

Computer Security Division



2003

Annual

Report



National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

TABLE OF CONTENTS

Welcome Letter	2
The Computer Security Division Responds to the Federal Information Security Management Act of 2002	3
Outreach, Awareness and Education	4
Security Management and Guidance	8
Security Testing and Metrics	14
Security Research and Emerging Technologies	16
Cryptographic Standards and Applications	26
Honors and Awards	32
Computer Security Division Publications – 2003	34
Ways to Engage Our Division & NIST	36



Welcome

For many years, the Computer Security Division has made great contributions to help secure our nation's sensitive information and information systems. Our work has paralleled the evolution of IT, initially focused principally on mainframe computers, to now encompass today's wide gamut of information technology devices. Our important responsibilities were re-affirmed by Congress with passage of the Federal Information Security Management Act (FISMA) of 2002 and the Cyber Security Research and Development Act of 2002.

Beyond our role to serve the Federal Agencies under FISMA, our standards and guidelines are often voluntarily used by U.S. industry, global industry, and foreign governments as sources of information and direction for securing information systems. Our research also contributes to securing the nation's critical infrastructure systems. Moreover, the Division has an active role in both national and international standards organizations in promoting the interests of security and U.S. industry.

We are very proud of our extraordinarily talented and knowledgeable co-workers in the Division, many of whom are recognized as leading professionals in their fields. Most have come to us from the private sector and other agencies, bringing with them a diverse set of perspectives and expertise, and a solid commitment to public service. We are proud to highlight their achievements in this report and note the honors and awards that were received this year celebrating their achievements.

Our key 2003 accomplishments include advancing development of our cryptographic standards toolkit, our E-authentication work, our management and technical security guidelines, and expanding our Cryptographic Module Validation Program. Our research efforts include advancing development of (1) better means of access controls, (2) means to secure personal digital assistants, and (3) specifications to promote smart card

interoperability and attendant security uses. The Division also added public and private security practices to our Computer Security Resource Center (CSRC) website (<http://csrc.nist.gov>), held an IT Security Capital Investment Planning Workshop, and updated Special Publication 800-38B specifying the RMAC algorithm to provide example vectors with the AES algorithm as the underlying block cipher. Many more projects and details are included in our report.

Along with many other NIST units, our Division is taking a significant budget cut in 2004. The work planned for 2004, as described in this report, therefore is very conditional. This budget cut will delay and curtail some of our planned work. We will, however, continue to engage federal agencies, industry, and academia to build stronger partnerships and leverage as many opportunities as possible.

As you browse this report of the Computer Security Division's activities for 2003, we hope you will want to learn more. We invite you to visit the Computer Security Resource Center (<http://csrc.nist.gov>) or to contact any of the Division experts noted in the report.

We hope that this annual report, our first, conveys the excitement and commitment to be found in NIST's Computer Security Division. We appreciate your interest in our Division.

Edward Roback
Division Chief

Alicia A. Clay
Deputy Division Chief

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 (FISMA), included duties and responsibilities for the Computer Security Division in Section 303 "National Institute of Standards and Technology." In 2003, we met the new requirements in the following ways:

- ◆ Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels – SP 800-37 *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, second public draft issued June 2003
- ◆ Guidelines recommending the types of information and information systems to be included in each category – FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*, public draft issued May 2003
- ◆ Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category – 800-53 *Security Controls for Federal Information Systems*, public draft to be issued FY 2004 first quarter
- ◆ Incident detection and handling guidelines – 800-61 *Computer Security Incident Handling Guide*, public draft issued September 2003
- ◆ Assistance – Agencies and Private Sector – NIST conducts substantial reimbursable and non-reimbursable assistance support, including many outreach efforts such as FISSEA, the Forum, the Small Business Corner, and the reimbursable program CSEAT
- ◆ Developing performance indicators/metrics -- 800-55 *Security Metrics Guide for Information Technology Systems*, released June 2003
- ◆ Evaluating security policy and technologies for federal use – private sector and national security systems -- Practices, Checklists, & Implementation Guides, NIAP & Product Testing (CCEVS and CMVP)
- ◆ Identification of national security systems guidelines -- 800-59 *Guideline for Identifying an Information System as a National Security System*, released August 2003
- ◆ Solicit recommendations of the Information Security and Privacy Advisory Board on draft standards and guidelines – Recommendations of the Board are regularly solicited at the quarterly meetings. The Board is in the process of issuing comments regarding FIPS 199 to Dr. Susan Zevin, Acting Director of NIST's Information Technology Laboratory.
- ◆ Annual NIST reporting requirement – Meeting this requirement begins with this report.



Outreach, Awareness and Education

GOAL ▶ *To promote awareness and understanding of information technology security.*

STRATEGY ▶ *The strategy to meet this goal is to focus on activities to support wider awareness of the importance and need for information technology (IT) security, promoting the understanding of IT security vulnerabilities and corrective measures, and in facilitating greater awareness of the Division's programs and projects.*

INTENDED OUTCOME AND BACKGROUND:

The Computer Security Division (CSD) is legislatively mandated to provide IT security standards and guidelines to federal government agencies. Providing useful and timely materials to the federal agencies, however, cannot be accomplished in a vacuum. In a world of growing inter-connectivity, it is crucial to stay abreast of IT security issues and happenings in industry and academia as well as in government. Consensus building with the IT industry, academia, and federal agencies allows us to provide quality products and services. At the same time, reaching out only to U.S. federal agencies and industry would be limiting usefulness needlessly. We, therefore, reach out to engage other governments, other levels of U.S. government, small and medium-sized businesses nationwide, and even directly to citizens.

Through a range of organizations and efforts, the CSD provides materials, information, and services useful from the agency level to the home-user level. Every Federal Information Processing Standard (FIPS) and Special Publication (SP) document produced by the CSD

has an open, public comment vetting process. The division houses a Web site that is a central repository for all of the materials and resources we have developed, as well as pointers to other types of IT security work and resources. The division also hosts several organizations that reach specific portions of the government and industry. These organizations are discussed in greater detail later in this report.

Our outreach efforts over the previous year have sought to go beyond previous years to find new and expanded ways we may reach out to our potential audiences. Membership in organizations has grown and been refreshed. Content on the division's Computer Security Resource Center (CSRC) Web site has grown and been updated. New workshop ideas were implemented.

The next year will see another time of growth of effort and new ideas to reach those that may benefit from our work, as well as those who can greatly contribute to initiatives. These partnerships are vital to our success in improving security world-wide.

ACCOMPLISHMENTS

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 Office of Management and Budget, 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 Board's membership draws from experience at all levels of information security and privacy work. The members' careers cover government – the Executive and Congressional branches, civil service and Senior Executive Service, and military service; industry – some of the largest corporations worldwide as well as small and medium-sized businesses; and academia – positions at some of the top universities in the Nation. The members' experience likewise covers a broad spectrum of activities – many

different engineering disciplines, computer programming, systems analysis, and mathematics; management positions; information technology auditing; legal experience (two Board members are attorneys); an extensive history of professional publications; and professional journalism. Members have worked (and in many cases, are continuing to work in their full time jobs) on the development and evolution of some of the most important pieces of information security and privacy in the Federal Government, including the Privacy Act of 1974, the Computer Security Act of 1987, the Federal Public Key Infrastructure (PKI) effort, and numerous e-Government services and initiatives.

This combination of experienced, dynamic, and knowledgeable professionals in 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.

The 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 Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act of 2002, 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 the Office of Management and Budget (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 membership of the Board consists of twelve individuals and a Chairperson. The Director of NIST approves membership appointments and appoints the Chairperson. Each Board member normally serves for a four-year term. The Board meets quarterly throughout the year, and all meetings are open to the public.

The Board has been very active in the past year. Early this year, the Board offered observations and recommendations to Mr. David Howe, Chief of Staff, Office of Cyberspace Security, on the September 2002 draft of the National Strategy to Secure Cyberspace. In January 2003 the Board issued a white paper entitled "Questions to Establish Potential Chilling Effects of the Digital Millennium Copyright Act (DMCA) on the Conduct of Computer Security Research." In April 2003 the Board conveyed its views on the ongoing development of the National Strategy to Secure Cyberspace to the Director of OMB. In August 2003 the Board again offered its observations and recommendations to the Director of OMB regarding the Federal Government e-Authentication initiative and the importance of establishing privacy policies and practices as mandatory components of technical models and systems being considered to support e-authentication services. The Board is currently considering additional matters on which it will seek to make appropriate recommendations during its December 2003 quarterly meeting.

To support its activities, the Board has also received numerous briefings from Federal, private sector, and international representatives on a wide range of privacy and security topics. These have included the Federal Government's e-Authentication effort, certification and accreditation standards and guidelines under development at NIST, certification of IT security profes-

sionals, the DMCA, privacy and e-government issues, and other emerging IT security issues.

The Board will be addressing several issues in the coming year, including the privacy and security implications of customer relation management and e-Authentication in the Federal Government.

<http://csrc.nist.gov/ispab/>
Contacts: Ms. Joan Hash
(301) 975-3357
joan.hash@nist.gov

Ms. Elaine Frye
(301) 975-2819
elaine.frye@nist.gov

FEDERAL INFORMATION SYSTEMS SECURITY EDUCATORS' ASSOCIATION (FISSEA)

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 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 throughout the federal government. 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. Contractors of these agencies and faculty members of accredited educational institutions are also welcome. There are no member-

ship fees for FISSEA; all that is required is a willingness to share products, information and experiences. Each year, an award is presented to a candidate selected as Educator of the Year, honoring distinguished accomplishments in information systems security training programs. FISSEA has a quarterly newsletter, an actively maintained Web site, and a listserve as a means of communication for members. The Computer Security Division (CSD) assists FISSEA with its operations by providing it staff support for several of its activities, and by being FISSEA's host agency. Members are also encouraged to participate in the annual FISSEA conference, and to serve on the FISSEA ad-hoc task groups.

FISSEA membership in 2003 spanned federal agencies, industry, military, contractors, state governments, academia, the press, and foreign organizations to reach 970 members. The 613 federal agency members represent 91 agencies from all three branches of government. The Educator of the Year Award for 2002 was presented to Patricia Black, U.S. Department of Treasury, at the FISSEA Annual Conference in March 2003. FISSEA also hosted its first free workshop, Developing Role-Based Training for System Administrators and Managers, in September 2003.

The 17th Annual FISSEA Conference will be held March 9th to 11th at the Inn and Conference Center at the University of Maryland in College Park Maryland. The 2003 Educator of the Year Award will be presented at the Conference. FISSEA will also be holding another free workshop in late spring 2004, with the possibility of more workshops to be held in the future.

<http://csrc.nist.gov/fisseas/>
Contacts: Mr. Mark Wilson
(301) 975-3870
mark.wilson@nist.gov

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

COMPUTER SECURITY RESOURCE CENTER (CSRC)

The Computer Security Resource Center (CSRC) is the Computer Security Division's Web site. The CSD uses the CSRC to encourage broad sharing of information security tools and practices, to provide "one-stop shopping" for information security standards and guidelines, and to identify and link key security web resources to support the industry. The CSRC is an integral piece to all of the work we currently conduct and produce. It is our repository for anyone, public or private sector, wanting access to our documents and information. It serves as a vital link between our division and the various groups we wish to reach.

In the last year the CSRC had over 19.1 million requests – an average of over 1.5 million requests per month. Each document released for public comment or published through our division has been posted to the CSRC. Updates have been made to a large number of areas of the site as work within the division has changed or been developed. And in the summer of 2003 the CSRC began an evaluation and analysis project that will allow the division to deal with issues of scale, organization, and volume as CSRC has quickly grown well beyond its originally conceived size.

The CSRC will continue to grow and be updated in 2004. It is anticipated that the usefulness of the site will be further enhanced from the results of the evaluation and analysis project.

<http://csrc.nist.gov/>
Contacts: Ms. Joan Hash
(301) 975-3357
joan.hash@nist.gov

Mr. Patrick O'Reilly
(301) 975-4751
patrick.oreilly@nist.gov

SMALL & MEDIUM-SIZED BUSINESS OUTREACH

What do a business's invoices have in common with email? If the business does both on the same computer, they may want to think more about computer security. Payroll, proprietary information, client or employee data – information is essential to a business's success. A computer failure or other system breach could cost a business anything from its reputation to its competitive advantage. The small business owner who recognizes the threat of computer crime and who 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. However, over 95 percent of all U.S. businesses are small and medium-sized 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 cannot always justify an extensive security program, or often a single full time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs.

The difficulty for these organizations is to identify needed/cost-effective security mechanisms and obtain training that is practical and cost effective. Such organizations also need to become more educated consumers in terms of security, so that their limited security 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) have entered into a Co-sponsorship Agreement for the purpose of

conducting a series of regional meetings on IT security for small businesses. NIST hosts the meetings with SBA and FBI as cosponsors. The purpose of the meetings is to have individuals knowledgeable in information technology (IT) security 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 IT personnel can apply directly or use to task contractor personnel.

In 2003 the SMB outreach effort focused on expanding opportunities to reach small businesses in new ways. For the second year, a Computer Security Division representative has attended the Annual Small Business Development Centers Conference to reach out to this public-private organization sponsored by SBA. The CSD also now contributes to SBA Solutions, a free monthly newsletter co-sponsored by SBA and Staples. This newsletter is sent to small businesses to help with a number of issues, including "cyber security" tips. This newsletter is freely available on the Web, and has a mail distribution of approximately 25,000. The Web presence of the SMB outreach project has also expanded to include a site, the Small Business Corner, dedicated to housing informational resources for small businesses.

The next year will see several regional workshops hosted across the country, including Kansas City and Orlando. Further development of our Web site is planned. Discussions are also beginning with SBA and the FBI to determine new avenues this outreach project may take.

<http://csrc.nist.gov/securebiz/>
<http://sbc.nist.gov/>
 Contacts: Mr. Richard Kissel
 (301) 975-5017
 richard.kissel@nist.gov

Ms. Tanya Brewer-Joneas
 (301) 975-4534
 tbrewer@nist.gov

FEDERAL COMPUTER SECURITY PROGRAM MANAGERS' FORUM

The Federal Computer Security Program Managers' Forum (Forum) is an informal group of over five hundred members sponsored by NIST to promote the sharing of computer security information among federal agencies. The Forum strives to provide an ongoing opportunity for managers of federal computer security programs to exchange computer security materials and information of use to other programs in a timely manner, build upon the experiences of other programs, and reduce possible duplication of effort; to provide an organizational mechanism for NIST to exchange information directly with federal agency computer security program managers in fulfillment of its leadership mandate under the Federal Information Security Management Act (FISMA); to establish and maintain relationships with other individuals or organizations that are actively addressing computer security issues within the federal government; and to establish and maintain a strong proactive stance identifying and resolving strategic and tactical computer security issues involved in the development and application of new and emerging information technologies.

The Forum hosts the Federal Agency Security Practices (FASP) Web site, maintains an extensive e-mail list, and holds an annual conference and bi-monthly 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)]. A NIST staff person serves as the Chairperson. The Forum is assisted by a Steering Committee, which helps plan meetings by identifying topics and speakers of interest to the

members. NIST serves as the secretariat of the Forum, providing necessary administrative and logistical support. Participation in Forum meetings is open to federal government employees who participate in the management of their organization's computer security program. There are no membership dues.

Topics of discussion at Forum meetings in the last year have included briefings on certification and accreditation, wireless communications, status reports from the Office of Management and Budget (OMB), the General Accounting Office (GAO), and the Department of Homeland Security (DHS), as well as half-day workshops on developing security metrics and using the new NIST developed automated security self-evaluation tool.

In the next year there are plans to have a half-day workshop on automated tools that are being employed by agencies, and briefings on agency implementation of their certification and accreditation program, and security training and awareness program.

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



Security Management and Guidance

GOAL ▶ *To improve information technology security management.*

STRATEGY ▶ *The strategy to meet this goal is to provide federal agencies with relevant, timely, and useful computer security policy and management tools.*

INTENDED OUTCOME AND BACKGROUND:

The intended outcome for our Security Management and Guidance area is to assist managers at all levels that deal with, or have ultimate responsibility for, information technology (IT) security programs in understanding the activities that must be initiated and completed to develop a sound information security program. This can include an awareness of and understanding of how to deal with new issues solely from a management view, and how to effectively apply NIST guidelines and recommendations.

Information security is an integral element of sound management. Information and computer systems are often critical assets that support the mission of an organization. Protecting them can be as critical 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.

This area of work collaborates with a number of entities. Federally, we collaborate with the Office of Management and Budget (OMB), the General Accounting 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, and public and private organizations.

During the coming year new initiatives will be completed in support of: the Healthcare Information Portability and Accountability Act (HIPAA), integrating security into the capital planning and investment control process, certification and accreditation, the Federal Information Security Management Act (FISMA) directives for Fiscal Year 2004 (FY04), extended outreach initiatives and information security training, awareness and education. Key to success of the program is our ability to interact with a broad constituency-federal and non-federal, in order to ensure that our program is consistent with national objectives related to or impacted by information security.

ACCOMPLISHMENTS

SECURITY CERTIFICATION AND ACCREDITATION (C & A) PROJECT

It is essential that agency officials have the most complete and accurate information possible on the security status of their information systems in order to make credible, risk-based decisions on whether to authorize operation of those systems. Security evaluations are detailed and comprehensive assessments of the technical and non-technical aspects of information systems and networks in operational environments by security professionals. These provide senior executives with the necessary information to authorize the secure operation of those systems and networks. The management responsibilities required by law of executive agencies presume that responsible agency officials understand the risks and other factors that could adversely affect their missions. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the

agency and to accomplish the agency's stated missions with what OMB Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

System security accreditation is the official management decision to authorize operation of an information system. This authorization, given by a senior agency official, is applicable to a particular environment of operation, and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, remaining after the implementation of an agreed upon set of security controls. By accrediting an information system, the agency official is not only responsible for the security of the system but is also accountable for adverse impacts to the agency if a breach of security occurs. Security accreditation, which is required under OMB Circular A-130, provides a form of quality control and challenges managers and technical staff at all levels to implement the most effective security controls and techniques, given technical constraints, operational constraints, cost and schedule constraints, and mission requirements.

In addition to risk assessments and security plans, security evaluation also plays an important role in the security accreditation process. It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make credible, risk-based decisions on whether to authorize operation of those systems. This information and supporting evidence for system authorization is often developed during a detailed security review of the information system, typically referred to as *security certification*. Security certification is the comprehensive evaluation of the management, operational, and technical

security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls.

The results of the security certification are used to reassess the risks and update the security plan for the information system—thus, providing the factual basis for the authorizing official to render the security accreditation decision. By accrediting the information system, the agency official accepts the risk associated with it and the implications on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Formalization of the security accreditation process ensures that information systems will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically and whenever there is a significant change to the system or its environment.

The Computer Security Division is currently revising its 1983 Federal Information Processing Standard (FIPS) 102, *Guidelines for Computer Security Certification and Accreditation*. While the initial goal of the effort is to develop a methodology/approach for use by Federal, State, and Local governments, significant effort will be made to obtain input and consensus from the commercial sector to achieve an additional goal that the methodology/approach become an industry-wide standard for the assessment of a systems IT security (e.g., used by commercial sector organizations, adopted by cyber-insurance companies and used as the basis of issuing cyber-insurance policies). The guidelines/procedures incorporate International Organization of Standardization (ISO) 17799 as it applies to systems.

The security C&A guideline is being proposed in the context of a broader security framework for categorizing the criticality of an IT system; and for selecting and assessing/verifying the effectiveness of a system's security controls on a continuing basis. Figure 1 shows how the elements of this project are designed to fit into the life cycle of a system.

Final versions of Special Publication 800-37 *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems* and FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* are due in early FY 04. Draft versions will be issued during FY 04 of Special Publications 800-53 *Security Controls for Federal Information Systems*, 800-53A *Guide for Assessing the Security Controls in Federal Information Systems*, and 800-60 *Guide for Mapping Types of Information and Information Systems to Security Categories*.

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

SENSITIVITY STANDARDS AND GUIDELINES

The E-Government Act of 2002 (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), tasked NIST with responsibilities for standards and guidelines, including the development of:

- ◆ Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- ◆ Guidelines recommending the types of information and information systems to be included in each category;
- ◆ and; Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category.

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. Subsequent NIST standards and guidelines will address the second and third tasks cited.

FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

FIPS Publication 199 defines three levels of *potential impact*—low, moderate, and high—on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The security category of an information type can be associated with both user information and system information and can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system. Establishing an appropriate security category of an information type essentially requires determining the *potential impact* for each security objective associated with the particular information type.

Special Publication 800-59 *Guideline for Identifying an Information System as a National Security System* provides guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system.

Except for national security systems as defined by FISMA, the Secretary of Commerce is responsible for prescribing standards and guidelines pertaining to Federal information systems on the basis of standards and guidelines developed by NIST. The Committee on National Security Systems (CNSS) along with Federal agencies that operate systems falling within the definition of national security systems provide security standards and guidance for national security systems. In addition to defining the term *national security system* FISMA amended the NIST Act, at 15 U.S.C. 278g-3(b)(3), to require NIST to provide guidelines for identifying an information system as a national security system. As stated in the House Committee report, "This guidance is not to govern such systems, but rather to ensure that agencies receive consistent guidance on the identification of systems that should be governed by national

security system requirements." (Report of the Committee on Government Reform, U. S. House of Representatives, Report 107-787, November 14, 2002, p. 85.)

Accordingly, the purpose of this document is not to establish requirements for national security systems, but rather to assist agencies in determining which, if any, of their systems are national security systems as defined by FISMA and are to be governed by applicable requirements for such systems, issued in accordance with law and as directed by the President.

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

SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS

The selection of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization. Security controls are the management, operational, and technical safeguards and countermeasures prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information. There are three important questions that should be answered by organization officials when addressing the security considerations for their information and information systems:

- ◆ What security controls are needed to adequately protect the information and information system that supports the operations and assets of the organization in order to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?

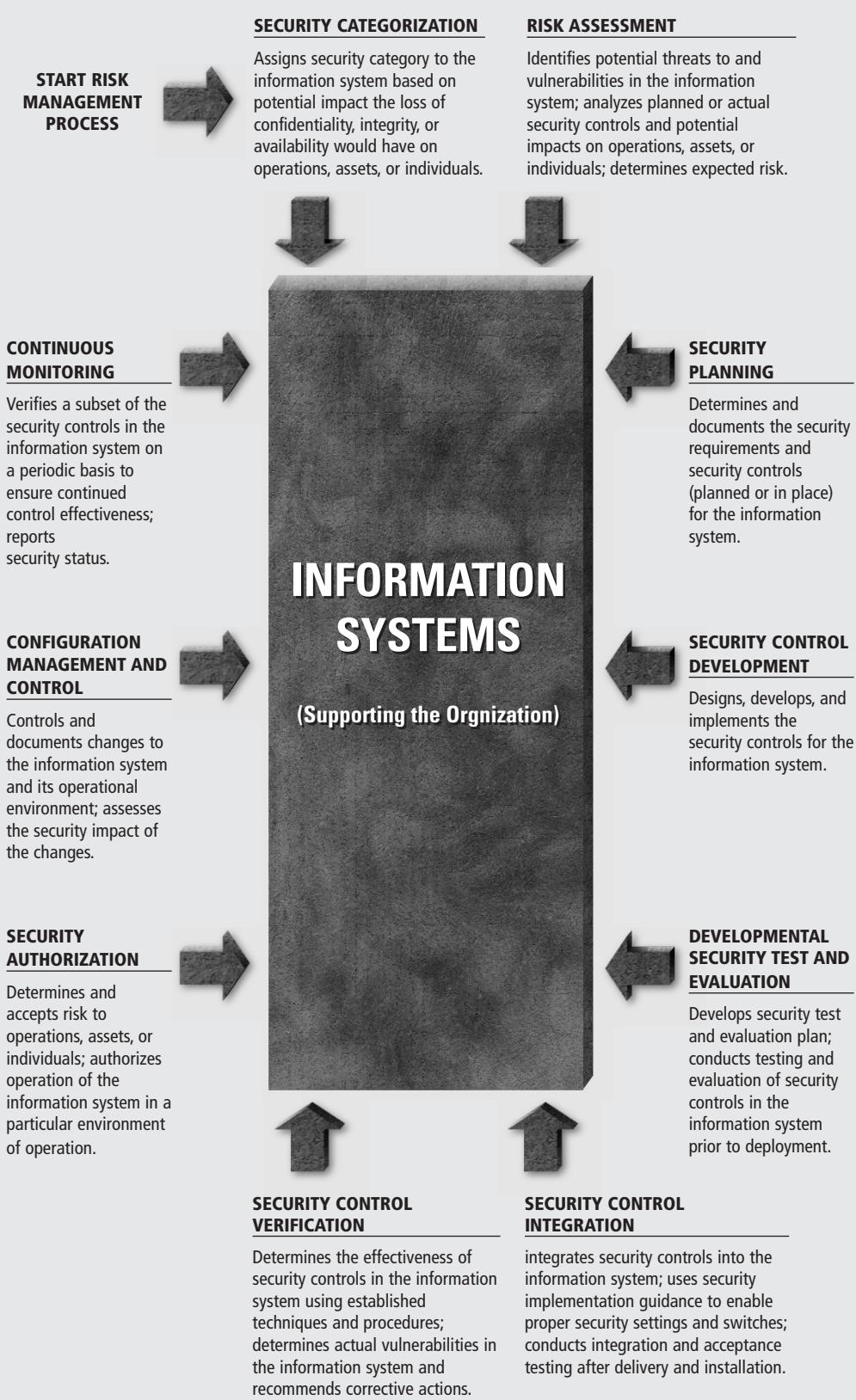
- ◆ Have the selected security controls been implemented or is there a realistic plan for their implementation?
- ◆ What is the desired level of assurance, (i.e., grounds for confidence), that the selected security controls, as implemented, are effective in their application?

The answers to these questions cannot be given in isolation. They must be given in the context of an information security program for the organization that identifies, controls, and mitigates risks to its information and information systems. During the last year we have worked to create a list of security controls to be recommended for use by organizations in protecting their information systems in conjunction with and as part of a well-defined information security program.

In an attempt to create the most technically sound and broadly applicable set of security controls for information systems, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, and intelligence communities as well as controls defined by national and international standards organizations. The objective of NIST Special Publication 800-53 is to provide a sufficiently rich set of security controls that satisfy the breadth and depth of security requirements for information systems and that are consistent with and complementary to other established security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of the respective organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated

FIGURE 1: INFORMATION SECURITY PROGRAM ACTIVITIES



security requirements. The security control objectives and control descriptions within the catalog facilitate the development of verification techniques and procedures that can be employed during testing and evaluation to demonstrate control effectiveness in a consistent and repeatable manner—thus, contributing to the organization's confidence that there is ongoing compliance with security requirements.

Federal agencies will be required to use FIPS Publication 199 standards to define security categories for their information systems. The recommendations for baseline (minimum) security controls from Special Publication 800-53 can subsequently be used as a starting point for and input to the organization's risk assessment processes and the development of security plans for those information systems. While the FIPS Publication 199 security categorization associates the operation of the information system with a "worst-case" impact on an organization's operations and assets (providing an upper bound on risk), the incorporation of refined threat and vulnerability information during the risk assessment process facilitates the tailoring of the baseline security controls to address organizational needs and tolerance for risk. Deviations from the recommended baseline security controls should be documented (along with supporting rationale) in the security plan for the information system. The use of security controls from Special Publication 800-53 and the incorporation of baseline (minimum) controls as a starting point in the control selection process facilitate a more consistent level of security in an organizational information system. At the same time it offers the needed flexibility to fine tune and adjust the controls based on specific organizational policy and requirements documents, particular conditions and circumstances, known threat and vulnerability information, or tolerance for risk to the organization's operations and assets.

Draft versions of Special Publication 800-53 will be published in 2004.

<http://csrc.nist.gov/sec-cert/ca-controls.html>

Contacts: Dr. Ron Ross
(301) 975-5390
rross@nist.gov

Mr. Gary Stoneburner
(301) 975-5394
gary.stoneburner@nist.gov

PRACTICES, CHECKLISTS, & IMPLEMENTATION GUIDES

Today's federal networks and systems are highly interconnected and interdependent with non-federal systems. Protection of the Nation's critical infrastructure 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 be applied to enhance the overall performance of Federal information security programs. The Computer Security Division (CSD) is 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 (CIP) and security. CSD was asked to undertake the transition of this pilot effort to an operational program. As a result, NIST developed the FASP Web site. The FASP site contains agency policies, procedures and practices; the CIO pilot BSPs; and, a Frequently-Asked-Questions (FAQ) section. The FASP site differs from the BSP pilot in material provided and in 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 technology (IT) security information and IT 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, 38 practices and examples have been added to the collection bring the total to 115.

One of the newer features added to the FASP Web site are IT product specific checklists for settings and configurations. These checklists are discussed more fully earlier in this report. These checklists are recommendations, not mandatory requirements, and are offered freely to IT professionals. These checklists are not to be seen as an endorsement by NIST for any products, but as potential aids in securing certain products.

Also in the past year, the CSD has invited public and private organization to submit their information security practices for consideration to be included in the list of practices maintained on the Division's web site, the Computer Security Resource Center (CSRC). Nominated candidate policies and procedures may be submitted to NIST in any area of information security including, but not limited to: 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 (to include specific course and awareness materials), and security planning. Current participants include Computer Associates, the Internet Security Task Force, Microsoft, the SANS Institute, and the Carnegie Mellon University CERT Coordination Center.

The coming year will see an effort to greatly expand each of the parts of this project. We are currently identifying robust sources for each of these elements, and plan to expand the number of resources available to Federal Agencies.

<http://csrc.nist.gov/pcig/>
 Contact: Ms. Marianne Swanson
 (301) 975-3293
 marianne.swanson@nist.gov

COMPUTER SECURITY EXPERT ASSIST TEAM

The Computer Security Division's Computer Security Expert Assist Team (CSEAT) was established to improve federal critical infrastructure protection planning and implementation efforts by assisting governmental entities in improving the security of their IT assets. The CSEAT provides an independent review of the maturity of an agency's IT security program. CSEAT accomplishes this by performing a review of an agency's computer security program. The review is based upon a combination of proven techniques and best practices and results in an action plan that provides a federal agency with a roadmap to cost-effectively enhance the protection of the information systems assets. The CSEAT has three primary purposes: to assist agencies in improving the security of federal IT systems; to help reduce disruption of critical federal systems/services; and to improve federal agency CIP planning and implementation efforts. The CSEAT helps Federal agencies understand how to protect information systems, identify and fix existing vulnerabilities, and prepare for future security threats. The CSEAT also facilitates exchange of best security practices among government agencies and between the government and private sector.

The CSEAT review, which is not an audit or an inspection, begins with an assessment of the maturity of the agency's IT security program. This includes the agency's IT security policies, procedures, and security controls implementa-

tion and integration across all business areas. CSEAT performs a comparable review of the agency's organizational structure, culture, and business mission. After the assessment is performed, the CSEAT documents issues identified during the assessment phase and provides corrective actions associated with each issue. These corrective actions are then provided as a prioritized action plan for the agency to use to improve their computer security program. The resulting action plan is weighted to provide the agency the greatest improvements most cost effectively. The corrective actions CSEAT identifies include the time frame for implementation and the projected resource impact. The action plan can readily be used to develop scopes of work for quick "bootstrapping" of the cyber security program.

A CSEAT review focuses on nine primary review areas, each of which were derived from a combination of NIST 800-26 Self-Assessment Guide for Information Technology Systems as supplemented by other criteria from requirements and guidance such as NIST Special Publication 800-18 Guide for Developing Security Plans for Information Technology Systems and Office of Management and Budget (OMB) guidance on the development of the Federal Information Security Management Act (FISMA) annual summary.

In 2003, several CSEAT reviews were completed, the supporting CSEAT database redesigned to provide more comprehensive analytical and reporting functions and the option model for the customer was adjusted to be more streamlined. Work was also initiated to do the necessary analysis to modify the criteria based on the recent release of Special Publication 800-53.

<http://cseat.nist.gov>
 Contacts: Ms. Joan Hash
 (301) 975-3357
 joan.hash@nist.gov
 Ms. Pauline Bowen
 (301) 975-2938
 pauline.bowen@nist.gov

AUTOMATED SECURITY SELF-EVALUATION TOOL – ASSET

An important element of measuring the status of IT security within an organization is to perform routine self-assessments of an organization's IT systems. There are many methods and tools available to help agency officials determine the current status of their security programs relative to existing policy. Ideally many of these methods and tools would be implemented on an ongoing basis to systematically identify programmatic weaknesses and, where necessary, establish targets for continuing improvement. In testimony given on November 19, 2002, before the House Committee on Government Reform, the Associate Director for Information Technology and Electronic Government, Office of Management and Budget described eight achievements that have been made toward improving the Federal government's IT security. One of the achievements was the development of the NIST Automated Security Self-Evaluation Tool (ASSET), which automates the process of completing a system self-assessment. ASSET will assist organizations in completing the self-assessment questionnaire contained in NIST Special Publication 800-26 *Security Self-Assessment Guide for Information Technology Systems*. ASSET is provided to federal agencies as a cost-free tool.

ASSET was first developed and released in 2002. The past year has seen several developments, including a FISMA reporting template and an updated ASSET v1.4 being released in early October 2003. The CSD held several training sessions during 2003, and will continue to hold training sessions in 2004. More updates are under development that will result in a new 2.0 version being released in early 2004.

<http://csrc.nist.gov/asset/>
 Contact: Ms. Marianne Swanson
 (301) 975-3293
 marianne.swanson@nist.gov



Security Testing and Metrics

GOAL ▶ *To make systems and networks more secure.*

STRATEGY ▶ *The strategy to meet this goal is to provide federal agencies, industry, and the public with a proven set of IT security services based upon sound testing methodologies and test metrics.*

INTENDED OUTCOME AND BACKGROUND:

The intended outcome for this area is to establish more secure systems and networks by developing, managing and promoting security assessment tools, techniques, services, and supporting programs for testing, evaluation and validation; to establish security-specific criteria for laboratory accreditation; to produce guidance on the use of evaluated and tested products; to conduct research to address assurance methods and system-wide security and assessment methodologies; to conduct security protocol validation activities; and to establish appropriate coordination with assessment-related activities of voluntary industry standards bodies and other assessment regimes. Our testing-focused activities include the validation of cryptographic modules and cryptographic algorithm implementations, Common Criteria (CC) evaluation and validation programs, international recognition arrangements, testing laboratory accreditation, automated security testing, and test suite development, industry forums, and education, training, and outreach programs.

Activities in this area have historically, and continue to, involve large amounts of collaboration and the facilitation of relationships with other entities. The 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 Office of Management and Budget, the Social Security Administration, the United States Postal Service, the Department of the Treasury, the Department of Veterans Affairs, the Department of Transportation, the Department of Justice, the Federal Aviation Administration, and the National Voluntary Laboratory Accreditation Program. The list of industry entities that have worked with the Division in this area is long, and includes the American National Standards Institute (ANSI), Oracle, CISCO, Hewlett-Packard, Lucent Technologies, Microsoft, IBM, VISA, Mastercard, Amex, Computer Associates, RSA Security Inc., Sun Microsystems, Network Associates, Entrust, and Silicon Graphics. The Division also has collaborated at the global level with Canada, the United Kingdom, France, Germany, and Korea in this area.

ACCOMPLISHMENTS

LABORATORY ACCREDITATION

The goals of this project are to accredit fully qualified Common Criteria Testing laboratories and Cryptographic Module Testing laboratories, and to promote the technical competence of accredited and applicant laboratories. Vendors use independent, National Voluntary Accreditation Laboratory Accreditation Program (NVLAP) accredited testing laboratories. This project develops new methods of proficiency testing for accreditation and re-accreditation of these laboratories, as well as continuous training opportunities for laboratories. This leads to consistent evaluation and validations for use by Federal agencies and the private sector, and to highly qualified accredited labs.

In 2003, one Common Criteria testing lab and five Cryptographic Module testing labs were re-accredited. One laboratory was accredited for Cryptographic Module Testing, and two new accreditations were issued for Common Criteria Testing. Revisions were made to the NIST Handbook 150-17 NVLAP Cryptographic

Module Testing. A testing artifact was also developed for Federal Information Processing Standard (FIPS) 140-2 Level 3 hardware testing.

Currently there are seven labs accredited to perform Cryptographic Module testing: four in the United States, two in Canada, and one in the United Kingdom. Six labs are to be re-accredited in 2004, and four new labs will be accredited: two in the U.S., two internationally. Five Common Criteria testing labs are due to be re-accredited in 2004, and three new labs are in the process to be accredited.

<http://ts.nist.gov/ts/htdocs/210/214/214.htm>

Contacts: Mr. Jeffrey Horlick
Standards Services Division
(301) 975-4020
jeffrey.horlick@nist.gov

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

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP)

The goals of this project are to improve the security and technical quality of cryptographic products, to provide U.S., Canadian, and U.K. Federal agencies with a security metric to use in procuring cryptographic equipment, and to promote the use of tested and validated cryptographic algorithms, modules, and products. This program is a collaborative one that involves the Computer Security Division and the Communication Security Establishment (CSE) of the Canadian Government. All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP).

Federal agencies, industry, and the public now 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 are used in products and systems to provide security services such as confidentiality, integrity, and authentication. Though 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 cryptographic algorithms against established standards is essential to provide security assurance.

Under this program, vendors of cryptographic modules use independent private sector, accredited testing laboratories to have their modules tested. This program provides Federal agencies – U.S., Canada, and U.K. – with confidence that a validated cryptographic product meets a claimed level of security. The program validates a wide variety of modules including secure Internet browsers, secure radios, tokens, and products supporting Public Key Infrastructure and electronic commerce. To give a sense of the quality improvement that the program achieves, consider that our statistics from the testing laboratories show that 48 percent of the modules 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 350 certificates have been issued for validated products by the CMVP, representing over 100 vendors. Over 90 of these certificates were issued during 2003. The Division initiated work this past year in the

International Organization for Standardization for the international adoption of Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. The Cryptographic Algorithm Validation System (CAVS) was designed and developed. This new system is used by the CMVP testing laboratories to test and validate all cryptographic algorithm implementations contained in FIPS 140-2 validated modules. Previously the laboratories had to run each algorithm test individually, but now may run CAVS as an umbrella system. This year also saw the development of the Advanced Encryption Standard (AES) test suite and the enhancement of the Digital Encryption Standard/Triple Digital Encryption Standard (DES/TDES) validation tests to include multi-block testing.

One goal for the next year is to have FIPS 140-2 established as an International Organization of Standardization (ISO) standard – ISO 19790. The Third Cryptographic Module Validation Program Workshop & Conference is being planned for 2004. The development of Key Establishment and Key Transport validation test suites, as well as Validation Test Suites for new algorithms/protocols, is slated for this coming year. Research will also continue to be conducted into new areas, particularly wireless, JAVA, and FIPS 140-2 Level 5.

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

Security Research and Emerging Technologies

GOAL ▶ *To support and conduct research in order to enhance information technology security.*

STRATEGY ▶ *The strategy to meet this goal is to focus on the research necessary to understand and enhance the security utility of new technologies while also working to identify and mitigate vulnerabilities.*

INTENDED OUTCOME AND BACKGROUND:

The mission of our 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; to 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; and to transfer new technologies to industry, produce new standards, develop tests, test methodologies, and assurance methods.

Most people in the U.S. today are aware of the speed with which technology, particularly computer-related technology, has been progressing and changing over the last decade. What was once considered "fast," "powerful," and "flexible" in computers is now antiquated in many cases. Every day new developments, new products, new advances in technology and science, and new vulnerabilities change the face of IT security. The time between a vulnerability in software being announced to the public and an exploitation of that vulnerability is measurable in days and hours.

To keep pace with the rate of change in information technology (IT) technologies we conduct a large of amount of research into existing and emerging technologies. We develop prototypes, reference implementations, and demonstrations. Some of the many topics we research include smart card infrastructure and security, wireless and mobile device security, access control and authorization management, Internet Protocol security, intrusion detection systems, quantum information system security and quantum cryptography, and vulnerability analyses. Our research helps fulfill specific needs by the Federal Government. We collaborate extensively with government, academia, and private sector entities. These have recently included: International Business Machines (IBM) Corporation, Microsoft Corporation, Sun Microsystems, the Boeing Company, Intel Corporation, Lucent Technologies, Oracle Corporation, MITRE, the SANS Institute, the University of Maryland, Ohio State University, the University of Tulsa, George Mason University, Rutgers University, Purdue University, George Washington University, the University of West Florida, University of California – San Diego, University of Maryland – Baltimore County, the National Security Agency, the Department of Defense, the U.S. Navy Research Laboratory, the Defense Advanced Research Projects Agency, the Department of Justice, and others.

ACCOMPLISHMENTS

WINDOWS 2000 PROFESSIONAL SYSTEMS ADMINISTRATION GUIDANCE

It is a complicated, arduous, and time-consuming task for even experienced system administrators to determine a reasonable set of security settings for a complex operating system. The Computer Security Division (CSD) sought to make this task simpler, easier, and more secure. In partnership with major segments of the security community, we helped develop, review and test the Windows 2000 Professional (Win2K Pro) consensus baseline settings. Implementation of these settings can make a substantial improvement in the security posture of Win2K Professional systems and hence markedly reduce vulnerability exposure.

The *Systems Administration Guidance for Windows 2000 Professional* (NIST Special Publication 800-43) is intended to assist the users and system administrators of Windows 2000 Professional systems in configuring their hosts by providing configuration templates and security checklists. The guide provides detailed information about the security features of Win2K Pro, security configuration guidelines for popular applications, and security configuration guide-

lines for the Win2K Pro operating system. The guide documents the methods that the system administrators can use to implement each security setting. The principal goal of the document is to recommend and explain tested secure settings for Win2K Pro workstations with the objective of simplifying the administrative burden of improving the security of Win2K Pro systems. This document was published in November 2002.

The special publication was developed by the CSD. We started with some excellent material developed by the National Security Agency (NSA) and the broader IT security community. Development of the NIST security templates was initially based in part on the NSA's Win2K Pro guidance. We examined the NSA settings and guidance, and built on the material they developed. The CSD conducted extensive analysis and testing of the NSA settings, substantially extended and refined the NSA template settings, and developed additional template settings. Detailed explanatory material for the template settings, Win2K Pro security configuration, and application specific security configuration guidance was then developed. Subsequently, CSD led the development of a consensus baseline of Win2K security settings in collaboration with the public and private sectors, specifically NSA, the Defense Information Systems Agency (DISA), the Center for Internet Security (CIS), and the SysAdmin Network Security Institute (SANS). Microsoft also provided valuable technical commentary and advice. The General Services Administration has also reviewed and concurred with the baseline.

Looking ahead, in conjunction with our partners and with the support of the Department of Homeland Security, we are also undertaking the development of a Windows XP Professional System draft document and accompanying template, similar to the Windows 2000 Professional guidance previously developed by the CSD.

<http://csrc.nist.gov/itsec/>
 Contacts: Mr. Murugiah Souppaya
 (301) 975-4758
 murugiah.souppaya@nist.gov

IT SECURITY CHECKLISTS FOR COMMERCIAL IT PRODUCTS

Various Federal organizations, consortia, and some commercial vendors currently produce checklists and associated templates that describe sets of security configurations for IT products. Such checklists, when combined with well-developed guidance and leveraged with high-quality security expertise, vendor product knowledge, and operational experience and tools, can markedly reduce the vulnerability exposure of an organization. To meet this challenging requirement to produce checklists for the spectrum of IT products widely used in the government, CSD has developed a proposal to have IT vendors, consortia, industry, other government organizations, and others in the public and private sector provide additional checklists and associated guidance material to NIST. These materials can then be made available for display and downloading from the NIST Computer Security Resource Center (CSRC) Web site. This will provide a central repository of recommended security checklists, benchmarks, and configuration guides to help Federal Agencies and industry secure their commercial IT products.

In September 2003, the CSD hosted a workshop to identify current and planned Federal government checklist activities and related needs, existing and planned voluntary efforts for building security checklists, and current industry capabilities for the development of checklists and the associated templates for IT products widely used in the United States Government (USG). This workshop was an effort to present NIST's checklist development template proposal to current and potential checklist producers.

Federal Government, consortia, and commercial IT product vendors currently developing, or planning to develop, security configuration checklists for IT products were encouraged to attend. Workshop topics addressed included: government and commercial requirements, the NIST checklist template framework, the NIST checklist development process, defining checklist target environments, a vendor session to discuss business case advantages/disadvantages for checklist development, methods and incentives to gain commercial vendor support, ideas and proven methods for producing high quality checklists, and deploying and verifying checklists.

One of the next steps for this project is to produce a step-by-step document that would assist regular users and novice system administrators in utilizing the various checklists and guidance for commonly used IT products. We are also undertaking the development of a Windows XP Professional System draft document and accompanying template, similar to the Windows 2000 Professional guidance previously developed by the CSD. We will continue to solicit checklists from vendors, government agencies, academia, and consortia.

<http://csrc.nist.gov/pcig/cig.html>
 Contacts: Mr. John Wack
 (301) 975-3411
 john.wack@nist.gov
 Mr. Murugiah Souppaya
 (301) 975-4758
 murugiah.souppaya@nist.gov

MULTI-CARD TECHNOLOGY

Plastic cards that include information storage and processor components are employed in both the public and private sector for identification, authentication, authorization, and mobile personal information storage. Government agencies have used various storage and

processor card technologies for decades. Many technologies (e.g., optical stripe media, barcodes, magnetic stripes, and contactless, as well as smart card integrated circuit chips) have been implemented on card platforms. Card platforms now include anti-counterfeiting elements to increase the security of the physical platform, and some cards now support multiple technologies. The advent of rapid technological advancements and changing user requirements prompted the need for new applications and enhancement of the existing implementations. Some applications have been designed and implemented in response to a specific need such as ID proofing, whereas others have been adopted to provide an added value to an existing legacy system such as magnetic stripe.

The General Accounting Office (GAO) issued a report dated January 2003 that evaluates the progress in promoting the use of smart cards across the Federal Government. The *Progress in Promoting Adoption of Smart Card Technology* (GAO-03-144 report) sets forth recommendations regarding the role of NIST in the United States Government Smart Card (GSC) program.

In support of the GAO recommendation, NIST initiated an effort intended to identify the state of operational and developmental storage and processor card-based technologies and the nature of user requirements for and constraints associated with integrating these technologies onto single platforms. The initial activities associated with this effort included a NIST-hosted Storage and Processor Card-Based Technologies Workshop in July 2003, distribution of requirements and capabilities questionnaires, and interviews with federal government agencies to identify user requirements and the state of current and planned card programs. Each of these activities included fact-finding regarding individual technologies, integration of technologies, and interoperability of technology applications across organizational boundaries.

At the workshop, representatives of user communities, smart card suppliers, print-based technologies, and optical storage and identification technologies addressed general technology, multi technology integration issues, and both inter-jurisdictional and inter-technology interoperability issues. It was noted that the user community expressed a need for clearer policies regarding card identification content and organization rather than more capable or versatile policy enforcement mechanisms. For example, there was no call by users for higher capacity storage devices but there was significant interest in the effect of privacy policies on the permissible content of cards.

Workshop presentations and interviews disclosed several issues associated with security and privacy, multi-technology integration, standardization of implementations across organizations, and interoperability. These issues have been examined for evidence of gaps in existing standards and other factors that hamper government-wide application integration. The findings from the initial efforts and suggested priorities for follow-on activities are being developed into NIST Interagency Report 7056, *Card Technology Developments and Gap Analysis Interagency Report*, which should be available in the first part of 2004.

<http://ccsrc.nist.gov/card-technology/>
 Contact: Mr. Curt Barker
 (301) 975-8443
 wbarker@nist.gov

GOVERNMENT SMART CARD PROGRAM

Many Federal agencies are interested in using smart cards, because of their intrinsic portability and security. A smart card is able to store and actively process information, in particular cryptographic keys and algorithms for providing digital signatures and for use with

other cryptographic functions. Approximately 30 to 40 million smart cards are due to be issued within the next few years for government purposes. However, a major impediment to the widespread use of smart cards has been the lack of interoperability: the majority of smart cards from different vendors require use of specific software and are not interchangeable within a given system.

In 1999, NIST agreed to lead the development of technical specifications and standards related to the U.S. Government Smart Card (GSC) program. These technical specifications and standards provide interoperability specifications and guidelines to provide organizations with an open and standard method for using smart cards. NIST represents the GSC program in industry, government, and formal standards organizations to promote GSC technology. NIST is also charged with developing a comprehensive GSC conformance test program. The Computer Security Division has partnered with the Software Diagnostics and Conformance Testing Division (SDCT) for the work of this program.

The Government Smart Card Inter-Agency Advisory Board (GSCIAB) established the Architecture Working Group (AWG), which consists of representatives from the federal agencies and industry partners. The AWG is chaired by NIST and chartered to develop technical solutions for identified government requirements. The GSCIAB and AWG fall under the purview of the Federal Identity Credential Committee (FICC), a committee under the Chief Information Officers (CIO) Council e-Authentication activity. The AWG developed the *Government Smart Card Interoperability Specification* (GSC-IS), Version 1.0. This specification defines the Government Smart Card Interoperability Architecture, which satisfies the core interoperability requirements of the Common Access Smart ID Card contract and the GSC Program as a whole. In July of 2003, NIST Interagency Report 6887 *Government Smart*

Card Interoperability Specification, version 2.1 was released. Among other improvements, this version provided mechanisms for contactless interoperability. The Smart Card Alliance has said of the GSC-IS:

The release of the Government Smart Card Interoperability Specification is a significant event in the smart card world as it is the first comprehensive effort to address the interoperability requirements of the enterprise market. It will become as important as Europay/Mastercard/Visa (EMV) specification is to the Payment market and Global System Mobile (GSM) specification is to the mobile telephony market..

GSC-ISv2.1 has been submitted for consideration as a formal standard. In the coming year, NIST will work with International Organization of Standardization (ISO) Sub Committee 17 and InterNational Committee for Information Technology Standards/American National Standards Institute (INCITS/ANSI) B10, the U.S. Technical Advisory Group to ISO SC17, on formal standardization efforts. Work will also continue on harmonizing GSC-ISv2.1 with the NIST biometric standard initiatives, Common Biometric Exchange File Format (CBEFF) and Bio Application Programming Interface (BioAPI). Continued collaboration with the International Aviation Civil Organization (ICAO), the UN organization responsible for travel documents, during the development of the next generation passport, which includes contactless technology, will ensure harmonization of selected protocols with GSC-IS. Finally, close collaboration with the FICC will continue to ensure synchronization of policy, standardization, and technical activities of the Federal community.

<http://smartcard.nist.gov/>
 Contacts: Mr. James Dray, technical lead
 (301) 975-3356
 james.dray@nist.gov

Ms. Teresa Schwarzhoff, standards lead
 (301) 975-5727
 teresa.schwarzhoff@nist.gov

MOBILE AGENT SECURITY

Mobile agents are autonomous software entities that can halt themselves, ship themselves to other agent-enabled hosts on the network, and continue execution deciding where to go and what to do along the way. Mobile agents are goal-oriented, can communicate with other agents, and can continue to operate even after the machine that launched them has been removed from the network. The mobile agent computing paradigm raises several privacy and security concerns, which clearly are one of the main obstacles to the widespread use and adaptation of this new technology. Mobile agent security issues include: authentication, identification, secure messaging, certification, trusted third parties, non-repudiation, and resource control. Mobile agent frameworks must be able to counter new threats as agent hosts must be protected from malicious agents, agents must be protected from malicious hosts, and agents must be protected from malicious agents. This project is directed towards evaluating existing mobile agent security mechanisms and developing new countermeasures for mobile agent security threats.

In the past, the Computer Security Division (CSD) has looked at the possibility and usefulness of various ways to apply mobile agents to the problem of detecting and responding to intrusions. As part of this effort, we devised a privilege management scheme to protect mobile agent systems used in such activities. More recently, we have been working with the University of West Florida through a cooperative research and development agreement (CRADA) to integrate our privilege

management components into an existing mobile agent framework. Work has also progressed in transferring this technology to interested parties. We are tentatively looking into solutions for secure privilege delegation within mobile agent frameworks.

<http://csrc.nist.gov/mobilesecurity/index.html>
 Contact: Mr. Wayne Jansen

(301) 975-5148
 wjansen@nist.gov

MOBILE DEVICE SECURITY

With the trend toward a highly mobile workforce, the acquisition of handheld devices such as Personal Digital Assistants (PDAs) and PC tablets is growing at an ever-increasing rate. These devices offer productivity tools in a compact form and are quickly becoming a necessity in today's business environment. Many manufacturers make handheld devices using a broad range of hardware and software. Handheld devices are characterized by small physical size, limited storage and processing power, restricted stylus-oriented user interface, and the means for synchronizing data with a more capable notebook or desktop computer. Typically, they are equipped with the capability to communicate wirelessly over limited distances to other devices using infrared or radio signals. Many handheld devices can also send and receive electronic mail and access the Internet. While such devices have their limitations, they are nonetheless extremely useful in managing appointments and contact information, reviewing documents, corresponding via electronic mail, delivering presentations, and accessing corporate data. Moreover, because of their relatively low cost, they are becoming ubiquitous within office environments, often purchased by the employees themselves as an efficiency aid. Unfortunately, several major



issues loom over the use of such devices, including: small handheld devices may be misplaced, left unattended, or stolen; user authentication may be disabled, a common default mode, divulging the contents of the device to anyone who possesses it; even if user authentication is enabled, the authentication mechanism may be weak or easily circumvented; wireless transmissions may be intercepted and, if unencrypted or encrypted under a flawed protocol, their contents made known; the ease with which handheld devices can be interconnected wirelessly, combined with weak or no authentication of the parties involved, provides new avenues for the introduction of viruses or other types of malicious code, and also other forms of attack such as a man-in-the-middle attack.

To protect the information on these devices, several programs began development in 2002 and continued into this past year. These programs are designed first to authenticate the user of the PDA when he/she logs on. The user is authenticated under a multi-mode authentication framework that supports various types of authentication mechanisms chosen by

a system administrator, including visual passcode authentication, biometric voiceprint identification, and smart card tokens. Once authenticated, policy mechanisms take over to protect the device. The system administrator can authorize or deny privileges to run applications, to access files, to initiate a wireless connection to the Internet, to connect to other devices using infrared or BlueTooth, and to sync to specific computers inside or outside of a network. A log of security-related activities is also maintained on the device, should the system administrator need that information. The development of this security solution involved many pieces, including the design and implementation of the multiple authentication framework, improvements to the accuracy and performance of various authentication mechanisms, the means to describe and enforce device policies, the capability to support multiple echelons of policy, and the development of policy management tools.

This project will move forward in several ways. First, we will incorporate new authentication mechanisms, such as MMC-type (MultiMedia Card) smart cards and trusted proximity beacons, under the framework, while expanding the framework to support encrypted repositories. Second, we will develop an intrusion detection system (IDS) for Mobile Ad Hoc Networks (MANets), and investigate forming and applying ad hoc secure enclaves over wireless networks. Finally, we will evaluate existing forensic software tools for mobile devices as a means to improve both device security and forensic examination techniques.

<http://csrc.nist.gov/mobilesecurity/index.html>

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

Dr. Tom Karygiannis
(301) 975-4728
tom.karygiannis@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 WiFi devices have flexibility to move their laptop computers from one place to another within their offices while maintaining connectivity with the network. WiFi, 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 quickly becoming more wide-spread in use. Wireless personal networks 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 personal digital assistants (PDAs) and cell phones can synchronize data between PDAs and personal computers and can use network services such as wireless email, web browsing, and Internet access. Further, wireless communications can help organizations cut their wiring costs.

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

In December 2002, NIST held a workshop on 802.11 Wireless LAN Security in Falls Church, Virginia. The workshop comprised approximately 30 individuals from the US Federal Government, the WiFi industry and the security and academic communities. Participants included individuals from NIST, the National Security Agency (NSA), the National Communication System (NCS), US Secret Service

(USSS), Boeing Corporation, Cisco Systems, Microsoft Corporation, Intel Corporation, TruSecure, Agere Systems, Booz-Allen-Hamilton, Vigil Security, Virginia Tech, the University of Maryland, and the Burton Group.

The primary objectives of the workshop were: to ensure that NIST and other interested Federal Agencies understand the current direction of the 802.11 wireless LAN (or WiFi) Industry; to convey the Federal government cryptographic security requirements to the WiFi Industry; to map a strategy for the expeditious roll-out of a very robust WiFi security solution; and to identify areas in which NIST can, given adequate resources, play a productive role in the development of WiFi security standards. Specific working sessions within the workshop included an overview of NIST and an explanation of its roles and responsibilities, an informative session on FIPS-140 (*Security Requirements for Cryptographic Modules*), an enlightening "user perspective" on implementing 802.11 securely in a large enterprise, an overview of the WiFi Alliance industry organization, and very detailed discussions on the characteristics and rationale of the short-term (WPA—WiFi Protected Access) and long-term (RSN—Robust Security Networks) 802.11 security solutions. The 2-day workshop concluded having produced a list of "actionable" items to address the high-level strategy established during the workshop.

This workshop followed the publication of NIST Special Publication 800-48 *Wireless Network Security – 802.11, Bluetooth and Handheld Devices*. This document addresses three aspects of wireless security: security issues associated with WLANs that are based on the IEEE 802.11 standard; security issues related to wireless personal area networks based on the Bluetooth specifications, which were developed by an industry consortium; and security of wireless handheld devices. A summary of this document was issued in the March 2003 *ITL Bulletin*.

The IEEE 802.11 Task Group i was tasked earlier this year to produce a security upgrade for the 802.11 standard. We will continue our analysis of one of the main developments from this standard, RSN, to ensure that the IEEE specifications will not preclude vendor solutions from gaining FIPS 140-2 validation. We expect to issue a publication regarding RSN within the next year. We will also be holding another industry and government 802.11 Wireless Security Workshop in the coming year.

<http://csrc.nist.gov/wireless/>
Contact: Ms. Sheila Frankel
(301) 975-3297
sheila.frankel@nist.gov

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

ICAT

The ICAT Metabase is a NIST-maintained searchable index of computer vulnerabilities. ICAT provides users with links to a variety of publicly available vulnerability databases and patch sites, thus enabling one to find and fix the vulnerabilities existing on their systems. ICAT allows one to search at a fine granularity, a feature unavailable with most vulnerability databases, by characterizing each vulnerability by over 21 attributes, including software name and version number. ICAT indexes the information available in Computer Emergency Response Team (CERT) advisories, Internet Security Systems X-Force (ISS X-Force), Security Focus, NTBugtraq, Bugtraq, and a variety of vendor security and patch bulletins. This system complements publicly available vulnerability databases as a search engine with pointers for users to other sites. ICAT uses, and is completely based on, the industry standard Common Vulnerabilities and Exposures (CVE) naming standard.

Many different types of people use ICAT for a variety of purposes. System administrators and computer security officers use ICAT to identify the known vulnerabilities (and patch information) associated with the software on critical systems. Law enforcement can use ICAT in forensics activities to determine the set of possible vulnerabilities that a hacker might have used to penetrate a system. Computer security researchers use ICAT to identify sets of vulnerabilities that have particular characteristics of interest. Auditors can use ICAT to check to see if particular vulnerabilities have been patched in audited systems.

The last year included a substantial amount of updating and use of ICAT. Over 1,500 new vulnerabilities were added to the database. The ICAT web site was highly utilized, totaling some 1.94 million hits.

Work on ICAT over the next year will focus largely on updating and improving an already successful project. We will continue analysis of feedback from users, using this feedback to improve the Web site. We plan on improving the frequency of the database updates, as well as improving the administrator interface. We will also work on communication problems previously experienced between the local and web database engines. Finally, we plan to continue updating the candidate and CVE entries into the database.

<http://icat.nist.gov/>
Contacts: Dr. Vincent Hu
(301) 975-4975
vincent.hu@nist.gov

Ms. Kathy Ton-Nu
(301) 975-3361
kathy.ton-nu@nist.gov

INTERNET PROTOCOL SECURITY (IPsec)

The NIST IPsec project concerns itself with the emerging Internet protocols that provide increased security services at the Internet level. These security facilities, known as IPsec, are significant since they will be used to secure the infrastructure of the Internet (routing, Domain Name System (DNS), etc.) and they can also be used to protect application-level Internet communications. They enable a centrally controlled access policy, as well as a multi-level, layered approach to security. IPsec provides the following security services: data origin authentication, connectionless integrity, replay protection, data confidentiality, limited traffic flow confidentiality, and key negotiation and management. The Internet Engineering Task Force (IETF) has mandated the use of IPsec wherever feasible.

To expedite the development of this crucial technology, Information Technology Laboratory (ITL) staff designed and developed Cerberus, a reference implementation of the IPsec specifications, and PlutoPlus, a reference implementation of the IKE (Internet Key Exchange) key negotiation and management specifications. Numerous organizations from all segments of the Internet industry have acquired these implementations as a platform for on-going research on advanced issues in IPsec technology.

To answer an industry call for more frequent and accessible interoperability testing for emerging commercial implementations of IPsec technology, ITL developed the NIST IPsec WWW-based Interoperability Tester, IPsec-WIT, which is built around the Cerberus and PlutoPlus prototype implementations. IPsec-WIT also serves as an experiment in test system architectures and technologies. The novel use of WWW technology allows IPsec-WIT to provide interoperability testing services anytime and anywhere without requiring any distribution of test system software, or relocation of the systems under

test. ITL staff also collaborated with key industry representatives to co-author protocol specifications and resolve technical impasses that threatened the progress of the IPsec design and standardization process.

During the past year division personnel authored two RFCs (Requests for Comments, the IETF's standards documents) dealing with the use of the Advanced Encryption Standard (AES) in IPsec. One RFC defines the use of AES in CBC (Cipher Block Chaining) mode for encryption and the other RFC defines the use of AES-XCBC (eXtended Cipher Block Chaining) for integrity-protection. The Division presented tutorials and invited talks on IPsec, Internet Key Exchange (IKE), and Public Key Infrastructure (PKI). A special version of PlutoPlus was begun this past year for User-to-Network Interface (UNI) and Network-to-Network Interface (NNI) with a user-friendly Graphic User Interface (GUI) for configuration. Network Associates also issued a final version of Simple Network Management Protocol (SNMP)-based IPsec policy configuration based on PlutoPlus.

In the coming year, the Division plans on issuing a special publication on IPsec configuration, deployment and use. The special version of PlutoPlus for UNI/NNI will be completed. Plans also include the addition of UNI/NNI tests to the IPsec-WIT tester.

<http://csrc.nist.gov/ipsec/>
 Contact: Ms. Sheila Frankel
 (301) 975-3297
 sheila.frankel@nist.gov

AUTHORIZATION MANAGEMENT AND ADVANCED ACCESS CONTROL MODELS

One of the basic tenets of IT security is controlling access to vital IT resources – answering the question, "who is allowed to do what?" A NIST research team created, and introduced in 1992, a new approach to

controlling user access called Role-Based Access Control (RBAC). What is most striking about RBAC is its rapid evolution from a theoretical model to commercial implementation and deployment. An independently conducted NIST-sponsored economic impact study estimated that RBAC will soon be used by some 30 million users for access to sensitive information. Further, the study estimated that RBAC technology will save the U.S. software development industry \$671 million, and that NIST is responsible for 44 percent of the savings. Most information technology vendors have incorporated RBAC into their product line, and the technology is finding applications in areas ranging from health care to defense in addition to the mainstream commerce systems for which it was designed.

The Computer Security Division (CSD) is currently considered one of the world leaders in Access Control technologies. To date, we have had 18 refereed papers in technical journals and conferences. We were invited to publish a book on RBAC, and have papers cited as the third and twelfth most referenced access control papers out of the top 200. There are 3 NIST U.S. patents for RBAC technologies, and one patent pending.

In the past year we published the Universal Policy Machine (Policy Engine and Policy Specification Language) model, an Economic Impact Study on RBAC, and the RBAC book. We received the 2003 Best Paper Award at the Systems, Cybernetics, and Informatics Conference.

Many different access control policies and models have been developed to suit a variety of goals; these include Role-Based Access Control, One-directional Information Flow, Chinese Wall, Clark-Wilson, *N*-person Control, and Discretionary Access Control (DAC), in addition to more informal ad hoc policies. While each of these policies has a particular area of strength, the notational differences between these policies are substantial. As a result it is difficult

to combine them, both in making formal statements about systems that are based on differing models and in using more than one access control policy model within a given system. Thus, there is a need for a unifying formalism that is general enough to encompass a range of these policies and models. We have proposed an open security architecture called the *Policy Machine (PM)* that would meet this need. We have also provided examples showing how the PM specifies and enforces access control policies. *PM* will be the main focus of our efforts in this area over the next year.

<http://csrc.nist.gov/rbac/>

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

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

VOICE OVER INTERNET PROTOCOL (VoIP) SECURITY ISSUES

Internet telephony refers to communications services—voice, facsimile, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). The basic steps involved in originating an Internet telephone call are conversion of the analog voice signal to digital format and compression/translation of the signal into Internet protocol (IP) packets for transmission over the Internet; the process is reversed at the receiving end. Originally regarded as a novelty, Internet telephony is attracting more and more users because it offers tremendous cost savings relative to the PSTN. Users can bypass long-distance carriers and their per-minute usage rates and run their voice traffic over the Internet for a flat monthly Internet-access fee.



Several factors will influence future developments in VoIP products and services. Currently, the most promising areas for VoIP are corporate intranets and commercial extranets. Their IP-based infrastructures enable operators to control who can—and cannot—use the network. Another influential element in the ongoing Internet-telephony evolution is the VoIP gateway. As these gateways evolve from PC-based platforms to robust embedded systems, each will be able to handle hundreds of simultaneous calls. Consequently, corporations may deploy large numbers of them in an effort to reduce the expenses associated with high-volume voice, fax, and videoconferencing traffic. The economics of placing all traffic—data, voice, and video—over an IP-based network may pull companies in this direction, simply because IP will act as a unifying agent, regardless of the underlying architecture (i.e., leased lines, frame relay, or Asynchronous Transfer Mode (ATM)) of an organization's network.

VoIP presents challenges from several dimensions. They are: the technology of call processing, a need to interface with legacy PBX (private branch exchange) systems, making the existing security solutions fit into the VoIP environment, and security for the new applications enabled by the switchover to VoIP from legacy voice systems.

NIST is looking into security issues arising from each of these dimensions and plans to develop assurance metrics and testing methodologies for several VoIP configurations. To achieve these goals, we also plan to leverage the large knowledgebase already available for various types of attacks against IP components and entities like routers, web servers, domain name servers, and so on.

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

AUTOMATED SECURITY TESTING

Independent security functional testing of a product is very rarely performed in many security evaluations due to cost and technical complexity, except in the case of high assurance products. Recognizing this, the CSD undertook a project in May 2000 to develop a methodology to automate or partially automate the process of security functional testing. The goals of the methodology were three fold: (a) to automate several of the steps involved in developing and generating tests for testing the various security functions of a product, (b) to improve the quality of tests generated through the use of formal methods to specify various security function behaviors, and (c) to use the text-based security function specifications provided by the product vendor in the

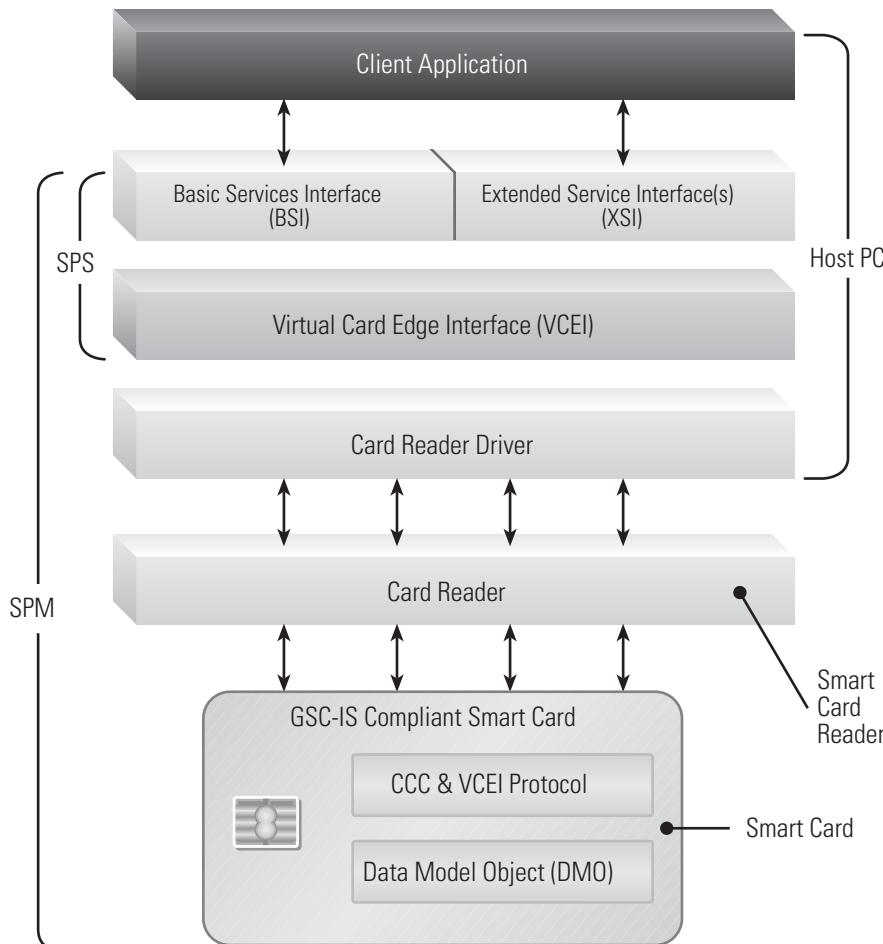
International Organization of Standardization/International Electrotechnical Commission (ISO/IEC) 15408 Security Target document as the basis for generating tests.

The project goals have been met by the development of the TAF-SFT (Test Automation Framework – Security Functional Testing) toolkit with a graphical user interface. The TAF-SFT has demonstrated its capability to model any security function that can be modeled using product's published interfaces and generate tests that conform to the chosen coverage criteria. These security functions cover the areas of authorization, access control, audit generation, security management, and identification and authentication and session management. The capabilities of the toolkit have been demonstrated by generating tests for testing the security functions of a commercial DBMS

(database management system) product based upon the text-based specifications in the product's ISO/IEC 15408 Security Target document. Further peer-reviewed technical papers describing the various stages of the methodology development have been accepted at 5 conferences.

The methodology and toolkit are now being deployed to generate the conformance tests for testing the various functions in the Government Smart Card Interoperability specification (GSC-IS) version 2.1. The outcome of this effort will not only cut down the overall costs of the development of these smart cards but also cut down the cycle time involved in the General Services Administration's (GSA's) issuance of these cards for thousands of federal employees.

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



CRITICAL INFRASTRUCTURE PROTECTION GRANTS PROGRAM

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include telecommunications, energy, banking and finance, transportation, water systems and emergency services. Due to advances in information technology (IT) and the necessity of improved efficiency, infrastructures have become increasingly automated and inter-linked. Most modern commercial infrastructures are composed of a collection of interconnected networks that serve different purposes and have different owners. Indeed, even parts of the information resident on a single sub-network may have different purposes and different owners. Critical information is passed between these component elements to coordinate necessary functions. The complexity and interdependency of this critical information flow introduces vulnera-

bilities into the entire critical infrastructure. Deliberate attacks or accidental system failure may result in serious consequences to the nation.

In September 2001, NIST awarded \$5 million to nine grant recipients under the Fiscal Year 2001 Critical Infrastructure Protection Grants Program (CIPGP) to improve the robustness, resilience, and security information in all the critical infrastructures. Under the competitive grant application process, we received 133 proposals requesting roughly \$73 million from applicants in both industry and academia. Proposals were required to clearly explain what commercial or government entities would likely utilize the solution and how the project would contribute to that utilization. We selected proposals in intrusion detection, telecommunications, wireless security, electric power infrastructure, and compiler security.

Funded research addresses a variety of topics to include tools and methods for analyzing security and detecting attacks due to vulnerabilities introduced by merging of data networks (i.e., the Internet) and voice networks (i.e. the public switched telephone network). Other topics being addressed are attack detection for wireless and converged networks, the development of security controls for protecting the North American power grid, and methods for evaluating intrusion detection systems.

We will continue to monitor the progress of the remaining research projects, as well as evaluate the progress of technical efforts happening within the projects. We will also monitor the status of transferring the technology to the commercial and government entities that will be using the final deliverables.

<http://csrc.nist.gov/grants/>
Contact: Mr. Tim Grance
(301) 975-4242
grance@nist.gov

SCALABLE QUANTUM INFORMATION NETWORK

Quantum mechanics, the strange behavior of matter on the atomic scale, provides entirely new and uniquely powerful tools for computing and communications. This field could revolutionize many aspects of computing and secure communications, and could have enormous impacts in homeland security. Quantum computers could perform processing tasks that would take billions of years on conventional computers. They also could solve problems that conventional computers could not manage given realistic amounts of time, memory, and processing power.

Exploiting quantum properties would be particularly valuable in cryptography, making codes that would be unbreakable by the best supercomputers of tomorrow, or breaking codes in seconds that could not be cracked in millions of years by the most powerful binary computers. Quantum information also can be used for remarkably secure communications. In this particular area, we are partnering closely with the Defense Advanced Research Projects Agency (DARPA).

The objective of this NIST project is to develop an extensible quantum information test-bed and the scalable component technology essential to the practical realization of a quantum communication network. The test-bed will demonstrate quantum communication and quantum cryptographic key distribution with a high data rate. This test-bed, once developed, will provide a measurement and standards infrastructure that will be open to the DARPA QuIST (Quantum Information Science and Technology) community and will enable wide-ranging experiments on both the physical- and network-layer aspects of a quantum communication system. The infrastructure will be used to provide calibration, testing, and development

facilities for the QuIST community. This project is one part of the broader Quantum Information Program at NIST.

Within the Quantum Information Program, we are developing and evaluating quantum cryptographic protocols, and investigating means of integrating quantum and conventional network technology. Controlling access to a large network of resources is one of the most common security problems. Any pair of parties in a network should be able to communicate, but must be authorized to do so, while minimizing the number of cryptographic keys that must be distributed and maintained. This project will develop an authentication solution based on a combination of quantum cryptography and a conventional secret key system. Two significant advantages of this approach over conventional authentication protocols are 1) timestamps and exact clock synchronization between parties are not needed; and 2) that even the trusted server cannot know the contents of the authentication ticket.

In 2003, we conducted a cryptanalysis of three published quantum key distribution protocols, and the lessons learned are being submitted for journal publication. We also evaluated an authentication protocol for resistance to cryptanalysis, and the results are likewise being submitted for journal publication.

In the coming year we will test and measure the performance of enhanced protocol on the test bed. We plan to implement and validate new cryptographic protocols. We will also generalize the results on cryptanalysis, and publish theorems on a generalized attack.

<http://math.nist.gov/quantum/>
Contact: Mr. D. Richard Kuhn
(301) 975-3337
kuhn@nist.gov



Cryptographic Standards and Applications

GOAL ▶ *To protect information resources through the use of cryptography.*

STRATEGY ▶ *The strategy to meet this goal is the development and improvement of cryptographic methods for protecting the integrity, confidentiality, and authenticity of information resources.*

INTENDED OUTCOME AND BACKGROUND:

The intended outcome of this area of work is to enable government and industry to be able to build secure, interoperable applications with high-assurance products that implement needed cryptographic security functionality. This includes the on-going development of cryptographic standards and testing methods, developing methods for securing e-Gov applications with cryptography, further developing key management guidelines and schemes, and the updating and creation of new modes of operation for use with the newer Advanced Encryption Standard (AES).

This area of work involves collaboration with a number of entities, both from federal agencies and industry. Some of the federal agencies include the Department of Treasury, agencies participating in the Federal PKI Steering Committee and Bridge CA Project, the Federal Deposit Insurance Corporation (FDIC), and the National Security Agency (NSA). Projects in this area have worked with the American National Standards Institute's (ANSI's) X9 Committee that develops standards for the financial industry, as well as with the Internet Engineering Task Force's (IETF's) PKIX Working

Group. Industry collaborators in this area have included RSA Security Entrust Technologies, IBM, Mastercard, Visa, Verizon, VeriSign, Microsoft, and others.

ACCOMPLISHMENTS

CRYPTOGRAPHIC STANDARDS TOOLKIT

The aim of the Cryptographic Standards Toolkit (CToolkit) project is to enable U.S. governmental agencies, and others, to select cryptographic security components and functionality for protecting their data, communications, and operations. The Toolkit helps to ensure that there is worldwide government and industry use of strong cryptography, and that secure interoperability is achieved through standard algorithms. The Toolkit also makes guidance and education available in the use of cryptography. The Toolkit currently includes a wide variety of cryptographic algorithms and techniques for encryption, authentication, non-repudiation, key establishment, and random number generation. The Toolkit is a collection of standards and guidance, and does not include any actual software implementations of the algorithms. Many of the projects discussed in this area of work are combined to form the CToolkit.

The past year has seen a great deal of work go into the CToolkit. A draft version of the NIST Special Publications 800-56 *Recommendation on Key Establishment Schemes* and 800-57 *Recommendation on Key Management* were issued for public review in January 2003. Drafts for public review and comment have also been issued of Special Publications 800-38B *Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode* (RMAC – Randomized Message Authentication Code) and 800-38C *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality* (CCM – Counter with CBC MAC). Revisions of Federal Information Processing Standard (FIPS) 112 Password Usage and NIST Special Publication (SP) 800-21 *Guideline for Implementing Cryptography* were begun during the past year. The revision of the Digital Signature Standard (DSS) has begun, and will be posted for public review in the future, prior to adoption as FIPS 186-3. Validation tests have also been developed for the Digital Signature Algorithm (DSA), the Secure Hash Algorithm (SHA), the Keyed-Hash Message Authentication Code (HMAC), and ANSI X9.62 the Elliptic Curve Digital Signature Algorithm (ECDSA), and will be delivered to the validation laboratories early next year.

Plans for 2004 include the completion of draft documents issued in 2003, as well as the completion of a draft document on password-based key establishment.

<http://csrc.nist.gov/CryptoToolkit/index.html>
 Contact: Ms. Elaine Barker
 (301) 975-2911
 elaine.barker@nist.gov

BIOMETRIC TECHNOLOGIES

Biometric technologies consist of automated methods of identifying a person or verifying the identity of a person based upon recognition of a physiological or a behavioral characteristic. Consumers need biometric-based high performance, interoperable systems (e.g. standards-based) developed in a timely fashion. In the absence of timely standards developments, migration from proprietary systems to open-systems standard-based solutions will be more difficult and expensive. Therefore, standards are the cornerstone of our biometrics program. Deploying new information technology systems for homeland security and for preventing ID theft will require both national and international consensus standards for biometrics. NIST is responding to post-9/11 market requirements for open system standards by accelerating development of formal, national and international biometric standards.

These standards need further development in order to help deploy significantly better, open-systems security solutions that are based on standards. NIST has identified the critical tasks that will help power the development of these standards so that the deployment of such systems may be accelerated. Consequently, in the past two years NIST has worked in close partnership with other U.S. government agencies and U.S. industry to establish two formal standards bodies for accelerating the development of formal national and interna-

tional biometric standards of high relevance to the U.S. Nationally, we established Technical Committee M1 under the InterNational Committee for Information Technology Standards (INCITS). Internationally we successfully petitioned the International Organization for Standardization/International Electro-technical Commission Joint Technical Committee 1 to establish Subcommittee 37-Biometrics (ISO/IEC JTC 1/SC 37-Biometrics), which NIST currently chairs. We have also participated in related consortia efforts. Our strategy in this program includes: (a) Leveraging existing consortia standards (e.g., the Bio Application Programming Interface (BioAPI) Consortium and Common Biometric Exchange File Format (CBEFF)); (b) Managing the national (INCITS Technical Committee M1 on Biometrics) and the international (ISO/IEC JTC 1/SC 37-Biometrics) biometric standards developments; (c) Providing expert technical leaders for critical standards projects; (d) Acting as an advisor to other federal government agencies (e.g., Department of Homeland Security (DHS), the National Security Agency (NSA) and the Department of Defense (DoD) Biometric Management Office); (e) Supporting required administrative infrastructures (e.g., ISO/IEC JTC 1/SC 37 Secretariat);

(f) Working through biometric standards "incubators" (e.g., Biometric Consortium); (g) Promoting fast processing of consortia specifications into national/international standards; and (h) Initiating development of technical implementations and software development for conformity assessment and interoperability tests to Application Profiles as required.

The U.S. Biometric Consortium (BC), which is considered to be a biometrics incubator, serves as a U.S. government focal point for biometrics. It currently consists of over nine hundred members representing over sixty government agencies, industry and academia. NIST co-chairs the Consortium with the NSA. The BC sponsors an annual conference, technical workshops and biometrics technical developments. The NIST/BC Biometric Working Group, sponsored by NIST and the BC has been working in the last few years with government users and industry developing biometric specifications. In the last 18 months it approved and provided to formal standards bodies three specifications for further processing as national and international standards: (a) Biometric Data Protection and Usage; (b) Biometric Application Programming Interface for Java Card; and (c) an augmented version of the Common Biometric Exchange File Format (the initial version of CBEFF was published as National Institute of Standards and Technology Interagency Report (NISTIR) 6529). The 2003 annual technical conference, held September 2003, in Crystal City, VA was sponsored by NIST/Information Technology Laboratory (ITL), NSA, The National Biometric Security Project (NBSP), DoD's Biometrics Management Office (BMO), the National Institute of Justice (NIJ), West Virginia U.S.A., the General Services Administration's Federal Technology Service (FTS) Center for Smart Card Solutions, and the National Science Foundation (NSF). Supporting organizations included the



American National Standards Institute (ANSI), the BioAPI Consortium, the International Biometric Industry Association (IBIA), INCITS, and the Biometric Foundation. This conference had over 900 attendees from government organizations, industry and academia. The two and a half days conference program included presentations, technology and business seminars, a biometric research symposium sponsored by the Biometric Knowledge Center at West Virginia University and the NSF and panel discussions with the participation of over 100 internationally recognized experts in biometric technologies, system and application developers, IT business strategists, and government and commercial officers. The conference included exhibits and technology demonstrations from 76 organizations.

NIST is also a member of the BioAPI Consortium and its Steering Committee. BioAPI Consortium's membership consists of over 100 organizations including biometric vendors, end-users, system developers and original equipment manufacturers (OEMs). This consortium developed the BioAPI specification, which was approved as ANSI INCITS 358 -2002. The BioAPI specification is an International Organization of Standardization (ISO) standard candidate (under development in JTC1/SC 37-Biometrics). NIST has recently developed the Linux version of the BioAPI reference implementation (originally developed as a Windows-compatible implementation) and harmonized the Linux implementation with a Unix implementation developed by another BioAPI Consortium member. The Linux/Unix reference implementation was released to the public at the 2003 Biometric Conference.

INCITS M1 is the Technical Committee in the U.S. responsible for representing the U.S., or the U.S. Technical Advisory Group (TAG), to the JTC1/SC 37. The purpose of INCITS M1 is to ensure a high priority, focused, and comprehensive approach in the U.S. for the rapid development and approval of formal national and international generic biometric standards. These standards are consid-

ered to be critical for U.S. needs, such as homeland defense, the prevention of identity theft and for other government and commercial applications based on biometric personal authentication. We provide the chairperson for these two standards bodies and manage their standards programs. The current INCITS M1 program of work includes biometric data interchange formats (finger image, finger minutiae, finger pattern-based, face and iris recognition, sign/signature recognition and hand geometry), data exchange framework formats (CBEFF), application programming interfaces (BioAPI), application profiles (transportation workers, border management and Point-of-Sale), and performance testing and reporting standards (technology, scenario and operational testing).

M1 has maintained an accelerated pace of biometric standards development. Several of the draft standards developed under INCITS M1 have been sent to Initial Public Review and are anticipated to become ANSI standards in the first quarter of 2004. Another major accomplishment where NIST was instrumental is a report developed by M1's Ad-Hoc Group on Biometric Interoperability in Support of the Government Smart Card (GSC) Framework. This group was formed by M1 to identify biometric interoperability requirements for the Government Smart Card Framework (GSCF) - NISTIR 6887-2003 Edition, Government Smart Card Interoperability Specification (GSC-IS) (v2.1). The almost 100 page report also identifies proposed extensions to the BioAPI standard to achieve a higher degree of interoperability with the GSC. It is expected that the result of this work will be taken internationally, through INCITS B10, to JTC 1 SC 17 as part of the proposed GSCF project and to JTC 1 SC 37 as extensions to the BioAPI specification.

Internationally, through an aggressive planned schedule, SC 37 has made excellent progress during the last year as evidenced by the number of approved projects and the advancement of many of these projects to Committee Draft status in a very short period. In addition to chairing SC37,

NIST contributes Mr. Michael D. Hogan, of the Information Technology Laboratory, to be the Convener of the Biometric Profiles Working Group (SC37 WG4) and supports SC37's program of work by supplying biometric technical experts and editors in the areas of CBEFF, BioAPI, performance testing and reporting, biometric data formats and reporting standards development. The BioAPI specification, the CBEFF and a number of the data interchange formats, contributed to SC37 by the U.S. through M1, are targeted to final approval as international standards at the end of 2004.

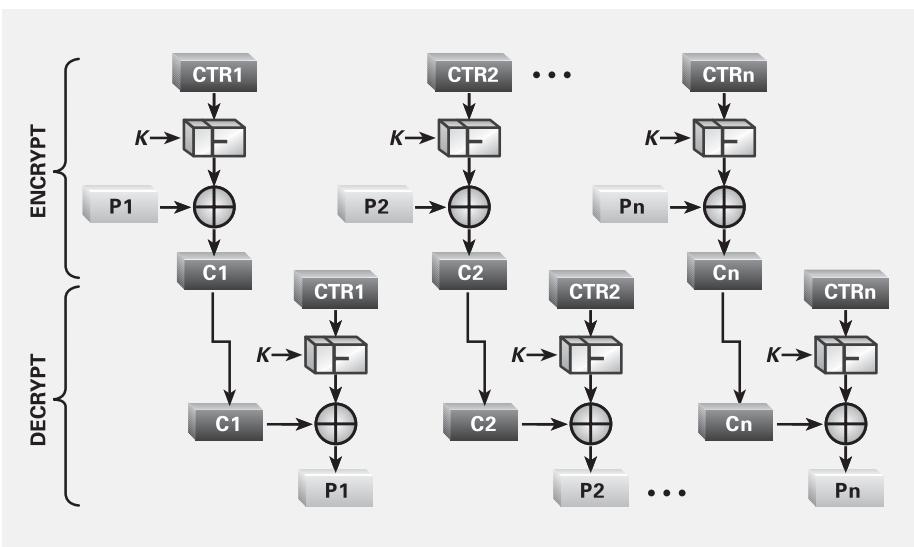
In 2003, this NIST program was awarded a Group Gold Medal Award for Scientific/Engineering Achievement for its impact in biometric standards development.

<http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html>
Contact: Mr. Fernando Podio
(301) 975-2947
fernando@nist.gov

KEY MANAGEMENT

The goals of this project are two-fold: to develop schemes for establishing cryptographic keying material for the protection of Federal Government sensitive, unclassified information, and to develop key management guidance for the handling of keying material from its creation through its destruction. The project will help secure e-commerce through the generation and protection afforded by secure cryptographic key establishment schemes. It will provide guidance for system and protocol developers to build more secure communication and storage products, as well as allowing commercial off-the-shelf (COTS) products to be validated that they comply with the key establishment schemes.

The Key Management Guideline saw periodic revisions made and published for review this past year. Revisions were also published for review for the Key Establishment Schemes document. In the next year there are plans to



complete parts one and two of the Key Management Guideline, as well as the Key Establishment Schemes Document. A draft of a Password-based Key Establishment Document will also be written and published for review.

<http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html>

Contact: Ms. Elaine Barker
(301) 975-2911
elaine.barker@nist.gov

MODES OF OPERATION FOR BLOCK CIPHER ALGORITHMS

A mode of operation, or mode, for short, is an algorithm that features the use of a symmetric key block cipher algorithm to provide an information service, such as confidentiality or authentication. With the advent of new block ciphers, such as the Advanced Encryption Standard (AES), there is a need to update long-standing modes of operation and an opportunity to consider the development of new modes. One important motivation for updating modes is the increased block size of the AES algorithm compared to the Digital Encryption Standard (DES) algorithm (128 bits instead of 64 bits).

NIST is in the process of specifying modes in the 800-38 series of special publications. The first document in the series specifies five confidentiality modes; the second document will specify an authentication mode; the third document will specify a combined mode for authentication and confidentiality.

A draft version of Special Publication (SP) 800-38B *Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode* (RMAC – Randomized Message Authentication Code) was released in October 2002, and is currently undergoing substantial revision to respond to public comment. The upcoming version will specify the OMAC (One-key Cipher Block Chaining Message Authentication Code) variation of the extended Ciphertext Block

Chaining (XCBC) authentication algorithm. After a second public comment period, the document will be finalized in 2004. The draft SP 800-38C specifies the CCM (Counter with CBC MAC) algorithm, a combined confidentiality-authentication mode that was developed for the Institute of Electrical and Electronics Engineers Inc. (IEEE) 802.11 standard for wireless local area networks (LANs). This document is undergoing minor revision in response to public comment before finalization in 2004.

Mode development is expected to be an ongoing effort. Later parts of the series may be devoted to the specification of new modes. In the next year, for example, NIST will consider whether to propose additional combined confidentiality-authentication modes, possibly including an AES key wrap.

<http://nist.gov/modes>
Contact: Dr. Morris Dworkin
(301) 975-3356
morris.dworkin@nist.gov

E-AUTHENTICATION

The Office of Management and Budget (OMB) has identified the remote identification of users, or e-Authentication, as a crosscutting impediment to the provision of Internet-based government services. To fully realize the benefits of the electronic government, government agencies require e-Authentication policies and corresponding technical guidance tailored to the protection of government systems and data. This project establishes a policy structure for e-authentication within the U.S. government, promoting consistent implementation of e-authentication across federal agencies. This consistency will in turn help to enhance



government efficiency by securing electronic processes needed to conduct more transactions through e-government applications.

NIST is assisting OMB in the development of *E-Authentication Guidance for Federal Agencies*, which is expected to be available in early 2004. This OMB guidance will define four levels of authentication, Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. The OMB guidance will define the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance will also increase. The OMB guidance will provide agencies with the criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction. For example, the level of authentication needed in order to let someone make a reservation at a National Park would be far less than the level needed to let someone view his or her social security benefits.

In early 2004, NIST will be releasing a companion publication, Special Publication (SP) 800-63 *Recommendation for Electronic Authentication*. This recommendation will provide technical guidance in the implementation of electronic authentication to allow an individual person to remotely authenticate his or her identity to a Federal IT system. Special Publication 800-63 will state specific technical requirements for each of the four levels of assurance in the following areas: identity proofing and registration, tokens, remote authentication mechanisms and assertion mechanisms. After completing a risk assessment and mapping the identified risks to the required assurance level, Federal agencies will be able to select appropriate technology for the required level of assurance.



Federal agencies may choose to authenticate users through credentials issued by industry, associations, or local government. NIST is supporting the development of accreditation procedures for Credential Service Providers (CSPs), based on the technical requirements in draft SP 800-63. These procedures will provide the foundation for efficient evaluation and selection of acceptable Credential Service Providers by Federal agencies without requiring specialized expertise.

In this project, NIST is collaborating with Federal agencies and industry partners. Federal agencies include the Office of Management and Budget, Government Services Administration, the Federal Identity and Credentialing Committee, and the Social Security Administration. Industry partners include Wells Fargo Bank, VeriSign, Digital Signature Trust/Identrus, ElectroSoft Systems, Phoenix Technologies, and Caradas.

Contacts: Mr. William Burr
 (301) 975-2914
burr@nist.gov

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

E-GOV IDENTITY MANAGEMENT INFRASTRUCTURE

For cost efficiency, authentication techniques cannot be implemented on an application-by-application basis. Identity management infrastructures bring scalability and cost-effectiveness, permitting many applications to authenticate identity using the same credentials. In the e-Gov Identity Management Infrastructure project, NIST is supporting the deployment and implementation of identity management infrastructures by and for government agencies. Under this project, NIST is supporting the deployment and maintenance of the Federal Public Key Infrastructure (PKI), development and deployment of a common federal credential, and development of an online e-Authentication credential validation infrastructure.

NIST continues to support the development and deployment of the Federal PKI, which permits cross-agency use of PKI-based credentials for authentication and related uses. NIST provides the vice-chair of the Federal PKI Policy Authority, which manages the suite of Federal PKI Certificate Policies and the operations of the Federal Bridge Certification Authority. By establishing interoperability with other PKIs, we will expand the range of applications supported by the Federal PKI.

NIST is also supporting a project for outsourcing PKI operations associated with the management of a common federal identity credential. To support this effort, NIST is drafting the Common Policy framework. The Common Policy will support issuing credentials to government employees, contractors, and affiliates that require access to government buildings and systems. This project will be coordinated with the Government Smart Card project to maximize the utility and interoperability of the common federal identity credential.

NIST is assisting the General Services Administration (GSA) in the development of an online e-Authentication credential validation infrastructure. The GSA e-Authentication Gateway will mediate between government applications and non-government CSP, permitting applications to accept a variety of identification credentials. For example, possible CSPs might include banks. This could mean in the future the passwords you use for your online banking or shopping services could be used to access some government services. NIST has participated in a review of the GSA E-Authentication Gateway architecture; the resulting enhancements will introduce additional flexibility and increase the range of government requirements that can be met by this system.

As part of this project, NIST is researching web services protocols (e.g., Simple Object Access Protocol (SOAP) and Security Assertion Markup Language (SAML)), effective password use, and registration and identity proofing. NIST is collaborating with many entities, including the Federal PKI Policy Authority (FPKIPA), the Federal Identity Credentialing Committee, the General Services Administration (GSA), the General Accounting Office (GAO), the National Security Agency (NSA), the Federal Deposit Insurance Corporation (FDIC), the Office of Management and Budget (OMB), the States of

Illinois and Washington, and EduCause, which includes 1,800 universities, colleges, and educational institutions.

Contacts: Mr. William Burr
(301) 975-2914
burr@nist.gov

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

SECURING E-GOV APPLICATIONS WITH CRYPTOGRAPHY

To reduce overhead and streamline operations, government agencies are transitioning from paper processing to electronic applications. To implement these processes, agencies may leverage commercial off the shelf (COTS) applications or build custom systems. In either case, agencies are facing new and unexpected security threats in the course of this transition. For example, information may be inadvertently disclosed or modified during transmission across networks. To safely implement these business processes, security controls must be implemented to protect against such threats. Cryptography is one of the most powerful tools available to agencies to implement such controls, but selection and installation of cryptographic controls is complex.

In this project, NIST is developing guidance for both COTS applications and assisting agencies in the design and implementation of custom applications. NIST is developing guidance documents for the selection and configuration of COTS systems based on standard protocols. NIST has recently published guidance for the selection and configuration of secure e-mail

clients based on S/MIME Version 3 standards. NIST is currently developing guidance for TLS servers and clients, to be completed in 2004.

To assist agencies in the development of secure custom applications, NIST is researching cryptographic Application Programming Interfaces (APIs), cryptographic message/object formats, and techniques for PKI-enabling legacy applications. Currently, PKI-enabled applications must use proprietary, vendor-provided APIs to interface with their PKI, thus making support across multiple PKI products difficult. To facilitate the development and wide-deployment of PKI-enabled applications, NIST is working with several federal agencies to make this interface to a PKI consistent, regardless of the PKI product being used. Once fully developed, the first APIs could be used for models for use with many other systems, despite what type of information and transactions it might be handling. For instance, a model used to secure an accounting system could be also used as a model to secure a human resources system.

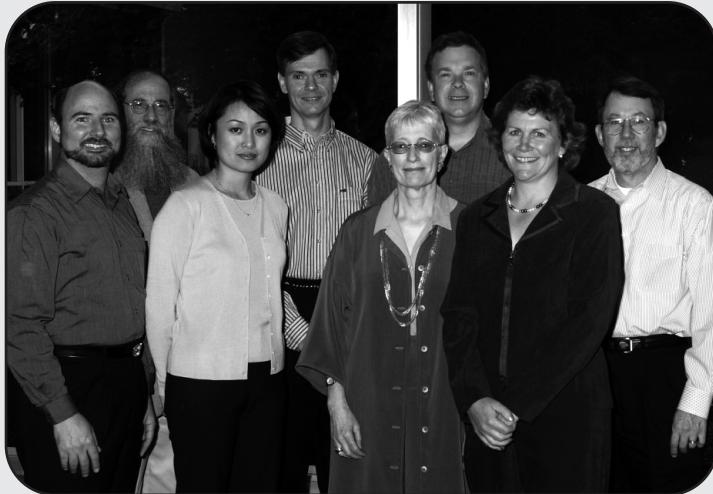
Finally, NIST is directly assisting agencies in the implementation of secure applications. NIST is currently working with the Army Corps of Engineers, Treasury Financial Management System (FNMS), and the Federal Deposit Insurance Corporation. NIST participation is focused upon appropriate application of cryptography to secure these business processes.

Contacts: Mr. William Burr
(301) 975-2914
burr@nist.gov

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

Honors and Awards

DEPARTMENT OF COMMERCE SILVER MEDAL



The Cryptographic Module Validation Program Team was awarded the Department of Commerce's Silver Medal for scientific/engineering achievement in conceiving, establishing, and operating the Cryptographic Module Validation Program and developing *Security Requirements for Cryptographic Modules*. The team's leadership, innovation, and vision, have enabled and strengthened the deployment of strong commercial cryptography to protect the nation's critical national infrastructures, in both the public and private sector. The team has established both a standard and a program that has brought and continues to bring international recognition and prestige to NIST, the Department of Commerce and the U.S. Federal Government. The Team consists of Ray Snouffer, Annabelle Lee, Randall Easter, Sharon Keller, Larry Bassham, Ron Tencati, Janet Jing, Gary Stoneburner, Lisa Carnahan, and Jeffrey Horlick.

DEPARTMENT OF COMMERCE BRONZE MEDAL

Tom Karygiannis was awarded the Department of Commerce's Bronze Medal for his leadership and scholarship in advancing and improving wireless and mobile security. He established a significant research and publication track record in wireless-related technologies such as mobile agents, mobile devices, and privilege management. This enabled him to co-write the widely heralded NIST Special Publication 800-48 *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*. This document garnered widespread industry support and generated swift action towards the use of federally approved cryptographic standards in wireless and mobile technologies.



DEPARTMENT OF COMMERCE BRONZE MEDAL

Murugiah Souppaya was awarded the Department of Commerce's Bronze Medal for his leadership in developing the Windows 2000 Professional Security Consensus Benchmark. He improved the security of hundreds of thousands of systems in the public and private sector by developing and recommending significantly improved security settings, clearly documenting and explaining those recommended parameters, 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.



FRANK B. ROWLETTE AWARD FINALIST



Elaine Barker was selected as a finalist for the Frank B. Rowlette Award for Individual Excellence by the National Security Agency. This prestigious award recognizes those who have made extraordinary contributions in the field of information security. A prolific writer and editor, Ms. Barker has authored, edited, co-authored, or co-edited eighteen ANSI and Federal Information Processing cryptographic standards. These encryption, signature and hashing standards are used throughout the Federal Government and around the world to protect the nation's critical infrastructures, sensitive communications, electronic commerce and financial transactions.

BEST PAPER AWARD



Ramaswamy Chandramouli was recognized by The Organizing Committee of The 7th World Multi-conference on Systemics, Cybernetics and Informatics (SCI 2003) for his authorship of "Specification and Validation of Enterprise Access Control Data for Conformance to Model and Policy Constraints." His paper was selected as the best paper presented in the Information Systems Development session.

SIGMA XI COLLEGE OF DISTINGUISHED LECTURERS



Alicia Clay was selected for membership in the prestigious 2004-2006 Sigma Xi College of Distinguished Lecturers. Founded in 1886 as an honor society for scientists and engineers, Sigma Xi is today an independent, non-profit research society of more than 80,000 members, with a distinguished history of service to science and society. Scientists and engineers are elected to membership based on their research potential or achievements. This is the 65th consecutive year Sigma Xi has maintained its College of Distinguished Lecturers, a program that is an opportunity for chapters to host visits from outstanding individuals who are at the leading edge of science. Dr. Clay will be lecturing on Information Security and the Small Business Owner, International Standards on Information Security Management, and NIST Guidelines on Information Security Management.

THE "FED 100" AWARD



Tim Grance was selected by Federal Computer Week for 2003 "Fed 100" recognition. The Federal 100 awards recognize that people, not technology, improve the way government works, delivers services and improves not only Americans' lives, but also those of people worldwide. Tim was recognized for his

work to produce technical guidelines by providing principal technical direction to the development of the technical guidelines and serving as key reviewer to ensure overall quality and consistency with legal, policy and other existing security guidelines. Tim was also recognized as having "an uncanny ability to translate what he learns into plain English, so that others can grasp it." "When he takes pen in hand, he reduces it to language that can be understood by nontechnical managers," said Lynn McNulty, former associate director for computer security at NIST.

2003 MATHEMATICS AND COMPUTER SCIENCES AWARD



Stuart Katzke was awarded the Washington Academy of Sciences 2003 Award for Scientific Achievement designating Dr. Katzke as a Fellow of the Academy. In order to recognize scientific work of merit and distinction, the Washington Academy of Sciences gives awards annually to scientists who work in the greater Washington D.C. area. The history of the Awards program, begun in 1940, is literally a catalog of over 60 years of scientific achievement.

THE "FED 100" AWARD



Edward Roback was selected by Federal Computer Week for 2003 "Fed 100" recognition. The Federal 100 awards recognize that people, not technology, improve the way government works, delivers services and improves not only Americans' lives, but also those of people worldwide. Ed was recognized for his raising awareness about ITL's security tools and expertise, and in coordinating the division's portfolio of products. As stated by FCW, "Edward Roback rose to the challenge last year when the Bush administration asked the National Institute of Standards and Technology to take on a larger role in shaping civilian agencies' security policies and practices."



Computer Security Division Publications

2003

NIST SPECIAL PUBLICATIONS

SP 800-43	System Administration Guidance for Windows 2000 Professional	November 2002
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices	November 2002
SP 800-49	Federal S/MIME V3 Client Profile	November 2002
SP 800-55	Security Metrics Guide for Information Technology Systems	July 2003
SP 800-59	Guideline for Identifying an Information System as a National Security System	August 2003

DRAFT NIST SPECIAL PUBLICATIONS

SP 800-35	Guide to Information Technology Security Services	October 2002
SP 800-36	Guide to Selecting Information Technology Security Products	October 2002
SP 800-37	Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems	October 2002, June 2003
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode	October 2002
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality	September 2003
SP 800-50	Building an Information Technology Security Awareness and Training Program	May 2002
SP 800-56	Recommendation on Key Establishment Schemes	January 2003
SP 800-57	Recommendation on Key Management	January 2003
SP 800-61	Computer Security Incident Handling Guide	September 2003
SP 800-64	Security Considerations in the Information System Development Life Cycle (originally was SP 800-4A)	October 2002

DRAFT FEDERAL INFORMATION PROCESSING STANDARDS

FIPS 199	Standards for Security Categorization of Federal Information and Information Systems	May 2003
----------	--	----------

NIST INTERAGENCY REPORTS

NIST IR 7046	A Framework for Multi-Mode Authentication: Overview and Implementation Guide	August 2003
NIST IR 7030	Picture Password: A Visual Login Technique for Mobile Devices	July 2003
NIST IR 6887	Government Smart Card Interoperability Specification (GSC-IS), v2.1	July 2003
NIST IR 7007	An Overview of Issues in Testing Intrusion Detection Systems	June 2003
NIST IR 6981	Policy Expression and Enforcement for Handheld Devices	May 2003
NIST IR 6985	COTS Security Protection Profile - Operating Systems (CSPP-OS) (Worked Example Applying Guidance of NISTIR-6462, CSPP)	April 2003

INFORMATION TECHNOLOGY LABORATORY BULLETINS WRITTEN BY THE CSD

October 2002	Security Patches And The CVE Vulnerability Naming Scheme: Tools To Address Computer System Vulnerabilities
--------------	--

November 2002	Security For Telecommuting And Broadband Communications
---------------	---

December 2002	Security of Public Web Servers
---------------	--------------------------------

January 2003	Security Of Electronic Mail
--------------	-----------------------------

February 2003	Secure Interconnections for Information Technology Systems
---------------	--

March 2003	Security For Wireless Networks And Devices
------------	--

June 2003	ASSET: Security Assessment Tool For Federal Agencies
-----------	--

July 2003	Testing Intrusion Detection Systems
-----------	-------------------------------------

August 2003	IT Security Metrics
-------------	---------------------



Ways to Engage Our Division and NIST

GUEST RESEARCH INTERNSHIPS AT NIST

Opportunities are available at NIST for 6 to 24 month internships within the CSD. Qualified individuals should contact the CSD and 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. Ed Roback, (301) 975-3696, edward.roback@nist.gov.

DETAILS AT NIST FOR GOVERNMENT OR MILITARY PERSONNEL

Opportunities are available at NIST for 6 to 24 month details at NIST in the CSD. Qualified individuals should contact the 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. Ed Roback, (301) 975-3696, edward.roback@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) 975-4242, tim.grance@nist.gov.

FUNDING OPPORTUNITIES AT NIST

NIST funds industrial and academic research in a variety of ways. Our Advanced Technology Program co-funds high-risk, high-payoff projects with industry. 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, academic, and other institutions are available on a

competitive basis through several different Institute offices. For general information on NIST grants programs, contact Ms. Joyce Brigham, (301) 975-6329, joyce.brigham@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 the National Institute of Standards and Technology, one of the world's leading research organizations and home to two 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 and from New York to New Mexico), sample the Washington, D.C., area. And, no kidding, 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.



Tanya Brewer-Joneas, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

NIST IR 7111
April 2004

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

