videos; and create, edit, and read digital documents. The significant amount of information that tends to accumulate on them over time may need to be protected from intruders or to be recovered as evidence for a security incident or crime investigation. For these reasons, mobile handheld devices are an emerging but rapidly growing area of computer security and forensics.

Although mobile handheld devices are approaching the functionality 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 traditional computer security and forensic techniques difficult.

The focus of the mobile security and forensics project is twofold:

- To improve the security of mobile devices; and
- To improve the state-of-the-art of mobile device forensics.

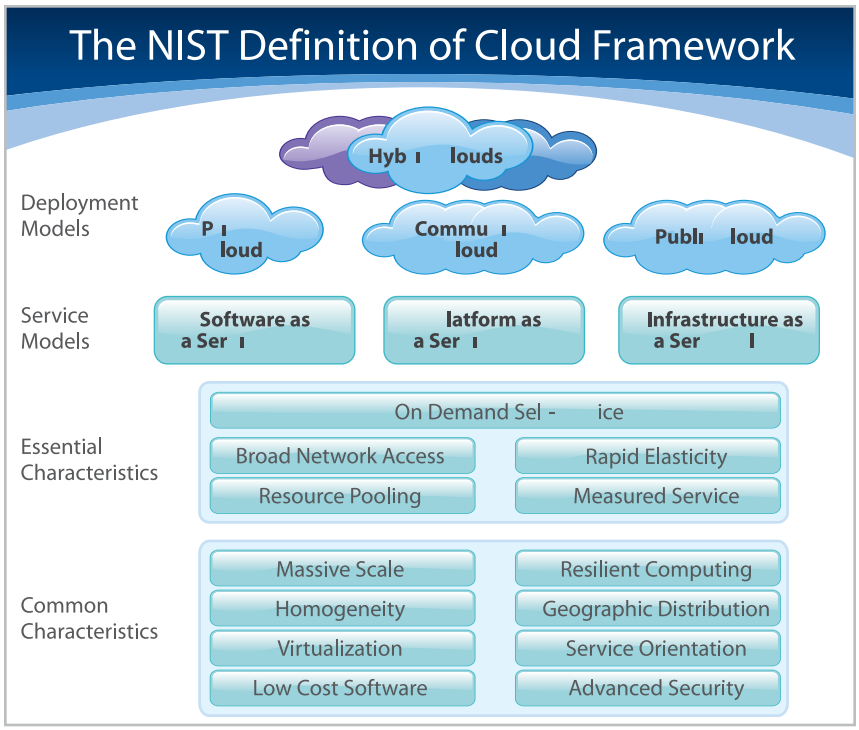
Past work in handheld device security includes several proof-of-concept implementations of security mechanisms suited for the capabilities and limitations of such devices. Detailed descriptions can be found on the project website (see below). This past year we published an additional conference paper on the design and implementation of an authentication mechanism that uses wireless security beacons to provide location data and control device behavior. We also finalized NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*. This publication provides an overview of security issues with mobile devices and offers insights into making informed security decisions. It includes details about the threats and technology risks involved and the available safeguards to mitigate them. Users of cell phones and other business-oriented mobile devices, as well as security professionals and officials responsible for information technology security in government and elsewhere, should find the information useful.

Prior work at NIST in the mobile device forensics area examined the quality and use of forensic tools and identified ways to remove impediments to the practice of cell phone forensics. During FY2009, our work has progressed along both fronts. We improved our methodology for validating the correct functioning of forensic tools quickly and accurately. The approach, called identity module programming, automatically populates devices with reference test data that serves as baseline reference material for validating the correct functioning of related forensic tools. An application and set of reference test data was developed that illustrates the methodology for identity modules of certain classes of cell phones. The

distribution package can be found at the project website. Draft NISTIR 7617, *Mobile Forensic Reference Materials: A Methodology and Reification* describes the methodology and test results from applying the distribution to assess popular forensic tools was also prepared and is available on the project website. This draft NISTIR will be finalized in early FY2010. Follow-on work includes investigating ways to improve the reference test data, using techniques such as fuzzing and combinatorial test generation. The intended audience for these products ranges broadly from computer response team members, to organizational security officials, to law enforcement.

---

http://csrc.nist.gov/groups/SNS/mobile_security/
Contact: Mr. Wayne Jansen
(301) 975-5148
wjansen@nist.gov



NIST Cloud Computing Project

NIST is promoting the effective and secure use of cloud computing within government and industry by providing technical guidance and promoting standards. Our first effort was to define cloud computing and its models so that organizations could prudently adopt technology that would best provide them the promised benefits. This includes reduced costs for enterprise applications and physical hardware, decreased power consumption, enabling data transparency, green computing, and increased organizational agility in deploying new IT services.

According to the NIST cloud computing definition, "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The full extended definition describes five essential characteristics, three service models, and four deployment models.

This definition is available from the NIST cloud computing website (http://csrc.nist.gov/groups/SNS/cloud-computing/) and will be published in our upcoming NIST cloud computing SP. The publication will also cover cloud security advantages and challenges, architecture strategies, and deployment guidance.

The NIST cloud computing project is also supporting the cloud computing groups under the Federal Chief Information Officers (CIO) Council. This includes providing technical advice to the Cloud Computing Executive Steering Committee (ESC), the Cloud Computing Advisory Council (CCAC), and the Information Security and Identity Management Committee's (ISIMC) Web 2.0 working group.

---

http://csrc.nist.gov/groups/SNS/cloud-computing/
Contact: Mr. Peter Mell
(301) 975-5572
peter.mell@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.

Lack of 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 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.

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 that 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., RBAC 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 FY2009, NIST developed new specifications for defining the new concept of PM process; creating, managing, and destroying PM processes; defining/generating constraints on processes; eliminating the computation and activation of a set of user attributes for a session in order to gain access to a resource; and redefining the link value attributes in order to improve scalability. In addition we implemented and tested the new specifications in our PM reference implementation.

Also, in FY2009, NIST and Symantec jointly submitted three PM related project proposals to International Committee for Information Technology Standards (INCITS) under the title of "Next Generation Access Control" (NGAC), which were approved:

- Project 2193-D: Next Generation Access Control - Generation Access Control - Implementation Requirements, Protocols and API Definitions;
- Project 2194-D: Next Generation Access Control - Functional Architecture; and
- Project 2195-D: Next Generation Access Control - Generic Operations & Abstract Data Structures.

The Technical Committee on Cyber Security of the InterNational Committee for Information Technology Standards, CS1, further created an "NGAC Ad Hoc" group, and directed the group to work on Projects 2193-D, 2194-D & 2195-D

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 e-mail, workflow management, and database management.
- Enterprise wide scope of protection – One administrative domain is provided vs. access control management being performed on an OS-by-OS and application-by-application basis. Also, access control policies are uniformly enforced over resources that are physically stored on a multitude of heterogeneous systems.
- Comprehensive enforcement – All user and process access requests, all exchange of data among applications and between sessions, and all exportation of data outside the PM's bounds of control can be uniformly controlled under the PM's protection policies.
- 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). and

- 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 FY2009, we researched the authorization and trust management in grid/scalable environment using Web 2.0 technologies. The result is published in the paper, *Access Control Policy Composition for Resource Federation Networks Using Semantic Web and Resource Description Framework (RDF)*. This paper is publicly available on-line at: http://dspace.lib.fcu.edu.tw/bitstream/2377/11126/1/ce07ics002008000070.pdf . We also researched the authorization and authentication for non-human pervasive devices, especially for the privacy and transfer-of-the-ownership capabilities. The result is incorporated in the "Device Lifecycle Identification Management" section of the document, *NIST Proposal for Supply Chain Product Counterfeiting Threat Assessment and Countermeasures*. This proposal is not publicly available.

In FY2010, we will continue our investigation on trust management frameworks, functional stacks, protocols, and application programming interfaces (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

Security Ontologies: Modeling Quantitative Risk Analysis of Enterprise Systems

Over the past years, computer security has become a very diversified field of research. It has become increasingly difficult for experts of different domains to understand each other and to use

a precisely defined terminology. Therefore, there is a need for a security ontology, which can clearly define security related concepts and their relationships, and which can then be used to do quantitative risk analysis for enterprise information systems. The main goal of our research in this project is to develop an ontology that "knows" which threats endanger which assets and which countermeasures can reduce the probability of attacks. In addition, each asset and each countermeasure in the ontology can be annotated with various types of costs as well as benefits. By comparing various scenarios during a quantitative risk analysis, companies can choose which safeguard packages are more effective. The ontology will guarantee a shared and accurate knowledge of threats and countermeasures. It will provide objective data for decision making about the countermeasures to implement and the countermeasures to avoid because they are not cost effective.

In FY2009, we developed a security ontology that describes entities such as threats, vulnerabilities, countermeasures, assets, and security objectives. We have described these entities in RDF and Web Ontology Language (OWL). In FY2010, we plan to develop graphical tools for a user to visualize and edit ontologies and to generate database schemas in Structured Query Language (SQL) that can be used to generate reports about enterprise level security metrics.

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 U.S. Government repository of standards-based vulnerability management reference data. The NVD provides information regarding security vulnerabilities and configuration settings, vulnerability impact metrics, technical assessment methods, and references to remediation assistance and IT product identification data. The NVD reference data supports security automation efforts based on the Security Content Automation Protocol (SCAP). As of September 2009, NVD contained the following resources:

- Over 38,000 vulnerability advisories with an average of 14 new vulnerabilities added daily;
- 17 SCAP-expressed checklists containing thousands of low-level security configuration checks that can be used by SCAP validated security products to perform automated evaluations of system state;
- 111 non-SCAP security checklists (e.g., English prose guidance and configuration scripts);
- 182 U.S. Computer Emergency Readiness Team (US-CERT) alerts, 2,346 US-CERT vulnerability summaries, and 2,517 SCAP machine-readable software flaw checks;
- Product dictionary containing over 18,000 operating system, application, and hardware name entries; and
- 23,335 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's effective reach has extended through the use of NVD SCAP data by commercial security products that are deployed to thousands of organizations worldwide. Increased adoption of SCAP is evidenced by the increasing demand for NVD XML data feeds and SCAP-expressed content from the NVD website.

NVD continues to play a pivotal role in the Payment Card Industry (PCI) efforts to mitigate vulnerabilities in credit card systems. PCI mandates the use of NVD vulnerability severity scores in measuring the risk to payment card servers worldwide and for prioritizing vulnerability patching. PCI's use of NVD severity scores helps enhance credit card transaction security and protects consumers' personal information.

Throughout FY2009, NVD continued to provide vulnerability reference data while expanding its support of security checklists, providing a data feed containing authoritative mappings of checklist-level security settings to NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. Accomplishments under the NVD program include development of an advanced product dictionary search capability and significant enhancements to the National Checklist Program website.

NVD data is a fundamental component of modern security infrastructure and is substantially increasing the security of networks worldwide. The CSD plans to expand and improve the NVD in FY2010.

---

http://nvd.nist.gov
Contact: Mr. Christopher Johnson
(301) 975-5981
christopher.johnson@nist.gov

Security Content Automation Protocol (SCAP)

To support the broad security automation vision, it is necessary to have both trusted information and a standardized means to store

and share it. Through close work with its government and industry partners, NIST has developed the Security Content Automation Protocol (SCAP) to provide the standardized technical mechanisms to share information between systems. Through the NVD and the National Checklist Program, NIST is providing relevant and important information to the areas of vulnerability and configuration management.

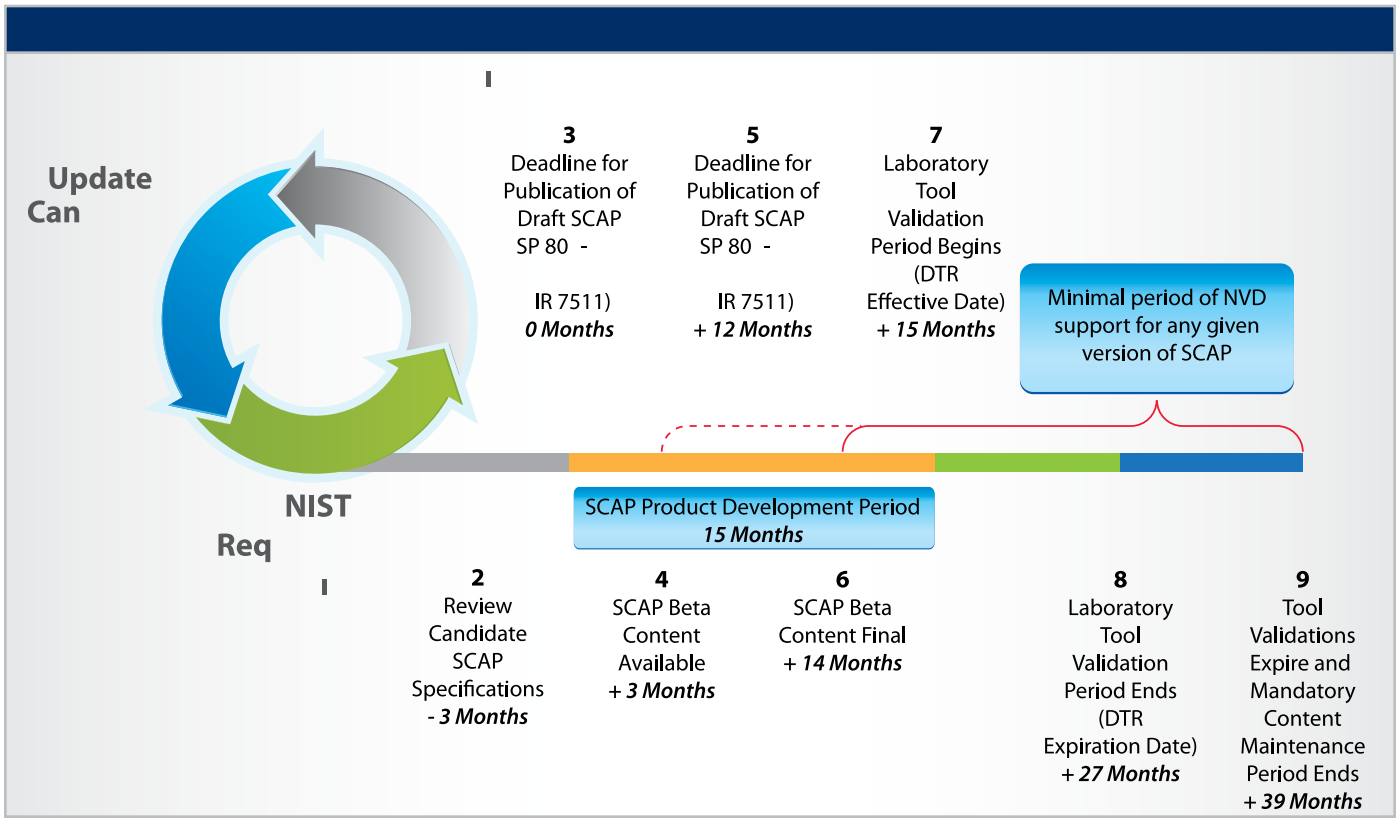
Combined, SCAP and the programs that leverage it are moving the information assurance industry in a direction of being able to standardize communications, collect and store relevant data in standardized formats, and provide automated means for the assessment and remediation of systems for both vulnerabilities and configuration compliance.

SCAP

SCAP is a suite of specifications that use the eXtensible Markup Language (XML) to standardize the format and nomenclature by which security software products communicate information about software flaws and security configurations. SCAP includes software flaw and security configuration standard reference data, also known as *SCAP content*. This reference data is provided by the NVD (The National Vulnerability Database can be found at http://nvd.nist.gov/), which is managed by NIST and sponsored by the Department of Homeland Security (DHS). SCAP is a multi-purpose protocol that supports automated vulnerability checking, technical control compliance activities, and security measurement. The U.S. Government, in cooperation with academia and private industry, is adopting SCAP and encourages its use in support of security automation activities and initiatives.

Draft NIST SP 800-126 is the SCAP technical specification (http://csrc/publications/drafts/sp800-126/Draft-SP800-126.pdf.) CSD plans to publish SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1*, in final form in the first quarter of FY2010. This document describes the six component specifications comprising SCAP:

- Extensible Configuration Checklist Description Format (XCCDF), an XML specification for structured collections of security configuration rules used by operating system (OS) and application platforms;
- Open Vulnerability and Assessment Language (OVAL), an XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and patches;
- Common Configuration Enumeration (CCE), a dictionary of names for software security configuration issues (e.g., access control settings, password policy settings);



- Common Platform Enumeration (CPE), a naming convention for hardware, OS, and application products;

- Common Vulnerabilities and Exposures (CVE), a dictionary of names for publicly known security-related software flaws; and

- Common Vulnerability Scoring System (CVSS), a method for classifying characteristics of software flaws and assigning severity scores based on these characteristics.

The SCAP specification identifies the SCAP components and how they relate to each other within the context of SCAP. However, the SCAP specification does not define the SCAP components themselves; each component has its own standalone specification. The SCAP components were created and are maintained by several entities, including the MITRE Corporation, the National Security Agency (NSA), and the Forum of Incident Response and Security Teams (FIRST).

SCAP is being widely adopted by major software and hardware manufacturers and has become a significant component of large information security management and governance programs. The protocol is expected to evolve and expand in support of the growing need to define and measure effective security controls, assess and monitor ongoing aspects of that information security, remediate non-compliance, and successfully manage systems in accordance with the risk management framework described in NIST SP 800-53 (The Risk Management Framework is described within NIST Special Publication 800-53, available at http://csrc.nist.gov/publications/.) To manage that evolution, a timeline has been constructed to balance progress against stability:

The timeline on the previous page allows for new specifications to be added to SCAP and the SCAP Validation Program, while ensuring vendors and users have a 15 month window to update their products and/or processes to accommodate for the changes. A full description of the timeline can be found at http://scap.nist.gov/timeline.html .

Specifications have both intrinsic and synergistic value. They have intrinsic value in that the specification demonstrates value on its own merits. For example, XCCDF is a standard way of expressing checklist content. XCCDF also has a synergistic value when combined with other specifications such as CPE, CCE, and OVAL to create an SCAP-expressed checklist that can be processed by SCAP-validated products. Likewise, CVE has use cases in simply being a consistent way to enumerate vulnerabilities for tracking purposes; however, when combined with CPE and OVAL, CVE is elevated to formulate a greater use case, namely that of automated checks for vulnerabilities that can be processed by SCAP-validated products. These relationships are captured in NIST SP 800-126. However, it is important to recognize that specifications can and should demonstrate value in their own right without being SCAP specifications. To address this, NIST will explore the possibility of implementing separate but related validation programs for individual specifications. For example, NIST is in the process of implementing an OVAL Validation program with the purpose of allowing products to be tested for OVAL functionality that may not be used in SCAP use cases.

It is expected that new specifications will be developed on an ongoing basis. In response, NIST has established an e-mail list and web page specifically for emerging specifications. More information can be found at http://scap.nist.gov/emerging-specs/.

Currently, NIST is leveraging SCAP in multiple areas, both to support their own mission and to enable other agencies and private sector entities to meet their goals. For NIST, SCAP is a critical component of the SCAP Validation Program, the NVD, and the National Checklist Program.

Contact: Mr. Dave Waltermire
(301) 975-3390
david.waltermire@nist.gov

National Checklist Program

There are many threats to users' computers, ranging from remotely launched network service exploits to malicious code spread through e-mails, malicious websites, and download of infected files. Vulnerabilities in 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.

To facilitate development of security configuration checklists for IT products and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). 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;

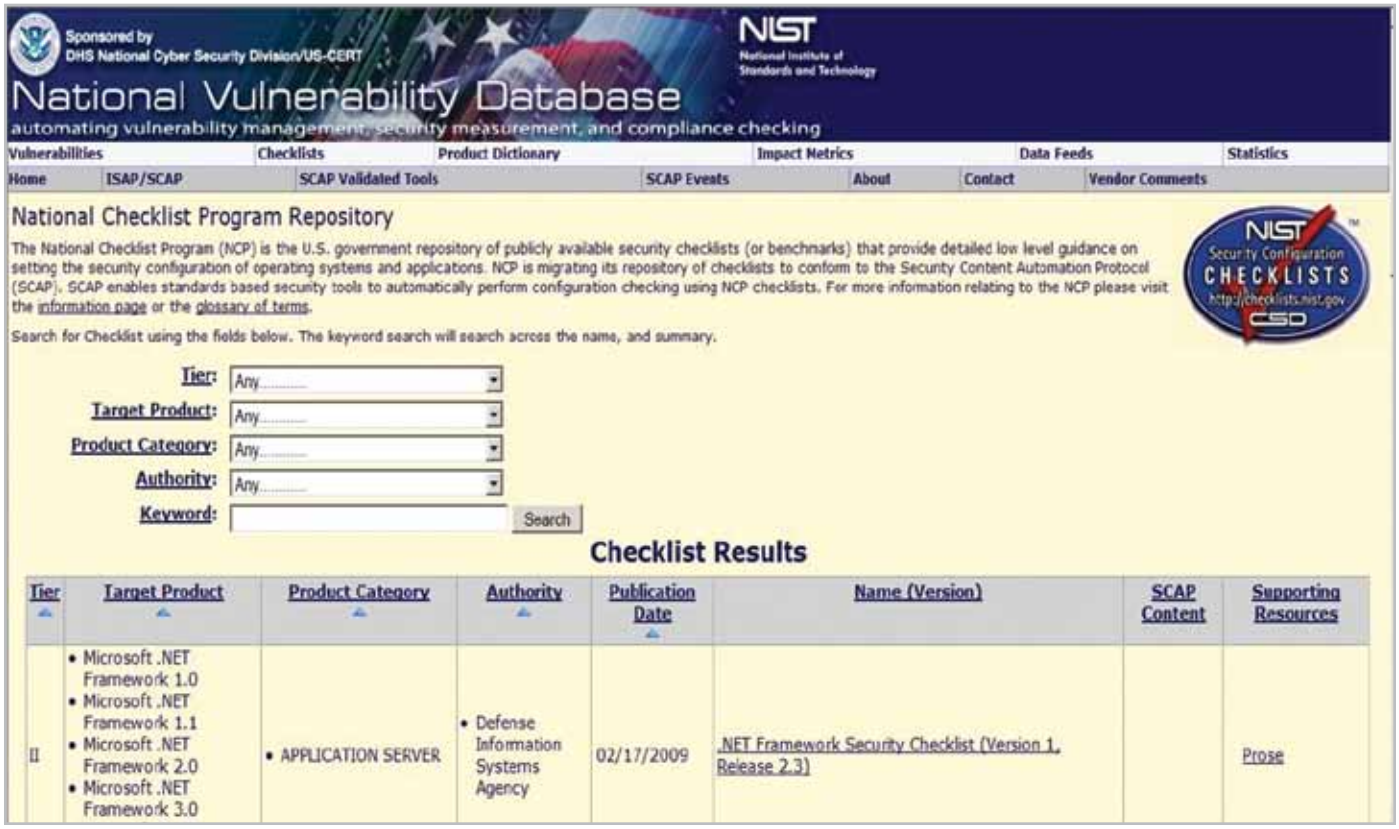
- Provide guidance to developers to help them create standardized, high-quality checklists that conform to common operations environments;

- 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; and
- Encourage the use of automation technologies for checklist application such as the SCAP.

Checklists can take many forms, including files that can automatically set or verify security configurations. Having 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 ensures 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. Security products and checklist authors assemble content from SCAP data repositories to create viable SCAP-expressed security guidance. A security configuration checklist that documents desired security configuration settings, installed patches, and other system security elements using SCAP in a standardized format is known as an SCAP-expressed checklist. Such a checklist would use XCCDF to describe the checklist, CCE to identify security configuration settings to be addressed or assessed, and CPE to identify platforms for which the checklist is valid. The use of CCE and CPE entries within XCCDF checklists is an example of an SCAP convention — a requirement for valid SCAP usage (See NIST SP 800-126 for more information.) Another example of an SCAP convention is the mapping of individual checks within a checklist to external requirements such as security controls from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. Organizations producing SCAP content should adhere to these conventions to ensure the highest degree of interoperability.

There are 128 checklists posted on the website; 17 of the checklists are SCAP-expressed and can be used with SCAP-validated products. It is anticipated that a minimum of 26 more SCAP-expressed checklists will be added in FY2010 as contributions come from other federal agencies and product vendors. This allows organizations to use checklists obtained from the NCP



website (checklists.nist.gov) for automated security configuration patch assessment. NCP currently hosts SCAP checklists for Internet Explorer 7.0, Office 2007, Red Hat Linux, Symantec AntiVirus, Windows 2000, Windows 2003 Server, Windows Vista, Windows XP and other products.

To assist users in identifying automated checklist content, NCP groups checklists into tiers, from tier I to tier IV as in Figure 2 on the previous page. NCP uses the tiers to rank checklists according to their automation capability. Tier IV checklists are considered production-ready and have been validated by NIST SP 800-70 Revision 1, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, to ensure, to the maximum extent possible, interoperability with SCAP-validated products. Tier III checklists have not been validated, but they can be executed by SCAP-validated products. Tier II checklists document recommended security settings in a machine-readable, non-standard format, such as a proprietary format or a product-specific configuration script. Tier I checklists are prose-based and contain no machine-readable content.

Checklists are sorted by default according to tier, from tier IV to tier I. Users can browse the checklists based on the checklist tier, IT product, IT product category, or authority, and also through a keyword search that searches the checklist name and summary for user-specified terms. The search results show the detailed checklist metadata and a link to any SCAP content for the checklist, as well as links to any supporting resources associated with the checklist.

Although checklists are encouraged for use in both the private and public sectors, 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 Memorandum M08-22, Office of Management and Budget (OMB) mandated the use of SCAP Validated products for continuous monitoring of Federal Desktop Core Configuration (FDCC) compliance.

The NCP is defined in NIST SP 800-70 Revision 1, which can be found at http://csrc.nist.gov/publications/ ,

---

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 individual specifications that work together to meet various use cases. A single error in product implementation could result in undetected vulnerabilities or policy non-compliance within agency and industry networks.

The SCAP Validation Program was created on request by the OMB to support the Federal Desktop Core Configuration (FDCC). It works with the NIST National Voluntary Laboratory Accreditation Program (NVLAP) to set up independent conformance testing laboratories that conduct the testing based on draft NISTIR 7511 Revision 1, *Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements*. When testing is completed, the laboratory submits a test report to NIST for review and approval. Product validations are currently active for one year, at which time vendors have the option to renew their validation by submitting the product for testing. SCAP validation testing has been designed to be inexpensive, yet effective. The SCAP conformance tests are either easily human verifiable or automated through NIST provided reference tools. To date, the program has accredited ten independent laboratories and validated 25 products from 19 different vendors.

While FDCC SCAP testing is an important part of the program, it is only one of several SCAP capabilities which vendors can apply to test their products. The others cover product capabilities such as configuration scanning, vulnerability scanning, patch checking, and remediation capabilities, all within the SCAP context.

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 and was publically announced on July 15, 2009. The Department of Defense (DOD) Computer Network Defense (CND) initiative also relies of SCAP validation for the future DOD cyber security strategy.

The SCAP Validation Program will continue to operate in FY2010. It will expand to include additional capabilities, will provide enhanced testing support, and will evolve to include new technologies as SCAP itself matures. This expansion may include changes to SCAP or the introduction of new validation program scopes.

Another new area, currently in its early stages, is the SCAP Content Validation Program. Its purpose will be to ensure that SCAP content is available through the National Checklist Program (NCP) is assured to work in SCAP Validation Products within the same use

case. As the use of SCAP continues to grow into mission critical areas, it is increasingly important that users of the technology can be assured that it will function as expected. This means that when SCAP content is processed by a SCAP validated product, it should work without error. Achieving this goal requires the creation of the SCAP Content Validation Program. Carried out in conjunction with the SCAP Product Validation Program and the NCP, SCAP Content Validation will ensure that content designed to meet a specific use case, such as configuration compliance, can be processed fully and accurately by SCAP validated products for that same use case. The NCP, using a tiered structure, will highlight SCAP validated content by placing it in the highest tier, Tier IV (See NIST SP 800-70 Rev 1 at http://csrc.nist.gov.) This provides end users a fast and simple way to identify the content they need, pair it with their SCAP validated products, and achieve their mission goals.

Contact: Mr. John Banghart
(301) 975-8514
john.banghart@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 FY2009, CSD continued its long-term research efforts on technical security metrics, focused primarily on attack, vulnerability, and security control measurement. 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. NIST also released NISTIR 7564, *Directions in Security Metrics Research*, in April 2009. NISTIR 7564 provides an overview of the security metrics area and looks at possible avenues of research that could be pursued to advance the state of the art.

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 NISTIR 7517, *The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities*, published in February 2009. CMSS adapts CVSS for use with feature misuse and trust relationship misuse vulnerabilities;

- Second public comment period for draft NISTIR 7502, *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*, published in June 2009. CCSS is based on CVSS and CMSS but has been customized for use with software security configuration-related vulnerabilities; and

- Paper on an analysis of CVSS version 2 measurements and scores from software flaw vulnerabilities in the National Vulnerability Database, to be presented at the 2009 International Workshop on Security Measurements and Metrics (MetriSec 2009) in October 2009.

During FY2010, we plan on finalizing the CMSS and CCSS specifications.

---

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 IT 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 networked 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 the 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; they are inexpensive to collect, are expressed numerically, have units of measure, and have specific context. 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. Our metric is consistent, unambiguous, and provides context for understanding security risk of computer networks.

In FY2009, we developed a new model of security analysis based on Bayesian Networks. This required the availability and widespread use of automated vulnerability scanning tools, and a new type of algorithm to construct attack graphs. We also did performance analysis of our techniques to understand how our method will scale up for enterprise networks consisting of several thousand hosts. Numerous papers were published in conferences and workshops based on this work. In FY2010, we plan to enhance our techniques to handle previously unknown types of exploits, such as "zero day attacks". We also plan to publish our results in conferences and journals.

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

Infrastructure Services, Protocols, and Applications

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 U.S. OMB mandated that government agencies should incorporate IPv6 capability into their backbone systems (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 precisely defined.

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. IPSec 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 it had been deployed for some time, 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 virtual private network (VPN) implementation may have flaws in algorithms or software, or insecure configuration settings and values that attackers can exploit.

NIST SP 500-267, A *Profile for IPv6 in the United States Government (USG) - 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 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. Developed to help ensure that IPv6-enabled federal information systems are interoperable and secure, the publication 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.

In OMB Memorandum 05-22 (OMB URL: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf) NIST is

tasked to develop a standard that addresses compliance with IPv6. The USG v6 Profile (USGv6 Profile: http://www.antd.nist.gov/usgv6/profile.html) has been published to specify the technical requirements for IPv6 in the federal government. In that document we suggest that product testing services are likely to be needed to ensure the confidence and to protect the investment of early IPv6 adopters. We surveyed the existing testing programs and concluded that a distinct USG testing program is needed, but with the commitment to harmonization and convergence into a broad collaborative user/vendor testing initiative, which can accommodate the technical and profiling requirements of the USG.

In order to promote confidence and mutual recognition of test results, we added the requirement for test results to be developed at laboratories that are accredited for these test methods in accordance with ISO/IEC 17025. The accreditation landscape has itself changed in recent years. Where it was once possible to designate a single, usually government-run accrediting authority, there is now competition from private accreditors who compete on a level playing field. The qualifications for laboratory accreditation organizations include compliance with ISO/IEC 17011, and being signatory to the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Agreement (MRA). In order to promote comparability of test results across the accredited testing laboratories, we encourage qualified accreditors to collaborate in the development of IPV6 testing specific accreditation requirements and to publish or reference the technical criteria to be applied in addition to the requirements of ISO/IEC 17025 in the accreditation of IPV6 testing laboratories. NIST SP 500-273, *USGv6 Test Methods: General Description and Validation*, was developed to provide guidance to all accreditors and test laboratories on units of accreditation, standard reference tests, test method validation criteria, and vital feedback mechanisms to maintain quality improvement in test suites, in addition to maintaining consistency of test interpretations.

Testing of network protection devices requires a separate infrastructure. It involves functional testing, local interface, environment, and document inspection.

Claims of compliance with the USGv6 profile shall be documented using a Supplier's Declaration of Conformity (SDoC) which details the USGv6 capabilities supported and the results of testing each capability by an accredited laboratory. In this scheme, the product is tested for conformance and interoperability in accredited laboratories; based on a review of the test results and the requirements of the USGv6 document, the supplier issues an SDoC recording what the product is, its specifications, equivalent machines, and the high level categories supported. A standardized format for the supplier's declaration will promote the acceptance of this approach to testing and conformity assessment of IPV6.

NIST SP 800-119, *Guidelines for the Secure Deployment of IPv6*, will be posted for public comment in FY2010. This document describes and analyzes the numerous protocols that comprise IPv6, including addressing, domain name system (DNS), routing, mobility, quality of service, multihoming, IPsec, etc. For each component, there is a detailed analysis of the differences between IPv4 and IPv6, the security ramifications and any unknown aspects. New sections were added to address late-breaking, significant changes in the approach to IPv6 transition.

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 a global distributed system in which Internet addresses in mnemonic form such as http://csrc.nist.gov are converted into the equivalent numeric Internet Protocol (IP) 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 with 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) to provide origin authentication and data integrity for all responses from the DNS. In partnership with the Department of Homeland Security, NIST has been actively involved in promoting the deployment of DNSSEC since 2004.

As part of this continuing effort, we published guidelines for DNSSEC deployment in NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, in May 2006. This year, the first revision was begun (SP 800-81r1). The revision includes updated configuration and operational guidance based on lessons learned from early deployments. Some of these changes include:

- Aligning cryptographic algorithm and key recommendations with NIST approved algorithms and key sizes;
- Guidance on the use of Next Secure 3 (NSEC3) DNS Resource Record that presents authenticated denial of existence so as to minimize information leakage; and
- Guidance on cryptographic algorithm rollover and DNSSEC deployment in split zones (e.g., firewall, Network Address Translation (NAT)) environments.

Because of the amount of new material in the revised publication, there have been two periods of public comments to enable us to gather the viewpoints of as broad a community as possible. The second public comment period ended on September 30, 2009 with the final version due after all comments are reviewed.

Also, NIST authors submitted an article to the IEEE Security & Privacy special issue on DNS Security. The article, titled *Open Issues in Secure DNS Deployment* addresses open issues in DNSSEC deployment such as algorithm maturity and migration, key sizes and response packet size problems, and operational considerations. It was published in the September/October 2009 issue of IEEE Security & Privacy.

NIST also assisted the General Services Administration (GSA) in deploying DNSSEC on the .gov Top Level Domain (TLD) to meet the OMB mandate. NIST provided a technical review of contractor plans, and developed a comprehensive test plan for the .gov delegation holder interface on http://www.dotgov.gov/. The DNSSEC deployment was successful, with NIST continuing to provide technical support for contractors.

NIST continued the Secure Naming Infrastructure Pilot (SNIP) operations in 2009. The SNIP is a distributed testbed to help U.S. Government DNS administrators deploy DNSSEC and test new DNSSEC implementations. Recent advancements on the SNIP include:

- Continued support for federal agencies to test DNSSEC operations. Support includes acting as the test registrar when performing key rollovers and monitoring test zone status;
- Granted delegation request to state and local governments as well as federal agencies; and
- Tested different implementations (Secure64, Microsoft Server, Xelerance) with the SNIP and the dotgov.gov interface and the signed .gov TLD.

NIST is also involved in providing technical review and assistance to the National Telecommunications and Information Administration (NTIA) in developing a set of requirements and testing plan for deploying DNSSEC at the root "." zone. Since the root zone is queried by every client connected to the Internet, it is important to ensure the security and stability of the system when deploying any new technology, including DNSSEC. NTIA, partnering with their contractors (Verisign and the Internet Corporation for Assigned Names and Numbers [ICANN]), plans to deploy DNSSEC on the root zone by December 2009. NIST will continue to provide technical comments to NTIA plans and tests as required to meet this deadline.

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

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

Wireless Security Standards

Wireless communications and devices are convenient, flexible, and easy to use. For example, users of many wireless devices have the flexibility to move from one place to another while maintaining connectivity with the wireless network.

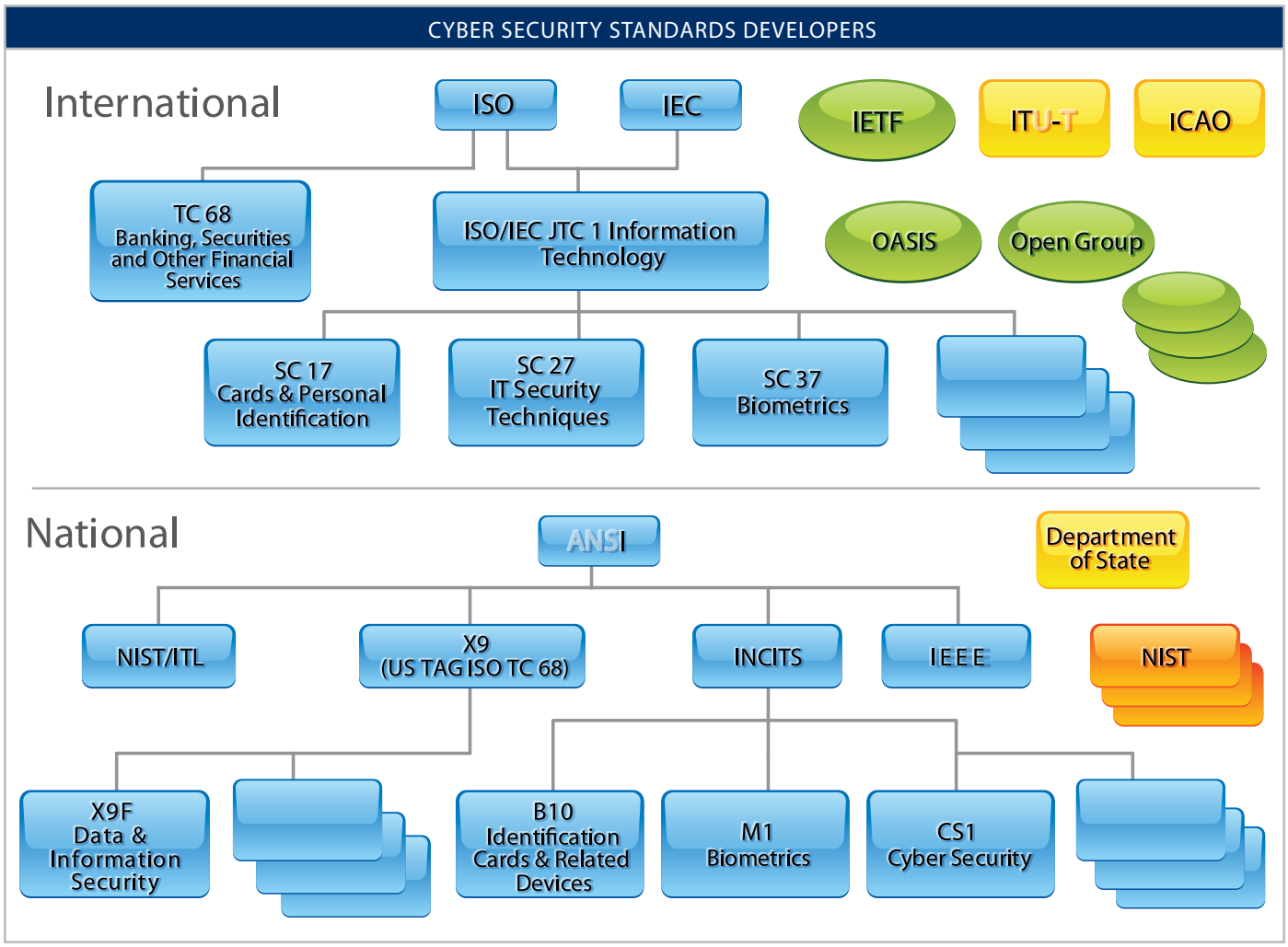
While wireless networks are exposed to many of the same risks as wired networks, they are vulnerable to additional risks as well. Wireless networks transmit data through radio frequencies and are open to intruders unless protected. Intruders have exploited this openness to access systems and services,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

This past year, we developed a new Special Publication (SP) dealing with wireless security issues. Draft NIST SP 800-127, *Guide to Security for WiMAX Technologies*, was published in September 2009. It discusses security considerations for current and past IEEE 802.16 specifications for Worldwide Interoperability for Microwave Access (WiMAX) technologies. WiMAX is a wireless metropolitan area network (WLAN) communications technology that can be used for last-mile broadband access or cellular-like mobile architectures. Draft SP 800-127 explains the security features provided by the IEEE 802.16 standards and provides recommendations to federal agencies on securing their WiMAX technologies. We expect to finalize the publication during FY2010.

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

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

Figure 1 on the next page shows the many national and international standards developing organizations (SDOs) involved in cybersecurity standardization. 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 the International Electrotechnical Commission (IEC).



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). 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; and
- 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; and

- 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; and
- SC 7 - Core Banking.

The American National Standards Institute (ANSI) is a private, non-profit organization (501(c)(3)) that administers and coordinates the U.S. 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 U.S. standards internationally, advocates U.S. 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 U.S. representative and dues-paying member of the two major non-treaty international standards organizations, the ISO and, via the U.S. 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 U.S. providers of IT 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); and
- T6 – Radio Frequency Identification (RFID) Technology.

As a technical committee of INCITS, CS1 develops U.S. 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, and

- 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, and
  - Outsourcing;
- Identity management, including:
  - Identity management framework,
  - Role-based access control, and
  - Single sign-on;
- Privacy technologies, including:
  - Privacy framework,
  - Privacy reference architecture,
  - Privacy infrastructure,
  - Anonymity and credentials, and
  - 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 (IETF), 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 U.S. 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 U.S. experts to work on various SC 27 projects or to serve in various SC 27 leadership positions. Currently a number of CS1 members are serving as 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*. Erika McCallister will take over as Editor of 29115, *Entity Authentication Assurance*.

All input from CS1 goes through INCITS to ANSI, then to SC 27. This arrangement is also a conduit for getting U.S.-based new work item proposals and U.S.-developed national standards into the international SC 27 standards development process. 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. In addition CS1 is making contributions on several new areas of work in SC 27, including study periods and/or new work item proposals on Information security management guidelines for financial and insurance services, Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001, Secure System Engineering principles and techniques (Technical report type 2), Lightweight cryptography, an Information security governance (ISG) framework, Guidelines for identification, collection and/or acquisition and preservation of digital evidence, Guidelines for security of outsourcing, Requirements on relative anonymity with identity escrow, and a Privacy Capability Maturity Model.

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. Internationally, there are over 80 published standards, and almost all are National Standards. There are more than 63 current international standards projects.

During this reporting period the following have been added to the CS1 membership roster: Plum Hall Inc., Veridion, Yaana Technologies, Amper Politziner & Mattia, Fidelity, GMAC Financial Services, VHA, Boeing, Home Federal, and Direct Computer Resources (DCR).

NIST's Cybersecurity research plays a direct role in the Cybersecurity Standardization efforts of CS1. During this fiscal year:

1. The CS1 Task Group CS1.1 RBAC has finished and INCITS is about to publish the national standard titled *Requirements for the Implementation and Interoperability of Role Based Access Control*. In addition, the task group has started work on the revision of INCITS 359 – 2004, *Role Based Access Control (RBAC)*. NIST originally authored RBAC, and both Rick Kuhn and Richard Kissel are working in this task group.

2. The NIST Policy Machine R&D has resulted in three national projects that CS1 has recommended, and which the INCITS Executive Board has recently approved as national standards projects:

   a. New INCITS Project Proposal -- Next Generation Access Control - Implementation Requirements, Protocols and API Definitions (NGAC-IRPADS). Its assigned project number is 2193-D, and Roger Cummings will be the editor;

   b. New INCITS Project Proposal -- Next Generation Access Control – Functional Architecture (NGAC-FA). Its as-

signed project number is 2194-D, and David Ferraiolo will be the editor; and

c. New INCITS Project Proposal -- Next Generation Access Control - Generic Operations & Abstract Data Structures (NGAC-GOADS). Its assigned project number is 2195-D, and Serban Gavrila will be the editor.

3. CS1 has an ad hoc group working on the national standards project titled *Small Organization Baseline Information Security Handbook*. The NIST Principal member of CS1 is Richard Kissel, who interacts with small business organizations on security issues. His recently released draft NISTIR 7621, *Small Business Information Security: The Fundamentals*, is the base document for this CS1 national standards project. This work will have a direct impact on NIST's outreach on security to small and medium sized businesses in future.

4. Two NIST documents recently became inputs to international projects:

   - NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, became an input to ISO/IEC 1st Working Draft 27036 -- *Information Technology -- Security techniques -- Guidelines for security of outsourcing*; and

   - NIST SP 800-27 Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Revision A, became an input to ISO/IEC TR 29193, *Secure System Design principles and techniques*

Within CS1, liaisons are maintained with nearly 20 organizations. In this reporting period, additional liaison relationships have been established with:

- Financial Services Technology Consortium (FSTC);
- American Bar Association (ABA) Science and Technology committee;
- Liberty Alliance Identity Assurance Expert Group, now known as Kantara Initiative (IAWG);
- Internet Security Alliance;
- SC 7 U.S. TAG;
- Scientific Working Group on Digital Evidence;
- Scientific Working Group on Imaging Technology;
- ITU-T Q4/17 and ITU-T Q10/17;
- Commercial Data Privacy Coordinating Committee (CDPCC);
- INCITS Technical Committee on Corporate Governance of IT; and
- Scientific Working Group on imaging Technology.

CS1 Chair Dan Benigni holds several liaison positions through CS1 and NIST:

1. He is currently a Liaison to the follow-on Phase II "Workshop of The Financial Impact of Cyber Risk- 50 Questions Every CFO Should Ask", a joint initiative to identify and respond to the current needs of the C-suite community regarding cyber risk. While Phase I focused on providing questions that organizations/CFOs should be asking and provided guidance on the identification and quantification of the financial risk associated with cyber security, Phase II focuses on the developing an implementation strategy/process for the Phase I questions. Additionally, this initiative is focusing on filling out that framework to make better informed decisions related to cyber risk from an economic standpoint. The final Workshop framework document from Phase I is available for your review at http://webstore.ansi.org/cybersecurity.

2. He is also the Liaison from CS1 to the newly formed INCITS technical committee on Corporate Governance of IT, which had its formation meeting in September 2009.

3. He represents Curt Barker, CSD Division Chief, at meetings of the Common Terrorism Information Sharing Standards (CTISS) committee. CTISS are business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the Information Sharing Environment (ISE).

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 publications during FY2009.

Security for WiMAX Technologies

NIST SP 800-127, *Guide to Security for WiMAX Technologies*, was released for public comment in September 2009. Worldwide In-

teroperability for Microwave Access (WiMAX) is a wireless metropolitan area network communications technology based on the IEEE 802.16 standard. WiMAX technologies were originally developed to provide last-mile broadband wireless access, but are now more focused on cellular-like mobile architectures. Draft SP 800-127 explains the basics of WiMAX, provides information on the security capabilities of WiMAX, and gives recommendations on securing WiMAX technologies effectively. It also explains the security differences among the major versions of the IEEE 802.16 standard.

SCAP Technical Specification

NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP)*, was released for public comment in July 2009. SCAP comprises specifications for organizing and expressing security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. SP 800-126 provides a technical overview of SCAP, focusing on how software developers can integrate SCAP technology into their product offerings and interfaces.

Securing Cell Phones and PDAs

NIST 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 and offers insights into making informed information technology security decisions on their treatment. SP 800-124 gives details about the threats and technology risks associated with the use of these devices and the available safeguards to mitigate them. Organizations can use the information presented in SP 800-124 to enhance security and reduce incidents involving cell phone and PDA devices. SP 800-124 was published as final in October 2008.

Protecting Personally Identifiable Information (PII)

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, was released for public comment in January 2009. SP 800-122 is intended to assist federal organizations in identifying PII and determining what level of protection each instance of PII requires, based on the potential impact of a breach of the PII's confidentiality. The publication also suggests safeguards that may offer appropriate protection for PII and makes recommendations regarding PII data breach handling.

Enterprise Password Management

NIST SP 800-118, *Guide to Enterprise Password Management*, is intended to help organizations understand and mitigate common threats against their character-based passwords. The guide focuses on topics such as defining password policy requirements and selecting centralized and local password management solutions. SP 800-118 was released for public comment in April 2009.

Adopting and Using SCAP

NIST SP 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, was released for public comment in May 2009. SCAP comprises specifications for organizing and expressing security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. SP 800-117 provides an overview of SCAP, focusing on how organizations can use SCAP-enabled tools to enhance their security posture. It also explains how IT product and service vendors can adopt SCAP's capabilities within their offerings.

DNS Security

NIST SP 800-81 Revision 1, *Secure Domain Name System (DNS) Deployment Guide*, assists organizations in understanding the secure deployment of Domain Name System (DNS) services in an enterprise. It provides practical guidelines on securing each facet of DNS within an organization based on an analysis of the operating environment and associated threats. SP 800-81 Revision 1 was released for public comment in February 2009, and an updated draft was released for a second public comment period in August 2009.

National Checklist Program

NIST SP 800-70 Revision 1, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, was published as final in September 2009. 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

NIST SP 800-68 Revision 1, *Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, was published as final in October 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.

Enterprise Telework and Remote Access Security

NIST SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security*, was released for public comment in February 2009 and published as final in June 2009. It is intended to help organizations understand and mitigate the risks associated with the technologies they use for telework. The guide emphasizes the importance of securing sensitive information stored on telework devices and transmitted across external networks, and it also provides recommendations for selecting, implementing, and maintaining the necessary security controls. SP 800-46 Revision 1 is a comprehensive update to the original SP 800-46, which was published in 2002.

Firewalls and Firewall Policy

NIST 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 published as final in September 2009, replaces the original version of SP 800-41, which was released in 2002.

System and Network Security Acronyms and Abbreviations

NIST Interagency Report (NISTIR) 7581, *System and Network Security Acronyms and Abbreviations*, was released for public comment in August 2009 and published as final in September 2009. The report contains a list of acronyms and abbreviations for selected system and network security terms, along with their generally accepted or preferred definitions. It is intended as a resource for federal agencies and other users of system and network security publications.

Security Metrics Research

NISTIR 7564, *Directions in Security Metrics Research*, was released for public comment in March 2009 and as final in September 2009. This report provides an overview of the security metrics area and identifies possible avenues of research that could be pursued to advance the state of the art.

Common Misuse Scoring System (CMSS)

NISTIR 7517, *The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities*, was released for public comment in February 2009. This report proposes a specification for CMSS, a set of standardized measures for the severity of software feature misuse vulnerabilities. NISTIR 7517 also provides examples of how CMSS measures and scores would be determined. Once CMSS is finalized, CMSS data can assist organizations in making security decisions based on standardized, quantitative vulnerability data.

Security Content Automation Protocol (SCAP) Test Requirements

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 originally released for public comment in August 2008 and updated in April 2009, was written primarily for accredited laboratories and for vendors interested in receiving SCAP validation for their products. A second version of this report, Revision 1, was also released for public comment in April 2009, and it defines a newer set of validation program test requirements.

Common Configuration Scoring System (CCSS)

NISTIR 7502, *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*, was released for a second public comment period in June 2009. CCSS is an open specification for measuring and communicating the characteristics and relative severity of software security configuration issues. This publication proposes a specification for CCSS, provides advice on performing scoring, and demonstrates the use of CCSS through a set of examples. Once the CCSS specification has been finalized and CCSS measures for products are available, organizations can use CCSS to help them make security decisions based on standardized, quantitative vulnerability data.

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

Honors And Awards

Department of Commerce Gold Medal Award

Stephen Quinn, Tim Grance, Peter Mell, Karen Scarfone, Christopher Johnson, Murugiah Souppaya, and Matthew Barrett

Leadership: The group is honored for pioneering a new model for computer security vulnerability identification and remediation (the Security Content Automation Protocol), including a database of security flaws (the National Vulnerability Database), a compendium of 142 security configuration guides, and metrics for scoring vulnerabilities. Their accomplishments include enabling the secure configuration of 5 million U.S. Government Windows desktop computers, increasing the security of credit card transactions worldwide, and enabling industry security tools to effectively monitor and implement secure configurations.

Pictured Left to Right: Stephen D. Quinn, Tim Grance, Peter M. Mell, Karen A. Scarfone, Christopher S. Johnson, Murugiah Souppaya, and Matthew P. Barrett

Department of Commerce Bronze Medal Award

Karen Scarfone

Ms. Scarfone is recognized for leading the development of one of the world's largest and most influential of computer security guidelines. Her authorship and leadership have taken the development of these publications to new heights in terms of volume, quality, and impact. Although prepared for use by federal agencies, these guidelines are also frequently adopted and applied by non-governmental organizations. Each Special Publication in some way directly improves the security posture of our government by providing actionable recommendations for mitigating emerging and existing threats that pertain to a specific information technology topic.

Karen Scarfone

Department of Commerce Bronze Medal Award

Athanasios T. Karygiannis and William I. MacGregor (ITL, Division 893, Computer Security Division) with Walter G. McDonough (Polymers division 854), Chad R. Snyder (854) and Michael H. Francis, Jeffrey R. Guerrieri, David R. Novotny, Perry F. Wilson (Electromagnetics, Division 818)

Pictured Left to Right: Chad R. Snyder (division 854), Walter G. McDonough (division 854), and William I. MacGregor (CSD, 893) Not Pictured in Division 893: Athanasios (Tom) Karygiannis

The Western Hemisphere Travel Initiative requires all travelers from Canada, Mexico, Central America, South America, the Caribbean and Bermuda to present acceptable documents to enter the U.S. The U.S. Passport Card (PASS Card) was a proposed alternative to the passport. Congress asked NIST to certify that the Department of Homeland Security and State selected a PASS Card architecture that met or exceeded ISO security standards and the best available practices for protection of personal identification documents. The NIST team met the Congressional mandate, improved the security, durability, and performance of the PASS Card, and enabled the State Department to issue the PASS Cards almost a full year before the planned implementation date.

Fed 100 Awards

Matthew Barrett

Matthew Barrett

Matthew Barrett, Computer Security Division, received the 2009 Federal 100 Award from *Federal Computer Week*. The Federal 100 Award recognizes individuals from government, industry, and academia who significantly influenced how the federal government buys, uses or manages information technology. Barrett was recognized for managerial and technical leadership in ensuring that the federal government and the private sector enjoy a single comprehensive solution to security automation through the Security Content Automation Protocol (SCAP). He received the award on March 25, 2009, at a gala at the Ritz-Carlton Tysons Corner.

Karen Scarfone

Karen Scarfone, Computer Security Division, received the 2009 Federal 100 Award from *Federal Computer Week*. The Federal 100 Award recognizes individuals in government and industry who made significant contributions to the federal information technology community in 2008. Scarfone was recognized for authorship and leadership in developing an unparalleled corpus of security publications on incident response, host security, and mobile device and telework security. The award was presented at a gala at the Ritz-Carlton Hotel in Tysons Corner, Virginia, on March 25, 2009.

Karen Scarfone

Information Systems Security Association (ISSA) Hall of Fame

Dr. Ronald Ross Inducted into Information Systems Security Association (ISSA) Hall of Fame

Dr. Ronald Ross

Ronald Ross, Computer Security Division, was selected for induction into the ISSA Hall of Fame for exceptional contributions to ISSA and the information security profession. Lynn McNulty, former ITL Associate Director for Computer Security, also received the award. Both were recognized at the ISSA Awards Ceremony on April 22, 2009, in San Francisco, California.

Computer Security Division Publications – FY2009

Key to Publications:
FIPS – Federal Information Processing Standards
SP – Special Publications
NISTIR – NIST Interagency Report

Draft Publications		
Type & Number	Title	Date Released
FIPS 186-3	*Digital Signature Standard*	November 2008
SP 800-16 Revision 1	*Information Security Training Requirements: A Role- and Performance Based Model*	March 2009
SP 800-38E	*Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*	August 2009
SP 800-46 Revision 1	*Guide to Enterprise Telework and Remote Access Security*	February 2009
SP 800-53 Revision 3	*Recommended Security Controls for Federal Information Systems and Organizations*	February 2009
SP 800-56B	*Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*	December 2008
SP 800-57 Part 3	*Recommendation for Key Management: Application Specific Key Management Guidance*	October 2008
SP 800-63 Revision 1	*E-Authentication Guideline*	December 2008
SP 800-65 Revision 1	*Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC)*	July 2009
SP 800-73-3	*Interfaces for Personal Identity Verification (PIV)*	August 2009
SP 800-81 Revision 1	*Secure Domain Name Systems (DNS) Deployment Guide*	February 2009
SP 800-85A-1	*PIV Card Application and Middleware Interface Test Guidelines*	February 2009
SP 800-85B-1	*PIV Data Model Conformance Test Guidelines*	September 2009
SP 800-102	*Recommendation for Digital Signature Timeliness*	November 2008
SP 800-117	*Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*	May 2009
SP 800-118	*Guide to Enterprise Password Management*	April 2009
SP 800-120	*Recommendation for EAP Methods Used in Wireless Network Access Authentication*	December 2008
SP 800-122	*Guide to Protecting the Confidentiality of Personally Identifiable*	January 2009
SP 800-126	*The Technical Specification for the Security Content Automation Protocol (SCAP)*	July 2009
SP 800-127	*Guide to Security for WiMAX Technologies. Worldwide Interoperability for Microwave Access*	September 2009
NISTIR 7497	*Security Architecture Design Process for Health Information Exchanges (HIEs)*	January 2009
NISTIR 7502	*The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*	June 2009
NISTIR 7517	*The Common Misuse Scoring System (CMSS)*	February 2009
NISTIR 7564	*Directions in Security Metrics Research*	March 2009
NISTIR 7581	*System and Network Security Acronyms and Abbreviations*	August 2009
NISTIR 7609	*Cryptographic Key Management Workshop Summary (June 8-9, 2009)*	August 2009
NISTIR 7621	*Small Business Information Security: The Fundamentals*	August 2009
NISTIR 7628	*Smart Grid Cyber Security Strategy and Requirements*	September 2009

FIPS PUBS		
Number	Title	Date Released
180-3	*Secure Hash Standard*	October 2008
186-3	*The Digital Signature Standard*	June 2009

Special Publications		
Number	Title	Date Released
800-41 Revision 1	*Guidelines on Firewalls and Firewall Policy*	September 2009
800-46 Revision 1	*Guide to Enterprise Telework and Remote Access Security*	June 2009
800-53 Revision 3	*Recommended Security Controls for Federal Information Systems and Organizations*	August 2009
800-56B	*Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*	August 2009
800-64 Revision 2	*Security Considerations in the System Development Life Cycle*	October 2008
800-66 Revision 1	*An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*	October 2008
800-68 Revision 1	*Guide to Securing Microsoft Windows XP Systems*	October 2008
800-70 Revision 1	*National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*	September 2009
800-85A-1	*PIV Card Application and Middleware Interface Test Guidelines*	March 2009
800-102	*Recommendation for Digital Signature Timeliness*	September 2009
800-106	*Randomized Hashing for Digital Signatures*	February 2009
800-107	*Recommendation for Using Approved Hash Algorithms*	February 2009
800-108	*Recommendation for Key Derivation Using Pseudorandom Functions*	November 2008
800-116	*A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*	November 2008
800-120	*Recommendation for EAP Methods Used in Wireless Network Access Authentication*	September 2009
800-124	*Guidelines on Cell Phone and PDA Security*	October 2008

NIST IRs		
Number	Title	Date Released
7536	*2008 Computer Security Division Annual Report*	March 2009
7539	*Symmetric Key Injection onto Smart Cards*	December 2008
7581	*System and Network Security Acronyms and Abbreviations*	September 2009
7611	*Use of ISO/IEC 24727 -- Service Access Layer Interface for Identity (SALII): Support for Development and use of Interoperable Identity Credentials*	August 2009

ITL / CSD Security Bulletins	
Date Released	Title
September 2009	*Updated Digital Signature Standard approved as Federal Information Processing Standard (FIPS) 186-3*
August 2009	*Revised Catalog Of Security Controls For Federal Information Systems And Organizations: For Use In Both National Security And Nonnational Security Systems*
July 2009	*Risk Management Framework: Helping Organizations Implement Effective Information Security Programs*
June 2009	*Security For Enterprise Telework And Remote Access Solutions*
April 2009	*The System Development Life Cycle (SDLC)*
March 2009	*The Cryptographic Hash Algorithm Family: Revision Of The Secure Hash Standard And Ongoing Competition For New Hash Algorithms*
February 2009	*Using Personal Identity Verification (PIV) Credentials In Physical Access Control Systems (PACS)*
January 2009	*Security Of Cell Phones And PDAs*
December 2008	*Guide To Information Security Testing And Assessment*
November 2008	*Bluetooth Security: Protecting Wireless Networks And Devices*
October 2008	*Keeping Information Technology (It) System Servers Secure: A General Guide To Good Practices*

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 2009 project highlights for this annual report. The editor would also liketo acknowledge Shirley Radack, Karen Scarfone, and Kevin Stine (NIST) for reviewing and providing feedback for this annual report.

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Director

NISTIR 7653

Computer Security Division, 2009 Annual Report
March 2010

Patrick O'Reilly, Editor

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

Visual Communications & Distribution

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.