Computer Security Division

2007 Annual Report

TABLE OF CONTENTS

Welcome

The primary goal of the Computer Security Division (CSD), a component of NIST's Information Technology Laboratory (ITL), is to provide standards and technology that protects information systems against threats to the confidentiality, integrity, and availability of information and services. During Fiscal Year 2007 (FY 2007), CSD successfully responded to numerous challenges and opportunities in fulfilling that mission. Through CSD's diverse research agenda and engagement in many national priority initiatives, high-quality, cost-effective security mechanisms were developed and applied that improved information security across the federal government and the greater information security community.
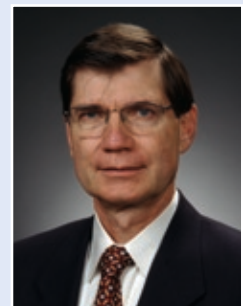
In FY 2007, CSD continued to develop standards, metrics, tests, and validation programs to promote, measure, and validate security in systems and services. Recognizing the potential benefits of more automation in technical security operations, CSD established the Information Security Automation Program (ISAP), which is intended to formalize and advance efforts to enable the automation and standardization of technical security operations, including automated vulnerability management and policy compliance evaluations. The CSD also worked closely with federal agencies to improve their understanding of the Federal Information Security Management Act (FISMA) and supported a major intelligence community initiative to build a unified framework for information security across the federal government. This initiative is expected to result in greater standardization and more consistent and cost-effective security for all federal information systems.

As technology advances and requirements evolve, it is critical to evaluate existing standards, guidelines, and technologies to ensure that they adequately reflect the current state of the art. In FY 2007, CSD released the first public draft of Federal Information Processing Standard (FIPS) 140-3 (*Security Requirements for Cryptographic Modules*) to meet new and revised requirements for federal agency use of cryptographic systems, and to address technological and economic changes that have occurred since the issuance of FIPS 140-2 in 2001.

Opportunities were presented during FY 2007 for CSD to apply its security research to national priorities and internal NIST initiatives. The CSD significantly expanded its support for two key national initiatives, electronic voting and health information technology, by researching the security requirements of those areas and applying the results of that research, along with current technologies, in furtherance of the stated goals of those initiatives. CSD also worked closely with the NIST ITL management team to integrate security projects into newly formed research programs. These programs, which include Cyber Security, Pervasive Information Technologies, Trustworthy Networking, and Trustworthy Software, are designed to organize and build ITL core competencies in the most efficient manner, and to maximize the use of ITL resources to address emerging information technology challenges.

These are just some of the highlights of the CSD program during FY 2007. 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
Division Chief

Division Organization

William Curtis Barker
Division Chief

Security Management & Assistance Group

Elizabeth Chew
Group Manager

Security Testing & Metrics Group

Ray Snouffer
Group Manager

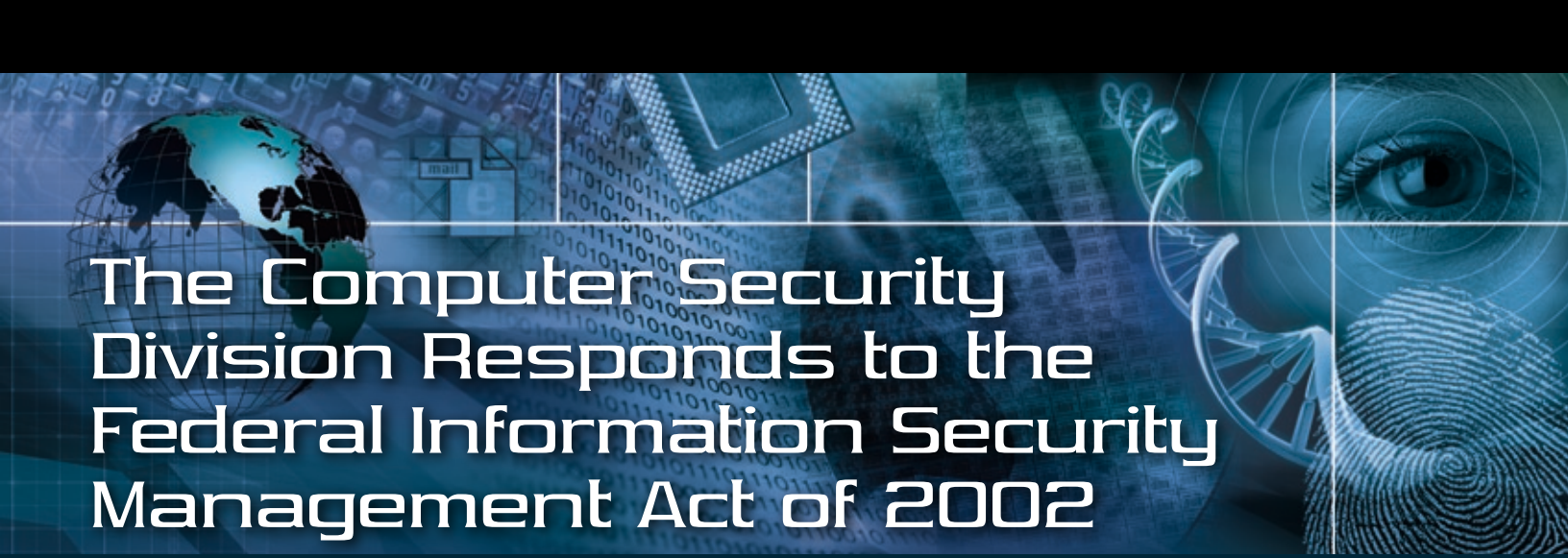**Security Technology Group**

William Burr
Group Manager

Systems and Network Security Group

Tim Grance
Group Manager

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

The E-Government Act [Public Law 107-347], passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), included duties and responsibilities for the Computer Security Division in Section 303 "National Institute of Standards and Technology." In 2007, we addressed these assignments as follows—

◆ **Provide assistance in using NIST guides to comply with FISMA –** Issued the *Guide to NIST Information Security Documents* in March 2007 to help make NIST information security documents more accessible.

◆ **Define minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category** – Issued revision 1 of SP 800-53, *Recommended Security Controls for Federal Information Systems*, in December 2006.

◆ **Identify methods for assessing effectiveness of security requirements –** Issued the third public draft of SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, in June 2007.

◆ **Bring the security planning process up to date with key standards and guidelines developed by NIST –** Initiated revisions to SP 800-16, *Information Technology Training Requirements*; SP 800-60, *Guide for Mapping Information and Information Types to Security Categories*; and SP 800-64, *Security Considerations in the System Development Life Cycle*.

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

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

◆ **Solicit recommendations of the Information Security and Privacy Advisory Board on draft standards and guidelines –** Solicited recommendations of the Board regularly at quarterly meetings on topics such as updates to special publications supporting the FISMA Implementation Project.

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

◆ **Satisfy annual NIST reporting requirement –** Produced an annual report as a NIST Interagency Report (IR). The 2003-2006 Annual Reports are available via the Web or upon request.

Security Management and Assistance

STRATEGIC GOAL ▶ *Provide federal agencies with relevant, timely and useful computer security publications and management tools, and engage in outreach activities to federal government agencies and, where appropriate, to industry, including small and medium size businesses, in order to raise awareness of the importance and need for information technology security.*

Overview

Information security is an integral element of sound management. Information and computer 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.

Major initiatives in this area include the FISMA Implementation Project; extended outreach initiatives and information security training, awareness and education; and producing and updating NIST Special Publications 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.

FISMA Implementation Project

The Computer Security Division 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—

◆ FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (Completed);

◆ FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (Completed);

◆ NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Completed);

◆ NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* (Completed);

◆ NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Target Completion February 2008);

◆ NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System* (Completed); and

◆ NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* (Completed).

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 FY 2007, the division completed a major revision of NIST SP 800-53, working with the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) to strengthen security controls in selected areas. The division also completed the third public draft of NIST SP 800-53A, which provides a new, streamlined, and flexible approach for developing security assessment plans containing assessment procedures to determine the effectiveness of security controls deployed in federal information systems. A revision of NIST SP 800-60 was also initiated to update the information types used by agencies to develop information system impact levels to help determine the criticality and sensitivity of federal information systems. On the education and training front, the division hosted two major FISMA workshops to assist federal agencies in understanding and applying the NIST security standards and guidelines.

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

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

Revision of the Risk Management Guidelines

Consistent with the security standards and guidelines being developed for the Federal Information Security Management Act of 2002, the Computer Security Division initiated revisions to its current risk management guidelines. The proposed revisions to NIST Special Publications will incorporate inputs from community-wide sources including, but not limited to: (i) the Information System Security Line of Business (ISSLOB) Certification and Accreditation (C&A) Working Group; (ii) the Department of Homeland Security (DHS) National Infrastructure Protection Plan (NIPP) and Sector Specific Plans (SSP); and (iii) the Director of National Intelligence/Department of Defense

(DNI/DOD) C&A Transformation Initiative. There are four major activities which started in FY 2007 and are expected to be completed in FY 2008:

◆ Develop NIST SP 800-39, *Managing Enterprise Risk: A Framework for Addressing Cyber Threats to Organizations, Individuals and the Nation*. This new Special Publication will formally describe the NIST Risk Management Framework and the associated components that are contained within the framework. SP 800-39 will be the flagship document for the NIST FISMA-related standards and guidelines and provide the overarching risk management strategy for federal agencies with regard to the use of information systems to support critical and sensitive enterprise missions and business functions.

◆ Revise NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002. The scope of SP 800-30 will be changed to focus specifically on the risk assessment process as a key component of managing enterprise risk resulting from the operation and use of information systems. SP 800-30, Revision 1, *Effective Use of Risk Assessments in Managing Enterprise Risk*, will describe how to apply risk assessments at various steps in the Risk Management Framework, for example, when assigning FIPS 199 security categories to information and information systems or when selecting, tailoring, supplementing, and assessing the security controls in an information system.

◆ Revise NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004. The revised SP will maintain the stability of the current four-phase security certification and accreditation (C&A) process while expanding the guidelines based on new computing paradigms, lessons learned from the first three years of implementation and use by federal agencies, and the desire for greater efficiencies in the process. The specific planned modifications to SP 800-37 include:

  ■ Redefining the C&A process as an integral part of the NIST Risk Management Framework

  ■ Tightly coupling the C&A process to the System Development Life Cycle

  ■ Placing greater emphasis on the continuous monitoring aspects of the C&A process to create a more dynamic, automated tool-driven process

  ■ Expanding the C&A process to apply to the enterprise (infrastructure) level as well as specific information systems; reinforcing the focus on enterprise missions and business functions first and foremost

  ■ Addressing the application of the C&A process to new enterprise operating paradigms (e.g., service-oriented architectures, software as a service, outsourcing).

◆ Develop *Authorizing Official's Handbook.* This new Special Publication (800-series number to be announced at a later date) will describe the authorizing official's oversight responsibilities with regard to the implementation of the NIST Risk Management Framework, culminating in the information system authorization decision. The guidelines provided in the Authorizing Official's Handbook will be tightly coupled to the NIST FISMA-related security standards and guidelines including SP 800-39 and the revisions to SPs 800-30 and 800-37.

Contact: Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Developing a Unified Framework for Information Security

The Computer Security Division provided technical support to the Chief Information Officer, Director of National Intelligence (DNI), in a major Intelligence Community initiative to transform the certification and accreditation process for information systems and to build a common framework for information security across the federal government. The division worked with the DNI to assist the Intelligence Community in reengineering the security standards and guidelines for national security systems, building on a common foundation established by NIST in its FISMA Implementation Project. The project is using as starting points the NIST Risk Management Framework, the security controls from NIST SP 800-53, and the security categorization paradigm from FIPS 199. The DNI hopes to adopt a common foundation for information security based on NIST security standards and guidelines and build unique national security system requirements on top of that foundation, when necessary. When completed, the project will result in greater standardization of information security standards and guidelines across the federal government which will lead to more cost-effective and consistent security for federal information systems, both for national security-related systems and non national security-related systems.

Contact: Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Organizational Accreditation Program

Phase II of the FISMA Implementation Project is focusing on the development of a program for credentialing public and private sector organizations to provide security assessment services for federal agencies in support of certification and accreditation of information systems. These security services involve the comprehensive assessment of the management, operational, and technical security controls in federal information systems to determine the extent to which the controls are implemented correctly, operating as

intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Agencies must rely on competent and capable security assessors to adequately assess the security controls and provide the necessary assessment results accreditation that authorities require to make critical security accreditation decisions for information systems, and for providing reliable information for reporting on compliance to FISMA. In addition, security assessments require expertise in 17 separate security areas as defined by FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and assessors must have an in-depth knowledge of the assessment procedures necessary for assessing these requirements. Agencies often do not have the required in-house resources or expertise needed to conduct the required assessments and thus are left with the uncertain task of acquiring competent and capable security assessment providers.

Organizations that successfully complete the credentialing program will be able to demonstrate competence in performing assessments of security controls implemented in an information system based on FISMA requirements and NIST standards and guidelines. Developing a network of accredited organizations that demonstrate competence in the provision of security assessment services will give federal agencies greater confidence in the acquisition and use of such services and lead to—

◆ More consistent, comparable, and repeatable security controls assessments of agencies' information security programs and systems;

◆ A better understanding of enterprise-wide mission risks resulting from the operation of information systems;

◆ More complete, reliable, and trustworthy information for authorizing officials—facilitating more informed information system security accreditation decisions; and

◆ More secure information systems within the federal government including critical infrastructures.

Development of the organizational credentialing program consists of four segments—

◆ Development and selection of an appropriate accreditation model for determining the competency of organizations desiring to provide security assessment services in accordance with NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;

◆ Development of detailed credentialing requirements for organizations seeking accreditation;

◆ Development of appropriate proficiency tests to determine the competency of prospective organizations seeking accreditation in key NIST Special Publications associated with the certification and accreditation of federal information systems; and

◆ Development of a strategy for implementing the accreditation program and selection of an appropriate accreditation body to conduct the organizational accreditations.

There will be extensive public vetting (i.e., from consumers—federal agencies, security assessment service providers, and accreditation bodies of security assessment service providers) of the credentialing program during each segment of development as described above. The vetting process will include public workshops to discuss various credentialing approaches, requirements and models, a public review of the proposed assessment methods and procedures contained in SP 800-53A, and a public review of the implementation strategy for the credentialing program.

Requirements and possible options for the credentialing of security assessment providers were presented and discussed at the first FISMA Implementation Project Phase II Workshop. The organization credentialing options were—

◆ **Option 1: Consumer-Based Credentialing** in which federal agencies draw upon credentialing requirements and guidance established from the FISMA phase II project to credential and acquire security assessment services;

◆ **Option 2: Public or Private Credentialing** in which the community develops and operates a credentialing process for security assessment providers based on service provider capability requirements, evaluation criteria, and training requirements established from the FISMA phase II project—albeit without NIST sponsorship; and

◆ **Option 3: NIST-Sponsored Credentialing** in which NIST sponsors (or partners with others) in the establishment of a credentialing process for security assessment providers based on service provider capability requirements, evaluation criteria, and training requirements established from the FISMA phase II project.

A follow-up workshop will be held in FY 2008 to further define and review the FISMA Implementation Project phase II credentialing program development.

http://csrc.nist.gov/sec-cert
Contacts: Mr. Arnold Johnson   Ms. Pat Toth
(301) 975-3247   (301) 975-5140
arnold.johnson@nist.gov   patricia.toth@nist.gov

Guide to NIST Computer Security Documents

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

For many years, CSD has made great contributions to help secure our nation's information and information systems. Our work has paralleled the evolution of IT, initially focused principally on mainframe computers, and now encompasses today's wide gamut of information technology devices.

Currently, there are over 250 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 Internal/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 with limited needs for the documents, CSD developed the *Guide to NIST Information Security Documents*. In addition to being listed by type and number, the guide presents three ways to search for documents: by topic cluster, by family, and by legal requirement. This guide is current through the end of FY 2006 and is currently undergoing updates to make access to CSD publications easier for our customers.

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

Revision of the NIST Security Managers' Handbook

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Typically, the organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying the controls' stated security requirements. The topics within this document were selected based on laws and regulations relevant to information security, including the Clinger-Cohen Act of 1996, FISMA, and the U.S. Office of Management and Budget (OMB) Circular A-130. The material in this handbook can be referenced for general information on a particular topic or can be used in the decision-making

process for developing an information security program. The purpose of this publication is to inform members of the information security management team—agency heads, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and security managers—about various aspects of information security that they will be expected to implement and oversee in their respective organizations. In addition, the handbook provides guidance for facilitating a more consistent approach to information security programs across the federal government.

http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Contacts: Ms. Pauline Bowen   Mr. Mark Wilson
(301) 975-2938   (301) 975-3870
pauline.bowen@nist.gov   mark.wilson@nist.gov

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

In FY 2007, CSD initiated an update to SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, for public review and comment. Originally published in April 1998, SP 800-16 contains a training methodology that federal departments and agencies, as well as private sector and academic institutions, can use to develop role-based information security training material.

We are updating the document to align it with information security training requirements contained in FISMA and the Office of Personnel Management (OPM) information security awareness and training requirement of June 2004.

We expect the update of SP 800-16 to be completed during early 2008.

Contacts: Mr. Mark Wilson   Ms. Pauline Bowen
(301) 975-3870   (301) 975-2938
mark.wilson@nist.gov   pauline.bowen@nist.gov

Information System Security Reference Model

Federal agencies implement information security programs to provide security for the information and systems that support there operations and assets. These programs, based on laws, regulations, standards, and guidelines, are intended to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements. A properly implemented information security program produces certain artifacts throughout its life cycle that are designed to demonstrate its maturity and the security status of its information systems.

Draft NIST SP 800-110, *Information System Security (ISS) Reference Model*, was developed on the fundamental premise that information system-specific security activities must be built on a comprehensive security program, and that many of the artifacts produced by these activities can be managed through automated tools. This publication and its associated Extensible Markup Language (XML) taxonomy and schema, is intended to:

◆ Serve as a guideline for software tool developers and federal agencies that wish to develop an automated process for managing an information security program

◆ Enable greater interoperability between information system security tools, resulting in more practical and cost-effective information security program management.

The XML taxonomy and schema, based on the security controls contained in NIST SP (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, and the NIST Risk Management Framework, provide a mechanism to denote or "tag" information security artifacts and enable FISMA related software tools to share information through a common nomenclature of data fields found in most information system security software tools. The process of documenting and confirming many of these artifacts can be automated, and this automation can be used to support legislative reporting requirements.

Draft SP 800-110 was released for public comment in September 2007.

Contacts:

Ms. Elizabeth Chew   Ms. Marianne Swanson   Mr. Kevin Stine
(301) 975-5236   (301) 975-3293   (301) 975-4483
elizabeth.chew@nist.gov   marianne.swanson@nist.gov kevin.stine@nist.gov

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, we wanted to increase consistency in definitions for key information security terms in our documents.

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

① Why do I need to invest in information security?

② Where do I need to focus my attention in accomplishing critical information security goals?

③ What are the key activities to build an effective information security program?

④ What are the information security laws, regulations, standards, and guidelines that I need to understand to build an effective security program?

⑤ Where can I learn more to assist me in evaluating the effectiveness of my information security program?

http://csrc.nist.gov/publications/nistir/#ir7359

Contacts: Ms. Pauline Bowen   Ms. Elizabeth Chew
(301) 975-2938   (301) 975-5236
pauline.bowen@nist.gov   elizabeth.chew@nist.gov

In 2007, CSD initiated an update to the Glossary to reflect new terms and any different definitions used in our publications, as well as to incorporate information security terms from the Committee on National Security Systems Instruction No 4009 (CNSSI-4009). An updated glossary is expected to be released in early 2008.

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

Information Security Guide for Government Executives

NIST Interagency Report (NISTIR) 7359, *Information Security Guide for Government Executives*, provides a broad overview of information security program concepts to assist senior leaders in understanding how to oversee and support the development and implementation of information security programs. Management is responsible for—

◆ Establishing the organization's information security program

◆ Setting program goals and priorities that support the mission of the organization

◆ Making sure resources are available to support the security program and make it successful.

Senior leadership commitment to security is more important now than ever before. Studies have shown that senior management's commitment to information security initiatives is the number one critical element that impacts an information security program's success. Meeting this need necessitates senior leadership to focus on effective information security governance and support, which requires integration of security into the strategic and daily operations of an organization. When considering this challenge, five key security questions emerge for the executive—

Program Review for Information Security Management Assistance

Several sources of guidelines, policies, standards, and legislative acts provide many requirements for federal agencies when protecting entrusted information. Various assessments, reviews, and inspections are an outcome of these information security requirements to monitor federal agency compliance. The manner in which these monitoring approaches are implemented may be very different, impacting agency resource constraints. FISMA charged NIST to provide technical assistance to federal agencies regarding compliance with the standards and guidelines developed for securing information systems, as well as information security policies, procedures, and practices. NIST Interagency Report (NISTIR) 7358, *Program Review for Information Security Management Assistance* (PRISMA), provides an overview of our program review methodology. PRISMA is a tool that we developed and implemented for reviewing the complex information security requirements and posture of a federal program or agency. This report is provided as a framework for instructional purposes as well as to assist information security personnel, internal reviewers, auditors, and agency Inspector General (IG) staff personnel.

The PRISMA database is developed in Microsoft Access 2003. The database is a companion to the NISTIR 7358 and should be used as a tool to collect the review information and generate a report in Microsoft Word format that can be edited and refined. The current data in the database is sample information to illustrate the functionality of the database. This information should be replaced, reset, or cleared before starting a review.

Agencies may download the PRISMA NISTIR 7358 and the companion database files to support their information security program review activities at *http://prisma.nist.gov*.

---

http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf
Contact: Ms. Pauline Bowen
(301) 975-2938
pauline.bowen@nist.gov

Performance Measures for Information Security

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

In September 2007, NIST released Draft SP 800-55, Revision 1, *Performance Measures for Information Security*. Draft SP 800-55, Revision 1, is a guide to assist in the development, selection, and implementation of measures to be used at the information system and program levels. This draft guideline indicates the effectiveness of security controls applied to information systems and supporting information security programs. Draft SP 800-55, Revision 1, supersedes Draft SP 800-80, *Guide for Developing Performance Metrics for Information Security*.

Contacts:

Ms. Elizabeth Chew	Ms. Marianne Swanson	Mr. Kevin Stine
(301) 975-5236	(301) 975-3293	(301) 975-4483
elizabeth.chew@nist.gov	marianne.swanson@nist.gov	kevin.stine@nist.gov

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

In FY 2007, NIST initiated an update to SP 800-60, Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*, and Volume 2, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*. SP 800-60, the companion guide to FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, was developed to assist federal agencies in categorizing information and information systems by facilitating provision of appropriate levels of information security according to a range of levels of impact or consequences that might result from the compromise of a security objective.

This revision of SP 800-60 will further clarify the system security categorization process; discuss the impact of security categorization results on other enterprise-wide activities such as capital planning, enterprise architecture, and disaster recovery planning; expand upon considerations when categorizing industrial control systems; and provide a mechanism for categorizing information types not captured in the Federal Enterprise Architecture's Consolidated Reference Model.

A public draft of SP 800-60 is expected to be released by the end of calendar year 2007, with a final publication expected early in 2008.

Contacts: Mr. Kevin Stine	Mr. Richard Kissel
(301) 975-4483	(301) 975-5017
kevin.stine@nist.gov	richard.kissel@nist.gov

Security Considerations in the Information System Development Life Cycle

Consideration of security in the System Development Life Cycle (SDLC) is essential to implementing and integrating a comprehensive risk management strategy for all information technology assets. In fiscal year 2007, NIST initiated an update to SP 800-64, *Security Considerations in the Information System Development Life Cycle*. This publication addresses the FISMA direction to develop guidelines recommending security integration into the agency's established SDLC.

This guideline is intended to help agencies understand how and to what degree security should be addressed in each phase of the SDLC and provide awareness to the types of associated outputs and control gates for effective implementation. It will show the relationship between the SDLC, the Capital Planning and Investment Control (CPIC) process, and the NIST Risk Management Framework. In addition, this revision will incorporate information from the latest FIPS and NIST Special Publications. The overall emphasis will be on making the document a useful (practical) document for use by SDLC and security practitioners.

A public draft of SP 800-64 is expected to be released by the end of calendar year 2007, with a final publication expected early in 2008.

Contacts: Mr. Richard Kissel	Mr. Kevin Stine
(301) 975-5017	(301) 975-4483
richard.kissel@nist.gov	kevin.stine@nist.gov

Outreach and Awareness

NIST Information Security Seminar Series

In 2007, NIST conducted two information-sharing seminars designed to bring together federal Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and Inspectors General (IGs) in a common setting for dialog and open discussion on FISMA standards and guidelines. More specifically, these seminars provided an in-depth look at NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, and enabled representatives from OMB, GAO, and the IG community to speak to, and answer questions from, the federal information security community about the current federal information security landscape and FISMA implementation techniques and considerations.

The initial seminar, held in January 2007, was open to federal CIOs, CISOs, and IGs. The second seminar, conducted in February 2007, was open to agency contractor support, in addition to CIOs, CISOs, and IGs.

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

Computer Security Resource Center

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

During FY 2007, CSRC had over 60.2 million requests, which included the additional traffic coming from the National Vulnerability Database (NVD) that became active late in FY 2005. Every draft document released for public comment or final document published through the Division has been posted to the CSRC.

The CSRC Web site is the primary source for gaining access to NIST computer security publications. The top five most requested CSD publications for FY 2007 were:
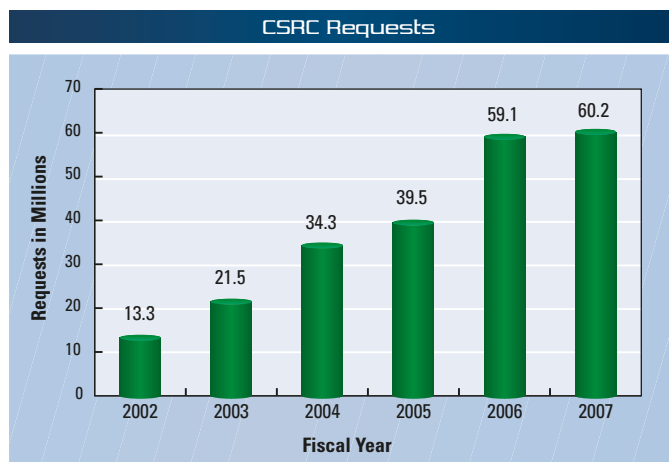
❶ Draft SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*

❷ SP 800-34, *Contingency Planning Guide for Information Technology Systems*

❸ SP 800-100, *Information Security Handbook: A Guide for Managers*

❹ SP 800-53, Revision 1 *Recommended Security Controls for Federal Information Systems*

❺ SP 800-30, *Risk Management Guide for Information Technology Systems*

During the past year, the CSRC Web site was redesigned with a new look and feel. The new and improved CSRC Web site standardizes the CSRC Web pages and menus, and is easier to navigate. The new site design features:

◆ Intuitive site navigation paths;

◆ Improved Publications section (organized by publication type, topic cluster, security control family, and legal requirements); and

◆ Improved site taxonomy/organization (highlighted by breadcrumb links on every page).

Comments on the CSRC Web site redesign can be submitted via the OMB Approved: 0693-0031 survey at: *http://csrc.nist.gov/survey.html*. Questions on the Web site should be sent to the CSRC Webmaster at: *webmaster-csrc@nist.gov*.

CSRC Requests

CSRC will continue to grow and be updated in 2008. In addition, we will be integrating CSRC into a NIST-wide implementation of a content management system.

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

Federal Information Systems Security Educators' Association

The Federal Information Systems Security Educators' Association (FISSEA) is an organization run by and for federal information systems security professionals. FISSEA assists federal agencies in meeting their computer security training 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.

Membership is open to information systems security professionals, trainers, educators, and managers who are responsible for information systems security training programs in federal agencies, as well as contractors of these agencies and faculty members of accredited educational institutions. There are no membership fees for FISSEA; all that is required is a willingness to share products, information, and experiences. Business is administered by an 11-member Executive Board that meets monthly. Board members serve two-year terms, and elections are held during the annual conference. In March 2007, NIST's Mark Wilson was elected to be the FISSEA Executive Board Chair.

Each year an award is presented to a candidate selected as Educator of the Year; this award honors distinguished accomplishments in information systems security training programs. The Educator of the Year for 2006, awarded in March 2007, was Colonel Curtis Carver, Jr, Ph.D. There is also a contest for information security posters, Web sites, and awareness tools with the winning entries listed on the FISSEA Web site. FISSEA has a semiannual newsletter, an actively maintained Web site, and a list serve as a means of communication for members. Members are encouraged to participate in the annual FISSEA Conference and to serve on the FISSEA ad hoc task groups. We assist FISSEA with its operations by providing staff support for several of its activities and by being FISSEA's host agency.

FISSEA membership in 2007 spanned federal agencies, industry, military, contractors, state governments, academia, the press, and foreign organizations to reach over 1,200 members in a total of 15 countries. The nearly 700 federal agency members represent 89 agencies from the Executive and Legislative branches of government.

FISSEA conducted three free workshops during 2007. On July 11th, board members Susan Hansche, Gretchen Morris, and Mark Wilson as well as other speakers conducted "*Reaching the Cyber Student: Distance Learning for Information Systems Security (ISS) Role-Based Training & Education*," which was held at NIST. "*Distance Learning – Making it Effective for Both Awareness and Training*" was held May 23rd and was conducted by FISSEA Board members Susan Hansche and Mary Ann Strawn. On May 10th, Board members Susan Hansche, Louis Numkin, and Jim Litchko presented "*What's New in Security Awareness*." FISSEA will continue to offer free workshops in 2008.

The 2007 Conference was held at the Bethesda North Marriott Hotel and Conference Center and 128 attended. The 2008 FISSEA Conference will be held at NIST on March 11-13. Information security awareness, resources, and FISMA will be discussed in the three-day, two-track conference. The FISSEA Conference provides a great networking opportunity for attendees. There will also be a one-day vendor exhibition. Further information regarding the conference is available on the FISSEA Web site.

http://csrc.nist.gov/fissea/
Contacts: Mr. Mark Wilson   Ms. Peggy Himes
(301) 975-3870   (301) 975-2489
mark.wilson@nist.gov   peggy.himes@nist.gov

Federal Computer Security Program Managers' Forum

The Federal Computer Security Program Managers' Forum (Forum) is an informal group of over 600 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 exchange information directly with federal agency information security program managers in fulfillment of our 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 federal agencies in establishing and maintaining a strong, proactive stance in the identification and resolution of new strategic and tactical IT security issues as they emerge.

The Forum hosts the Federal Agency Security Practices (FASP) Web site, maintains an extensive e-mail list, and holds an annual off-site workshop and bimonthly meetings to discuss current issues and developments of interest to those responsible for protecting sensitive (unclassified) federal systems [except "Warner Amendment" systems, as defined in 44 USC 3502 (2)].

The Information Security and Privacy Advisory Board Membership

Pictured above, Left to Right: **Back row** *Philip Reitinger, Howard A. Schmidt, Daniel Chenok, Fred Schneider, Brian Gouker, Joseph A. Guirreri;* **Front row** *Rebecca C. Leng, Leslie A. Reis, Susan Landau, Pauline Bowen, F. Lynn McNulty —* **Pictured right***, Left to Right: Annie Sokol and Jaren P. Doherty.* **Not pictured:** *Lisa Schossler.*

Ms. Marianne Swanson serves as the Chairperson of the Forum. We also serve 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 last year included briefings on NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, Program Review for Information Security Management Assistance (PRISMA), Draft NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, Security Content Automation Protocol (SCAP), Personal Identity Verification (PIV), NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, and NISTIR 7359, *Information Security Guide For Government Executives*. This year's 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, and the activities of the Department of Homeland Security. Briefings were also provided on electronic mail security, key management, National Archives and Records Administration guidance, wireless security, and secure configurations.

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

The Information Security and Privacy Advisory Board

The Information Security and Privacy Advisory Board (ISPAB) is a federal advisory committee that brings together senior professionals from industry, government, and academia to help advise the National Institute of Standards and Technology, 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.

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

This combination of experienced, dynamic, and knowledgeable professionals on an advisory board provides NIST and the federal government with a rich, varied pool of people conversant with an extraordinary range of topics. They bring great depth to a field that has an exceptional rate of change.

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

◆ Identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;

◆ Advise NIST, the Secretary of Commerce, and the Director of OMB on information security and privacy issues pertaining to federal government information systems, including thorough review of proposed standards and guidelines developed by NIST; and

◆ Annually report the Board's findings to the Secretary of Commerce, the Director of OMB, the Director of the National Security Agency, and the appropriate committees of the Congress.

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

Several areas of interest that the Board will be following in the coming year include privacy technology, Real ID, 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, continuity of operations, the role of chiefs (such as Chief Privacy Officer and Chief Security Officer), NIST's outreach, research, and partnering approaches, and cyber security leadership in the Executive Branch.

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

Security Practices and Policies

Today's federal networks and systems are highly interconnected and interdependent with nonfederal systems. Protection of the nation's critical infrastructures is dependent upon effective information security solutions

and practices that minimize vulnerabilities associated with a variety of threats. The broader sharing of such practices will enhance the overall security of the nation. Information security practices from the public and private sector can sometimes be applied to enhance the overall performance of federal information security programs. We are helping to facilitate a sharing of these practices and implementation guidelines in multiple ways.

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

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

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

The coming year will see an effort to 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.

http://fasp.nist.gov/
Contacts: Ms. Pauline Bowen   Mr. Mark Wilson
(301) 975-2938   (301) 975-3870
pauline.bowen@nist.gov   mark.wilson@nist.gov

Small and Medium-Size Business Outreach

What do a business' 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' 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, a figure which represents over 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. In the special arena of information security, vulnerable SMBs also run the risk of being compromised for use in crimes against governmental or large industrial systems upon which everyone relies. SMBs frequently cannot justify an extensive security program or a full-time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs.

The difficulty for these businesses is to identify needed security mechanisms and training that are practical and cost-effective. Such businesses also need to become more educated in terms of security so that limited resources are well applied to meet the most obvious and serious threats. To address this need, NIST, the Small Business Administration (SBA), and the Federal Bureau of Investigation (FBI) entered into a cosponsorship agreement for the purpose of conducting 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 2007, the SMB outreach effort focused on expanding opportunities to reach more small businesses. Discussions are under way with SBA and the FBI to expand the original partnership and to determine new avenues for this outreach project. In January 2007, two half-day workshops were held in San Jose and San Francisco, California. Similar workshops were held in March 2007 in Sacramento and Silicon Valley, California. Additional workshops were held in Massachusetts, Rhode Island, Connecticut, Pennsylvania, Alabama, Tennessee, Georgia and Florida. In 2007, a total of twenty-one SMB workshops were held across the country.

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

Health Information Technology

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

◆ Medical information will follow consumers so that they are at the center of their own care.

◆ Consumers will be able to choose physicians and hospitals based on clinical performance results made available to them.

◆ Clinicians will have a patient's complete medical history, computerized ordering systems, and electronic reminders.

◆ Quality initiatives will measure performance and drive quality-based competition in the industry.

◆ Public health and bioterrorism surveillance will be seamlessly integrated into care.

◆ Clinical research will be accelerated and post-marketing surveillance will be expanded.

Together, these tenets will revolutionize healthcare, making it more consumer-centric, and will improve both the quality and the efficiency of healthcare in the United States. One of the critical components of these tenets is the assurance of privacy of health-related information as well as assuring the confidentiality and integrity of all health information technology (HealthIT) data and maintaining the availability to HealthIT whenever it is needed. CSD is intricately involved in assisting healthcare providers in this effort.

At the federal level, CSD is involved with many of the agencies and organizations that are shaping the HealthIT space in order to meet the President's goals. CSD actively participates with:

◆ **American Health Information Community's (AHIC) Confidentiality, Privacy, and Security Workgroup** In the summer of 2006, the AHIC created a Workgroup - Confidentiality, Privacy, & Security (CPS) - specifically focused on nationwide privacy and security issues raised by health IT activities and the findings of the other AHIC workgroups. *http://www.hhs.gov/healthit/ahic/confidentiality/*

◆ **Nationwide Health Information Network (NHIN)** A critical portion of the required NHIN prototype deliverables is the development of security models that directly address systems' architecture needs for securing and

maintaining the confidentiality of health data. Participants are required to comply with security requirements established by the Department of Health and Human Services to ensure proper and confidential handling of data and information. Each architecture capability will be used in the next steps of the NHIN to address the complex issues of authentication, authorization, data access restrictions, auditing and logging, consumer controls of information access, and other critical contributions. *http://www.hhs.gov/healthit/healthnetwork/background/*

CSD also actively participates with several Standards Development Organizations that review existing standards for applicability, develop new standards where gaps are identified, and test HealthIT products that are built to these standards. These groups include:

◆ **Healthcare Information Technology Standards Panel (HITSP)** HITSP brings together the intellectual assets of over 260 organizations with a stake in health data standards to increase the interoperability of healthcare systems and information. It seeks to harmonize the critical standards needed to protect the privacy and security of health data. Once these standards have been identified to support specific clinical use-cases, the HITSP will develop implementation guides to support the activities of system developers in pursuing interoperable electronic health records. *http://www.ansi.org/standards_activities/ standards_boards_panels/hisb/hitsp.aspx?menuid=3*

◆ **The Certification Commission for Healthcare Information Technology (CCHIT)** An important part of CCHIT's work is to certify the security of health information systems. CCHIT's certification process promotes well-established, tested security capabilities in health IT systems. *http://www.cchit.org/*

CSD is also working to assist those covered entities described in the Health Insurance Portability and Accountability Act (HIPAA) in the implementation of security programs which will improve the privacy and security of HealthIT data and assist covered entities in HIPAA compliance. In FY 2007, CSD started a comprehensive update of NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.* This update is being led by CSD and involves multiple stakeholders from federal, commercial, and nonprofit organizations as we all seek to fully understand and improve the privacy and security of HealthIT related information.

Contacts: Mr. Matthew Scholl   Mr. Kevin Stine
(301) 975-2941   (301) 975-4483
mscholl@nist.gov   kevin.stine@nist.gov

Security Testing and Metrics

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

Overview

IT products make claims as to their functional and/or security capabilities. When protecting sensitive data, government agencies need to have a minimum level of assurance that a product's stated security claim is valid. There are also legislative restrictions regarding certain types of technology, such as cryptography, that require federal agencies to use only tested and validated cryptographic modules.

Federal agencies, industry, and the public rely on cryptography for the protection of information and communications used in electronic commerce, critical infrastructure, and other application areas. At the core of all products offering cryptographic services is the cryptographic module. Cryptographic modules, which contain cryptographic algorithms, are used in products and systems to provide security services such as confidentiality, integrity, and authentication. Although cryptography is used to provide security, weaknesses such as poor design or weak algorithms can render the product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.
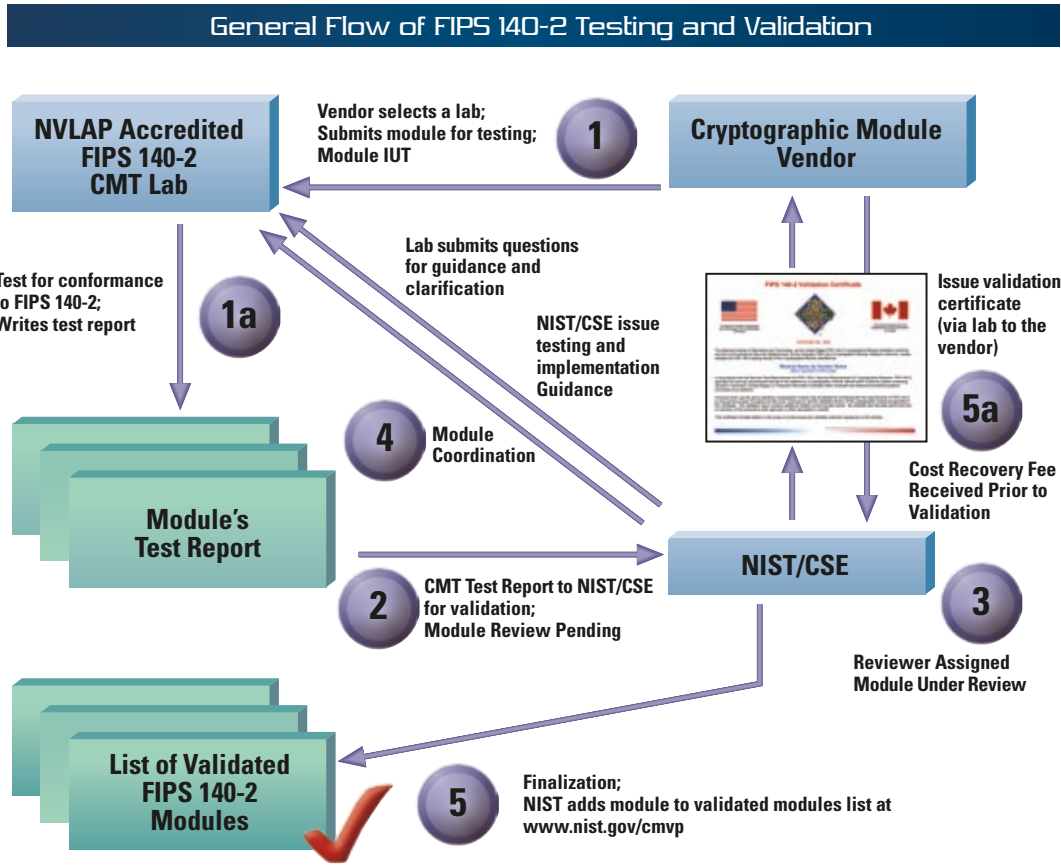
Our testing-focused activities include the validation of cryptographic modules and cryptographic algorithm implementations, development of test suites, providing technical support to industry forums, and conducting education, training, and outreach programs.

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

Validation Programs and Laboratory Accreditation

The underlying philosophy of the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) is that the user community needs strong independently tested and commercially available cryptographic products. The programs work with the commercial sector and the cryptographic community to achieve security, interoperability, and assurance. Directly associated with this philosophy is the goal 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

NVLAP Accredited FIPS 140-2 CMT Lab

Vendor selects a lab; Submits module for testing; Module IUT — **1**

Cryptographic Module Vendor

Test for conformance to FIPS 140-2; Writes test report — **1a**

Lab submits questions for guidance and clarification

NIST/CSE issue testing and implementation Guidance

Issue validation certificate (via lab to the vendor)

5a

4 Module Coordination

Module's Test Report

Cost Recovery Fee Received Prior to Validation

NIST/CSE

2 CMT Test Report to NIST/CSE for validation; Module Review Pending

3

Reviewer Assigned Module Under Review

List of Validated FIPS 140-2 Modules

5 Finalization; NIST adds module to validated modules list at www.nist.gov/cmvp

---

The CMVP offers 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. 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 Module Testing (CMT) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) provide vendors of cryptographic modules a choice of testing facilities and promote healthy competition.

Laboratory Accreditation

Vendors of cryptographic modules and algorithms use independent, private sector testing laboratories accredited as CMT 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. NVLAP has received several applications for the accreditation of CMT Laboratories, which has resulted in the accreditation of one new U.S.-based CMT Laboratory in 2007 and one other laboratory in the accreditation process. This brings the current total number of accredited CMT Laboratories to 14, spanning locations in the United States, Canada, the United Kingdom, and Germany.
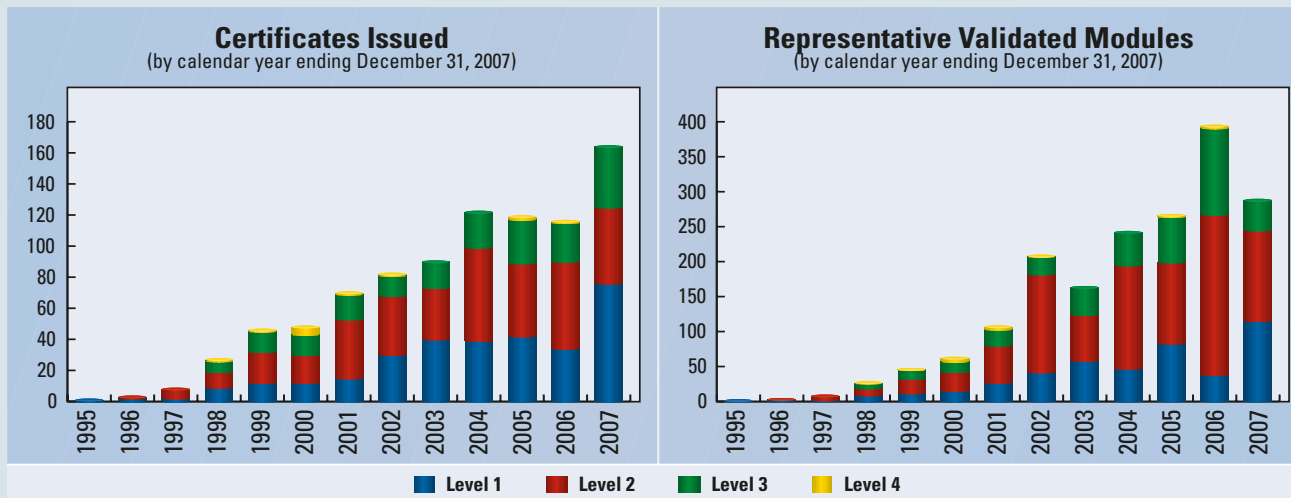
A complete list may be found at *http://csrc.nist.gov/cryptval/1401labs.htm*.

---

http://ts.nist.gov/Standards/214.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 Computer Security Division (CSD) and the Communication Security Establishment (CSE) of the Government of Canada. The programs provide federal agencies—in the United States, Canada, and the United Kingdom—with confidence that a validated cryptographic module meets a claimed level of security and that a validated cryptographic algorithm has been implemented correctly. The CMVP/CAVP validate modules and algorithms used in a wide variety of products including secure Internet browsers, secure radios, smart cards, space-based communications, munitions, security tokens, storage devices, and products supporting Public Key Infrastructure and electronic commerce. One module may be used in several products so that a small number of modules may account for

The Progress of the CMVP

Certificates Issued
(by calendar year ending December 31, 2007)

Representative Validated Modules
(by calendar year ending December 31, 2007)

■ Level 1   ■ Level 2   ■ Level 3   ■ Level 4

hundreds of products. Likewise, the CAVP validates cryptographic algorithms that may be housed in one or more cryptographic modules.

To give a sense of the quality improvement that both the CMVP and the CAVP achieve, consider that our statistics from the testing laboratories show that 48 percent of the cryptographic modules and 27 percent of the cryptographic algorithms brought in for voluntary testing had security flaws that were corrected during testing. In other words, without this program, the federal government would have had only a 50-50 chance of buying correctly implemented cryptography. To date, over 885 certificates have been issued, which represents over 1,800 validated modules by the CMVP. These modules have been developed by over 200 domestic and international vendors.

This fiscal year, the CMVP issued 135 module validation certificates. The number of modules in the CMVP pre-validation queue continues to grow, representing significant growth in future validation efforts.

The CAVP issued 1034 algorithm validation certificates in FY 2007, a substantial increase in validation certificates from last fiscal year where 635 algorithm validation certificates were issued.
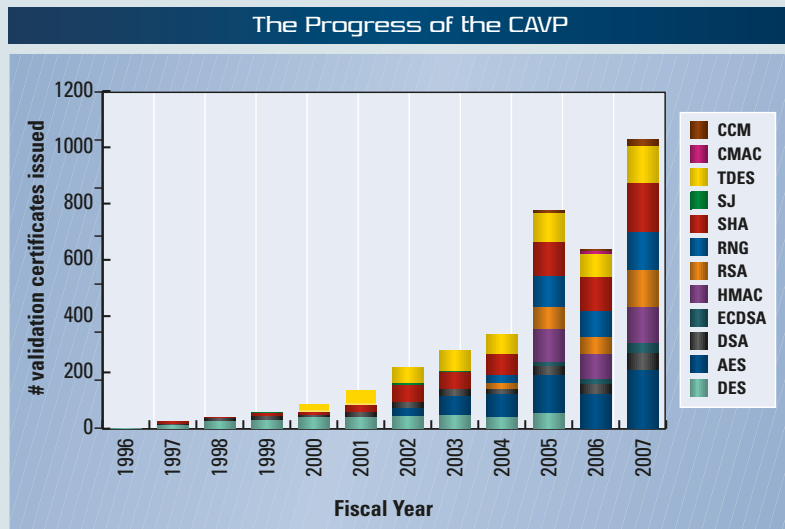
http://csrc.nist.gov/cryptval/
CMVP Contact: Mr. Randall J. Easter
(301) 975-4641
randall.easter@nist.gov

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

Automated Security Testing and Test Suite Development

Each approved and recommended cryptographic algorithm has an associated reference called a FIPS publication or a NIST 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 involved 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 Progress of the CAVP

validation certificates issued

Fiscal Year

CCM
CMAC
TDES
SJ
SHA
RNG
RSA
HMAC
ECDSA
DSA
AES
DES

There are several types of validation testing for each approved cryptographic algorithm. These 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 14 third-party laboratories that are accredited as CMT laboratories by NVLAP. We develop and maintain a Cryptographic Algorithm Validation System (CAVS) tool which automates the validation testing. The CAVS currently has algorithm validation testing for the following cryptographic algorithms:

◆ The Triple Data Encryption Standard (TDES) algorithm,

◆ The Advanced Encryption Standard (AES) algorithm,

◆ The Digital Signature Standard (DSS),

◆ Hashing algorithms SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512,

◆ Three random number generator (RNG) algorithms,

◆ The RSA algorithm,

◆ The Keyed-Hash Message Authentication Code (HMAC),

◆ The Counter with Cipher Block Chaining-Message Authentication Code (CCM) mode,

◆ The Cipher-based Message Authentication Code (CMAC) Mode for Authentication, and

◆ The Elliptic Curve Digital Signature Algorithm (ECDSA).

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

Cryptographic Validation Standards

With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. Therefore, except when using National Security Agency-approved cryptography, all Agencies must use cryptography validated under FIPS 140-2, *Security Requirements for Cryptographic Modules*. This standard specifically requires all hardware, software, and firmware employing cryptography—whether commercial-off-the-shelf or government-produced—to be validated through the Cryptographic Module Validation Program (CMVP) when used for the protection of sensitive unclassified information. Agency acquisition, development, and use of any hardware, software, or firmware using invalidated cryptography for the protection of sensitive unclassified information are not permitted, and no other validation process can substitute for FIPS validation.

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

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

In addition to constant analysis for new technologies, the standard is officially reexamined and reaffirmed every five years. In the fall of 2004, FIPS 140-2 entered the regularly scheduled five-year review for revision to FIPS 140-3. We are developing FIPS 140-3 to meet the new and revised requirements of federal agencies for cryptographic systems, and to address technological and economic changes that have occurred since the issuance of FIPS 140-2 in 2001. As the first step in the development of FIPS 140-3, we invited comments from the public, users, the information technology industry, and federal, state, and local government organizations concerning the need for and recommendations for a new standard. We were specifically interested in comments in the areas of compatibility with industry standards, new technology areas, introduction of additional levels of security, additional requirements specific to physical security, and portability of applications (including operating systems) based on platform and/or environment.

In September 2005, a workshop was conducted to address the areas of physical security protection methods and current state of the art in methods of attacks and compromise of cryptographic modules. The first draft of FIPS 140-3 underwent further development and research in FY 2006 as we reviewed the comments received and addressed the areas of the standard identified for improvement. Among the recommended changes were the stronger requirements on user authentication and data integrity verification, a new section focused on software modules, and the requirements to mitigate against noninvasive attacks that were not even feasible several years ago.

In July 2007, the first draft of the new FIPS 140-3 standard was released for public comment. This draft standard proposes increasing the number of security levels from four to five. Many other improvements have been introduced, reflecting the developing industry trends and our analysis of public's comments. The comment period ended on October 11, 2007. This was followed by a thorough review and analysis of all comments. Depending on the nature of the received comments and suggestions, FIPS 140-3 may either be finalized or, more likely, a second draft of the standard will be developed. The second draft would then be made available to the public for comments, with the final version of the standard expected in early FY 2009.

The FIPS 140-3 standard will take effect six months after the final version is signed by the Secretary of Commerce.

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

ISO Standardization of Cryptographic Module Testing

With the publishing of ISO/IEC 19790, Subcommittee 27 (SC27) approved and began work on ISO/IEC 24759, *Test requirements for cryptographic modules*. This project is registered in the work program of the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 Subcommittee 27 on IT Security Techniques (ISO/IEC JTC 1/SC 27-IT Security Techniques). At the spring 2007 ISO/IEC meeting, ISO/IEC JTC 1/SC 27 requested its Secretariat to register ISO/IEC 24759 *Test Requirements for Cryptographic Modules* CD/FCD/PDAM/ PDTR and to circulate the documents for balloting. When completed, this effort will bring consistent testing of cryptographic modules in the global community.

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

SECURITY TECHNOLOGY

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

Overview

Our work in cryptography is making an impact within and outside the federal government. Strong cryptography improves the security of systems and the information they process. IT users also enjoy the enhanced availability in the marketplace of secure applications through cryptography, Public Key Infrastructure (PKI), and e-authentication. Work in this area addresses such topics as secret and public key cryptographic techniques, advanced authentication systems, cryptographic protocols and interfaces, public key certificate management, biometrics, smart tokens, cryptographic key escrowing, and security architectures. This year, the work called for in Homeland Security Presidential Directive 12 (HSPD-12) has continued. A few examples of the impact this work has had include changes to federal employee identification methods, how users authenticate their identity when needing government services online, and the technical aspects of passports issued to U.S. citizens.

CSD collaborates with a number of national and international agencies and standards bodies to develop secure, interoperable security standards. Federal agency collaborators include the Department of Energy, the Department of State, the National Security Agency (NSA), 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) and the Internet Engineering Task Force (IETF). Industry collaborators include BC5 Technologies, Certicom, Entrust Technologies, Hewlett Packard, InfoGard, Microsoft, NTRU, Pitney Bowes, RSA Security, Spyrus, and Wells Fargo.

Cryptographic Standards Toolkit

Cryptographic Algorithm Development and Maintenance

A hash function takes binary data, called the message, and produces a condensed representation, called the message digest. A cryptographic hash function is a hash function that is designed to achieve certain security properties and is typically used with other cryptographic algorithms, such as digital signature algorithms, key derivation algorithms, keyed-hash message authentication codes, or in the generation of random numbers (bits). As a security primitive, cryptographic hash functions are frequently embedded in Internet protocols or in other applications; the two most commonly used cryptographic hash functions are MD5, which has been broken and is no longer approved for federal agency use, and the NIST-approved SHA-1.

In June 2007, NIST issued for public review and comment two draft FIPS publications, FIPS 180-2 and FIPS 198-1. FIPS 180-2, *Secure Hash Standard*, specifies five algorithms for computing cryptographic hash functions—SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. These five algorithms are called secure because, for a given algorithm, it is computationally infeasible (1) to find a message that corresponds to a given message digest, and (2) to find two different messages that produce the same message digest. FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, is the proposed revision of FIPS 198. This draft revision specifies a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions and shared secret keys. Comments on both draft standards were collected and addressed. The proposed standards have been submitted for review and approval by the Secretary of Commerce.

In 2005, a vulnerability was identified in the SHA-1 hash algorithm. In response, NIST held two cryptographic hash function workshops to assess the status of NIST's approved hash functions and to discuss the latest hash function research. NIST decided that it would be prudent to develop one or more additional hash functions through a public competition similar to the development process for the Advanced Encryption Standard (AES). Based on feedback from the workshops, draft minimum acceptability requirements, submission requirements, and evaluation criteria have been provided for public comment, with the expectation that the competition would be launched in late 2007.

In the past year, a revised version of the Digital Signature Standard (DSS), to be known as FIPS 186-3, was provided for public review and comment, as well as a related document, NIST SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*. The DSS revision included additional key sizes for the Digital Signature Algorithm (DSA) to provide higher security strengths and guidance on the use of RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA) to promote interoperability. SP 800-89 specifies methods for obtaining the assurances necessary to determine that digital signatures are valid. SP 800-89 has been completed, and the comments received on the draft of FIPS 186-3 are being addressed.

Random numbers are needed to provide the required security for most cryptographic algorithms. For example, random numbers are used to generate the keys needed for encryption and digital signature applications. In March 2007, a revision to NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs)*, was completed and is available on our Web site. Additional work is being conducted with Accredited Standards Committee X9 (ASC X9) to provide guidance for the development of entropy sources and the construction of Random Bit Generators from entropy sources and DRBGs.

An authenticated encryption algorithm called the Galois/Counter Mode (GCM) was submitted to NIST as part of the ongoing development of modes of operation of the Advanced Encryption Standard (AES) algorithm. GCM provides assurance of the authenticity of data as well as its confidentiality. GCM is designed to facilitate high throughput in hardware applications, such as high-speed Internet routers. The algorithm is recommended in SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*. An updated draft of this document was provided for a period of public review in the last year and was recently published in November 2007.

Another mode of operation of the AES algorithm is slated for recommendation soon—the AES Key Wrap (AESKW). Like GCM, AESKW uses the AES algorithm in a manner that combines assurance of confidentiality with authenticity. AESKW is intended for the protection of cryptographic keys and other specialized data without requiring a nonce, i.e., a unique per-message value. Although AESKW is not efficient, its security is believed to be particularly robust. In FY 2007, NIST served as the editor of the ASC X "key wrapping" standard that includes versions of the AESKW algorithm for use with AES and Triple DES.

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

Dr. Morris Dworkin
(301) 975-2354
morris.dworkin@nist.gov

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

Key Management

Recommendation for Key Management

The requirements for key management continue to expand as new types of devices and connectivity mechanisms become available (e.g., laptops, broadband access, Blackberries). 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).

Modifications were made to SP 800-57, *Recommendation for Key Management—Part 1: General*, which included an indication of the appropriate hash functions to be used for additional applications, depending on the security strength. Parts 1 and 2 provide general guidance and best practices for the management of cryptographic keying material. Part 3 of SP 800-57 on application-specific guidance is under development and is expected to be available for initial public comment in 2008. Part 3 is intended to address the key management issues associated with currently available cryptographic mechanisms.

Key Establishment using Public Key Cryptography

Key management efforts have included the completion of SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, and the commencement of a related document, SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography* (e.g., RSA).

Key Management for Wireless Applications

As they become a more convenient way to access the Internet, wireless technologies are being more widely adopted by government agencies. However, while wireless technologies can provide connections for mobile users, they are also vulnerable to various attacks. Security protocols have been developed by the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and other industry standards bodies in order to protect wireless networks and communications.

A new feature for wireless service is to allow a fast transition between different access points, called a handoff. This fast handoff proposes a new challenge to cryptographic key management. To make the handoff truly fast, cryptographic keys are derived and distributed among different access points so that whenever a mobile station is roaming to a different access point, the keys are ready for a secure connection. A key hierarchy is derived from a master key for the fast handoff purpose.

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

In order to make proper recommendations on key management in a timely manner for government agencies, we worked with IEEE 802.11 Task Group R to develop key management protocols and key derivation functions. The early involvement has made it possible to influence the industry standards in a more efficient and direct way to comply with government requirements. We are also simultaneously developing recommendations on key management for wireless and mobility, which will be included as one of the SP 800 series of documents.

Public Key Infrastructure

We continue to support the development and enhancement of key management standards related to Public Key Infrastructure (PKI). This standards work is primarily performed in the Internet Engineering Task Force (IETF), where NIST contributes coeditors for three documents under development within the Public Key Infrastructure X.509 (PKIX) working group. In 2007, work continued on a revised version of the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. This document, which profiles the X.509 standard for public key certificates and CRLs, is used as the basis for the development of most PKI products and the deployment of PKIs in both the public and private sector. NIST is also editing a companion document that specifies the encoding of certificates and CRLs that include public keys and digital signatures that are based on elliptic curves and the NIST-approved hash functions. Work on a third document, the *Server-based Certificate Validation Protocol (SCVP)*, neared completion in FY 2007. SCVP specifies a protocol that allows the work of validating certificates to be off-loaded to a delegated validation server.

In addition to PKI standards, we are focused on deploying a robust and comprehensive Federal PKI (FPKI) to support the deployment and management of Personal Identity Verification Cards (i.e., FIPS 201). NIST is a member of the FPKI Policy Authority, which manages the Federal Bridge Certification Authority (FBCA) and the Common Policy Root Certification Authority, and maintains the FPKI policies. During 2007, the Policy Authority's Certificate

Policy Working Group, which is chaired by NIST, continued to refine the FPKI policies to streamline deployment, enhance interoperability, and improve operational efficiency.

While agency PKIs for the early adopters are cross-certified with the FBCA, agencies currently deploying PKI are procuring the services of approved PKI service providers operating under a common certificate policy. NIST is a key participant in the Shared Service Provider Working Group that evaluates and approves the operations of these service providers. During 2007, three additional shared service providers were approved and were issued the requisite CA certificate by the Common Policy Root CA. At the end of 2007, an eighth service provider was in the review process.

Contacts:

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

Ms. Elaine Barker
(Digital signatures, RNG, SP 800-56B, SP 800-57)
(301) 975-2911
ebarker@nist.gov

Dr. Morris Dworkin (Modes)
(301) 975-2354
morris.dworkin@nist.gov

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

Mr. Tim Polk (PKI)
(301) 975-3348
william.polk@nist.gov

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

Response to Quantum Computing

Quantum computing has the potential to become a major disruptive technology in the areas of 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, published in May 1996, has the potential to provide 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 hopes to plan for this eventuality by adding primitives to the cryptographic toolkit for public key-based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. In the event that such algorithms cannot be found, 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 August 2007 the Computer Security Division sent Ray Perlner as a representative to the ARO/NSA/DTO Quantum Computing/Quantum Algorithms program review, and organized a "Birds of a Feather" session at the Crypto Conference in Santa Barbara to discuss procedures for standardizing new public key cryptographic primitives. The Computer Security Division has also begun a series of meetings with members of the Advanced Network Technology Division to discuss network layer implications of quantum key distribution.

During 2008, we will continue to study security technologies that may be resistant to attack by quantum computers, especially those which 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

CSD is completing its technical guidance for electronic authentication with an update to SP 800-63, *Electronic Authentication Guideline*, which supports the Office of Management and Budget (OMB) memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*. The OMB policy memorandum defined four levels of authentication in terms of the assurance that an asserted identity is valid. Our guidance provides technical requirements and example authentication technologies that work by making individuals demonstrate possession and control of a secret for each of the four levels. This year, we completed a draft update to SP 800-63 to address additional authentication mechanisms that are now available in the marketplace.

We also completed a project to support the development of an authentication effectiveness schema sponsored by the Department of Homeland Security. This project included a survey of known and emerging methods of establishing, authenticating, and securely communicating user and device identification information to a service, device, or system. From this effort,

we proposed a model for authentication that could be used for determining the effectiveness of different technologies.

Contacts: Mr. William Burr   Ms. Donna Dodson
(301) 975-2934   (301) 975-3669
william.burr@nist.gov   donna.dodson@nist.gov

Security Aspects of Electronic Voting

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

In the past year, we supported the TGDC in the final development of the next generation of the Voluntary Voting System Guidelines (VVSG) and delivery of the VVSG to the EAC. The next-generation VVSG addresses significant threats to voting systems and enhances the auditability of voting systems by containing new and updated requirements covering software independence (SI), independent voter verifiable records (IVVR), cryptography, system integrity management, access control, secure software installation and distribution, setup inspection, system event logging, secure communications, and physical security. In addition, we began developing tests for security requirements found in the next generation of the VVSG and supported the National Voluntary Laboratory Accreditation Program (NVLAP) accreditation efforts of voting system testing laboratories.

Plans for 2008 include continued development of tests for security requirements in the next generation of the VVSG, supporting the EAC and TGDC with resolution of public comments on the next-generation VVSG, supporting NVLAP accreditation efforts of voting system test laboratories, hosting the TGDC plenary meetings, supporting STS activities, and engaging the voting system vendor, voting system test laboratory, state election official, and academic communities to explore ways to increase voting system security and transparency.

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

SYSTEMS AND NETWORK SECURITY

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

Overview

O ur security research focus is to identify emerging technologies and conceive of 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 IP security issues, digital forensics tools and methods, access control and authorization management, Internet Protocol 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

Personal Identity Verification

Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When individuals attempt to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of identity is an important step in making sound access control decisions. A wide range of mechanisms is employed to accurately determine identity; as a result, the strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential.

On August 27, 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12), entitled "Policy for a Common Identification Standard for Federal Employees and Contractors." HSPD-12 requires the development and implementation of a governmentwide standard for secure and reliable

forms of identification for federal employees and contractors. As required by HSPD-12, NIST issued FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. Subsequently, NIST issued several Special Publications in support of FIPS 201.

To ensure interoperability and to enable agencies to meet the tight deadlines of HSPD-12, we provided substantial contributions towards implementing PIV this year. We continued to refine FIPS 201 and associated Special Publications based on the inputs received from actual implementations and lessons learned from the NIST reference implementation. According to vendors and government agencies, FIPS 201 and its associated Special Publications are the most thoroughly tested and widely implemented standards in the history of smart card implementations. The success of the PIV program gained from several contributions by NIST during the year:

◆ **Feasibility Study of Secure Biometric Match-On-Card –** The feasibility study enabled us to determine the state of the practice in smart card production and biometrics technology. We gained valuable input from vendor products on the effects of security on performance of secure data transfer over the contactless interface to perform Secure Biometric Match-On-Card (SBMOC) operations. The lessons learned from the study may drive an extension to the FIPS 201 standard that achieves secure biometric authentication in the contactless mode of operation, and will be valuable to other government and commercial identity credential programs.

◆ **Continued Evaluation of PIV Products –** In 2006, NIST established the NIST Personal Identity Verification Program (NPIVP) to validate PIV system components required by FIPS 201. The program facilitates rigorous testing of PIV products through National Voluntary Laboratory Accreditation Program (NVLAP)-approved test laboratories. During 2007, NIST validated seven PIV Card application and PIV middleware products. Additionally, the conformance test suite (SP 800-85-A) was enhanced and NPIVP has continued to aid in the iterative test and validation process with the laboratories, to provide additional clarifications and details on the implementation of the PIV standard.

◆ **Refinement of Standards —** During the last year, we enhanced and refined existing standards and guidelines so that the implementing agencies were able to interoperate and benefit from lessons learned. We revised SP 800-73, SP 800-76, and SP 800-78 to enhance interoperability and reduce the possibility of different interpretations. The PIV issuer Certification and Accreditation guideline, SP 800-79, is in the revision process. It will incorporate lessons learned in PIV-I implementation, development of HSPD-12 Shared Component Architecture and establishment of shared services organizations

such as the GSA Managed Service Office (MSO). We identified gaps in PIV standards and immediately moved to develop missing specifications. Specifically, we 1) developed standards for PIV Card Reader interoperability (SP 800-96) to foster interoperability between any card and any reader, 2) developed and published SP 800-104, *A Scheme for PIV Visual Card Topography*, to increase the reliability of PIV Card visual verification, 3) developed SP 800-116 to clarify PIV Card use cases for physical access control systems (PACS) and 4) updated unique agency code (SP 800-87) assignments. In response to critical agency requests, NIST initiated a revision of FIPS 201-1.

◆ **PIV Upgraded Reference Implementation —** To aid and guide proper PIV implementation, the PIV team also provided an upgraded reference implementation in response to updates to the PIV standards. Specifically, NIST updated and improved the PIV Card Simulator that behaves and responds exactly like a PIV Card. We also enhanced the PIV Middleware that implements the Application Programming Interface (API) as specified in SP 800-73-1. Both the source code and executables are available on the PIV Web site as a reference. Moreover, NIST enhanced the PIV data generator software tool to allow dynamic data production consistent with FIPS 201. The data generator and sample data are available on the PIV Web site. Finally, the PIV team developed a data loader utility that can be used to load the test data onto PIV-conformant cards.

◆ **PIV Card-Enabled Application Demonstrations –** In the last few months, the PIV team focused on demonstrating the FIPS-201-specified use cases for the PIV Card holder. Specifically, we developed PIV-enabling application examples for logical access applications that use the PIV Card to authenticate the claimed identities on the card. We have built the necessary software components that demonstrate PIV Card-enabled e-mail signing, e-mail encryption, Web authentication, and smart card OS logon. NIST also participated in the production of a technical report describing the application of the draft ISO/IEC 24727 middleware standard to PIV Card middleware.

Future plans include maintenance support activities such as developing implementation guidelines and refining standards. We plan to publish our findings on PIV Card-enabled applications and the SBMOC feasibility study as NIST reports and guidelines. We also plan to provide recommendations to federal agencies on adding other applications on a PIV Card or adding a PIV application to their existing smart cards.

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

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

According to recent reports, identity theft continues to be a growing problem. 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 provide the necessary elements of such a solution. They provide cryptographic mechanisms, store biometrics and keys, and, using certain techniques, address privacy considerations. Technological solutions for increased security of identity credentials improve the ability of the consumer to protect assets and informatics privacy.

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

During 2007, we continued the development of ISO/IEC 24727 *Identification Cards – Integrated Circuit Cards Programming Interfaces*, the multipart standard resolving current voids and interoperability challenges found in existing standards.

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

ISO/IEC 24727 provides a set of programming interfaces for interactions between integrated circuit cards (ICCs) and applications to include multi-sector use of generic services for identification, authentication, and signature. ISO/IEC 24727 is specifically relevant to identity management applications desiring 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.

The parts of ISO/IEC 24727 are—

◆ 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 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 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. This is the first time authentication protocols have been standardized in a formal standards-setting group.

◆ 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. It also provides a standard API for interface devices (card readers).

◆ ISO/IEC 24727-5 contains conformance testing requirements.

◆ ISO/IEC 24727-6 is a new development for 2007. This part is a registration authority that will contain the normative ISO/IEC 24727 authentication protocols. Using a registration authority prevents the need to amend the standard when new authentication protocols are introduced for ISO/IEC 24727-3.

At the time of this annual report, ISO/IEC 24727-1 was finalized and available for purchase. ISO/IEC 24727-2, -3, and -4 are at final committee draft and are anticipated to be finalized in 2008. ISO/IEC 24727-5 will be in committee draft now that a degree of stabilization has been achieved for the other parts. ISO/IEC 24727-6 is in a working draft stage, with a committee draft anticipated in 2008.

Although not yet finalized, this standard has been publicly adopted by the European community for the European Union Citizens Card, by Germany for the German health card, by Australia for their citizen social services card, 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.

ISO/IEC 24727 standards suite has and will establish prescriptive APIs and interfaces for years to come. It has achieved international support and

the initial reluctance to accept this body of work is now such that 'user resistance' is now 'user insistence.'

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

NIST Personal Identity Verification Program (NPIVP)

The mission of the NIST Personal Identity Verification Program (NPIVP) is to validate Personal Identity Verification (PIV) components required by FIPS 201 for conformance to specifications in the FIPS 201 companion document SP 800-73-1, *Interfaces for Personal Identity Verification*. The two PIV components that come under the scope of NPIVP are PIV Smart Card Application and PIV Middleware. All of the tests under NPIVP are conducted by third-party test facilities, which are accredited as Cryptographic Module Test (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP) and have extended their scope of testing to include PIV Smart Card application and PIV Middleware test methods (and hence called accredited NPIVP test facilities). As of September 2007, there are ten accredited NPIVP test facilities.

To facilitate development of PIV Smart Card Application and PIV Middleware for conformance to interface specifications in SP 800-73-1, NPIVP published SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines*. In addition to the tests, this document also provides an interpretation of SP 800-73-1 specifications through publication of C-language bindings for PIV Middleware interface commands as well as detailed mapping of PIV Card Command Interface return codes to PIV Middleware Interface return codes. We also developed an integrated toolkit called "PIV Interface Test Runner" for conducting tests on both PIV Card Application and PIV Middleware products, and provided the toolkit to accredited NPIVP test facilities.

In FY 2007, three PIV Card application products were validated and certificates issued, bringing the total number of NPIVP-validated PIV Card application products to nine. In addition, two PIV Card application products were revalidated after the vendors made changes to the products for efficiency reasons and for storage scalability. Three NPIVP-validated PIV Card application products passed the FIPS 140-2 validation, bringing the total number of NPIVP-validated PIV Card application products to six.

In order to facilitate testing of credential data on PIV Cards for conformance to the data model specifications in Appendix A of SP 800-73-1, NPIVP published SP 800-85B, *PIV Data Model Test Guidelines*, and developed an associated toolkit, "PIV Data Model Test Runner." In order to enable the toolkit to be used for supporting the GSA's FIPS 201 Evaluation Program's Electronic Personalization Product certification, NPIVP made several enhancements to the PIV Data Model Test Runner, including reporting capabilities. NPIVP also enhanced the PIV Data Model Test Runner to include the functionality to generate multiple sample data sets in addition to the feature for populating a PIV Card with a data set. To facilitate development of conformant Personal Identity Verification (PIV) products by vendors, NPIVP also made the PIV Data Model Test Runner available for download from the NIST Web site. As of September 24, 2007, 106 vendors/system integrators had downloaded the PIV Data Model Test Runner.

http://csrc.nist.gov/npivp

Contacts: Dr. Ramaswamy Chandramouli	Ms. Hildegard Ferraiolo
(301) 975-5013	(301) 975-6972
chandramouli@nist.gov	hildegard.ferraiolo@nist.gov

Conformance Tests for Transportation Worker Identification Credential (TWIC) Specifications

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

In order to facilitate 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. NIST provided the roadmap for development of the following categories of tests:

◆ TWIC Card Application Interface Conformance Tests; and

◆ TWIC Data Model Conformance Tests.

When DHS approved the roadmap, NIST initiated development efforts for the above categories of tests. In FY 2007, NIST developed the beta version of the tests and ran these tests against a test TWIC card provided by TSA. NIST provided to DHS not only the test results but also feedback on the specifications themselves to facilitate better interoperability.

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

Research in Emerging Technologies

Digital Handheld Device Forensics

Cell phones are ubiquitous today, used by individuals for both personal and professional purposes. Because of their pervasiveness and information content, cell phones are an emerging but rapidly growing area of computer forensics. Besides placing calls, cell phones can allow users to perform additional tasks such as Short Message Service (SMS) messaging, Multimedia Messaging Service (MMS) messaging, Instant Messaging (IM), e-mail exchange, Web browsing, Personal Information Management (PIM) administration (e.g., address book, task list, and calendar schedule), photo and video capture, and even the reading, editing, and production of digital documents. Over time, a significant amount of information tends to accumulate on them that may be connected with an incident or crime and recovered during an investigation.

While cell phones are gaining desktop-like functionally, their organization and operation are quite different from desktops in certain areas. For example, most cell phones do not contain a hard drive and rely instead on flash memory for persistent storage. Such differences make the application of classical computer forensic techniques difficult. The key to applying forensic principles correctly and answering questions that arise in an investigation is an understanding of the hardware and software characteristics of cell phones and of the intrinsic abilities of available cell phone forensic tools.

This past year, NIST produced Interagency Report (NISTIR) 7287, *Cell Phone Forensic Tools: An Overview and Analysis Update*, which provides an overview of current forensic software tools designed for the acquisition, examination, and reporting of data residing on cellular handheld devices, and reviews their capabilities and limitations. NIST also issued a companion guideline, SP 800-101, *Guidelines on Cell Phone Forensics*, which provides recommendations on forensic procedures and highlights key principles associated with the handling and examination of electronic evidence contained on cellular devices. The intended audience for these publications ranges broadly from response team members handling a computer security incident to organizational security officials investigating an employee-related situation to forensic examiners involved in criminal investigations.

The current focus of the project is to develop and demonstrate techniques for improving the practice of cell phone forensics. Two proof-of-concept implementations are under way. The first is a forensically sound method to address the problems forensic tools have with latency in coverage for newly available phone models coming onto the market. The approach, called phone manager protocol filtering, augments the functionality of off-the-shelf phone managers available from device manufacturers to block unsafe commands. The second is to provide a means to establish a baseline for validating the correct functioning of forensic tools. The approach, called identity module programming, populates the identity modules of certain classes of phones with reference test data that serves as a baseline for validating the correct functioning of related forensic tools.

http://csrc.nist.gov/mobile-forensics/projects.html
Contact: Mr. Wayne Jansen
(301) 975-5148
wayne.jansen@nist.gov

Grid Security

While grid computing has become closer to reality due to the maturity of the current computing technologies, it has greater challenges compared to non-grid systems with infrastructure security issues such as authorization, directory services, and firewalls. There is some research available on grid

security-related topics; however, most of the research is targeted to one specific grid 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 grid security is needed.

During the past year, we defined and classified general grid systems and identified security requirements and issues that are specific to grid computing. Our works were published at some major related symposiums and conferences. In the coming year, we will investigate architectures, functional stacks, protocols, and APIs for the grid communication and 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 systems of previous research are capable of providing. We will also develop a reference implementation using already-developed tools (such as Globus and Access Control languages) to demonstrate how to configure a grid system to satisfy the security requirements.

The success of this project will:

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

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

◆ Increase security and safety of non-grid distributed systems by applying the trust domain concept of grid; 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.

Contacts:

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

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

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

Network Security Analysis Using Attack Graphs

At present, computer networks constitute the core component of information technology infrastructures in areas such as power grids, financial data systems and emergency communication systems. Protection of these networks from malicious intrusions is critical to the economy and security of our nation. Having a standard way to measure network security will bring together users, vendors and researchers to evaluate methodologies and products for network security.

In the past, there has been some progress in standardizing security metrics. However, widely accepted metrics for network security are still unavailable. Typical issues currently addressed in the area of network security are:

◆ topological vulnerability analysis,

◆ network hardening, and

◆ attack response.

The current focus is on qualitative aspects rather than a quantitative study of network security. To measure the overall security of a network, one must first understand the vulnerabilities and how they can be combined to construct an *attack*. Our vision is that *attack graphs* can be used to measure the damage that can be caused by an attack, the cost of reconfiguration, and the amount of resistance to an attack. Network hardening and attack response will be guided by the pursuit of an optimal solution in terms of available metrics, rather than using an arbitrary solution.

This research is based on our experience with attack graph generation and analysis. Central to the framework are two types of composition operators that correspond to the case of serial and parallel connectivity between hosts. It is our belief that our research will lead to both theoretical results and practical advances in the design of network security metrics. It will also have a positive impact on the study of vulnerability analysis, network hardening, and attack response.

Contact: Dr. Anoop Singhal
(301) 975-4432
Anoop.singhal@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 a multitude of heterogeneous systems is a lack of interoperability. Although a lack of interoperability may not be a problem for systems that can adequately operate independently of one another, access control mechanisms clearly do not fall into this category of systems. Users with vastly different credentials have a need to access resources protected under different mechanisms, and resources that are protected under different mechanisms, differ vastly in their sensitivity and therefore accessibility. This lack of interoperability introduces significant privilege and identity management issues.

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

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

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

Comprehensive implementation PM features have been under development during the past year. In the coming year, we plan on releasing the version 1 PM implementation which will be made available for experimental deployment and we will begin the PM standardization process.

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 included in the PM's scope of control. Demonstrated application services include internal email, workflow management, and database management.

◆ Enterprise wide scope of protection – Access control policies are uniformly enforced over resources that are physically stored under different operating systems.

◆ Comprehensive enforcement – All user and subject (process) access requests, and all exchange of data to and from and among applications, between sessions, and outside the bounds of the PM could be uniformly controlled under the protection policies of the objects of concern (e.g., "cut and paste", e-mail, workflows, granting access, and writing to devices and ports).

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

◆ True single-sign on –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 effectively eliminates the need for a user to authenticate to multiple applications and systems.

Contacts: Mr. David Ferraiolo   Dr. Vincent Hu
(301) 975-3046   (301) 975-4975
david.ferraiolo@nist.gov   vhu@nist.gov

Automated Vulnerability Management and Measurement

Information Security Automation Program (ISAP) & Security Content Automation Protocol (SCAP)

The ISAP is a Department of Homeland Security (DHS)-sponsored initiative that includes interagency and interdepartmental participation from NIST, the National Security Agency (NSA), the Defense Information Systems Agency (DISA), and the Department of Defense (DoD). This program focuses on a standard, automated approach for the implementation of information system security controls, which includes the following objectives:

◆ Develop requirements for automated sharing of information security data;

◆ Customize and manage configuration baselines for various IT products;

◆ Assess information systems and report compliance status;

◆ Use standard metrics to weight and aggregate potential vulnerability impact; and

◆ Remediate identified vulnerabilities.

Recognizing that NIST has the responsibility to produce security configuration guidance for the U.S. Government, and that NSA and DISA provide the same service to DoD, ISAP consolidates data sources from these agencies and provides the data in a standardized XML format. Commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) software products and initiatives utilize this security-related data for the purposes of automating the identification and remediation of vulnerabilities, measuring potential impact, and conducting compliance reporting in the various computing infrastructures. The freely available information contained in ISAP files includes, but is not limited to:

◆ Checking for vulnerabilities (security-related software flaws and misconfigurations) on an information technology asset;

◆ Mapping to higher-level policies, such as FISMA via NIST SP 800-53, DoD 8500 Information Assurance (IA) controls, etc.; and

◆ Providing a standard impact metric for vulnerabilities and a capability to aggregate impact scores to the agency reporting level.

The FISMA Connection

As the FISMA Implementation Project moves into Phase II, we continue to look for ways to help our customers employ the most cost-effective information security solutions for their enterprises. One of the key challenges in effectively employing security controls in information systems is to ensure that security configuration settings are properly established and enforced. It is also important to establish traceability from the high-level security requirements in the FISMA legislation down to the specific mechanisms that provide the security capability in the hardware and software components that compose the information system. To establish this important linkage from legislation and policy to the mandatory security requirements and controls described in FIPS 200 and SP 800-53, and ultimately to the mechanisms at the systems-implementation level, we established the SCAP as part of the ISAP governing program.

SCAP Technical Composition

Through the interagency/interdepartmental ISAP effort, the federal government, in cooperation with academia and private industry, uses and encourages widespread support for SCAP, a suite of open standards—developed primarily by NSA, MITRE Corporation, and NIST—that provide technical specifications for expressing and exchanging security-related data. These interoperable standards identify, enumerate, assign, and facilitate the measurement and sharing of information security-relevant data. The SCAP is composed of the following standards—

Enumeration

◆ Common Platform Enumeration – CPE (*http://cpe.mitre.org*)

◆ Common Vulnerabilities and Exposures – CVE (NIST SP 800-51, *http://cve.mitre.org*)

◆ Common Configuration Enumeration – CCE (*http://cce.mitre.org*)

Metrics/Scoring

◆ Common Vulnerability Scoring System – CVSS (*http://nvd.nist.gov/cvss.cfm*, NISTIR 7435)

Languages for Expression

◆ eXtensible Checklist Configuration Description Format – XCCDF (NISTIR 7275)

◆ Open Vulnerability and Assessment Language – OVAL (*oval.mitre.org*)

The suite of standards within SCAP is extensible and will likely be expanded over time to include additional standards, such as Common Remediation Enumeration (CRE) and Open Vulnerability Remediation Language (OVRL).

The primary output from SCAP is a security checklist in standard XML format that customers can use via their COTS products to help build, operate, measure, and maintain more secure information systems according to official government security guidelines. A security checklist is a document that contains instructions for securely configuring an information technology (IT) product for an operational environment or verifying that an IT product has already been securely configured. Checklists can take many forms, including files that can automatically set or verify security configurations. Having such automated methods has become increasingly important for several reasons, including the complexity of achieving compliance with various laws, Executive Orders, directives, policies, regulations, standards, and guidance; the increasing number of vulnerabilities in information systems; and the growing sophistication of threats against those vulnerabilities. Automation is also needed to ensure that the security controls and configuration settings are applied consistently within an information system, and that the controls and settings can be effectively verified.

In response to these needs and working closely with government, industry, and academia, SCAP seeks to encourage the development of automated checklists, particularly those that are compliant or compatible with XCCDF and/or OVAL. These are widely used for automated checklists—XCCDF primarily for mapping policies and other sets of requirements to high-level technical checks, and OVAL primarily for mapping high-level technical checks to the low-level details of executing those checks on the operating systems or applications being assessed.

The SCAP Web site provides, or is scheduled to provide, automated security configuration and patching information for checklists obtained through the NIST National Checklist Program (*checklists.nist.gov*), including Windows

Vista, Windows 2003 Server, Windows XP, Windows 2000, RedHat Linux, desktop applications (e.g., Microsoft Office, Netscape Navigator, Internet Explorer), Oracle and Microsoft SQL Server, Sun Solaris, and Web servers (e.g., IIS, Apache).

Over the past year, NIST has:

◆ Completed development of SCAP version Beta;

◆ Managed SCAP education and awareness, through both informal interaction and speaking at a number of conferences and workshops;

◆ Hosted the 3rd Annual Security Automation Conference;

◆ Supported SCAP beta testing with the Office of Secretary of Defense (OSD), Department of Justice (DOJ), and the Office of Management and Budget (OMB); and

◆ Led a number of activities to prepare the National Vulnerability Database (NVD) for production support of SCAP version 1.0.

In fiscal year 2008, NIST will:

◆ Complete activities to evolve the NVD to production readiness for SCAP version 1.0;

◆ Communicate SCAP standards and guidelines through a combination of NISTIRs and SPs;

◆ Implement an SCAP compliance program;

◆ Continue beta test and production support;

◆ Continue education and awareness activities;

◆ Announce the readiness of the NVD to support SCAP version 1.0 and announce the final SCAP version 1.0 standards list; and

◆ Formalize discussions on the evolution of SCAP to version 2.0.

http://nvd.nist.gov/scap.cfm
Contacts: Mr. Stephen Quinn   Mr. Peter Mell
(301) 975-6967   (301) 975-5572
stephen.quinn@nist.gov   pmell@nist.gov

National Vulnerability Database

The National Vulnerability Database (NVD) is the U.S. Government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance checking. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product dictionaries, and impact metrics. NVD is provided as a Web service that receives over 60 million hits per year, and its greatest use comes from computer security vendors downloading the NVD SCAP data and incorporating it into their products. NVD is sponsored by the Department of Homeland Security's National Cyber Security Division.

NVD is a comprehensive cyber security vulnerability database that is updated daily with the latest vulnerabilities. Using a single search engine, one can find all publicly available U.S. Government vulnerability resources and references to industry resources. NVD also contains a statistics engine to enable users to gain a deeper scientific understanding of the nature of published vulnerabilities and associated trends. As of October 2007, NVD contains the following resources:

◆ 27,084 vulnerability advisories with an average of 18 new vulnerabilities added daily;

◆ 11 SCAP checklists that contain thousands of low-level security configuration checks that can be automatically processed by commercial tools;

◆ 114 non-SCAP capable checklists (i.e., English prose guidance and configuration scripts);

◆ 91 US-CERT alerts, 1999 US-CERT vulnerability summaries, and 2966 SCAP machine-readable vulnerability checks;

◆ 12,555 vulnerable products (this covers almost all software vendors and products in active use); and

◆ 11,663 vulnerability advisories translated into Spanish.

In FY 2007, NVD was restructured so that it is completely based upon and supports SCAP. This involved a major upgrade to the NVD architecture and migration of NVD data so that it conforms to the SCAP standards. With regards to vulnerability management data, we analyzed 6700 new vulnerabilities, created 11 SCAP checklists, and assisted the Spanish government in translating over 6000 vulnerabilities into Spanish. In fiscal year 2008, we will build automated management services for SCAP into the NVD architecture, upgrade the NVD servers to have high availability systems and expanded capacity, fully migrate the NIST checklist program into NVD,

and continue adding vulnerability management data (analysis of software flaws and creation of configuration checklists).

NVD has a substantial impact within both the government and industry:

◆ The NVD service is one of the most visited Web sites at NIST (rate of 60 million hits per year) with 2.2 million NVD vulnerability advisories being read every month.

◆ The Payment Card Industry (PCI) has mandated use of NVD data for securing PCI systems worldwide.

◆ Over 20 vendors are integrating NVD data into their products.

◆ The Office of Management and Budget (OMB) uses NVD SCAP checklists within the Federal Desktop Core Configuration (FDCC) initiative to securely configure government computers.

◆ The Office of the Secretary of Defense (OSD) uses NVD/SCAP data as a basis for its Computer Network Defense pilot.

◆ The Department of Homeland Security (DHS) uses NVD data to maintain its Cyber Bulletin capability.

◆ The Army is adopting NVD product data for the Army's information technology asset database.

◆ The NSA provides a mirror of NVD for the Department of Defense and uses it to integrate NSA security capabilities.

◆ NVD provides the operational capability and technical architecture that supports the NIST Information Security Automation Program (ISAP), the NIST National Checklist Program, and NIST's work developing the Common Vulnerability Scoring System (CVSS).

NVD reference data is increasingly becoming the foundation for a variety of vulnerability management initiatives, and the Computer Security Division plans to expand and mature NVD appropriately in fiscal year 2008.

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

Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is an industry standard that enables the security community to calculate the impact of low level vulnerabilities within information technology systems through sets of security metrics and equations. The CVSS 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 and mathematicians provided technical leadership and support for the development of version 2 of CVSS, which was finalized in June 2007. This work also resulted in the development of the following publications:

◆ Article in the November/December 2006 issue of the journal IEEE Security & Privacy on the original version of the CVSS standard and some of its shortcomings;

◆ Article in the September 2007 issue of the journal *IET Information Security* on an analysis of the deficiencies of the original version of the CVSS standard and recommendations for addressing those deficiencies;

◆ Two technical reports published by FIRST in June 2007: one defines the CVSS version 2 standard and the other provides a historical account of the changes from CVSS version 1 to version 2; and

◆ NIST Interagency Report (NISTIR) 7435, *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems,* published in September 2007.

NIST has adopted CVSS version 2 for use in the National Vulnerability Database (NVD) to provide scores for each vulnerability in NVD. We have also been studying how CVSS could be adapted for calculating the impact of security misconfigurations, and we have documented a preliminary proposal for how this could be achieved. We plan to continue researching this topic and develop a report on scoring security misconfigurations. Also, because CVSS version 2 will enable consistent and accurate measurement of low-level security flaws that can be used by attackers to penetrate systems, we plan to recommend usage of CVSS by federal agencies to perform more quantitative measurement of technical security deficiencies in support of FISMA compliance efforts. Accordingly, CVSS version 2 has been included as one of the components of the Security Content Automation Protocol (SCAP) developed by NIST.

http://nvd.nist.gov/cvss.cfm?version=2
Contacts: Mr. Peter Mell   Ms. Karen Scarfone
(301) 975-5572   (301) 975-8136
mell@nist.gov   karen.scarfone@nist.gov

Infrastructure Services, Protocols, and Applications

Automated Combinatorial Testing for Software

NIST research suggests that software faults are triggered by only a few variables interacting (1 to 6). 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.

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

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

Our focus is on empirical results and real-world problems. Accomplishments for FY 2007 include the following:

◆ The project team implemented (joint work with University of Texas, Arlington) covering array algorithms designed in FY 2006 into a user-friendly tool for release in November 2007. The new tool can be used by software testers to quickly produce test data with high-strength combinatorial coverage. A parallel version of one of the covering array algorithms was implemented on the NIST cluster. Comparison of both new algorithms with conventional algorithms showed that the NIST-UT algorithms outperformed others, in some cases by several orders of magnitude.

◆ Empirical data on interaction strength required to detect software faults was extended with a study of over 3000 vulnerability reports from the National Vulnerability Database, a collection of all known software security vulnerabilities maintained by NIST.

◆ A repository for covering arrays, the first of its kind, was established on the NIST Mathematical and Computational Sciences Division server. The repository will collect covering arrays for use by researchers in a variety of fields, including biotechnology and statistics, and software testing.

Plans for FY 2008 include a new effort using combinatorial testing for XML validation and Web application testing, security policy and firewall testing, and working with industry researchers and practitioners to transition the tools and methods into practical application. We are working with researchers from several major universities, other NIST divisions and labs, and private industry.

http://csrc.nist.gov/acts
Contacts: Mr. Rick Kuhn   Dr. Raghu Kacker
(301) 975-3337   Mathematical and Computational Sciences Division
kuhn@nist.gov   (301) 975-2109
                                 raghu.kacker@nist.gov

Border Gateway Protocol

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

The BGP project was initiated in February 2004. The project aims to help industry to understand the potential risks to inter-domain routing and the design and implementation trade-offs of the various BGP security mechanisms currently proposed in the Internet Engineering Task Force (IETF) community. Previously, there was a lack of awareness and knowledge in the information technology (IT) sector of the potential threats, risks, mitigation techniques, and their costs. The project also seeks to expedite convergence towards standardized, implemented, and deployed BGP security solutions.

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

◆ Identify the threats and vulnerabilities of BGP/inter-domain routing;

◆ Document best common practices in securing the current BGP deployments; and

◆ Provide deployment and policy guidance for emerging BGP security technologies.

In June 2007, we issued NIST SP 800-54, *Border Gateway Protocol Security,* to provide a guideline of best practices for securing BGP.

The focus of our 2008 activities will be to continue to extend modeling and analysis tools to incorporate significantly larger and more realistic topologies, and to actively contribute to the IETF Routing Protocols Security Working Group and other Internet standards bodies, helping to move the results of this research into practice.

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

Contacts: Mr. Rick Kuhn   Mr. Douglas Montgomery (ANTD)
(301) 975-3337   (301) 975-3630
kuhn@nist.gov   dougm@nist.gov

Industrial Control Systems Security

Industrial control systems (ICSs) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations often found in the industrial control sectors. Our work focuses on SCADA systems and DCSs, which are used in the electric, water, oil and gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries.

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in the distribution operations of water supply systems, oil and gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks. This includes monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

DCSs are used to control industrial processes such as electric power generation, oil and gas refineries, wastewater treatment, and chemical, food, and automotive production. DCSs are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated subsystems that are responsible for controlling the details of a localized process. DCSs are used extensively in process-based industries.

Most ICSs in use today were developed years ago, long before public and private networks, desktop computing, or the Internet were a common part of business operations. These systems were designed to meet performance, reliability, safety, and flexibility requirements and were typically physically isolated and based on proprietary hardware, software, and communication protocols. These proprietary communication protocols included basic error detection and correction capabilities, but nothing that guaranteed secure communications. The need for cyber security measures within these systems was not anticipated, and at the time, security for ICSs meant physically securing access to the network and the consoles that controlled the systems.

As microprocessor, personal computer, and networking technology evolved during the 1980s and 1990s, the design of ICSs changed to incorporate the latest technologies. Internet-based technologies started making their way into ICS designs in the late 1990s. These changes to ICSs exposed them to new types of threats and significantly increased the likelihood that they would be attacked. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new IT security solutions are needed.

In the past year, we have collaborated with the NIST Manufacturing Engineering Laboratory (MEL) in developing a guide to ICS security, draft 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).* The purpose of this document is to provide guidance for establishing secure SCADA systems and other ICSs. The document provides an overview of ICSs and typical system topologies, identifies typical vulnerabilities and threats to these systems, and provides recommended security countermeasures to mitigate the associated risks. The second public draft of SP 800-82 was released in September 2007, and the final document is expected to be completed in early 2008. This guideline is being prepared for use by federal agencies, but it may be used by nongovernmental organizations on a voluntary basis.

The draft underwent subject matter expert review by the NIST-led Process Control Security Requirements Forum (PCSRF), which was formed in the spring of 2001 by the MEL Intelligent Systems Division (ISD) in cooperation with the Computer Security Division (CSD). The PCSRF is a working group of users, vendors, and integrators in the process control industry that is addressing the cyber security requirements for industrial process control systems and components, including SCADA systems, DCS, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). Members of the PCSRF represent the critical infrastructures and related process-control industries including oil and gas, water, electric power, chemicals, pharmaceuticals, metals and mining, and pulp and paper. There are currently over 700 members in the PCSRF from government, industry, and academe. ISD leads the NIST effort with additional support provided from CSD and the NIST Electronics and Electrical Engineering Laboratory (EEEL).

http://www.isd.mel.nist.gov/projects/processcontrol/

Contacts: Mr. Keith Stouffer Ms. Karen Scarfone
Intelligent Systems Division, MEL (301) 975-8136
(301) 975-3877 karen.scarfone@nist.gov
keith.stouffer@nist.gov

Internet Protocol Version 6 (IPv6) and Internet Protocol Security (IPSec)

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

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

The U.S. Office of Management and Budget (OMB) has mandated that government agencies will incorporate IPv6 capability into their backbones (routers, gateways, etc.) by 2008. NIST personnel are actively participating in the federal IPv6 Working Group, formed to help government agencies plan and execute the transition in an interoperable and secure manner. We are also developing an IPv6 profile to define which pieces and features of IPv6 are mandatory for government agencies, which are optional, and where these elements are definitively defined.

Internet Protocol Security (IPSec) is a framework of open standards for ensuring private communications over IP networks, which has become the most popular network layer security control. It can provide several types of data protection—confidentiality; integrity; data origin authentication; prevention of packet replay and traffic analysis; and access control. IPSec typically uses the Internet Key Exchange (IKE) protocol to negotiate IPSec connection settings, exchange keys, authenticate endpoints to each other, and establish security associations, which define the security of IPSec-protected connections. IPSec and IKE were added to IPv4 after the fact, but are now integrated into all of the major operating systems. For IPv6, IPSec and IKE are planned to be an integral part of the network protocols.

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

SP 500-267, *A Profile for IPv6 in the U.S. Government - Version 1.0*, was released for public comment in February 2007. This document is a draft profile to assist federal agencies in developing plans to acquire and deploy products that implement Internet Protocol version 6 (IPv6). The profile recommends IPv6 capabilities for common network devices, including hosts, routers, intrusion detection systems, and firewalls, and includes a selection of IPv6 standards and specifications needed to meet the minimum operational requirements of most federal agencies. It was developed to help ensure that IPv6-enabled federal information systems are interoperable and secure and addresses how such systems can interoperate and coexist with the current IPv4 systems. Agencies with unique information technology requirements are expected to use the NIST profile as a basis for further refined specifications and policies.

We are currently writing a guidance document on IPv6 and IPSec, to be released in FY 2008. This document will describe IPv6's new and expanded protocols, services, and capabilities. It will characterize new security threats posed by the transition to IPv6. It will issue guidance on IPv6 deployment, including transition, integration, configuration, and testing. It will also include several practical IPv6 transition scenarios. In addition, our personnel are planning research on the challenges posed to intrusion detection systems (IDSs) and firewalls by adding IPv6 to networks.

Contacts: Ms. Sheila Frankel Mr. Douglas Montgomery (ANTD)
(301) 975-3297 (301) 975-3630
sheila.frankel@nist.gov dougm@nist.gov

Radio Frequency Identification Technology: Security Aspects

NIST published SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, in April 2007. SP 800-98 provides an overview of RFID technology, the associated security and privacy risks, and recommended practices that will help organizations mitigate these risks, safeguard sensitive information, and protect the privacy of individuals.

SP 800-98 seeks to assist organizations in understanding the risks of RFID technology and security measures to mitigate those risks. It provides practical, real-world guidelines on how to initiate, design, implement, and operate RFID solutions in a manner that mitigates security and privacy risks. The document also provides background information on RFID applications, standards, and system components to assist in the understanding of RFID security risks and controls. The document presents information that is independent of particular hardware platforms, operating systems, and applications. The emphasis is on RFID solutions that are based on industry and international standards, although the existence of proprietary approaches is noted when they offer relevant security features not found in current standards.

The document has been created for executives, planners, systems analysts, security professionals, and engineers who are responsible for federal business processes or information technology systems. Professionals with similar responsibilities outside the government should also benefit from the information this document provides. It addresses both the needs of those considering an RFID implementation and those with an existing RFID solution. SP 800-98 is also useful for those who seek an overview of RFID technology and related security issues.

Contact: Dr. Tom Karygiannis
(301) 975-4728
karygiannis@nist.gov

Counterfeit RFID Detection

RFID is a form of automatic identification and data capture (AIDC) technology that uses electric or magnetic fields at radio frequencies to transmit information. An RFID system can be used to identify many types of objects, such as manufactured goods, animals, and people. Each object that needs to be identified has a small object known as an RFID tag affixed to it or embedded within it. The tag has a unique identifier and may optionally hold additional information about the object. Devices known as RFID readers wirelessly communicate with the tags to identify the item connected to each tag and possibly read or update additional information stored on the tag. This communication can occur without optical line of sight and over greater distances than other AIDC technologies. RFID technologies support a wide range of applications, everything from asset management and tracking to access control and automated payment. The use of RFID tags is being studied by the pharmaceutical industry to ensure drug pedigree and to help detect counterfeit drugs in the supply chain. Many RFID tags, however, can be easily cloned and therefore present a risk to the supply chain. NIST has been conducting a study to determine if physical differences between cards can be readily identified and quantified. Manufacturing processes have some degree of random error and the hope is that every card has a slightly different but specific set of hardware parameters that affect the electrical signals produced in a readily recognizable and quantifiable manner. The set of quantified abnormalities would be known as an electromagnetic (EM) signature. The goal of this research is to be able to detect counterfeit RFID tags by comparing the electromagnetic signature of an RFID tag in the supply chain to its electromagnetic signature of record.

Contact: Dr. Tom Karygiannis
(301) 975-4728
karygiannis@nist.gov

Securing the Domain Name System (DNS)

The Domain Name System (DNS) is the method by which Internet addresses in mnemonic form such as **http://csrc.nist.gov** are converted into the equivalent numeric 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 trying to perform a translation may communicate with other Internet DNS servers if it does not have the data needed to translate the address itself.

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

As part of this continuing effort to promote the deployment of DNSSEC, we published technical papers and guideline documents, and contributed three DNS-related controls to NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, thereby prescribing mandatory controls for securing the DNS infrastructure in U.S. Government agencies.

In addition to technical papers, guideline documents, and mandatory controls, we are also involved in developing performance data related to deployment of the new security controls in DNS. We developed tests to measure the impact on performance on DNS zones due to supporting and providing additional security records related to "Authenticated Proof of Non-Existence," and published the results at *http://www-x.antd.nist.gov/dnssec*.

NIST continued its efforts with the U.S. General Services Administration (GSA) to set in motion the process for securing the top-most DNS domain of the U.S. Government (i.e., .gov). In FY 2007, in collaboration with DHS and SPARTA Inc., NIST set up a pilot Internet domain with DNSSEC features (called the Secure Naming Infrastructure Pilot [SNIP]) with the following objectives:

◆ To enable U.S. Government DNS stakeholders to become familiar with the DNS Security Extensions (DNSSEC) and to understand their impact on current DNS operations; and

◆ To help agency DNS administrators to learn and deploy DNSSEC on their zones in order to meet the new DNSSEC-related FISMA controls.

NIST is tracking the progress of DNSSEC implementations in several DNS products and is planning to update the SP 800-81 document in FY 2008 to cover these technologies. The update will include guidelines for secure configuration and deployment of these new products with DNSSEC features to meet a federal agency's security goals. NIST is also working with standards organizations to ensure that the DNSSEC specifications keep up with current best security practices with regards to cryptographic algorithm deployment options and cryptographic key sizes.

Contacts: Dr. Ramaswamy Chandramouli   Mr. Scott Rose
(301) 975-5013   (301) 975-8439
mouli@nist.gov   scott.rose@nist.gov

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

Secure Sockets Layer (SSL) virtual private networks (VPNs) provide users with secure remote access to an organization's resources. An SSL VPN consists of one or more VPN devices to which users connect using their Web browsers. The traffic between the Web browser and SSL VPN device is encrypted with the SSL protocol. SSL VPNs can provide remote users with access to

Web applications and client/server applications, as well as connectivity to internal networks. They offer versatility and ease of use because they use the SSL protocol, which is included with all standard Web browsers, so special client configuration or installation is often not required. In planning VPN deployment, many organizations are faced with a choice between an Internet Protocol Security (IPSec) based VPN and an SSL-based VPN. In 2005, we published NIST SP 800-77, *Guide to IPSec VPNs*.

A complementary document, SP 800-113, *Guide to SSL VPNs*, was released for public comment in August 2007. It seeks to assist organizations in understanding SSL VPN technologies. The publication also makes recommendations for designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions. SP 800-113 provides a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also includes a comparison with other similar technologies such as IPSec VPNs and other VPN solutions.

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

Voice over Internet Protocol Security Issues

Voice over IP (VoIP)—the transmission of voice over packet-switched IP networks—is one of the most important emerging trends in telecommunications. As with many new technologies, VoIP introduces both security risks and opportunities. For several years, VoIP was a technology prospect, something on the horizon for the "future works" segment of telephony and networking papers. Now, however, telecommunications companies and other organizations have already moved, or are in the process of moving, their telephony infrastructure to their data networks. The VoIP solution provides a cheaper and clearer alternative to traditional Public Switched Telephone Network (PSTN) telephone lines. Although its implementation is widespread, the technology is still developing. It is growing rapidly throughout North America and Europe, but it sometimes can be difficult to integrate with existing systems. Nevertheless, VoIP will capture a significant portion of the telephony market, given the fiscal savings and flexibility that it can provide.

VoIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units, and mobile units. In addition to end-user equipment, VoIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Most of these components have counterparts used in data networks, but the performance demands of VoIP mean that ordinary network software and hardware must be supplemented with special VoIP components. Not only does VoIP require higher performance than most data systems, but critical services, such as Emergency 911, must be accommodated. One of the main

sources of confusion for those new to VoIP is the (natural) assumption that because digitized voice travels in packets just like other data, existing network architectures and tools can be used without change. However, VoIP adds a number of complications to existing network technology, and these problems are magnified by security considerations.

Quality of Service (QoS) is fundamental to the operation of a VoIP network that meets users' quality expectations. However, the implementation of various security measures can cause a marked deterioration in QoS unless VoIP-specific equipment and architectures are used. These complications range from firewalls delaying or blocking call setups to encryption-produced latency and delay variation (jitter). Because of the time-critical nature of VoIP and its low tolerance for disruption and packet loss, many security measures implemented in traditional data networks are simply not applicable to VoIP in their current form; firewalls, intrusion detection systems, and other components must be specialized for VoIP. Most current VoIP systems use one of two standards—H.323 or the Session Initiation Protocol (SIP). Although SIP seems to be gaining in popularity, neither of these protocols has become dominant in the market yet, so it often makes sense to incorporate components that can support both.

With the introduction of VoIP, the need for security is compounded because now we must protect two invaluable assets—our data and our voice. Federal agencies are required by law to protect a great deal of information, even if it is unclassified. Both privacy-sensitive and financial data must be protected, as well as other government information that is categorized as sensitive but unclassified. Protecting the security of conversations is thus required. In a conventional office telephone system, intercepting conversations requires physical access to telephone lines or compromise of the office private branch exchange (PBX). Only particularly security-sensitive organizations bother to encrypt voice traffic over traditional telephone lines. The same cannot be said for Internet-based connections. For example, when ordering merchandise over the telephone, most people will read their credit card number to the person on the other end. The numbers are transmitted without encryption to the seller. In contrast, the risk of sending unencrypted data across the Internet is more significant. Packets sent from a user's home computer to an online retailer may pass through 15 to 20 systems that are not under the control of the user's ISP or the retailer. Anyone with access to these systems could install software that scans packets for credit card information. For this reason, online retailers use encryption software to protect a user's information and credit card number. So it stands to reason that if we are to transmit voice over the Internet Protocol, and specifically across the Internet, similar security measures must be applied.

The current Internet architecture does not provide the same physical wire security as the telephone lines. The key to securing VoIP is to use the security mechanisms like those deployed in data networks (firewalls, encryption, etc.) to emulate the security level currently enjoyed by PSTN network users.

VoIP can be done securely, but the path is not smooth. It will likely be several years before standards issues are settled and VoIP systems become a mainstream commodity. Until then, organizations must proceed cautiously and not assume that VoIP components are just more peripherals for the local network. Above all, it is important to keep in mind the unique requirements of VoIP, acquiring the right hardware and software to meet the challenges of VoIP security.

During the past year, CSD has worked toward an update of SP 800-58, *Security Considerations for Voice Over IP Systems*, which was published in January 2005. This publication investigates the attacks and defenses relevant to VoIP and explores ways to provide appropriate levels of security for VoIP networks at reasonable cost. More than 1.2 million copies of the publication have been downloaded since its release. The updated publication will reflect changes in technology, potential interactions between protocol features that could result in security weaknesses, revisions of standards, and new applications of VoIP and related technologies, such as video over Internet.

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

Web Services Security

The advance of Web services technologies promises to have far-reaching effects on the Internet and enterprise networks. Web services based on the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and related open standards, and deployed in Service Oriented Architectures (SOAs) allow data and applications to interact without human intervention through dynamic and ad hoc connections. Web services technology can be implemented in a wide variety of architectures, can coexist with other technologies and software design approaches, and can be adopted in an evolutionary manner without requiring major transformations to legacy applications and databases.

The security challenges presented by the Web services approach are formidable and unavoidable. 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. Difficult issues and unsolved problems exist, such as protecting—

◆ Confidentiality and integrity of data that is transmitted via Web services protocols in service-to-service transactions, including data that traverses intermediary (pass-through) services

◆ Functional integrity of the Web services that requires both establishment in advance of the trustworthiness of services in orchestrations or

choreographies, and the establishment of trust between services on a transaction-by-transaction basis

◆ Availability in the face of denial of service attacks that exploit vulnerabilities unique to Web service technologies, especially targeting core services, such as discovery service, on which other services rely.

In August 2007, we released SP 800-95, *Guide to Secure Web Services*, in final. This publication was issued in order to improve the understanding of different aspects of Web services security. This document discusses the different technologies and standards for securing Web services applications. It also provides some specific recommendations that Web services application developers and architects can use to secure their applications.

The SOA processing model requires the ability to secure SOAP messages and XML documents as they are forwarded along potentially long and complex chains of consumer, provider, and intermediary services. The nature of Web services processing makes those services subject to unique attacks, as well as variations on familiar attacks targeting Web servers.

The following is a summary of security techniques for Web services that are discussed in the document:

◆ Confidentiality of Web Services Using XML Encryption: This is a specification from the World Wide Web Consortium (W3C), and it provides a mechanism to encrypt XML documents

◆ Integrity of Web Services Using XML Signature: This is a specification produced jointly by the W3C and IETF. The power of XML signature is to selectively sign XML data

◆ Web Services Authentication and Authorization using Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML) as proposed by the OASIS standards group

◆ PKI for Web Services using XML Key Management Specification (XKMS)

◆ WS-Security: This specification defines a set of SOAP header extensions for end-to-end SOAP messaging security. It supports message integrity and confidentiality by allowing communicating partners to exchange signed encrypted messages in a Web services environment.

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

Wireless Security Standards

Many organizations and users have found that wireless communications and devices are convenient, flexible, and easy to use. Users of wireless local area network (WLAN) or Wi-Fi devices have the flexibility to move from one place to another while maintaining connectivity with the network. Wi-Fi, short for Wireless Fidelity, is an operability certification for WLAN products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard that is widely used today. Wireless personal area networks (WPANs) allow users to share data and applications with network systems and other users with compatible devices without being tied to printer cables and other peripheral device connections. Users of handheld devices such as PDAs and cellular phones can synchronize data between PDAs and personal computers, and can use network services such as wireless e-mail, Web browsing, and Internet access. Further, wireless communications can help first responders to emergencies gain critical information, coordinate efforts, and keep communications working when other methods may be overwhelmed or are nonfunctioning.

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, destroy

and steal data, and launch attacks that tie up network bandwidth and deny service to authorized users.

This past year, we completed two Special Publications dealing with wireless security issues. The first, SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, provides readers with a detailed explanation of next-generation 802.11 wireless security. It describes the inherently flawed Wired Equivalent Privacy (WEP) and explains 802.11i's two-step approach (interim and long-term) to providing effective wireless security. It describes secure methods used to authenticate users in a wireless environment and presents several sample case studies of wireless deployment. It also includes guidance on best practices for establishing secure wireless networks using the emerging Wi-Fi technology. This SP was published in February 2007.

The second publication on wireless security was released for public comment in August 2007. SP 800-48 Revision 1, *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*, is an update to the original version of SP 800-48, which was published in 2002. It provides recommendations on securing older 802.11 networks (pre-802.11i), including the use of additional security controls to compensate for WEP's weaknesses. It also discusses the security features of the WPAN protocol IEEE 802.15.1, better known as Bluetooth, and explains how these security features can be used to protect Bluetooth communications from common attacks.

Contacts: Ms. Sheila Frankel   Ms. Karen Scarfone
(301) 975-3297   (301) 975-8136
sheila.frankel@nist.gov   Karen.scarfone@nist.gov

Biometrics

Biometric technologies are able to establish or verify personal identity against previously enrolled individuals based upon recognition of a physiological or behavioral characteristic. Examples of biological characteristics include hand, finger, facial, and iris. Behavioral characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. Using biometrics for identifying human beings offers some unique advantages because only biometrics can identify you as you. Used alone, or together with other authentication technologies such as tokens, biometric technologies can provide higher degrees of security than other technologies employed alone and can also be used to overcome their weaknesses. For decades, biometric technologies were used primarily in law enforcement applications, and they are still a key component of these important applications. Over the past several years, the marketplace for biometrics solutions has widened significantly. Currently, they are increasingly being used in multiple public and private sector applications worldwide to verify a person's identity, secure national borders, and restrict access to secure sites including buildings and computer networks.

As the marketplace for biometric-based solutions has widened significantly, the importance of these biometric technologies has also dramatically increased. Homeland security is the highest priority for many countries. Biometric-based solutions play an important role in these applications. Biometric technologies can be found in identification cards, loyalty programs, associated with the management of welfare programs, and in such diverse environments as amusement parks, banks, mobile devices, passport programs, driver's licenses, and college and school lunch programs. As stated in the National Biometric Challenge document developed by the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management, "biometrics are the most definitive, real-time identity management tools currently available."[1]

Meeting Government and Other Customers' Needs

Government users and other consumers need biometric-based, high-performance, interoperable, standards-based information systems. In the absence of the timely availability of open systems standards, users may choose to adopt proprietary solutions. Migration from these proprietary systems to standards-based open-system solutions is usually difficult and expensive. Deploying these new information technology systems for homeland security, for preventing ID theft, and for other government and commercial applications requires national and international consensus standards for biometrics. These biometric standards support the mass-market adoption of biometric technologies by helping customers to achieve higher levels of security and interoperability in personal verification and identification applications using biometric-based, open-systems solutions. Therefore, supporting the national strategy on biometrics and the development of these standards and related testing technology such as conformance testing architectures is the cornerstone of our biometrics standards program.

We are responding to government and market requirements for open-systems standards by accelerating development of formal national and international biometric standards and associated conformity assessments, educating their

users on the capability of these standards-based open-systems solutions, by promoting their adoption and by supporting these standards with the required conformance test tools. This strategy requires comprehensively identifying and planning for the development of the required biometric standards and associated research and technology developments and testing.

In order to meet these immediate government and private sector needs for high performance and highly secure open systems, in the past year we have worked in close partnership with other U.S. Government agencies and U.S. industry to establish standards bodies for accelerating the development of formal national and international biometric standards of high relevance to the nation. We are an active participant on NSTC's Subcommittee on Biometrics and Identity Management. NIST experts also participate in its Standards and Conformity Assessment Working Group (SCA WG).

In addition, we are actively participating in biometric working groups established by other U.S. Government agencies, such as the Department of Homeland Security (DHS) and the Departement of Defense (DoD), in order to support coordination and harmonization of efforts in biometric standards bodies and conformity assessment activities.

Our program is well aligned to and supports the goals of NSTC's National Biometrics Challenge document released in August 2006, as well as the principles and goals of NSTC's recently issued document delineating policy for enabling the development, adoption, and use of biometric standards.[2] These common goals include support for the continued development of voluntary consensus standards for biometrics vital to the security of the nation and the stability of the U.S.-based community and technology development in support of rigorous testing that is required to ensure vendor and system compliance with biometric standards. Our program experts work in close collaboration with the NIST/ITL and ITL's Information Access Division's biometric experts. This program is considered to be a major catalyst for biometric standardization and adoption of biometric standards and has gained national and international recognition for its achievements. (During Fiscal Year 2007, the biometric standards program lead, Fernando Podio, was a recipient of the ANSI Meritorious Service Award in recognition of his many contributions to the ANSI Federation and the voluntary standardization community.)

Conformance Testing of Standard Biometric Interface Implementations

The existence of standards alone is not enough to demonstrate that products meet the technical requirements specified in the standards. Conformance testing captures the technical description of a specification and measures whether an implementation faithfully implements the specification. A conformance test suite implementation is test software that is used to ascertain conformance to a testing methodology described in a specification or standard. We support the development of national and international biometric standards and conformity assessment through active technical participation in the development of these standards, sponsorship of specific biometric standard projects (e.g., conformance testing methodologies for biometric technical interfaces), and the development of associated conformance testing architectures designed to test for conformance to a number of biometric standards. We have developed conformance test suites in support of the adoption and implementation of key biometric interface standards such as the BioAPI specification and Biometric Information Records conforming to Common Biometric Exchange Format Framework (CBEFF) standards. These records are able to transport metadata related to the biometric data that they contain as well as biometric data of any modality and security and integrity data.

In 2006 we released a Conformance Test Suite (CTS) developed to test implementations of ANSI INCITS 358-2002, the BioAPI specification. We cosponsored with other members of the national committee developing biometric standards (InterNational Committee for Information Technology Standards – INCITS M1) a conformance testing methodology standard for BioAPI. This standard was completed during 2007 and is about to be published as an American National Standard. The CTS implementation was developed using concepts and principles specified in the conformance testing methodology standard. This CTS was thoroughly tested with a number of commercially available vendor biometric subsystems for different modalities (e.g., face, iris and fingerprint recognition) claiming conformance to the BioAPI standard. The test results were successfully cross-validated with another similar CTS independently developed by DoD's Biometric Task Force. The NSTC Subcommittee on Biometrics and Identity Management listed the BioAPI CTS developments as one of the "Technology Successes" of 2006.

During 2007, we completed the development of a testing architecture and a CTS implementation to test CBEFF Biometric Information Records (BIR). The conformance testing architecture supports CTS for the three components of these BIRs including: (1) CBEFF headers, which contain metadata on the biometric data contained in the record such as the creator, validity period, biometric modality and format on the biometric data, the biometric product identifier, and the security and integrity options adopted for the data structure; (2) the Biometric Data Block, which contains the biometric data; and (3) Signature/security block, which contains integrity/encryption information. In addition, we developed the initial version of an advanced Conformance Testing Suite architecture that was designed to support CTS testing modules for the three elements of a CBEFF BIRs structure. This experimental architecture allows local testing of the three components of these BIRs as well as remote testing of the components of these BIR through Web services.

The Biometric Consortium

We have continued to participate in related consortia efforts such as the U.S. Biometrics Consortium (BC). The BC currently consists of hundreds of members representing over 60 government agencies, industry, and academia. NIST cochairs the BC with NSA. The BC sponsors an annual conference and technical workshops. The BC 2007 conference was held at the Baltimore Convention Center in September. The two-and-a-half day conference, recognized by attendees as one of the largest conferences dedicated to biometrics worldwide, had over 100 speakers from government, industry, and academia, and over 1000 participants.

National Standards Development Work

In late 2001, our biometric standards program helped establish INCITS M1. Since its inception, the purpose of INCITS M1 has been to ensure a high-priority focused and comprehensive approach in the United States for the rapid development and approval of formal national and international biometric standards, considered to be critical for U.S. needs, such as homeland defense, ID management, the prevention of identity theft, and for other government and commercial biometric-based personal verification or identification applications. CSD provides the Chair of INCITS M1, provides a Chair of one of the five INCITS M1 Task Groups, and actively participates in the development of its standards.

INCITS M1 is currently developing revision/amendment projects for its portfolio of biometric data interchange format standards to clarify original standards, address technology innovation and new customers' needs, and address the development of a new data interchange format for voice data. INCITS M1 is also developing conformance testing methodology standards for a number of the biometric data interchange formats. As stated above, we cosponsored with other INCITS M1 members the development of conformance testing methodology standards for key biometric technical interface standards such as the BioAPI specification and the Common Biometric Exchange Frameworks Format (CBEFF). The development of the BioAPI conformance testing methodology standard was completed and is in final public review before approval as an American National Standard. Development of the conformance testing methodology standard for CBEFF Biometric Information Records conforming to CBEFF instantiations is underway. INCITS M1 is also addressing the development of standards to support multi-biometrics and biometric fusion data, a biometric sample quality standard, and a standard to specify biometric performance and interoperability testing of data interchange format standards. NIST experts have been very active in all of these standards developments.

International Standards Development Work

In 2002, we successfully supported the establishment of Subcommittee 37-Biometrics under the ISO/IEC Joint Technical Committee 1 (ISO/IEC JTC 1/SC 37-Biometrics). INCITS M1 is the national Technical Committee responsible for representing the U.S. in JTC1/SC 37. CSD provides the Chair of SC37, and NIST/ITL provides a person to serve as the Chair of one of the six Working Groups operating under the Subcommittee.

JTC 1/SC 37's ongoing work includes 15 projects subdivided into 54 subprojects (standards and technical reports). They include revision and amendments of a number of data interchange format standards and technical interfaces to clarify original standards and to address technology innovations, and also address the development of two new data interchange formats for voice data and DNA. During 2007, the subcommittee made significant progress in the development of other biometric standards, including biometric performance testing, as well as reporting standards and biometric profiles for interoperability and data interchange. JTC 1/SC 37 has initiated the development of conformance testing methodology standards for the biometric data records specified in the biometric data interchange format standards (multi-part standard), as well as a multi-part technical report on cross-jurisdictional aspects of the use of biometrics, and a comprehensive harmonized biometric vocabulary.

NIST is very active in the development of JTC 1/SC 37's standards portfolio. Our experts, in collaboration with other U.S. national body members from government, industry, and academia, are examining innovations in biometrics technologies and personal recognition systems. We have taken steps to start the development of the "second generation" of international biometric standards. The standard development body is concurrently considering new projects to complement and enhance functionality of the existing standards and to meet new customers' needs.

Impact of biometric standards

A number of the "first generation" biometric standards are already being required by customers of personal authentication applications. Large organizations such as the International Civil Aviation Organization (ICAO) (for Machine Readable Travel Documents), the International Labour Office of the United Nations (for the Seafarers Identification Credential program) as well as the European Union (EU) have published requirements that include the use of international biometric standards developed by JTC 1/SC 37. The EU password specification working document describes solutions for chip-enabled EU passports, based on EU's Council Regulation on standards for security features and biometrics in passports and travel documents issued by member states. The specification relies on international standards, especially ISO standards and ICAO recommendations on Machine Readable Travel Documents, and includes specifications for biometric face and fingerprint identifiers; thus, the

specifications are underpinned by ISO standards resulting from the work of JTC 1/SC37. Several JTC 1/SC 37 national bodies refer to certain international standards developed by the subcommittee. Spanish e-Passports, for example, require face image data based on the face image recognition developed by JTC 1/SC 37.

In the United States, several organizations require selected biometric data interchange standards developed by JTC 1/SC 37. Examples include applications and tests performed by government organizations, private industry, and consortia. The Transportation Security Administration (TSA), a part of DHS, has issued guidance for use of biometric technology in airport access control systems and is performing tests to establish a qualified products list of biometric technologies which meet standards set forth in the aforementioned guidance. Products tested in TSA Qualified Product List (QPL) Testing include enrollment stations and biometric sensors/readers that can be deployed at access points to secure airport areas. The test requirements reference two parts of the multi-part standard developed by JTC 1/SC 37 on biometric performance testing and reporting. NIST used a part of this multi-part standard for the "Minutiae Interoperability Exchange Test (MINEX)" tests. The Registered Traveler Interoperability Consortium (RTIC) uses some of the JTC 1/SC 37 standards as well.

INCITS M1 biometric standards are also required in major U.S. Government programs, including the DHS/TSA Transportation Worker Identification Credential (TWIC), the DoD IT Standards Registry, the Personal Identity Verification (PIV) specification (NIST SP 800-76-1) and the Registered Traveler Technical Interoperability specification.

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

References:

❶ *"The National Biometrics Challenge"*, National Science and Technology Council, Subcommittee on Biometrics (now Subcommittee on Biometrics and Identity Management), August 2006.

❷ *"NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards"*, NSTC Subcommittee on Biometrics and Identity Management, September 7, 2007.

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

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

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

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

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

◆ design and development of IT systems and tools

◆ performance and quality of IT products and systems

◆ security of IT systems and information

◆ portability of application programs

◆ interoperability of IT products and systems

◆ unified tools and environments

◆ harmonized IT vocabulary

◆ user-friendly and ergonomically designed user interfaces.

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

◆ SC 06 - Telecommunications and Information Exchange Between Systems

◆ SC 17 - Cards and Personal Identification

◆ SC 27 - IT Security Techniques

◆ SC 37 - Biometrics

◆ JTC1 also has—

Technical Committee 68 – Financial Services

◆ SC 2 - Operations and Procedures including Security

◆ SC 4 - Securities

◆ SC 6 - Financial Transaction Cards, Related Media and Operations

◆ SC 7 - Core Banking

American National Standards Institute (ANSI) is a private, nonprofit organization (501(c)(3)) that administers and coordinates the 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, 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 information technology products and services. INCITS currently has more than 750 published standards.

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

◆ B10 – Identification Cards and Related Devices

◆ CS1 – Cyber Security

◆ E22 – Item Authentication

◆ M1 – Biometrics

◆ T3 – Open Distributed Processing (ODP)

◆ T6 – Radio Frequency Identification (RFID) Technology

As a technical committee of INCITS, CS1 develops 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

  ■ digital signatures

◆ Future service and applications standards supporting the implementation of control objectives and controls as defined in ISO 27001, in the areas of—

  ■ business continuity

  ■ outsourcing

◆ Identity management, including:

- identity management framework

- role-based access control

- single sign-on

◆ Privacy technologies, including:

- privacy framework

- privacy reference architecture

- privacy infrastructure

- anonymity and credentials

- specific privacy enhancing technologies.

The scope of CS1 explicitly excludes the areas of work on cyber security standardization presently underway in INCITS B10, M1, T3, T10 and T11; as well as other standard groups, such as the Alliance for Telecommunications Industry Solutions, the Institute of Electrical and Electronics Engineers, Inc., the Internet Engineering Task Force, the Travel Industry Association of American, 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 9 CS1 members are SC 27 document editors or coeditors on various standards projects, including Randy Easter of NIST for ISO/IEC 24759, Test Requirements for Cryptographic Modules. One CS1 member serves as Rapporteur for the Study Period on Secure System Design. All input from CS1 goes through INCITS to ANSI, then to SC 27. It 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. CS1 is making contributions on several new areas of work in SC 27, including study periods and new work item proposals on technical information system management audits, low power encryption, and signcryption, three-party entity authentication, responsible vulnerability disclosure, and secure system design.

Through its membership on CS1, where Dan Benigni serves as the nonvoting chair, and Richard Kissel is the NIST Primary with vote, NIST contributes to all CS1 national and international IT security standards efforts. NIST can also initiate IT security-related projects for national or international standardization through its membership on CS1. As an example, CSD staffer David Ferraiolo recently discussed initiating a new project in CS1 concerning an access control mechanism that can be embedded into operating systems. Dan Benigni also serves as CS1 Liaison to a new INCITS Study Group on Security Best Practices, whose charter is to study the security needs and requirements of the financial and insurance services industries, assess what is missing in current standards and practices, and make recommendations on an approach to create deployable best practices and frameworks for security in these industries.

CS1 has created a task group called CS1.1 RBAC, with one national standards project called "Requirements for the Implementation of Role-Based Access Control (RBAC)" INCITS Project 1794. This standard will provide implementation requirements for RBAC systems, which use RBAC components defined in INCITS 359-2004. The implementation requirements in this standard are intended to ensure the interchange of RBAC data (e.g., roles, permissions, users) and promote functional interoperability among RBAC services and applications. Within the next several months, this work will be ready for its first public review.

In addition, CS1 has recently created another national standards project, "Minimum Security Guidelines for Protecting Personal Identifiable Information and Sensitive Information Stored on and Exchanged between Information Systems." The project is expected to result in an ANSI-INCITS Technical Report. In the future, this document may be submitted as an input document to SC 27. The document will also take into account certain publications in the NIST SP 800 series and incorporate those aspects that apply to the scope of protection of personal identifiable information.

As regards international efforts, CS1 has consistently, efficiently, and in a timely manner responded to all calls for contributions on all international security standards projects in ISO/IEC JTC1 SC 27. Contributions from CS1 members have included NIST publications. For instance, FIPS 199 and 200 have been cited as contributions to ongoing work at the international level.

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

Systems and Network Security Technical Guidelines

Securing External Telework Devices

SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, is intended to help teleworkers secure the external devices they use for telework, such as personally owned desktop and laptop computers and consumer devices (e.g., cell phones, personal digital assistants [PDAs]). The publication, which was released for public comment in June 2007, focuses on security for telework involving remote access to an organization's nonpublic computing resources. It provides practical, real-world advice on securing telework computers' operating systems and applications and teleworkers' home networks, and it gives basic recommendations for securing consumer devices. The publication also provides tips on assessing the security of a device owned by a third party before deciding whether it should be used for telework.

SSL VPNs

SP 800-113, *Guide to SSL VPNs*, was released for public comment in August 2007. It seeks to assist organizations in understanding Secure Sockets Layer (SSL) Virtual Private Network (VPN) technologies. The publication makes recommendations for designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions. SP 800-113 provides a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also includes a comparison with other similar technologies such as Internet Protocol Security (IPSec) VPNs and other VPN solutions.

Storage Encryption for End User Devices

SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, was released for public comment in August 2007. The publication

is intended to assist organizations in understanding storage encryption technologies for end user devices, such as laptops, PDAs, smart phones, and removable media, and in planning, implementing, and maintaining storage encryption solutions. The publication provides practical, real-world recommendations for three classes of storage encryption techniques: full disk encryption, volume and virtual disk encryption, and file/folder encryption. It also discusses important security elements of a storage encryption deployment, including cryptographic key management and authentication.

Cell Phone Forensics

SP 800-101, *Guidelines on Cell Phone Forensics*, provides general principles and technical information to aid organizations in developing appropriate policies and procedures for preserving, acquiring, and examining digital evidence found on cell phones, and for reporting the results. Cell phones are an emerging but rapidly growing area of computer forensics. SP 800-101, which was published as final in June 2007, also explains the relationship between key aspects of cell phone technology and the operation and use of available forensic tools.

Securing Radio Frequency Identification (RFID) Systems

SP 900-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, was published as final in April 2007. This publication seeks to assist organizations in understanding the risks of RFID technology and security measures to mitigate those risks. It provides practical, real-world guidance on how to initiate, design, implement, and operate RFID solutions in a manner that mitigates security and privacy risks. The document also provides background information on RFID applications, standards, and system components to assist in the understanding of RFID security risks and controls. This document presents information that is independent of particular hardware platforms, operating systems, and applications. The emphasis is on RFID solutions that are based on industry and international standards, although the existence of proprietary approaches is noted when they offer relevant security features not found in current standards.

Wireless Security Using IEEE 802.11i

SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, was published as final in February 2007. The publication provides detailed information on the Institute of Electrical and Electronics Engineers (IEEE) 802.11i standard for wireless local area network (WLAN) security. IEEE 802.11i provides security enhancements over the previous 802.11 security method, Wired Equivalent Privacy (WEP), which has several well-documented security deficiencies. IEEE 802.11i introduces a range of new security features that are designed to overcome the shortcomings of WEP. This document explains these security features and provides specific

recommendations to ensure the security of the WLAN operating environment. It gives extensive guidance on protecting the confidentiality and integrity of WLAN communications, authenticating users and devices using several methods, and incorporating WLAN security considerations into each phase of the WLAN life cycle. The document complements, and does **not** replace, NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, and SP 800-48 Revision 1, *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*.

Secure Web Services

SP 800-95, *Guide to Secure Web Services*, seeks to assist organizations in understanding the challenges in integrating information security practices into Service Oriented Architecture (SOA) design and development based on Web services. SP 800-95, which was published as final in August 2007, also provides practical, real-world guidance on current and emerging standards applicable to Web services, as well as background information on the most common security threats to SOAs based on Web services. This document presents information that is largely independent of particular hardware platforms, operating systems, and applications. Supplementary security devices (i.e., perimeter security appliances) are considered outside the scope of this publication. Interfaces between Web services components and supplementary controls are noted as such throughout this document on a case-by-case basis.

Intrusion Detection and Prevention Systems (IDPS)

SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, was published as final in February 2007. It replaces SP 800-31, *Intrusion Detection Systems*. SP 800-94 provides guidelines for designing, implementing, configuring, securing, monitoring, and maintaining four classes of IDPS systems: network-based, wireless, network behavior analysis software, and host-based. It focuses on enterprise IDPS solutions, but most of the information in the publication is also applicable to standalone and small-scale IDPS deployments.

Computer Security Incident Handling Guide

SP 800-61 Revision 1, *Computer Security Incident Handling Guide*, was released for public comment in September 2007. It seeks to assist organizations in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. The publication includes guidelines on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents. SP 800-61 Revision 1 updates the original publication, which was released in 2004.

Border Gateway Protocol Security

SP 800-54, *Border Gateway Protocol Security*, introduces the *Border Gateway Protocol (BGP)*, explains its importance to the Internet, and provides a set of best practices that can help in protecting BGP. Best practices described in the publication are intended to be implementable on nearly all currently available BGP routers without the installation of additional hardware or software. SP 800-54 was published as final in July 2007.

Wireless Security for IEEE 802.11a/b/g and Bluetooth

SP 800-48 Revision 1, *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*, was released for public comment in August 2007. The publication provides an overview of wireless networking technologies and gives detailed information on two standards commonly used in office environments and by mobile workforces: Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g and IEEE 802.15.1, better known as Bluetooth. The publication seeks to assist organizations in reducing the risks associated with these forms of wireless networking. SP 800-48 Revision 1 updates the original version of SP 800-48, which was released in November 2002. SP 800-48 Revision 1 complements, and does not replace, SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*. People seeking information on IEEE 802.11i should consult SP 800-97.

E-mail Security

SP 800-45 Version 2, *Guidelines on Electronic Mail Security*, was published as final in February 2007. It is an update to the original guideline issued in 2002, which it replaces. The publication is intended to aid organizations in the installation, configuration, and maintenance of secure mail servers and mail clients. Topics covered include e-mail standards, e-mail encryption and signing, mail server application security, and e-mail content filtering. SP 800-45, Version 2, also gives recommendations for securing the e-mail server operating systems, applications, and content as well as the supporting network infrastructure.

Public Web Server Security

SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, was published as final in September 2007. SP 800-44, Version 2 is intended to aid organizations in the installation, configuration, and maintenance of secure public Web servers. It presents recommendations for securing Web server operating systems, applications, and content; protecting Web servers through the supporting network infrastructure; and administering Web servers securely. SP 800-44, Version 2 also provides guidelines on using

authentication and encryption technologies to protect information on Web servers. This publication replaces the original version of SP 800-44, which was released in 2002.

Active Content and Mobile Code

SP 800-28, Version 2, *Guidelines on Active Content and Mobile Code*, was released for public comment in August 2007. It provides an overview of active content and mobile code technologies currently in use and offers insights for making informed information technology (IT) security decisions on their application and treatment. SP 800-28, Version 2, gives details about the threats, technology risks, and safeguards for end user systems related to active content and mobile code. This publication replaces the original version of SP 800-28, which was released in 2001.

Common Vulnerability Scoring System (CVSS)

NIST Interagency Report (NISTIR) 7435, *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems*, was published as final in August 2007. CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. This publication defines and describes the CVSS standard, provides advice on performing scoring, and discusses how federal agencies can incorporate Federal Information Processing Standards (FIPS) 199 impact ratings into their CVSS scores to generate scores that are specifically tailored to particular federal agency environments.

Cell Phone Forensic Tools

NISTIR 7387, *Cell Phone Forensic Tools: An Overview and Analysis Update*, provides an overview of current forensic software tools designed for the acquisition, examination, and reporting of data residing on cellular handheld devices. It is a follow-on publication to NISTIR 7250, which originally reported on the topic, and includes several additional tools. NISTIR 7387, which was published as final in June 2007, reviews the capabilities and limitations of each tool in detail through a scenario-based methodology.

Extensible Configuration Checklist Description Format (XCCDF)

NISTIR 7275 Revision 2, *Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.3*, was published as final in June 2007. The publication describes XCCDF, which is a standardized XML format that can be used to hold structured collections of security configuration rules for a set of target systems. The XCCDF specification is designed to provide automated testing and scoring that can support FISMA compliance and other efforts. NISTIR 7275 specifies the data model and Extensible Markup Language (XML) representation for version 1.1.3 of XCCDF; the previous revision of NISTIR 7275 addressed version 1.1 of XCCDF.

HONORS AND AWARDS

Gold Medal Award for Distinguished Service

The Computer Security Division's Personal Identity Verification (PIV) Team was awarded the Department of Commerce Gold Medal Award for Distinguished Service for their leadership in producing the standards, guidelines, and test programs required to implement Homeland Security Presidential Directive (HSPD) 12. This effort required coalescing disparate United States Government requirements, reconciling diverse technical and policy interests, assessing competing technologies, inventing new methods of interoperability, and developing improved methods of identity verification. PIV team award recipients include, from left to right, **William Polk, Donna Dodson, William Barker, Teresa Schwarzhoff, William MacGregor, Ramaswamy Chandramouli, James Dray, Hildegard Ferraiolo,** and **Patrick Grother.** Not pictured is **Timothy Grance**.

Silver Medal Award for Exceptional Service

Ron Ross, as a member of a multiagency team, was awarded the Department of Commerce Silver Medal Award for Exceptional Service in the Personal and Professional Excellence Category for working in close coordination with a team from various components of the International Trade Administration over a two-year period to overturn Korean market barriers preventing U.S. information technology firms from participating in the one billion dollar Korean public and financial sectors.

Bronze Medal Award for Superior Federal Service

Murugiah Souppaya was recognized for his leadership in developing the Windows XP Security Consensus Benchmarks. He improved the security of millions of systems in the public and private sector. His efforts included developing and recommending significantly improved security settings, clearly documenting and explaining those settings, publishing supporting rationale, providing an automated mechanism to apply these settings, and engaging and leading a broad and diverse community to support and adopt those settings

FED 100 Award – Federal Computer Week

William MacGregor, pictured above as a member of the PIV team, was selected by Federal Computer Week to receive a 2007 "Fed 100" Award. The judges for these awards look for someone who has made a noticeable difference in an agency or in the community at large. Mr. MacGregor was recognized for leading the team that established 14 standards and guidelines for the PIV Card that federal employees and contractors are required to carry to comply with Homeland Security Presidential Directive 12. Under his leadership, the PIV team produced publications that defined the standards and specifications for the card topography, biometric interfaces, and middleware and management systems.

COMPUTER SECURITY DIVISION PUBLICATIONS – FY 2007

NIST Special Publications

SP 800-104	A Scheme for PIV Visual Card Topography	June 2007
SP 800-101	Guidelines on Cell Phone Forensics	May 2007
SP 800-100	Information Security Handbook: A Guide for Managers	October 2006
SP 800-98	Guidelines for Securing Radio Frequency Identification (RFID) Systems	April 2007
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	February 2007
SP 800-95	Guide to Secure Web Services	August 2007
SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)	February 2007
SP 800-90	Recommendation for Random Number Generation using Deterministic Random Bit Generators	March 2007
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	November 2006
SP 800-87	Codes for the Identification of Federal and Federally-Assisted Organizations	March 2007
SP 800-78-1	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	August 2007
SP 800-76-1	Biometric Data Specification for Personal Identity Verification	January 2007
SP 800-57	Recommendation for Key Management	March 2007
SP 800-56 A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	March 2007
SP 800-54	Border Gateway Protocol Security	June 2007
SP 800-53 Rev 1	Recommended Security Controls for Federal Information Systems	December 2006
SP 800-45, Ver 2	Guidelines on Electronic Mail Security	February 2007
SP 800-44, Ver 2	Guidelines on Securing Public Web Servers	September 2007

NIST Draft Special Publications

SP 800-113	Guide to SSL VPNs	August 2007
SP 800-111	Guide to Storage Encryption Technologies for End User Devices	August 2007
SP 800-110	Information System Security Reference Data Model	September 2007
SP 800-107	Recommendation for Using Approved Hash Algorithms	July 2007
SP 800-106	Randomized Hashing Digital Signatures	July 2007
SP 800-103	An Ontology of Identity Credentials, Part I: Background and Formulation	October 2006
SP 800-82	Guide to Industrial Control Systems (ICS) Security (Second public draft)	September 2007
SP 800-61 Rev 1	Computer Security Incident Handling Guide	September 2007
SP 800-55 Rev 1	Performance Measurement Guide for Information Security	September 2007
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems (Third public draft)	June 2007
SP 800-48 Rev 1	Wireless Network Security for IEEE 802.11 a/b/g and Bluetooth	August 2007
SP 800-44, Ver 2	Guidelines on Securing Public Web Servers	June 2007
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication	June 2007
SP 800-28 Rev 2	Guidelines on Active Content and Mobile Code	August 2007

Federal Information Processing Standards

FIPS 198-1	The Keyed-Hash Message Authentication Code (HMAC)	Draft, June 2007
FIPS 180-3	Secure Hash Standard (SHS)	Draft, June 2007
FIPS 140-3	Security Requirements for Cryptographic Modules	Draft, July 2007

NIST Interagency Reports

NISTIR 7435	The Common Vulnerability Scoring System (CVSS) and its Applicability to Federal Agency Systems	August 2007
NISTIR 7427	6th Annual PKI R&D Workshop: "Applications-Driven PKI" Proceedings	September 2007
NISTIR 7399	2006 Annual Report: Computer Security Division	April 2007
NISTIR 7387	Cell Phone Forensic Tools: An Overview and Analysis Update	March 2007
NISTIR 7359	Information Security Guide for Government Executives	January 2007
NISTIR 7358	Program Review for Information Security Management Assistance (PRISMA)	January 2007
NISTIR 7328	Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems (DRAFT)	September 2007
NISTIR 7275 Rev 2	Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.3	May 2007

Information Technology Laboratory Bulletins written by CSD

August 2007	Secure Web Services	
July 2007	Border Gateway Protocol Security	
June 2007	Forensic Techniques For Cell Phones	
May 2007	Securing Radio Frequency Identification (RFID) Systems	
April 2007	Securing Wireless Networks	
March 2007	Improving The Security Of Electronic Mail: Updated Guidelines Issued By NIST	
February 2007	Intrusion Detection And Prevention Systems	
January 2007	Security Controls For Information Systems: Revised Guidelines Issued By NIST	
December 2006	Maintaining Effective Information Technology (IT) Security Through Test, Training, And Exercise Programs	
November 2006	Guide To Securing Computers Using Windows XP Home Edition	
October 2006	Log Management: Using Computer And Network Records To Improve Information Security	

WAYS TO ENGAGE OUR DIVISION AND NIST

Guest Research Internships at NIST

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