
Security Practices
FISMA
Cybersecurity Framework
Roadmap
Cloud Computing
Security Controls
Mobile Devices
FIPS 140-2
Evaluation
Continuous Monitoring
Authorization
Critical Infrastructure
Cryptography
EO 13636
Assets
Biometrics
Policy Machine
Verification
Guidelines
Validated Products List
Risk Management Framework
Systems
Computer
Security
Division
2013 Annual Report
IC17
IC18
Vcc
NIST Special Publication 800-170
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-170

Computer Security Division

2013 Annual Report

Patrick O'Reilly, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Co-Editors:
Chris Johnson
Doug Rike
Greg Witte
G2, Inc.

Lorie Richards
Facilities Services Division
Creative and Printing Service

This publication is available free of charge from
http://dx.doi.org/10.6028/NIST.SP.800-170

June 2014

U.S. Department of Commerce
Penny S. Pritzker, Secretary

National Institute of Standards and Technology
Dr. Willie E. May, Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology Special Publication 800-170 Natl. Inst. Stand. Technol. Spec. Pub., 93 pages (June 2014) CODEN: NSPUE2

Table of Contents

Welcome Letter

The Computer Security Division (CSD), a component of the Information Technology Laboratory at the National Institute of Standards and Technology (NIST) is responsible for developing standards, guidelines, tests, and metrics for protection of non-national security federal information systems. NIST standards and guidelines are developed in an open and transparent manner that enlists broad industry and academia expertise from around the world. While developed for federal agency use, these resources are voluntarily adopted by other organizations because they are effective and accepted throughout the world.

The need for cybersecurity standards and best practices that address interoperability, usability and privacy continues to be critical for the Nation. In Fiscal Year (FY) 2013, CSD continued to align its resources to enable greater development and application of practical, innovative security technologies and methodologies that enhance our ability to address current and future computer and information security challenges. Our foundational research and applied cybersecurity programs continue to advance in many areas including cryptography; identity and access management; cloud, virtualization, and mobile technologies; and advanced security testing and measurement.

Strong partnerships with diverse stakeholders are vital to the success of our technical programs. In February 2013, the President issued Executive Order 13636 that directed NIST to work collaboratively with industry to develop a voluntary framework - based on existing standards, guidelines, and practices - to improve critical infrastructure cybersecurity practices. NIST held several workshops, meetings, webinars, and informal sessions to gather feedback with the goals of generating content for the framework and discuss several topics that help inform and guide NIST in this effort. In August 2013, we produced a discussion draft of the preliminary framework.

Working closely with standards developing organizations, industry and interagency partners, we are evolving and expanding security automation capabilities to help organizations manage and measure the security of systems and technologies. Our cybersecurity awareness, training, and education programs also exemplify the importance of these partnerships by engaging with academic institutions, federal agencies, small and medium businesses and others to increase awareness and enhance the overall cybersecurity posture of the Nation.

Active engagement with the diverse federal community continues to be critical to our success. This interaction is most prominent in our strengthened collaborations with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems to establish a common foundation for information security across the federal government. Through this partnership, NIST released Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, in April 2013. This guideline provides organizations with state-of-the-practice security controls to fundamentally strengthen their systems and the environments in which those systems operate. SP 800-53 Revision 4 and other NIST standards and guidelines contribute to systems that are more resilient in the face of cyber attacks and other threats.

Late in FY 2013, news reports about leaked classified documents caused concern from the cryptographic community about the security of NIST cryptographic standards and guidelines. Recognizing community concern regarding some specific standards, we reopened the public comment period for three Special Publications to give the public a second opportunity to view and comment on the documents. This initial step will be followed by a review of our cryptographic development process and NIST cryptographic standards and guidelines in FY 2014.

For many years, CSD, in collaboration with our global partners across industry, academia, and government, has made great contributions to help secure the nation's critical information and infrastructure. We look forward to furthering these relationships in FY 2014 as we lead the development and practical implementation of scalable and sustainable information security standards and practices in areas such as cyber-physical and industrial control systems, privacy engineering, security automation, and mobile technologies.

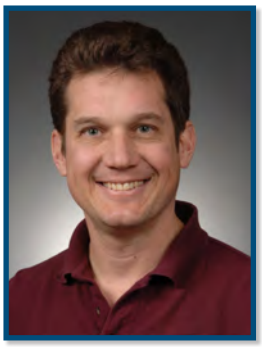
To participate in any CSD research areas – whether current or future – or to learn more about our programs and activities, please visit http://csrc.nist.gov.

Donna Dodson
Chief, Computer Security Division
& Deputy Chief Cybersecurity Advisor

Computer Security Division (CSD) Management Team

Donna Dodson

Chief, Computer Security Division, Acting Associate Director & Acting Chief Cybersecurity Advisor, Cybersecurity Advisor Office, and Acting Executive Director, National Cybersecurity Center of Excellence



Matthew Scholl

Deputy Chief, Computer Security Division and Acting Associate Director of Operations, National Cybersecurity Center of Excellence

GROUP MANAGERS

Lily Chen

(Acting Group Manager)
Cryptographic Technology Group

David Ferraiolo

Secure Systems and Applications Group

Mark (Lee) Badger

Security Components and Mechanisms Group

Kevin Stine

Security Outreach and Integration Group

Michael Cooper

Security Testing, Validation and Measurement Group

Computer Security Division Organization

The Computer Security Division's computer scientists, mathematicians, IT specialists, administrative staff and others support CSD's mission and responsibilities through five groups that are described in the following sections:

- Cryptographic Technology Group
- Security Components and Mechanisms Group
- Secure Systems and Applications Group
- Security Outreach and Integration Group
- Security Testing, Validation, and Measurement Group

Cryptographic Technology Group (CTG)

Mission Statement:

Research, develop, engineer, and standardize cryptographic algorithms, methods, and protocols.

Overview:

CTG's work in the field of cryptography includes researching, analyzing, and standardizing cryptographic technology, such as hash algorithms, symmetric and asymmetric cryptographic techniques, key management, authentication, and random number generation. CTG's goal is to identify and promote methods to enhance trust in communications, data, and storage through cryptographic technology, encouraging innovative development and helping technology users to manage risk.

In Fiscal Year (FY) 2013, CTG continued to make an impact in the field of cryptography, both within and outside the Federal Government, by collaborating with national and international agencies, academic and research organizations, and standards bodies to develop interoperable security standards and guidelines. In addition, CTG worked with industry partners to promote the use of NIST-approved cryptographic methods.

Federal agency collaborators include the National Security Agency (NSA), the Intelligence Advanced Research Projects Activity (IARPA), the National Telecommunications and Information Administration (NTIA), the National Strategy for Trusted Identities in Cyberspace (NSTIC), General Services Administration (GSA), the United States Postal Service (USPS), and the Election Assistance Commission (EAC).

CTG also works closely with foreign government agencies, such as the Communications Security Establishment of Canada and Australia's Defense Signals Agency and Centrelink. Additionally, CTG is active in national and international standards bodies, including the Accredited Standards Committee (ASC) X9 (financial industry standards), the International Organization for Standardization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the American National Standards Institute (ANSI), and the Trusted Computing Group (TCG). Industry collaborators include Intel, Microsoft, and Cisco.

Academic collaborators include Carnegie Mellon University, Yale University, University of Southern Denmark, the University of Milan, Malaga University, and the University of Lisbon. Research organizations include the Information-technology Promotion Agency (IPA)/Cryptography Research and Evaluation Committees (CRYPTREC) and the Ministry of Economy, Trade and Industry (METI) of Japan.

Group Manager (Acting):

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

Security Components and Mechanisms Group (SCMG)

Mission Statement:

Research, develop, and standardize foundational security mechanisms, protocols, and services.

Overview:

The SCMG's security research focuses on the development and management of foundational building-block security mechanisms and techniques that can be integrated into a wide variety of mission-critical U.S. information systems. The group's work spans the spectrum from near-term hardening and improvement to the design and analysis of next-generation, leap-ahead security capabilities. Computer security depends fundamentally on the level of trust for computer software and systems. This work, therefore, focuses strongly on assurance building activities ranging from the analysis of software configuration settings to advanced trust architectures to testing tools that surface flaws in software modules. This work also focuses significantly on increasing the applicability and effectiveness of automated techniques, wherever feasible. The SCMG conducts collaborative research with government, industry, and academia. Outputs of this research consist of prototype systems, software tools, demonstrations, NIST Special Publications (SP), NIST Interagency or Internal Reports (NISTIR), and conference and journal papers.

SCMG works on a variety of topics, such as specifications for the automated exchange of security information between systems, computer security incident handling guidelines, formulation of high-assurance software configuration settings, hardware roots of trust for mobile devices, secure Basic Input Output System (BIOS) layers, combinatorial testing techniques, conformity assessment of software implementing biometric standards, and adoption of Internet Protocol Version 6 and Internet Protocol security extensions. SCMG collaborates extensively with government, academia, and the private sector.

In FY 2013, collaborations have included Carnegie Mellon University (test development environment), Johns Hopkins Applied Physics Lab (practical application of combinatorial coverage measurement tool), North Carolina State University (access control policy testing), University of North Texas and University of Maryland-Baltimore County (test prioritization algorithms), University of Texas at Arlington (covering array generation algorithm), Mexico's Centro Nacional de Metrología (constraints for testing coverage tool), National Aeronautics and Space Administration (NASA) (practical application for combinatorial coverage measurement), U.S. Air Force Test and Evaluation (a new event sequence testing method), the National Security Agency (secure software tool chain competition development), and the Department of Homeland Security (incident coordination).

SCMG accomplishments include the Advanced Combinatorial Testing System (ACTS) software and documentation, the NIST BioCTS 2013 biometric conformance testing tool and test assertions, and a security log analysis tool.

Group Manager:

Mr. Mark (Lee) Badger
(301) 975-3176
mark.badger@nist.gov

Secure Systems and Applications Group (SSAG)

Mission Statement:

Integrate and apply security technologies, standards, and guidelines for computing platforms and information systems.

Overview:

SSAG's security research focuses on the identification of emerging and high-priority technologies and on the development of security solutions that will enhance the security of U.S. critical information infrastructure. The group conducts 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. SSAG works to transfer new technologies to industry; to produce new standards and guidance for federal agencies and industry; and to develop tests, test methodologies, and assurance methods.

SSAG investigates topics such as mobile device security, cloud computing and virtualization, identity management, access control and authorization management, and software assurance. SSAG research helps federal agencies meet information security requirements that might not be fully addressed by existing technology. The group collaborates extensively with government, academia, and private sector entities.

Example successes from this work include tools for access control policy testing, new concepts in access control and policy enforcement, methods for achieving comprehensive policy enforcement and data interoperability across enterprise data services, and test methods for mobile device (smart phone) application security. For example, the SSAG Mobile Application Testing Portal (ATP) went operational for military use (known in the U.S. Army as PANTHR) and is in the process of transitioning to other federal agencies as open source. In support of the Federal Government's cloud computing initiatives, SSAG led the NIST Security Working Group that published the NIST Cloud Computing - Security Reference Architecture. The SSAG also completed revision of Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which was approved by the Secretary of Commerce and published in September of 2013.

To improve access to new technologies, SSAG chaired, edited, and participated in the development of a wide variety of national and international security standards.

Group Manager:

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

Security Outreach and Integration Group (SOIG)

Mission Statement:

Develop, integrate, and promote the mission-specific application of information security standards, guidelines, best practices, and technologies.

Overview:

The U.S. economy, citizens, and government rely on information technology (IT); so the protection of IT and information infrastructure is critical. SOIG leverages broad cybersecurity and risk management expertise to develop, integrate, and promote security standards, guidelines, tools, technologies, methodologies, tests, and measurements to address cybersecurity needs in many areas of national and international importance.

The SOIG collaborates with stakeholders to address cybersecurity considerations in many diverse program areas, including the Information and Communications Technologies (ICT) supply chain, Smart Grid, Electronic Voting, Health Information Technology, and Cyber Physical and Industrial Control Systems. The group continues to increase its efforts to research, develop, and align cybersecurity standards, practices, and testing methods necessary to foster interoperable and secure public safety communications. In our Federal Information Security Management Act (FISMA) implementation program, the group produces standards and guidelines to help federal agencies build strong cybersecurity risk management programs. In each of these program areas, the group extends outreach to stakeholders across federal, state, and local governments; industry; academia; small businesses; and the public. The SOIG also leads several broad cybersecurity awareness, training, education, and outreach efforts, including the National Initiative for Cybersecurity Education (NICE), the Small- and Medium-sized Business (SMB) outreach program, the Federal Computer Security Managers' Forum, and the Federal Information Systems Security Educators' Association (FISSEA).

Key to the group's success is the ability to interact with a broad constituency to ensure that SOIG's program is consistent with national objectives related to or impacted by information

security. Through open and transparent public engagement, collaboration, and cooperation, the group works to address critical cybersecurity challenges, enable greater U.S. industrial competitiveness, and facilitate practical implementation of scalable and sustainable information security standards and practices.

Group Manager:

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

Security Testing, Validation, and Measurement Group (STVMG)

Mission Statement:

Advance information security testing, measurement science, and conformance.

Overview:

Federal agencies, industry, and the public rely on cryptography for the protection of information and communications used in electronic commerce, critical infrastructure, and other application areas. The STVMG supports testing and validation of underlying cryptographic modules and cryptographic algorithms in consideration of established standards. These cryptographic modules and algorithms enable products and systems to provide security services, such as confidentiality, integrity, and authentication. Although cryptography provides security, poor designs or weak algorithms can render a product insecure and place highly sensitive information at risk. When protecting sensitive data, Federal Government agencies require a minimum level of assurance that cryptographic products meet established security requirements and use only tested and validated cryptographic modules.

STVMG's testing-focused activities include validating cryptographic algorithm implementations, cryptographic modules, and Security Content Automation Protocol (SCAP)-compliant products; developing test suites and test methods; providing implementation guidance and technical support to industry forums; and conducting education, training, and outreach programs.

STVMG's validation programs work together with independent Cryptographic and Security Testing laboratories that are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). Based on the independent laboratory test report and test evidence, the Validation Program then validates the implementation under test. NIST publishes, through public websites, lists of validations awarded.

Group Manager:

Mr. Michael Cooper
(301) 975-8077
michael.cooper@nist.gov

The Computer Security Division Implements the Federal Information Security Management Act

The CSD Implements the Federal Information Security Management Act

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) of 2002, included duties and responsibilities for the National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division (CSD). In 2013, CSD addressed its assignments through the following activities:

- Issued two final Federal Information Processing Standards (FIPS): FIPS 186-4, *Digital Signature Standard (DSS)*, which specifies a suite of algorithms that can be used to generate digital signatures, and FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors.
- Issued 25 draft and final NIST Special Publications (SP) that provide management, operational, and technical security guidelines in areas such as personal identity verification, cryptographic key generation, cryptographic key management systems, random bit generators, transport layer security, mobile devices and mobile device forensics, hardware-rooted security in mobile devices, malware incident prevention and handling for desktops and laptops, industrial control systems security, e-authentication, security and privacy controls for federal information systems and organizations, patch management technologies, attribute based access control, and supply chain risk management practices.
- Issued 13 draft and final NIST Interagency or Internal Reports (NISTIR) on a variety of topics, including cryptographic key management issues and challenges in cloud services, cybersecurity in cyber-physical systems, the SHA-3 cryptographic hash algorithm competition, combinatorial coverage measurement, credential reliability and revocation model for federated identities, security automation, reference certificate policy, trusted geolocation in the cloud, and a glossary of key information security terms.
- Performed research and conducted outreach on standards, practices, and technologies to enable prompt and effective computer security incident handling and coordination.
- Continued the successful collaboration with the Office of the Director of National Intelligence (ODNI), the Committee on National Security Systems (CNSS), and the Department of Defense (DOD) to establish a common foundation for information security across the Federal Government, including a structured, yet flexible approach for managing information security risk across an organization. In 2013, this collaboration produced updated guidelines for selecting and specifying security controls, and an updated catalog of security and privacy controls for federal information systems and organizations.
- Provided assistance to agencies and the private sector through many outreach efforts associated with the Federal Information Systems Security Educators' Association (FISSEA), the Federal Computer Security Managers' Forum, the National Initiative for Cybersecurity Education (NICE), and the Small Business Information Security Corner.
- Conducted workshops, awareness briefings, and outreach to CSD customers to ensure comprehension of standards and guidelines, to share ongoing and planned activities, and to aid in scoping guidelines in a collaborative, open, and transparent manner. CSD public workshops addressed a diverse range of information security and technology topics, including cloud and mobile technologies, voting systems security, cyber physical systems, improving trust in the online marketplace, safeguarding health information, attribute based access control, supply chain risk management, improving critical infrastructure cybersecurity, and broad computer security awareness, training, and education forums and events.
- Engaged with international standards bodies in a variety of areas, including promoting broader international adoption of security automation specifications. Additionally, NIST continued to lead, in conjunction with the Government of Canada's Communications Security Establishment, the Cryptographic Module Validation Program (CMVP). The Common Criteria Evaluation and Validation Scheme (CCEVS) and CMVP facilitate security testing of IT products usable by the Federal Government.
- Solicited recommendations of the Information Security and Privacy Advisory Board (ISPAB) on draft standards and guidelines, and on information security and privacy issues.
- Produced the CSD 2013 annual report and released it as a NIST SP. CSD annual reports from fiscal years 2003 through 2013 are available on the Computer Security Resource Center (CSRC) at http://csrc.nist.gov/publications/PubsTC.html#Annual Reports.

Program and Project Achievements for Fiscal Year 2013

In FY 2013, CSD continued to research and develop guidance for a broad array of technical areas, including supply chain risk management; security analytics; cloud, mobile, and privacy-enhancing technologies; hardware-enabled security; and cyber-physical and embedded systems. The staff and guest researchers within CSD have collaborated with global partners from government, industry, and academia, making significant contributions to help secure critical information and infrastructure. The following sections describe CSD's programs and project achievements that include extensive research and development for high-quality, cost-effective security and privacy mechanisms, standards, guidelines, tests, and metrics that address current and future computer and information security challenges.

NIST Responsibilities Under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013. This Executive Order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices – for reducing cybersecurity risks to critical infrastructure.

The Cybersecurity Framework will provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy, and civil liberties. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will not prescribe particular technological solutions or specifications.

In FY 2013, NIST worked with a diverse stakeholder community to develop the Framework through an open public process. This process included:

- Issuing a Request for Information (RFI) in the Federal Register in February 2013
- Conducting five open workshops to provide the public with additional opportunities to provide input. These workshops were hosted at the Department of Commerce in Washington, D.C. (April 2013), Carnegie Mellon University in Pittsburgh, Pennsylvania (May 2013), the University of California, San Diego (July 2013), the University of Texas at Dallas (September 2013), and the North Carolina State University in Raleigh, North Carolina (November 2013)
- Preparing a Preliminary Cybersecurity Framework for official public review and comment

In FY 2014, NIST will continue to conduct stakeholder outreach and will work collaboratively to further develop and issue the Cybersecurity Framework. NIST will initiate a 45-day public comment period on the Preliminary Cybersecurity Framework, review and adjudicate all public comments received, and issue a final Cybersecurity Framework (version 1.0) in February 2014 as specified in the Executive Order.

http://www.nist.gov/cyberframework

Contacts:

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

Mr. Adam Sedgewick
(301) 367-4678
adam.sedgewick@nist.gov

Contributions to National and International Standards Development

Figure 1 (below) shows many of the national and international Standards Developing Organizations (SDOs) involved in cybersecurity standardization. CSD participates in cybersecurity standards activities in many of these organizations, either in leadership positions or as editors and contributors. Many of CSD's publications have been the basis for both national and international standards projects. This section discusses CSD standards activities in conjunction with InterNational Committee for Information Technology Standards (INCITS) Technical Committee Cyber Security 1 (CS1), where Dan Benigni serves as Chair and U.S. Head of Delegation to subcommittee SC 27, and Sal Francomacaro serves as CS1 Vice Chair.

The International Organization for Standardization (ISO)

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

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

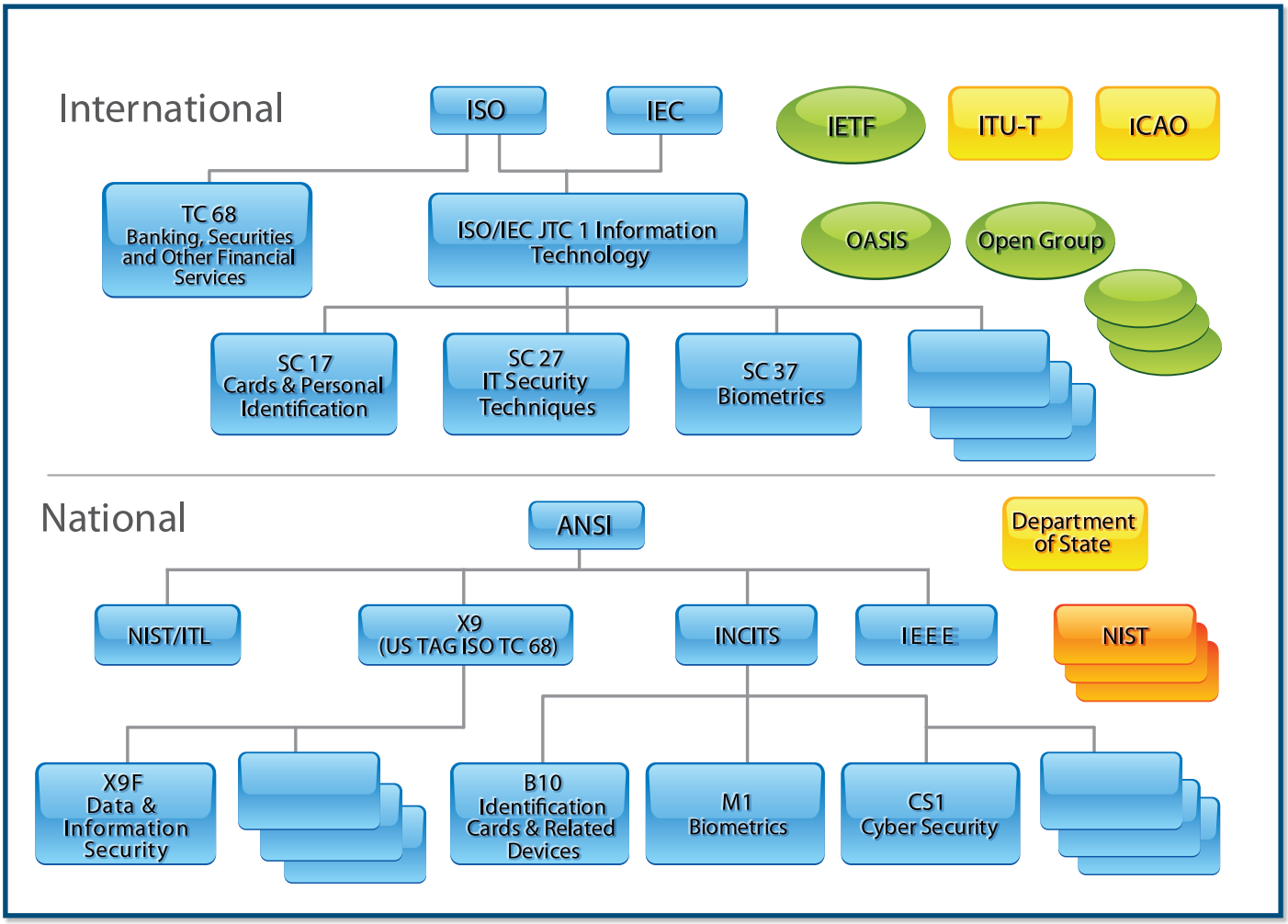


Figure 1: Cybersecurity Standards Development Organizations (SDOs)

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

- Design and development of IT systems and tools
- Performance and quality of IT products and systems
- Security of IT systems and information
- Portability of application programs
- Interoperability of IT products and systems
- Unified tools and environments
- Harmonized IT vocabulary
- User-friendly and ergonomically designed user interfaces

JTC 1 consists of a number of subcommittees (SCs) and working groups that address specific technologies. SCs that produce standards relating to IT security include:

- SC 06 – Telecommunications and Information Exchange Between Systems
- SC 17 – Cards and Personal Identification
- SC 27 – IT Security Techniques
- SC 37 – Biometrics (Fernando Podio, NIST, Chair)

JTC 1 also has:

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

The American National Standards Institute (ANSI)

ANSI is a private, nonprofit organization (501(c)(3)) that administers and coordinates the U.S. voluntary standardization and conformity assessment system and facilitates the development of American National Standards (ANS) by accrediting the procedures of SDOs.

ANSI promotes the use of U.S. standards internationally, advocates U.S. policy and technical positions in international and regional standards organizations, and encourages the adoption of international standards as national standards where they meet the needs of the user community. ANSI is the sole U.S. representative and dues-paying member of the two major non-treaty international standards organizations, ISO and, via the United States National Committee (USNC), the IEC.

INCITS is accredited by ANSI and serves as the ANSI Technical Advisory Group (TAG) for ISO/IEC Joint Technical Committee 1. INCITS is sponsored by the Information Technology Industry (ITI) Council, a trade association representing the leading U.S. providers of information technology products and services.

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

- B10 – Identification Cards and Related Devices
- CS1 – Cyber Security (Dan Benigni, NIST, Chair; Sal Francomacaro, NIST, Vice Chair; and Richard Kissel, NIST, Principal voting member)
- E22 – Item Authentication
- M1 – Biometrics (Fernando Podio, NIST, Chair)
- T3 – Open Distributed Processing (ODP)
- T6 – Radio Frequency Identification (RFID) Technology
- GIT1 – Governance of IT
- DAPS38 – Distributed Application Platforms and Services

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

- Management of information security and systems
- Management of third-party information security service providers
- Intrusion detection
- Network security
- Cloud computing security
- Supply chain risk management
- Incident handling
- IT security evaluation and assurance
- Security assessment of operational systems

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

The scope of CS1 explicitly excludes the areas of work on cybersecurity standardization presently under way in INCITS B10, M1, T3, T10, and T11, as well as other standard groups, such as the Alliance for Telecommunications Industry Solutions (ATIS), the Institute of Electrical and Electronics Engineers, Inc. (IEEE), the Internet Engineering Task Force (IETF), the Travel Industry Association of America (TIAA), and the Accredited Standards Committee (ASC) X9. The CS1 scope of work includes standardization in most of the same cybersecurity areas as are covered in the NIST CSD.

As the U.S. TAG to ISO/IEC JTC 1/SC 27, CS1 contributes to the SC 27 program of work on IT Security Techniques in terms of U.S. comments and contributions on SC 27 standards projects; votes on SC 27 standards documents at various stages of development; and nominates U.S. experts to work on various SC 27 projects as editors, coeditors, or in other SC 27 leadership positions. Currently, over a dozen CS1 members are serving as SC 27 document editors or coeditors on various standards projects, including CSD staff Randy Easter and Richard Kissel.

All input from CS1 is processed through INCITS to ANSI, then to SC 27. CS1 also serves as a conduit for getting U.S.-based new work item proposals and U.S.-developed national standards into the international SC 27 standards development process. In its international efforts, CS1 responded to all calls for U.S. contributions and/or voting positions on all international security standards projects in ISO/IEC JTC1 SC 27 in a consistent, efficient, and timely manner.

NIST contributes to many of CS1's national and international IT security standards efforts through its membership on CS1, where Dan Benigni serves as the non-voting chair and Richard Kissel as the NIST Principal voting member. Internationally, there are over 100 published standards, and almost all have been adopted as U.S. national standards. There are more than 80 current international standards projects. During FY 2013, 29 new standards were published in SC 27, and most of them have been recommended by CS1 for adoption as U.S. national standards.

CSD Contributions to Cybersecurity Standardization in INCITS CS1

CSD's cybersecurity research also plays a direct role in the Cybersecurity Standardization efforts of CS1 at the national level. Nationally during FY 2013:

- The NIST Policy Machine research and development has resulted in three ongoing national standards projects in CS1, each in the early stages of development. They include:
  - INCITS 499-2013, "Next Generation Access Control –Functional Architecture (NGAC-FA)", David Ferraiolo, NIST, Editor, Published May 2013
  - "Next Generation Access Control – Generic Operations & Abstract Data Structures (NGAC-GOADS)", Project Number: 2195-D, Serban Gavrila, NIST, Editor (Planned Publication FY 2014)
  - "Next Generation Access Control-Implementation Requirements, Protocols and API Definitions (NGAC-IRPADS)", Project Number: 2193-D

Within CS1, liaisons are maintained with nearly 20 organizations, including:

- ABA Federated Identity Management Legal (IdM Legal) Task Force
- American Bar Association (ABA), section on Science and Technology
- Cloud Security Alliance
- Forum of Incident Response and Security Teams (FIRST)

- IEEE P1700 and P1619
- INCITS T11, M1, GIT1, DAPS38, and PL22
- Internet Security Alliance
- Kantara Initiative Identity Assurance Working Group (IAWG)
- Open Group
- SC 7 TAG
- Scientific Working Group on Digital Evidence (SWGDE)
- The Storage Networking Industry Association (SNIA)
- Trusted Computing Group

Dan Benigni also serves as cybersecurity standards coordinator in CSD.

Contact:

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

Identity Management Standards within INCITS B10 and ISO JTC1/SC 17

CSD supports identity management standardization activities through participation in national and international standards bodies and organizations. CSD actively participates in the INCITS B10 committee, which is focused on interoperability of Identification Cards and Related Devices. CSD staff serves as Chair and Vice Chair of the B10.12 committee, which develops interoperable standards for Integrated Circuit Cards with Contacts. CSD staff also serves as the U.S. Head of delegation to ISO/IEC JTC1 SC 17 Working Groups 4 and 11.

In addition to chairing the B10.12 committee, CSD provides technical and editorial support in the development of national and international standards. Specifically, CSD staff serves as the technical editor of ANSI 504-1, Generic Identity Command Set (GICS). GICS enables PIV, PIV-Interoperable (PIV-I) and Common Access Card (CAC) card applications, and others, to be built from a single platform. GICS defines an open platform where identity applications can be instantiated, deployed, and used in an interoperable way between the credential issuers and credential users. CSD staff also provides significant input to standards of major interest to U.S. government agencies and U.S. markets. CSD influences the development and revision of ISO/IEC 7816 (Identification Cards, Integrated Circuit Cards), ISO/IEC 24727 (Identification Cards, Integrated Circuit Card Programming Interfaces), and ISO/IEC 24787 (Biometrics "Match On Card" Comparison).

During FY 2013, INCITS 504 Parts 1, 2, and 4 were published and ISO/IEC 7816 Part 4 was published with significant changes added per NIST's request. CSD provides contributions and feedback on many other INCITS B10 identity management standards projects.

During the FY 2014, the INCITS B10 committee, along with the active collaboration of CSD staff, plans to publish Part 3 of INCITS 504 and contribute to the publication of several standards of the ISO/IEC 7816 family (all relevant to FIPS 201 specifications). CSD staff will continue actively supporting relevant ID management standard initiatives.

CSD's investment in these activities is motivated by new technical ideas that emerge from these standards. For example, INCITS 504 is an ID platform that leverages the FIPS 201 infrastructure to support a larger number of government and enterprise initiatives. In particular, INCITS 504 aims to support initiatives such as the NSTIC. ISO/IEC 24727 aims to create an interoperability framework that increases the resilience and scalability of identity management solutions and fosters domestic and international interoperability.

Contact:

Mr. Salvatore Francomacaro
(301) 975-6414
salvatore.francomacaro@nist.gov

Federal Information Security Management Act (FISMA) Implementation Project

The FISMA Implementation Project focuses on:

- Developing a comprehensive series of standards and guidelines to help federal agencies build strong cybersecurity programs, defend against increasingly sophisticated cyber attacks, and demonstrate compliance to security requirements set forth in legislation, Executive Orders, Homeland Security Directives, and Office of Management and Budget (OMB) policies
- Building common understanding and reference guides for organizations applying the NIST suite of standards and guidelines that support the NIST Risk Management Framework (RMF)
- Developing minimum criteria and guidelines for recognizing security assessment organization providers as capable of assessing information systems consistent with NIST standards and guidelines supporting the RMF

- Conducting FISMA outreach to public and private sector organizations

During 2013, CSD strengthened its collaboration with the Department of Defense (DoD), the Intelligence Community, and the Committee on National Security Systems (CNSS), in partnership with the Joint Task Force Transformation Initiative, which continues to develop key cybersecurity guidelines for protecting federal information and information systems for the Unified Information Security Framework. Previously, the Joint Task Force developed common security guidance in the critical areas of security controls for information systems and organizations, security assessment procedures to demonstrate security control effectiveness, security authorizations for risk acceptance decisions, and continuous monitoring activities to ensure that decision makers receive the most up-to-date information on the security state of their information systems. In addition, CSD worked with the General Services Administration (GSA) Federal Risk and Authorization Management Program (FedRAMP) to identify security assessment requirements, and prototype a process for approving Third-Party Assessment Organizations (3PAOs) that demonstrate capability in assessing Cloud Service Providers (CSP) information systems for conformance to NIST standards and guidelines.

In FY 2013, CSD worked on the following three initiatives:

1. ***Risk Management and Risk Assessment Guidelines:*** Developed a comprehensive risk assessment guideline examining the relationships among key risk factors, including threats, vulnerabilities, impact, and likelihood. Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides a holistic approach to information security and risk management. The publication provides organizations with security controls necessary to appropriately strengthen their information systems and the environments in which those systems operate – contributing to systems that are resilient in the face of attacks and other threats. This "Build It Right" strategy combines with a variety of security controls for "Continuous Monitoring" to give organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.

   To take advantage of the expanded set of security and privacy controls, and to give organizations greater flexibility and agility in defending their information systems, the revision introduces the concept of

GENERIC RISK MODEL WITH KEY RISK FACTORS

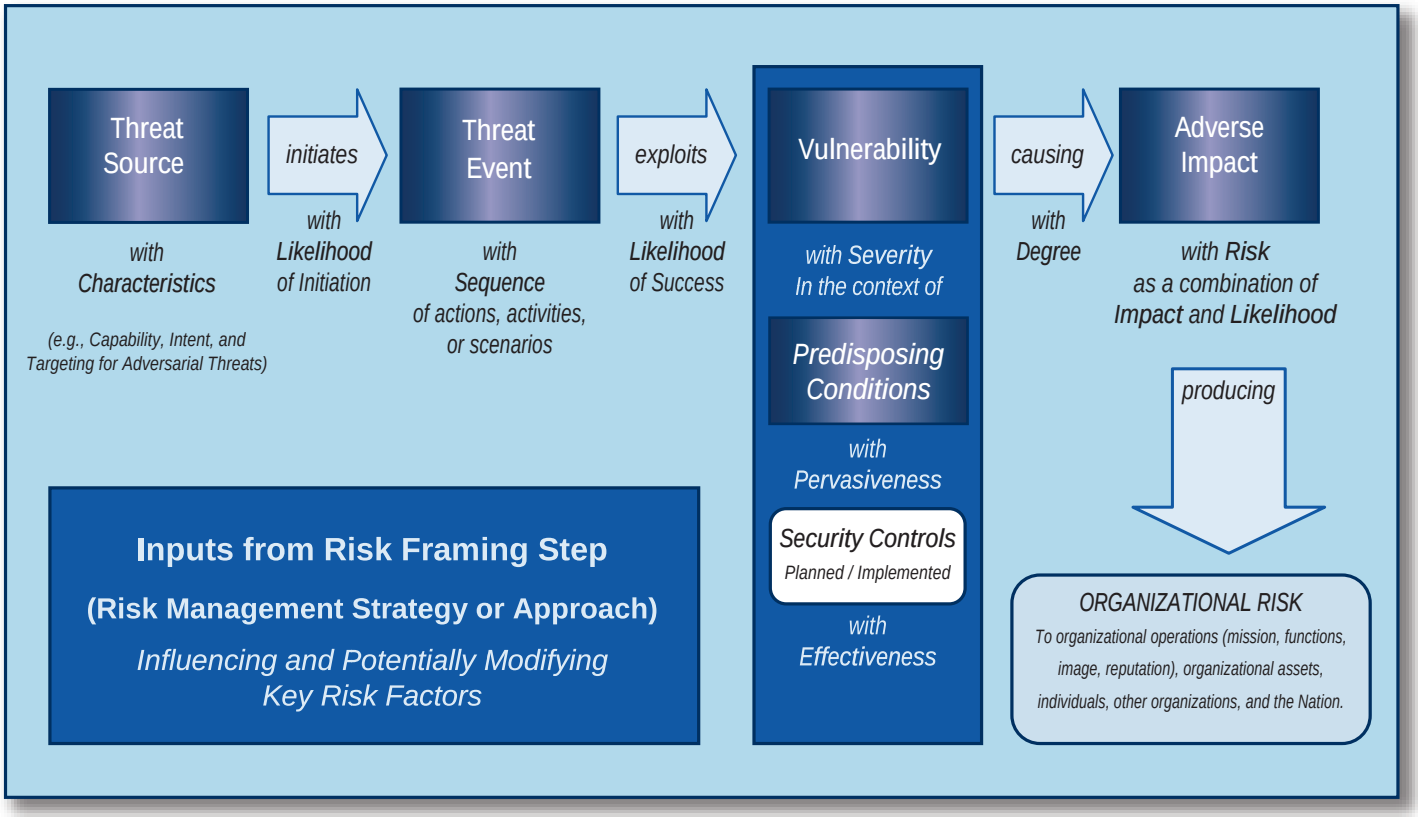


Figure 2: Generic Risk Model with Key Risk Factors

overlays. Overlays provide a structured approach to help organizations tailor security control baselines and develop specialized security plans for specific missions/business functions, environments of operation, and/or technologies. This specialization approach is important as the number of threat-driven controls and control enhancements in the catalog increases and organizations develop risk management strategies to address their specific protection needs within defined risk tolerances.

2. ***Criteria and Guidelines for Recognizing Security Assessment Provider Organizations:*** CSD updated proficiency tests and technical requirements for evaluating FedRAMP 3PAO providers' capability to conduct security assessment of cloud-based information systems for compliance with FISMA in accordance with FedRAMP and ISO/IEC 17020 Inspection Bodies requirements. Additionally, CSD provided input to GSA requirements (including orientation and training) for private sector accreditation body of FedRAMP 3PAOs that resulted in GSA FedRAMP Program Management Office (PMO) selecting one 3PAO private sector accreditation body.

3. ***FISMA Outreach Activity to Public and Private Sector Organizations:*** CSD conducted cybersecurity outreach briefings and provided support to state and local governments as well as private sector organizations on topics of interest, such as effective implementation of the NIST Risk Management Framework. In addition, CSD conducted outreach activities with academic institutions, providing information on NIST's security standards and guidelines, and exploring new areas of cybersecurity research and development.

In FY 2013, CSD completed the following outreach activities:

- Finalized SP 800-53, Revision 4
- Collaborated with the ITL Software and Systems Division and the NIST Standards Coordination Office using the International Standard ISO/IEC 17020:2008, *Conformity Assessment – Requirements for the operation of various types of bodies performing inspection,* in support of GSA in establishing a process for qualifying 3PAOs to conduct security assessments of CSPs information systems consistent with GSA requirements based on NIST standards and guidelines
- Developed a preliminary draft of SP 800-53A, Revision 4, *Guide for Assessing the Security and Privacy Controls in Federal Information Systems and Organizations*
- Developed a preliminary draft of SP 800-18, Revision 2, *Guide for Developing Security Plans for Federal Information Systems and Organizations*

In FY 2014, CSD intends to:

- Finalize SP 800-53A, Revision 4, *Guide for Assessing the Security and Privacy Controls in Federal Information Systems and Organizations*
- Finalize SP 800-60 Revision 2, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- Finalize SP 800-18 Revision 2, *Guide for Developing Security Plans for Federal Information Systems and Organizations*
- Expand cybersecurity outreach to include additional state, local, and tribal governments, as well as private sector organizations and academic institutions
- Continue to support federal agencies in effective implementation of the NIST Risk Management Framework.

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

Contacts:

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

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

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

Ms. Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

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

Biometric Standards and Associated Conformity Assessment Testing Tools

The CSD staff responds to government, industry, and market requirements for open systems standards by:

- Accelerating development of formal biometric standards
- Providing effective leadership and technical participation in the development of these standards
- Developing Conformance Test Architectures (CTA) and Conformance Test Suites (CTS) designed to test implementations of biometric standards
- Supporting harmonization of biometric, tokens, and security standards

- Promoting biometric standards adoption
- Promoting conformity assessment efforts

To achieve these project goals, CSD continues to work in close partnership with government agencies, industry partners, and academic institutions. CSD actively participates in a number of biometric standards development projects, contributes to the development of biometric standards, and leads national and international biometric standards bodies. Nationally, CSD's staff leads the INCITS Technical Committee 1 (M1) – *Biometrics*; international efforts include ISO JTC 1 and IEC Subcommittee SC 37 - Biometrics - JTC 1/SC 37. CSD plans to continue this work in FY 2014.

During FY 2013, the development of object-oriented CTAs and CTSs to test implementations of biometric standards progressed at an accelerated pace. CSD developed and publicly released two fully functional object-oriented CTAs. One CTA supports CTSs designed to test implementations of Extensible Markup Language (XML) encoded biometric data interchange formats and the other supports CTSs designed to test implementations of ISO/IEC data formats developed by JTC 1/SC 37 as well as PIV profiles of biometric standards. CSD released these test tools as "BioCTS 2013 for ANSI/NIST 1-2011" and "BioCTS 2013 for ISO/IEC" respectively. As depicted in the figure, CTA/CTSs' key features include search capabilities of the Text Log Outputs (very useful to debug errors in large implementations), formatted test results, and test result basic statistics (on batch of files or individual files).

In addition to previously designed CTSs (e.g., CTS for ANSI/NIST-ITL 1-2011 [AN-2011] traditional encoding transactions and ISO/IEC biometric data interchange format implementations), BioCTS 2013 conformance test software includes a CTS designed to test National Information Exchange Model (NIEM) XML encoded AN-2011 implementations. The functionality of this tool goes beyond the existing basic XML testing techniques, such as schema validation. CSD's project team concluded that the XML schema validation was insufficient to address full conformance testing of the AN-2011 requirements. The team implemented over 1,200 test assertions beyond the schema validation (validating an XML file against an XSD file) for this standard, including those for AN-2011 Record Types 1, 4, 10, 13, 14, 15, and 17. NISTIR 7957, *Conformance Test Architecture and Test Suite for ANSI/NIST-ITL 1-2011 NIEM XML Encoded Transactions* (September 2013) and a presentation delivered at the last Biometric Consortium conference discussed these test tools and provided technical implementation details.

BioCTS 2013 conformance test software also includes CTSs to test PIV profiles (e.g., finger minutia and image data formats) and to test implementations of the second-generation face recognition data format developed by JTC 1/SC 37 (published in 2011). The PIV profile of the SC 37 iris data format was aligned with SP 800-76-2, *Biometric Specifications for Personal Identity Verification*. The face recognition CTS was aligned with the associated conformance testing methodology developed by JTC 1/SC 37.

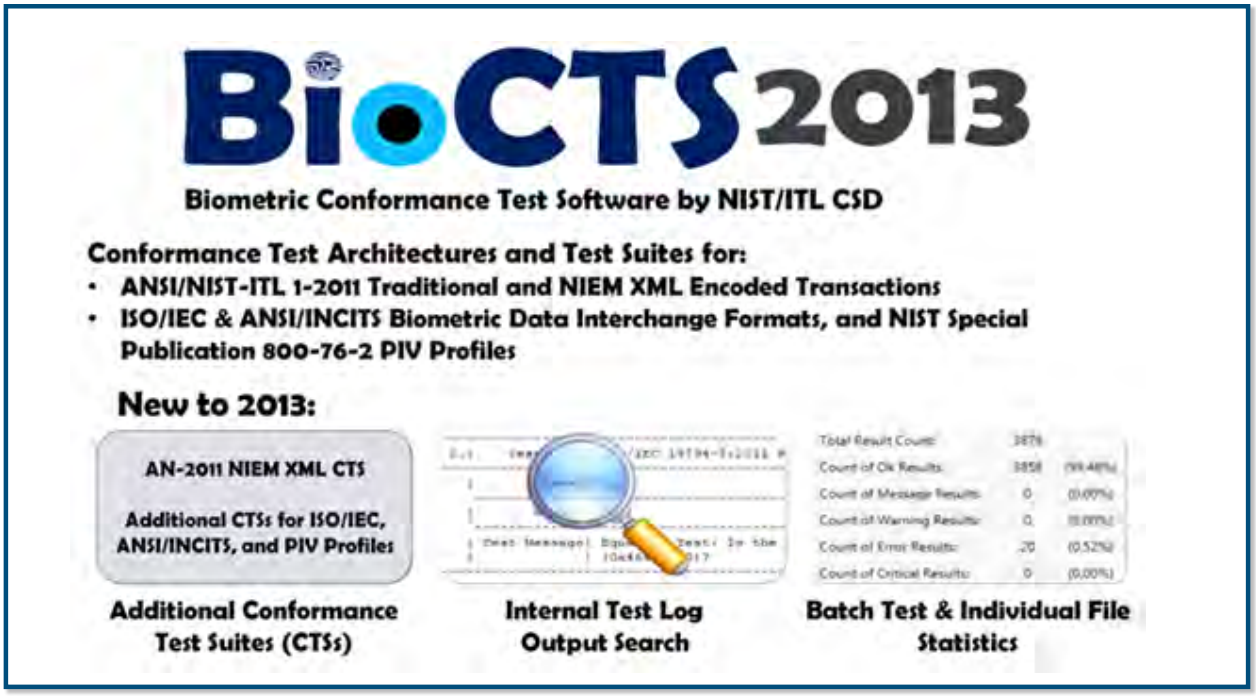


Figure 3: Biometric Conformance Test Software by NIST/ITL CSD

These conformance-testing tools provide significant functionality, usability, and performance. In addition to supplying an installer version of the CTAs, which supports new and existing CTSs with new graphical user interface enhancements, the CSD project team extended the work to a command line interface version for AN-2011 traditional encoding that runs under Windows and Linux (with Mono). The test tools developed support a Web-based environment. A prototype was developed, tested, and demonstrated at the last Biometric Consortium Conference.

Based on the detailed analysis of the biometric standards (ISO/IEC and AN-2011) required to develop the associated conformance test tools, the CSD team provided technical contributions to the relevant standards bodies. In FY 2013, these included:

- Over 200 test assertions for AN-2011 Record Type 18 – DNA Data Record
- Technical contributions on the AN-2011 standard and the published XML schema
- Technical contributions to JTC 1/SC 37 (via INCITS M1) on SC 37 XML namespaces, data elements, schemas, and related items; an XML-based data interchange format framework and DNA data interchange format

In addition to ongoing participation and management of biometric standards activities in INCITS M1 and JTC 1/SC 37, in FY 2014, CSD plans to develop additional CTSs to test implementations of selected international biometric data interchange formats specified in XML encoding (under development in JTC 1/SC 37). The CSD team also plans to develop conformance test assertions for selected record types of the 2013 version of the ANSI/NIST standard and plans to develop the associated CTA/CTS for traditional and XML encoded transactions. The latest version of the ANSI/NIST standard now incorporates extended forensics-related data, such as a dental supplement and additional record types, such as voice data record. The team will continue researching and developing additional test environments support, such as web services and tools in the cloud. The research plan expands to technical interfaces, such as Biometric Application Programming Interface standards specified in Object Oriented Programming and Biometric Information Assurance Services standards.

Outreach efforts in FY 2013 in support of biometric standards development and conformity assessment efforts included:

- Contribution of the area editor for articles on biometric standards for Springer's second edition of the Biometrics Encyclopedia (under development), where 25 papers were reviewed and edited
- Keynote talks and presentations on biometric standards and conformity assessment at national and international conferences
- Related technical publications and participation in conference program committees and paper reviews

NIST helped develop the program of the 2013 Biometric Consortium Conference, which CSD's Mr. Fernando Podio co-chaired. Held September 17-19, 2013, in Tampa, Florida, this year's conference included nearly 1,600 attendees from 30 countries representing government, industry, and academia.

CSD supported a booth at the conference's technical exposition and presented material regarding the conformance test tool development project. The conference program included sessions on Federal Government programs, advances in biometric technologies and standards, and Biometrics Identity and Security (BIdS) research. NIST's session highlighted achievements and ongoing biometric research, testing, and standards projects. Over 140 speakers participated in the program.

ITL's Biometric Resource Center:
http://www.nist.gov/biometrics

BioCTS 2013 - Biometric Conformance Test Tool Downloads:
http://www.nist.gov/itl/csd/biometrics/biocta_download.cfm#CTAdownloads

Biometric Consortium website:
http://www.biometrics.org

Biometric Consortium 2013 conference program (released presentations are linked):
http://www.biometrics.org/bc2013/program.pdf

Contact:

Mr. Fernando Podio
(301) 975-2947
fernando.podio@nist.gov

Cybersecurity of Cyber-Physical Systems (CPS)

Leveraging CSD's expertise in cybersecurity for industrial control systems, smart grid, hardware-enabled security, and embedded systems, the division is now researching cybersecurity needs of the broader landscape of cyber-physical systems (CPS). CPS are hybrid networked cyber and engineered physical elements co-designed to create adaptive and predictive systems that respond in real-time to enhance performance with varying degrees of human interaction, and are commonly used in the nation's critical infrastructure. Such systems control the electrical grid, provide clean water, produce chemicals, and underlie transportation systems. CPS capabilities continue to grow as a result of technological advances, enabling future engines of growth, such as advanced manufacturing, and advancements in safety initiatives, such as autonomous vehicles.

Cybersecurity is an important crosscutting discipline that is critical to safeguarding CPS and supporting communications and information infrastructure. CPS presents unique challenges, including the need for real-time response in support of extremely high availability, predictability, and reliability. Despite the ubiquity and criticality of CPS, additional thought is required regarding the design of secure CPS. As a result, there have been numerous successful attacks targeting CPS for the control of critical infrastructure (e.g., Stuxnet, Duqu, Flame, Gauss).

In April 2013, CSD and the Cyber Security Research Alliance (CSRA) co-hosted a 2-day workshop to explore emerging research needs for cybersecurity in CPS with the diverse cyber-physical community at large. The workshop brought together engineering and IT experts who have dealt with security issues related to CPS. Representatives from industry, academia, and government engaged in interactive discussions during the workshop in the areas of supply chain, assurance, threat information, identifying existing tools and practices to secure CPS, security in acquisition and implementation, and trustworthy operations. Attendees were invited to participate in break-out sessions where the discussion topics were briefly framed, allowing the attendees to explore the discussion topics and to share their experiences with integrating security into existing organizations (e.g., lessons learned and examples).

CSD, in conjunction with ITL's Advanced Network Technologies division, Information Access division, and NIST's Engineering Laboratory, collaborated to develop an initial NIST notional reference architecture for CPS. This notional reference architecture was designed at such a level of abstraction that it can be applied across the breadth of the CPS, yet provides modularization and context for integration. The notional CPS reference architecture was driven from a community need to provide a common lexicon and taxonomy, a common architectural vision to help facilitate interoperability between elements and systems, and promotes communication across the breadth of CPS stakeholders.

CSD, in conjunction with NIST's Engineering Laboratory, will finalize the revision of SP 800-82 in FY 2014. CSD will continue to participate in the International Society of Automation (ISA) 99 Committee, which develops and establishes standards, recommended practices, technical reports, and related information that define procedures for implementing electronically secure industrial automation and control systems and security practices, and for assessing electronic security performance. Leveraging the initial NIST notional reference architecture as a starting point to address the lack of an industry-wide consensus definition, reference architecture, and taxonomy for CPS, CSD will work in collaboration with NIST's Engineering Laboratory and ITL's Software and Systems division, and Advanced Networking Technologies division to lead a public-private working group of government, academia, and industry stakeholders. The working group will consist of 5 technical subgroups: 1) Definitions and Taxonomy, 2) Reference Architecture, 3) Use Cases, 4) Cybersecurity and Privacy, and 5) Timing. CSD will lead the Cybersecurity and Privacy subgroup focused on identifying strategies for cybersecurity and privacy in CPS, and work collaboratively with the other subgroups to ensure that cybersecurity is included as a design principle in development.

Contacts:

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

Ms. Suzanne Lightman
(301) 975-6442
suzanne.lightman@nist.gov

Ms. Vicky Yan Pillitteri
(301) 975-8542
victoria.yan@nist.gov

Federal Cybersecurity Research & Development (R&D)

The Networking and Information Technology Research and Development (NITRD) Program provides a framework in which many federal agencies come together to coordinate their networking and IT research and development (R&D) efforts. CSD remained committed to the value of communicating its R&D efforts to other federal colleagues and identifying the opportunities to support R&D efforts throughout the Federal Government.

In FY 2013, the CSIA Interagency Working Group (IWG) monthly meetings provided an opportunity to learn and share about

ongoing research related to the themes and thrusts expressed in the Strategic Plan for the Federal Cybersecurity Research and Development. CSD briefed the working group regarding efforts on Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," under which NIST has been directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. CSD also described work on the Advanced Network Technologies division's High Assurance Domain project, which exists to foster development and deployment of new network security technologies to increase trust in online communications.

CSD is also a regular participant in the coordination activities of the federal Special Cyber Operations Research and Engineering (SCORE) Committee. SCORE enables technology transfer through the sharing of NIST cybersecurity expertise and output. The SCORE committee interacts with federal leaders as part of the White House's Comprehensive National Cybersecurity Initiatives (CNCI).

Contacts:

Mr. Bill Newhouse
CSIA IWG, CSIA SSG
(301) 975-2869
william.newhouse@nist.gov

Dr. Ernest McDuffie
SEW Education Team and SCORE rep
(301) 975-8897
ernest.mcduffie@nist.gov

Security Aspects of Electronic Voting

In 2002, Congress passed the Help America Vote Act (HAVA) to encourage the upgrade of voting equipment across the United States. HAVA established the Election Assistance Commission (EAC) and the Technical Guidelines Development Committee (TGDC), chaired by the Director of NIST. HAVA directs NIST to provide technical support to the EAC and TGDC in efforts related to human factors, security, and laboratory accreditation. As part of NIST's efforts, CSD supports the activities of the EAC related to voting equipment security.

In the past year, NIST supported the EAC by developing responses to public comments on the Voluntary Voting System Guidelines (VVSG) 1.1. The security guidelines were updated in FY 2012 to improve the auditability of voting systems, to provide greater software integrity protections, to expand and improve access control requirements, and to help ensure cryptographic security mechanisms are implemented properly. In addition, CSD supported the efforts of the EAC and Federal Voting Assistance Program (FVAP) of DoD to improve the voting process for citizens under the Uniformed and Overseas Citizens Voting Act (UOCAVA) by leveraging electronic technologies. The team worked with the TDCG's UOCAVA Working Group to develop a risk analysis on technologies used in current UOCAVA voting processes, including vote-by-mail, online voter registration, electronic ballot delivery, and online ballot marking.

In FY 2014, NIST will continue to assist the EAC in developing responses to public comments and providing updates to VVSG 1.1. Additionally, CSD will continue to support efforts for the EAC and FVAP to improve the voting process for UOCAVA voters. CSD will continue security research efforts to support future standards development efforts, particularly in the areas of risks to voting systems and innovative voting system architectures.

http://vote.nist.gov

Contacts:

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

Mr. Joshua Franklin
(301) 975-8463
joshua.franklin@nist.gov

Health Information Technology Security

Health information technology (HIT) enables better patient care through secure use and sharing of health information. It leads to improvements in healthcare quality, reduced medical errors, increased efficiencies in care delivery and administration, and improved population health. Central to reaching these goals is the assurance of the confidentiality, integrity, and availability of health information. CSD works with government, industry, academia, and others to provide security tools, technologies, and methodologies that provide for the security and privacy of health information.

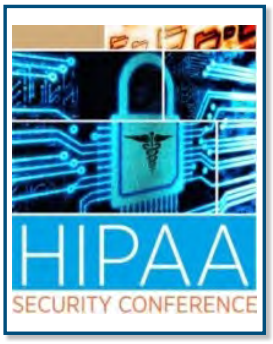
NIST continued its HIT security outreach efforts in FY 2013. NIST and the Department of Health and Human Services' (DHHS) Office for Civil Rights (OCR) cohosted the sixth annual HIPAA Security Rule conference, "*Safeguarding Health Information: Building Assurance through HIPAA Security*," in May 2013 at

the Ronald Reagan Building and International Trade Center in Washington, D.C. The conference offered important sessions that focused on broad topics of interest to the healthcare and health IT security community. Over 600 in-person and virtual attendees from federal, state, and local governments, academia, HIPAA-covered entities and business associates, industry groups, and vendors heard from, and interacted with, healthcare, security, and privacy experts on technologies and methodologies for safeguarding health information and for implementing the requirements of the HIPAA Security Rule. Presentations covered a variety of current topics including:

- Updates on the OCR privacy, security, and breach notification audit program
- Patient and provider identity management, HIPAA requirements in cloud and mobile environments
- HIPAA rule changes affecting breach notification and HIPAA security
- Cybersecurity Framework for improving critical infrastructure cybersecurity
- Health IT activities at the National Cybersecurity Center of Excellence
- Methods for managing insider threat
- Tools available to manage security settings on end-user devices

The keynote address was delivered by Eric Dishman, Fellow and General Manager of the Health Strategy & Solutions Group at Intel.

In FY 2014, NIST plans to issue a draft revision to Special Publication (SP) 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule*. As part of its continued outreach efforts, NIST also plans to co-host the seventh annual *Safeguarding Health Information* conference with OCR.



http://www.nist.gov/healthcare/security/

Contact:

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

Supply Chain Risk Management (SCRM) for Information and Communications Technology (ICT)

Federal agency information systems are increasingly at risk of both intentional and unintentional supply chain compromise. The management of ICT supply chain risk includes ensuring the integrity, security, and resilience of the supply chain and the products and services it delivers (Figure 4). Today's ICT supply chains have increased complexity, diversity, and scale. Federal Government information systems have rapidly expanded in terms of capability and number, with an increased reliance on outsourcing and commercially available products. These trends have caused federal departments and agencies to have a lack of visibility and understanding of how acquired technology is developed, integrated, and deployed. Supply chain risks also affect the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of products and services. This lack of visibility and understanding, in turn, has decreased federal departments' and agencies' control regarding decisions affecting the inherited supply chain risks and the ability to manage those risks.

Figure 4: The Four Elements of ICT SCRM

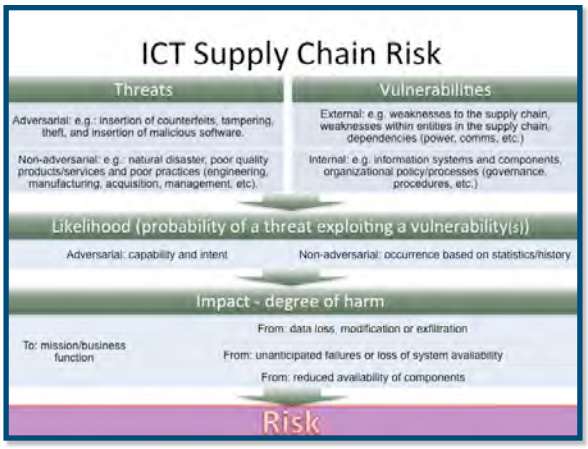


Figure 5: ICT Supply Chain Risk

The ICT SCRM project seeks to provide federal agencies with a toolkit of standardized, repeatable, and practical resources to strategically manage supply chain risk throughout the entire lifecycle of systems, products, and services.

In October 2012, NIST held a workshop with industry, academic, and government stakeholders to discuss:

- The fundamental underpinnings of ICT SCRM (terms, definitions, characterizations)
- Current and needed commercially reasonable ICT SCRM-related standards and practices (need, scope, and development approach)
- Current and needed ICT SCRM tools, technology, and techniques useful in securing the ICT supply chain
- Current and needed research and resources

NIST used input from the workshop and additional stakeholder forums to begin developing an initial public draft of NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* which is scheduled to be finalized in FY 2014. This document provides guidance to federal departments and agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels in their organizations and utilizes and builds on existing guidance in the unified information security framework.

Additionally in FY 2013, a grant was awarded to the University of Maryland's Supply Chain Management Center to support the development and hosting of a web application with the following capabilities:

- Enterprise Risk Assessments: A three-tier risk analysis system based on the ICT SCRM Community Framework Reference Architecture – A Strategic Assessment/ Organizational Readiness, Best Practices and Standards, and a composite network vulnerability map of physical and cyber hubs and nodes, with risk ratings
- Collaboration/Crowdsourcing Portal: User-documented ICT SCRM use/abuse cases and real-time polling about vulnerabilities and responses
- ICT SCRM Initiatives: A dynamic matrix of current industry and public sector ICT SCRM best practices, standards, and policy reform initiatives that can be updated by appropriate individuals from across industry, academia, and government
- ICT SCRM Digital Library: An online repository of policy and academic documents related to ICT SCRM

In FY 2014, CSD will continue its work to develop and publish draft NIST SP 800-161. It will research and develop tools and guidance to help agencies more effectively manage their ICT supply chain risk. Additionally, NIST will continue to co-chair Working Group 2 of the White House's Comprehensive National Cybersecurity Initiative (CNCI) 11, *Develop a Multi-Pronged Approach for Global Supply Chain Risk Management,* and participate in national and international standards activities related to supply chain risk management. Feedback from organizations implementing ICT SCRM programs will be evaluated, and best practices will be accumulated. NIST will continue to engage stakeholders to identify needs and opportunities for providing additional guidance regarding identifying and implementing supply chain protections.

http://csrc.nist.gov/scrm/
ICT SCRM Team email: scrm-nist@nist.gov

Contacts:

Mr. Jon Boyens
Project Lead
(301) 975-5981
jon.boyens@nist.gov

Ms. Celia Paulsen
(301) 975-5549
celia.paulsen@nist.gov

Nationwide Public Safety Broadband Network (NPSBN) Security

In February 2012, Congress passed the Middle Class Tax Relief and Job Creation Act. One portion of this legislation calls for the establishment of a nationwide, interoperable public safety broadband network based on Long-Term Evolution (LTE) technology. The network will be deployed and operated by the First Responder Network Authority (FirstNet). The planned National Public Safety Broadband Network (NPSBN) will "*create a much needed nationwide interoperable broadband network that will help police, firefighters, emergency medical service professionals and other public safety officials stay safe and do their jobs.*" (http://www.ntia.doc.gov/category/public-safety). NIST is directed to establish a list of certified devices and required components for interacting with the nationwide network by public safety officials, vendors, and other interested parties. NIST is directed to conduct research and development that supports the acceleration and advancement of the nationwide network.

Image Source: http://www.pscr.gov/index.php

In FY 2013, CSD supported the joint National Telecommunications and Information Administration (NTIA) and NIST Public Safety Communications Research (PSCR) program (http://www.pscr.gov) efforts by developing and establishing security-related activities to support the proposed NPSBN. CSD presented details of the PSCR security-related activities at PSRC's Annual Public Safety Broadband Stakeholder Conference in June 2013.

CSD provided comments and contributed text for the security-related aspects of the National Public Safety Telecommunications Council (NPSTC) *Public Safety Broadband High-Level Launch Requirements,* published in December 2012, that describe, in increasing levels of detail, the technical requirements of the NPSBN infrastructure, equipment, and communications.

CSD began participating in the standards development process for LTE technology within the 3rd Generation Partnership Project (3GPP) supporting public safety's security requirements related to Proximity Services (ProSe) and Group Communication System Enablers (GCSE). In addition, CSD broadened its scope within the IETF to include efforts related to public safety.

In FY 2014, CSD will continue supporting NPSTC's efforts related to NPSBN and to representing public safety in international standardization efforts, such as IETF and 3GPP. CSD will work to incorporate security capabilities into the PSCR's Public Safety Broadband Demonstration Network located in Boulder, conduct research into identity management technologies for mobile devices that can support the NPSBN, and investigate ways to enhance the security of mobile applications used by the public safety community. CSD will continue to engage the public safety communications community by participating in events such as PSRC's Annual Public Safety Broadband Stakeholder Conference.

Contacts:

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

Dr. Nelson Hastings
(301) 975-5237
nelson.hastings@nist.gov

Smart Grid Cybersecurity

Figure 6: Smart Meter

The major elements of the smart grid are the information technology, the industrial control systems, and the communications infrastructure used to send command information across the electric grid from generation to distribution systems, and to exchange usage and billing information between utilities and their customers. Key to the successful deployment of the smart grid infrastructure is the development of the cybersecurity strategy that includes cybersecurity as a design consideration for new and emerging systems, and an approach to adding cybersecurity into existing systems. The electric grid is critical to the economic and physical well-being of the nation, and emerging cyber threats targeting power systems highlight the need to integrate advanced security to protect critical assets.

In January 2013, the Smart Grid Interoperability Panel (SGIP) became a membership-supported organization. The SGIP Cybersecurity Working Group (CSWG) was renamed the Smart Grid Cybersecurity Committee (SGCC). All three of these groups have been led by a NIST representative since their respective

creations, originating with the Cybersecurity Coordination Task Group (CSCTG), created by NIST in support of the Energy Independence and Security Act of 2007. The SGIP SGCC includes additional leadership by a management team, comprised of three volunteer vice-chairs representing the Department of Energy (DOE), an electric utility, and a smart grid vendor, and a volunteer secretariat.

During the past year, members of the CSWG/SGCC worked to revise NISTIR 7628, *Guidelines for Smart Grid Cybersecurity,* to address changes in technologies and implementations since the publication's original release. The revision updates and expands the development strategy, cryptography and key management, privacy, vulnerability classes, research and development topics, standards review, and key power system use cases to reflect changes in the smart grid environment since 2010. The final version is expected to be posted in FY 2014.

In addition to the revision of NISTIR 7628, the CSWG/SGCC has focused on specific topics such as cybersecurity risk management, security architecture, security testing and certification, Advanced Metering Infrastructure (AMI) security, the development of a User's Guide for NISTIR 7628, and cloud computing and privacy for the smart grid. Work in these areas is completed through SGCC subgroups, which are created and disbanded in order to meet present needs. The SGCC currently consist of the following subgroups:

- The **Architecture subgroup** continues to refine the smart grid cybersecurity architecture in coordination with the SGIP Smart Grid Architecture Committee on the European Union architecture harmonization effort.
- The **Cloud Computing subgroup** is addressing the unique cybersecurity issues of using and managing smart grid applications that utilize the cloud.
- The **High-Level Requirements subgroup** maintains the high-level security requirements in NISTIR 7628 and develops analyses between NISTIR 7628 and other documents, standards, and guidelines.
- The **NISTIR 7628 User's Guide subgroup** is developing a User's Guide for utilities and other entities involved in implementing smart grid systems can use to apply the NISTIR 7628; including the identification, risk assessment and selection of the applicable security requirements needed to secure their smart grid systems.
- The **Privacy subgroup** identifies and describes privacy risks and concerns within developed or emerging interoperability standards for the smart grid, and then determines the most appropriate and feasible practices for mitigating the risks.
- The **Standards subgroup** assesses cybersecurity requirements associated with SGIP-identified smart grid standards and other documents for the SGIP Catalog of Standards (CoS). The subgroup has reviewed over 75 documents to date.

An example of a SGCC deliverable in 2013 is the analysis of cybersecurity regulations relevant to electricity subsector stakeholders and of NIST security guidance. The analysis identifies the relationship, similarities, and differences among NISTIR 7628, SP 800-53, and the draft North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIP) v5, recognizing that each document has a different scope and audience.

The SGCC also supports the SGIP Catalog of Standards (CoS), a compendium of standards, practices, guidelines and other technical documents considered relevant for the development of a robust, secure, and interoperable smart grid. Through the ongoing efforts of the SGCC, these documents are reviewed for cybersecurity, and recommendations are made for how to include cybersecurity in future revisions and in the implementation of the standards. CSD supports the SGCC in assessing the security of cryptographic methods used in these standards, practices, guidelines, and other technical documents. In many cases, the standards bodies have taken the results of the reviews and modified the standards or documents to address our recommendations. The SGCC has worked closely with some of the standards bodies to ensure that the recommendations are interpreted correctly and that the mitigation strategies selected meet the intent of the NISTIR 7628 high-level security requirements. The result is cybersecurity "baked-in" to the standards rather than "bolted-on" after the standard is implemented.

In FY 2014, CSD will continue to support the SGCC in the evaluation of the cryptographic methods used standards, practices, guidelines, and other technical documents for inclusion in the SGIP CoS.

Future activities include working with the SGIP Committees, Domain Expert Working Groups, and Priority Action Plans to integrate cybersecurity into their work efforts. The SGCC will establish a new subgroup to produce a cybersecurity risk

management process case study to accompany the Department of Energy Risk Management Process guideline. Members of the committee will produce white papers on security defense in depth and breadth, unique cloud computing considerations for the smart grid, as well as a User's Guide for NISTIR 7628. Additionally, the SGIP SCCC will continue to collaborate with industry, academia, other working groups, and government agencies to address the cybersecurity needs for the smart grid.

In addition to the SGIP SGCC activities, CSD will also coordinate with NIST's Engineering Laboratory (EL) and Smart Grid Program Office on the development of a Cybersecurity Smart Grid Test Lab, part of the NIST Smart Grid Testbed Facility now under construction. CSD will also collaborate with ITL's Software and Systems Division on cybersecurity research in relation to the IEEE 1588, *Precision Time Protocol*, a standard on time synchronization that is used for the electric grid and other special-purpose industrial automation and measurement networks.

http://www.sgip.org

Contacts:

Ms. Vicky Yan Pillitteri
(301) 975-8542
victoria.yan@nist.gov

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

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

Cybersecurity Awareness, Training, Education, and Outreach

National Initiative for Cybersecurity Education (NICE)

NIST has served as the lead for the National Initiative for Cybersecurity Education (NICE) since 2010. NICE is responsive to President Obama's declaration that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and "America's economic prosperity in the 21st century will depend on cybersecurity."

The goal of NICE is to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace for all. NICE addresses this challenging goal by:

- Raising national awareness about risks in cyberspace
- Broadening the pool of individuals prepared to enter the cybersecurity workforce
- Cultivating a globally competitive cybersecurity workforce

This initiative comprises four component areas:

- National Cybersecurity Awareness
- Formal Cybersecurity Education
- Cybersecurity Workforce Structure
- Cybersecurity Workforce Training and Professional Development

CSD is home to the NIST NICE Leadership Team (NNLT) that focuses on the following activities:

- Developing planning documents and building consensus on the strategy and implementation activities of NICE
- Facilitating cross-functional cooperation among NICE component lead agencies
- Fostering communication between the component lead agencies by coordinating meetings, facilitating discussions, and disseminating information
- Promoting the initiative and its efforts by representing NICE and speaking at cybersecurity events nationwide
- Planning and hosting an annual workshop to promote and support the evolving issues in cybersecurity education
- Coordinating with other federal initiatives and efforts related to NICE
- Maintaining and updating the NICE website

In FY 2013, NIST stewarded the National Cybersecurity Workforce Framework (NCWF), developed within NICE's Cybersecurity Workforce Training and Professional Development Component, through government-wide review. NIST also planned, organized and hosted the fourth annual NICE Workshop, "Navigating the National Cybersecurity Education Interstate Highway," from September 17-19, 2013. The workshop highlighted cybersecurity awareness, education, and training programs that can be adopted, copied, used, or built-on by small businesses, educational institutions, industry, and government at the state, local, tribal and federal levels to advance the strategic goals of NICE.

The NNLT attended more than 100 events, symposia, forums, competitions, educational outreach meetings, and workshops to promote the activities within NICE. The NNLT worked with the Office of Personnel Management (OPM) on the OPM Cross-Agency Priority Goal: "Closing Skills Gap" for IT/Cybersecurity and on the OPM Special Cybersecurity Workforce Project focused on reducing cybersecurity workforce skills gaps. The project will allow agencies to identify and address their needs for cybersecurity skill sets to meet their missions. In accomplishing this project, agencies will also be updating their cybersecurity positions with codes that revise the definitions of and taxonomy used for cybersecurity work. In FY 2013, the NNLT supported DHS in the launch of the National Initiative for Cybersecurity Careers and Studies (NICCS), (http://niccs.us-cert.gov), an online resource for cybersecurity career, education, and training information. NICCS leverages efforts of government, industry, and academia to provide a comprehensive, single resource to address the nation's cybersecurity knowledge needs.

In FY 2014, NIST will continue to promote the coordination of existing and future cybersecurity education, training, and awareness activities while planning the transition of NICE leadership. NIST will also identify opportunities to extend and integrate NICE activities to raise cybersecurity awareness in the context of other sectors, and promote the NCWF as a resource to be used to identify workforce gaps, lead bi-weekly NICE component meetings, and continue to conduct broad outreach on the NICE program.

http://www.nist.gov/nice/

Contacts:

Dr. Ernest McDuffie
NICE Project Lead
(301) 975-8897
ernest.mcduffie@nist.gov

Mr. Bill Newhouse
NICE Program Lead
(301) 975-2869
william.newhouse@nist.gov

Computer Security Division Publications

During FY 2013, CSD continued its efforts to improve the quality of information about its publications on various NIST websites. CSD also explored new ways to make those publications available to CSD's customers, who access CSD's technical security publications in various ways: (1) directly from the CSRC website, (2) through the NIST Publications Portal, via Internet search or (3) direct links from digital content, or (4) from external information providers. By the end of FY 2013, CSD had more than 270 current publications in the NIST technical series (FIPS, Special Publications (SPs) and NISTIRs).

Providing accurate metadata about publications improves users' abilities to locate the information they are seeking. In FY 2013, CSD cleaned up the NIST Publications Portal records and PDF metadata for all of its NIST technical series publications and for more than 100 journal articles and conference papers co-authored by CSD staff in recent years. By improving the metadata—such as title, authors, report numbers and keywords—within the PDFs themselves, Internet searches provide more informative results and make NIST's security publications easier to find. CSD continues to apply those consistent metadata practices to all new publications.

Additionally, CSD expanded the dissemination of its publications to the Association for Computing Machinery (ACM) Digital Library (DL). ACM DL now has a "collection" of NIST Computer Security Publications, which includes SP 800-series publications. CSD initiated an internal project to test the feasibility of creating electronic book (e-book) editions of its FIPS, SPs and NISTIRs, to supplement the PDF editions currently available on CSRC. The aim is to provide a wider range of options for CSD customers to view and use CSD's technical publications. The pilot project uses the EPUB file format, an open standard for e-books from the International Digital Publication Forum (IDPF). CSD intends to begin posting EPUB versions of selected publications in FY 2014, which will especially benefit users of mobile devices.

In FY 2014, CSD intends to explore more ways to improve the consistency of its publications and associated metadata, enhance users' ability to browse and search publications on CSRC, make more e-book editions available, and expand publication availability on external sites.

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

Contact:

Mr. Jim Foti
(301) 975-8018
jfoti@nist.gov

Computer Security Resource Center (CSRC)

The Computer Security Resource Center (CSRC), CSD's website, is one of the most visited websites at NIST. CSRC encourages broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies and links key security web resources to support industry and government users. CSRC is an integral component of all of the work that CSD conducts and produces. It is CSD's repository for anyone wanting to access these documents and other valuable security-related information. During FY 2013, CSRC had more than 53 million page views and downloads.

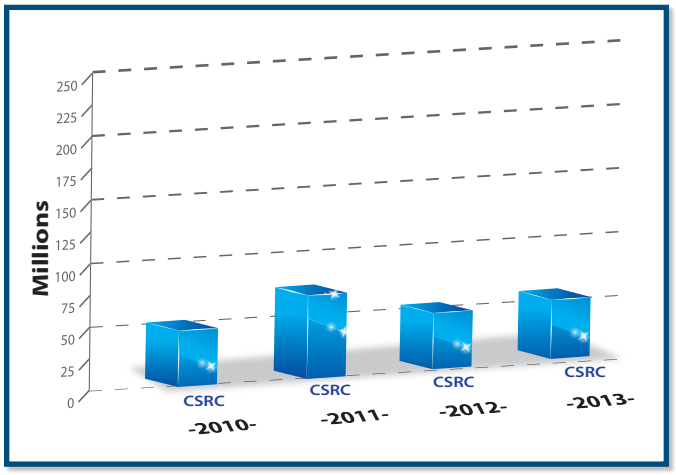


Figure 7: Total Number of CSRC Website Requests for 2013 (Oct. 1, 2012 to Sept. 30, 2013)

CSRC is the primary gateway for gaining access to NIST computer security publications, standards, and guidelines, and serves as a vital link to CSD's customers. Publications are organized to help users locate relevant information quickly and are arranged by topic, relevant security control family, and legal requirements.

During FY 2013, the top ten most downloaded publications were:

1. SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
2. SP 800-12, *An Introduction to Computer Security: The NIST Handbook*
3. FIPS 140-2, *Security Requirements for Cryptographic Modules*
4. FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
5. SP 800-100, *Information Security Handbook: A Guide for Managers*
6. SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
7. SP 800-57, *Recommendation for Key Management: Part 1: General*
8. SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
9. NISTIR 7916, *Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop*, April 23-24, 2012
10. SP 800-123, *Guide to General Server Security*

In the FIPS publication series, the top three most downloaded FIPS were:

1. FIPS 140-2, *Security Requirements for Cryptographic Modules*
2. FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
3. FIPS 197, *Advanced Encryption Standard*

In the SP publication series, the top three most downloaded SPs were:

1. SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
2. SP 800-12, *An Introduction to Computer Security: The NIST Handbook*
3. SP 800-100, *Information Security Handbook: A Guide for Managers*

In the NISTIR publication series, the top three most downloaded NISTIRs were:

1. NISTIR 7916, *Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop, April 23-24, 2012*
2. NISTIR 7250, *Cell Phone Forensic Tools: An Overview and Analysis*
3. NISTIR 7896, *Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition*

In addition to CSRC, CSD maintains a publication announcement mailing list. This free email list notifies subscribers about publications that have been posted to the CSRC website. The email list is a valuable tool for more than 28,000 subscribers from the Federal Government, industry, academia, and individuals with a personal interest in IT security. Individuals who are interested in subscribing to this list should visit http://csrc.nist.gov/publications/subscribe.html for more information.

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

Contacts:

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

Ms. Judy Barnard
(301) 975-5502
jbarnard@nist.gov

Federal Computer Security Program Managers' Forum

The Federal Computer Security Program Managers' Forum is sponsored by NIST to promote the sharing of security-related information among federal agencies. The Forum, which serves more than 1,100 members, strives to provide an ongoing opportunity for managers of federal information security programs to exchange information security materials in a timely manner, build upon the experiences of other programs, and reduce possible duplication of effort. It provides a mechanism for NIST to share information directly with federal agency information security program managers in fulfillment of NIST's leadership mandate under FISMA. It assists NIST in establishing and maintaining relationships with other individuals or organizations that are actively addressing information security issues within the Federal Government. NIST serves as the Secretariat of the Forum, providing necessary administrative and logistical support. Kevin Stine serves as the Chairperson.

The Forum maintains an extensive email subscription service. Participation in the service is only open to Federal Government employees who participate in the management of their organization's information system security program. There are no membership dues. The Forum also holds bimonthly meetings and an annual 2-day conference to discuss current issues and developments of interest to those responsible for protecting sensitive (unclassified) federal systems. Participation in Forum meetings is open to Federal Government employees, and their designated support contractors, who participate in the management of their organization's information security program.

Topics of discussion at Forum meetings in FY 2013 included briefings from various federal agencies on Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance; Software Assurance: Enabling Security throughout the Software Development Lifecycle; Use of Cybersecurity Function Code; Census Risk Management Program Implementation; National Cybersecurity Center of Excellence (NCCoE); demonstration of Trusted Geolocation in the Cloud; and Policy Machine: Enabling an Enterprise-wide, Data Centric Computing Environment.

This year's annual 2-day offsite meeting featured updates on the computer security activities of the Government Accountability Office (GAO), General Services Administration (GSA), Bureau of the Fiscal Service, and NIST. Recent administration guidance directing federal agencies to reduce travel and conference budgets significantly reduced attendance. Technical sessions included briefings on evolving cybersecurity strategies, IT security concerns during a consolidation (merger), supply chain risk management activities, the National Vulnerability Database (NVD), SP 800-53 Revision 4, continuous monitoring, industrial control systems security, and EO 13636.

On August 8, 2013, a Cybersecurity and Risk Management Training Workshop was held at the Department of Commerce with over 500 registrants. Attendees gained a greater understanding of the Risk Management Framework (RMF) and its practical application. Dr. Ron Ross discussed SP 800-53 Revision 4 and the fundamentals of continuous monitoring. Two afternoon panels discussed case studies regarding RMF and "ongoing authorization."

The Forum plays a valuable role in helping NIST and other federal agencies to develop and maintain a strong, proactive stance in the identification and resolution of new strategic and tactical IT security issues as they emerge. The number of members on the email list has grown steadily and provides a valuable resource for federal security program managers. To join, email your name, affiliation, address, phone number, title, and confirmation that you are a federal employee to sec-forum@nist.gov.

http://csrc.nist.gov/groups/SMA/forum/

Contacts:

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

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

Federal Information Systems Security Educators' Association (FISSEA)

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

FISSEA membership is open to information systems security professionals, professional trainers and educators, and managers responsible for information systems security training programs in federal agencies, as well as contractors of these agencies and faculty members of accredited educational institutions who are involved in information security training and education. There are no membership fees to join FISSEA; all that is required is a willingness to share products, information, and experiences. A working group meets monthly to administer business activities

FISSEA maintains a website, a mailing list, and participates in a social networking site as a means of communication for its members. NIST assists FISSEA with its operations by providing staff support for several of its activities and by being FISSEA's host agency.

FISSEA membership in 2013 spanned federal agencies, industry, military, contractors, state governments, academia, the press, and foreign organizations to reach over 1,395 members in a total of ten countries. The 700 federal agency members represent 89 agencies from the executive and legislative branches of government.

The 26th Annual FISSEA Conference occurred March 19-21, 2013, at NIST. Approximately 140 information systems security professionals and trainers attended from federal agencies, academia, as well as industry representatives from firms that support federal information systems and security programs. Recent government sequestration efforts prevented some from receiving permission to attend, which had a noticeable effect on attendance. NIST's Pat Toth and Peggy Himes, as well as Gretchen Morris, Susan Hansche, and other members of the FISSEA Technical Working Group, were integral to the effort to support the conference.

This year's theme was, "Making Connections in Cybersecurity and Information Security Education," to solicit presentations that reflect current projects, trends, and initiatives that provide for future solutions in federal security programs. Attendees gained new techniques for developing/conducting training, cost-effective practices, workforce development, free resources and contacts, as well as an update on NICE activities.

NIST ITL Computer Security Division Deputy Chief, Matthew Scholl, welcomed attendees. Keynote presentations were given by John J. Suess, VP of IT & CIO, University of Maryland, Baltimore County; Bryant Tow, Vice President, InfraGard National Members Alliance; and Lamont Hames, Chief Development Officer, UNCF Special Programs Corporation. Mr. Hames presented on Expanding the Role of Minorities in Cyber Security.

Presenters represented NIST, DHS, DOS, DOE, NSA and the Library of Congress as well as private industry and academia. Conference attendees had the opportunity to visit vendors, receive a government best practice poster, and attend a demonstration session, which provided an opportunity for agencies to share about their specific awareness and training programs.

Traditional FISSEA conference events included announcing the winners of FISSEA contests and awarding prize drawings. Susan Hansche, Avaya Gov/U.S. Department of State, presented the FISSEA Educator of the Year plaque to Mr. J. Paul Wahnish, Career Technical Education Foundation, Inc., for his work in preparing the future workforce. The FISSEA Security Awareness, Training & Education Contest includes five categories from one of FISSEA's three key areas of Awareness, Training, and Education. The winner is selected from each category and awarded a certificate. The categories include: (1) awareness poster, (2) motivational item (e.g., pens, stress relief items, t-shirts), (3) awareness website, (4) awareness newsletter, and (5) role-based training & education.

The winners of the 2013 FISSEA Awareness, Training, and Education Contest are:

- Poster Winner: Alexis Benjamin – Department of State, Office of Computer Security
- Website Winner: Sara Fitzgerald and Kimberly Conway – Food & Drug Administration (FDA)

- Motivational Item Winner: Jennie Blizzard, Shannon Jones, and Shirley Clement – Federal Reserve Bank
- Newsletter Winner: Deborah Coleman – Department of Education, Office of the Chief Information Officer
- Role-Based Training Winner: DISA, SAIC, and Carney, Inc. (submitted by Carmina Carper)

Conference attendees selected their *Peer's Choice Awards*, and they are...

- Poster Winner: Deborah Coleman – Department of Education, Office of the Chief Information Officer
- Website Winner: Deborah Coleman – Department of Education, Office of the Chief Information Officer
- Motivational Item Winner: Chrisan Herrod – University of Maryland University College
- Newsletter Winner: Sara Fitzgerald and Kimberly Conway – Food & Drug Administration (FDA)
- Role-Based Training Winner: Sara Fitzgerald and Kimberly Conway – Food & Drug Administration (FDA)

New this year was the Pecha Kucha session on the third day. During Pecha Kucha (Lightning Round) speakers had 6 minutes 40 seconds to present a limited number of slides (20 slides at most), and only 20 seconds per slide. The presentation method is challenging for the speaker and enjoyable for audience members. There were four participants and their fast-paced talks proved to be lively and entertaining.

Attendee networking is a valuable benefit of attending the FISSEA conference. The conference continues to be a valuable forum in which individuals from government, industry, and academia who are involved with information systems/ cybersecurity workforce development (awareness, training, education, certification, and professionalization) learn of ongoing and planned training and education programs and initiatives. It provides NIST the opportunity to provide assistance to departments and agencies as they work to meet their FISMA responsibilities.

The 2014 FISSEA conference is planned for March 18-20, 2014, at NIST.

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

Contacts:

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

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

Information Security and Privacy Advisory Board (ISPAB)

The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

In drafting the Computer Security Act of 1987, which created this Advisory Board, the Congress saw a need for an independent, non-federally dominated group of computer security experts to offer its advice to senior government officials on emerging computer security areas. The Board members, with their individual and collective skills, responsibilities, and experiences fulfill this requirement. No other similar group of experts meets regularly to review information security issues involved in unclassified Federal Government computer systems and networks. Also, Title III of the E-Government Act of 2002 reaffirmed the need for this Board by giving it additional responsibilities.

The ISPAB's statutory purpose is to advise the Secretary of Commerce, the Director of the NIST, and the Director of the OMB on information security and privacy related issues. Title III of the E-Government Act of 2002 also mandated the Board to thoroughly review all of the proposed information technology standards and guidelines developed under Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) as amended.

The charter (http://csrc.nist.gov/groups/SMA/ispab/documents/ispab_charter-2012-2014.pdf) defines that the Board's membership should consist of 12 members and a Chairperson. The Secretary of Commerce appoints the Chairperson, and the Board members are selected for their preeminence in the information technology industry or related disciplines. The term of office for each board member is four years.

The Board is comprised of members from a broad range of interested parties. There are three main categories and each category has four members. Category 1 includes members from outside the Federal Government eminent in the information technology industry, at least one of whom is representative of small or medium-sized companies in such industries. Category 2 also includes members from outside the Federal Government and not employed by or representative of a producer of information but are eminent in the field of information technology, or related disciplines. Category 3 includes experienced information system managers from the Federal Government, including

From Left to Right: Tatiana Laszczak, Chris Boyer, Annie Sokol, Ed Roback, Greg Garcia, Matt Thomlinson (Chair), Peter Weinberger, John Centafont, Toby Levin, Matt Scholl, Gale Stone.Not Present for photo: Julie Boughn

those with experience in information security and privacy, at least one of whom should be from the National Security Agency. Federal members bring a detailed understanding of the federal processing environment; industry brings concerns and experiences regarding product development and market formation, while private computer security experts are able to bring their experiences of commercial cost-effective security measures into Board discussion.

In October 2012, Matt Thomlinson agreed to assume the responsibilities of Chairperson from Dan Chenok. The Board expressed its gratitude to Dan Chenok for his leadership and contributions to ISPAB both as a member and Chair since 2005. Presently, ISPAB has nine members and a Chairperson. The ISPAB Board members are:

- Matthew Thomlinson, (Chair), Microsoft
- Daniel Chenok (Chair – Retired from the Board in October 2012), IBM Center for The Business of Government
- Julie Boughn, Center for Medicare and Medicaid Innovation, Department of Human Health and Services, Centers for Medicare & Medicaid Services (DHHS/CMS)
- Christopher Boyer, AT&T
- John Centafont, National Security Agency (NSA)
- Kevin Fu, The University of Michigan
- Gregory Garcia, Garcia Cyber Partners
- Brian Gouker, NSA - U.S. Army War College
- Toby Levin, Retired
- Edward Roback, U.S. Department of Treasury
- Phyllis Schneck, (Retired from the Board in September 2013), McAfee, Inc.
- Gale Stone, Social Security Administration
- Peter Weinberger, Google, Inc.

During FY 2013, ISPAB held three meetings, all held in Washington D.C:

- October 10-12, 2012
- February 13-15, 2013
- June 12-14, 2013

It is of particular interest to mention ISPAB's involvement with the EO Cybersecurity Framework and that prior to opening the ISPAB meeting on February 15, 2013, the Board attended the presentation of cybersecurity policy discussion and launch of the Executive Order (EO) to improve the Cybersecurity of the U.S.'s critical infrastructure at the U.S. Department of Commerce. The President signed the EO and also approved the presidential directive to improve the security and resilience of critical infrastructure in both the cyber and physical realms. Dr. Patrick Gallagher, Under Secretary of Commerce for Standards and Technology and NIST Director, provided the opening remarks on the EO. A group of distinguished panelists presented more information:

- Andy Ozment, Senior Director of Cybersecurity, Executive Office of the President
- Samara Moore, Cyber Director for Critical Infrastructure, Executive Office of the President
- Adam Sedgewick, Senior Information Technology Policy Advisor, National Institute of Standards and Technology
- Bruce McConnell, Senior Counselor for Cybersecurity, Department of Homeland Security
- Ari Schwartz, Internet Policy Advisor, National Institute of Standards and Technology
- Jenny Menna, Director, Stakeholder Engagement and Cyber Infrastructure Resilience Division, Department of Homeland Security

ISPAB meeting agendas are established based on the Board's list of emerging issues developed from previous meetings. The meeting agenda topics also include non-work list items that are of immediate security and privacy concerns to the Board. During FY 2013, the Board provided guidance on many issues relating to security and privacy such as:

- Security and Privacy Controls
- Digital and Mobile Security
- FISMA as privacy appendix on SP 800-53, metrics, FISMA review, reduction of reporting
- A130 Appendix A
- GAO Reports: Security and Privacy
- Medical Device Security
- Cybersecurity – Education, Training, Awareness
- Cross-Agency Priority (CAP) Goals
- Cloud Computing and Security Challenges
- Exploring the Future of Privacy for Federal IT
- IT System Performance
- Supply Chain and Risk Management
- SEC Security Breach Notification

The presenters at every Board meeting were leaders and experts from private industries, academia, federal agency CIOs, IGs and CISOs.

Copies of the current list of members and their bios, the Board's charter and past Board activities can be located at http://csrc.nist.gov/groups/SMA/ispab. Information on ISPAB Meetings is published in Federal Register Notice at least 16 days prior to the meeting. Those interested in receiving meeting notices may email name, affiliation, and address to:

Contact:

Ms. Annie Sokol
DFO, ISPAB
(301) 975-2006
annie.sokol@nist.gov

Small and Medium Size Business (SMB) Outreach

Small business owners face a broad range of information security issues. A computer failure or system breach could jeopardize the company's reputation and may result in significant damage and recovery cost or going out of business. The small business owner who recognizes the threat of computer crime and takes steps to deter inappropriate activities is less likely to become a victim.

The U.S. Small Business Administration (SBA) reports that over 27 million U.S. companies - more than 99 percent of all U.S. businesses - are SMBs of 500 employees or fewer (http://www.sba.gov/sites/default/files/allprofiles12.pdf). While the threats to individual SMBs may not be significantly different from those facing larger organizations, a SMB frequently has fewer resources available to protect systems, detect attacks, or respond to security issues. A vulnerability common to a large percentage of SMBs could pose a threat to the nation's information infrastructure and economic base.

To help address information security risk, these businesses require assistance with identification of security mechanisms and with practical, cost-effective training. Training helps SMB's use their limited resources most effectively to address relevant and serious threats. In response to this need, NIST, the SBA, and the Federal Bureau of Investigation (FBI) co-sponsor a series of cyber security training workshops for small businesses. These workshops provide an overview of cyber security threats, vulnerabilities, and corresponding protective tools and techniques, with a special emphasis on information that small business personnel can apply directly.

In FY 2013, the SMB outreach team provided 15 workshops in 15 cities: Toledo, Ohio; Burlington, Vermont; Portland, Maine; Providence, Rhode Island; Lexington, Kentucky; Louisville, Kentucky; Pittsburgh, Pennsylvania; Cleveland, Ohio; Detroit, Michigan; Portland, Oregon; Little Rock, Arkansas; Shreveport, Louisiana; Alexandria, Louisiana; Ruston, Louisiana; and Monroe, Louisiana.

In collaboration with the SBA and the FBI, CSD is planning locations for small business cyber security workshops in FY 2014.

http://sbc.nist.gov

Contact:

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

Cryptographic Technology

Cryptographic Standards Program

Hash Algorithms and the Secure Hash Algorithm (SHA-3) Standard (Draft FIPS 202)

In response to vulnerabilities discovered in 2005 in the NIST-approved, government hash algorithm standard, SHA-1, NIST opened a public competition in 2007 to develop a new cryptographic hash algorithm, SHA-3, to augment the hash algorithms specified in FIPS 180-4, *Secure Hash Standard*. After 64 entries, 3 rounds of the competition, and 5 years of intensive analysis, provided mostly by the world cryptographic community, NIST announced the selection of Keccak as the winning algorithm on October 2, 2012, and summarized its decision in NISTIRs after each round.

After the competition had ended, NIST invited the winning team to NIST in February 2013, and hosted a 2-day workshop to discuss the Keccak features and options for standardization as the new SHA-3 hash standard. CSD developed a standardization plan and shared with the Keccak designers and subsequently with the cryptographic community at the 2013 RSA Conference, the 2013 Workshop on Cryptographic Hardware and Embedded Systems (CHES), and at the IETF 86 and 87 Workshops. In addition, this standardization plan was posted at the NIST hash website for public comment.

A draft of the *SHA-3 Permutation-based Hash Standard* (Draft FIPS 202) is being finalized, and NIST is preparing a Federal Register Notice to announce this draft standard. NIST expects to release the draft standard during FY 2014 and plans a 60-day public comment period. After the comment period closes, NIST will analyze the comments, make changes to the document, as appropriate, and propose the draft standard to the Secretary of Commerce for approval as a FIPS. In addition to publishing FIPS 202 in FY 2014, NIST is also considering standardizing a generic "tree hashing" mode and other Keccak features. NIST plans to host a workshop in FY 2014 to discuss these options.

Information about the SHA-3 competition and the SHA-3 standardization effort is available at http://www.nist.gov/hash-competition.

Contact:

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

Hash Algorithm Standards and Security Guidelines

CSD's Cryptographic Technology Group (CTG) is responsible for the maintenance and development of the FIPS 180-4, *Secure Hash Standard (SHS)*. A hash algorithm processes a message, which can be very large, and produces a condensed representation, called a message digest. A cryptographic hash algorithm is a fundamental component of many cryptographic functions, such as digital signature algorithms, key derivation functions, keyed-hash message authentication codes, and random number generators. Cryptographic hash algorithms are frequently used in Internet protocols and other security applications.

FIPS 180-4 specifies seven hash algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256. Their security properties in different cryptographic applications are discussed in SP 800-107, Revision 1, *Recommendation for Applications Using Approved Hash Algorithms*.

CSD authored an article, "*Changes in Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard*," which was published in the January 2013 issue of the journal *Cryptologia*. The article describes the rationale behind the standardization of the SHA-512/224 and SHA-512/256 hash algorithms in FIPS 180-4 and the performance advantage of these two hash algorithms over the SHA-224 and SHA-256 hash algorithms. This article was written to help the adoption of the two new hash algorithms in security protocols and applications to improve performance.

Contacts:

Mr. Quynh Dang
(301) 975-3610
quynh.dang@nist.gov

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

Transport Layer Security (TLS)

SP 800-52, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, provides recommendations regarding TLS server and client implementations. TLS is a widely used cryptographic protocol that provides communication security for a variety of network applications, such as email, e-commerce, and healthcare.

The first version of SP 800-52, published in 2005, was withdrawn in March 2013. A draft of SP 800-52 Revision 1 was issued for public review and comment in September 2013. The revision is a substantially different document than the original and includes recommendations providing higher levels of security, both for TLS and aspects of the Public Key Infrastructure (PKI) that TLS relies on. New recommendations include the support of TLS versions 1.1 and 1.2, guidance on certificate profiles and validation methods, TLS extensions, and support for a greater variety of cryptographic algorithms.

The final version of SP 800-52 Revision 1 will be published in FY 2014.

Contacts:

Dr. Kerry McKay
(301) 975-4969
kerry.mckay@nist.gov

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

Random Number Generation (RNG)

Random numbers provide the required security for many cryptographic algorithms. For example, random numbers are used to generate the keys needed for encryption and digital signature applications.

In the late 1990s, a project to develop more rigorous requirements and specifications for random number generation (RNG) was initiated in coordination with the American National Standards Institute's (ANSI) Accredited Standards Committee (ASC) X9. The resulting standard (X9.82) contains four parts: Part 1 provides general information; Part 2, which is nearing completion, will provide requirements for entropy sources; Part 3 provides specifications for deterministic random bit generator (DRBG) mechanisms; and Part 4 provides guidance on constructing random bit generators (RBGs) from entropy sources and DRBG mechanisms.

In March 2007, NIST published SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, which contained the DRBG mechanisms in Part 3 of ANS X9.82, plus an additional DRBG mechanism. This recommendation was revised as SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, in January 2012 to include additional capabilities identified during the development of Part 4 of ANS X9.82. Two additional documents (SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation* and SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*) are under development and are available for public comment. SP 800-90B addresses the development and testing of entropy sources, including descriptions of the validation tests for NIST's Cryptographic Algorithm Validation Program to validate candidate entropy sources. SP 800-90C provides basic guidance on the construction of RBGs from entropy sources and DRBG mechanisms.

CSD held a workshop in December 2012 to discuss the drafts of SP 800-90B and C, after which NIST began the adjudication of the comments received during the public comment period and the workshop.

In September 2013, articles from major news organizations based on leaked classified documents raised public concern that one of the DRBGs specified in SP 800-90A, the Dual_EC_DRBG, could contain a backdoor. This could allow attackers to successfully predict the secret cryptographic keys that form the foundation for the assurances provided by security products. Taking these concerns seriously, NIST assured the community of its commitment to producing strong cryptographic standards, and took immediate steps to examine and remediate the issue.

Shortly after these concerns were raised, CSD published an ITL Bulletin that provided a high-level discussion of the issues, reopened the SP 800-90 series of publications for public comment, and recommended that the Dual_EC_DRBG no longer be used, pending the resolution of the comments. Since that time, NIST has released a revised draft of SP 800-90A that removes the questioned algorithm and addresses other issues that were identified in the public comment process. NIST intends to finalize the revised SP800-90A publication in FY14.

Contacts:

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

Mr. John Kelsey
(301) 975-5101
john.kelsey@nist.gov

Key Management

NIST continues to provide guidelines on cryptographic key management for the Federal Government, and to coordinate with other national and international organizations, industry, and academia. The guidelines are available at http://csrc.nist.gov/publications.

SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, specifies approved methods for key establishment using Diffie-Hellman and Menezes-Qu-Vanstone (MQV) schemes. This document was first published in 2006 and was revised in May 2013 to provide further clarification and additional methods for key derivation.

SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography,* was first published in August 2009. It is under revision to provide further clarification and additional methods for key derivation; these changes are consistent with those made in SP 800-56A. The revision of SP 800-56B will be available for public comment in FY 2014.

SP 800-57, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance,* was first published in 2009. A revision of this document has been under development. The revision will include an additional section on the Secure Shell (SSH) protocol and the removal of the Transport Layer Security (TLS) section, which is now being addressed in SP 800-52, Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. The revised SP 800-57, Part 3 will be available for public comment in FY 2014.

SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*, was completed in August 2013 and provides guidance on a Cryptographic Key Management System (CKMS) framework.

SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*, is under development. This document is intended to provide refinements of the framework requirements in SP 800-130 that are appropriate for use in a CKMS employed by the Federal Government, plus guidance on its implementation, procurement, installation, configuration, and operation. This document will be available for public comment in early FY 2014.

A new publication will provide guidance on the security strength of a cryptographic key that is used to protect data (i.e., a data-protection key), given the manner in which the key was generated and handled prior to its use to protect the target data. This document, SP 800-158, *Key Management: Obtaining a Targeted Security Strength*, involves a considerable amount of new research, since it is an area that has not been fully addressed to date. This publication will be available for public comment in FY 2014.

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

Contacts:

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

Dr. Dustin Moody
(301) 975-8136
dustin.moody@nist.gov

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

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

Mr. Quynh Dang
(301) 975-3610
quynh.dang@nist.gov

Digital Signatures

FIPS 186-4, *Digital Signature Standard (DSS)*, specifies three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA), and the Rivest-Shamir-Adleman (RSA)

algorithm. A digital signature is represented in a computer as a string of bits and is computed using a set of rules and a set of parameters that allow the identity of the signatory and the integrity of the data to be verified.

FIPS 186, first published in 1994, has been revised several times since then. In FY 2013, the Secretary of Commerce approved the latest version of the standard, FIPS 186-4.

Contacts:

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

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

Block Cipher Modes of Operation

The engine for many of the techniques in NIST's cryptographic toolkit is a block cipher algorithm, such as the Advanced Encryption Standard (AES) algorithm or the Triple Data Encryption Algorithm (TDEA). A block cipher transforms some fixed-length binary data (i.e., a "block") into seemingly random data of the same length. The transformation is determined by the choice of some secret data called the "key." The key can also be used to recover the original block of data.

A method of using the block cipher to protect one or more blocks of data is called a block cipher mode of operation. The approved modes are specified in the SP 800-38 series. Each approved mode provides data confidentiality and/or authenticity/integrity.

In December 2012, NIST approved block cipher modes for key wrapping (i.e., the protection of the confidentiality and integrity of cryptographic keys). In particular, SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, identifies existing methods that are approved for key wrapping, and also specifies three deterministic authenticated-encryption modes: the AES Key Wrap (KW) mode, the AES Key Wrap with Padding (KWP) mode, and one TDEA mode, called TKW.

Block cipher modes can also provide format-preserving encryption (FPE). A format can be a sequence of decimal digits, such as a credit card number or a social security number; formats can also be defined for other sets of characters besides decimal digits. FPE is expected to be very useful because this property facilitates the retrofitting of encryption to existing applications.

NIST proposed the approval of three block cipher modes for FPE in Draft SP 800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*, which was released for a 60-day period of public comment in July 2013. This publication specifies three schemes for FPE: FF1, FF2, and FF3. These schemes were submitted for NIST's consideration in recent years under the names FFX-base, VAES3, and BPS; the original submission documents are available at http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html, in the FFX and BPS entries under the heading "Encryption Modes."

Contact:

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

Cryptographic Research

Post-Quantum Cryptography

In FY 2013, NIST researchers Stephen Jordan, Yi-Kai Liu, Dustin Moody, Ray Perlner, and Daniel Smith-Tone internally presented status reports in the areas of quantum computation, coding-based cryptography, lattice-based cryptography, and multivariate cryptography, which included detailed surveys of the respective fields, as well as security overviews and specific results. The project members also created evaluation criteria to compare proposed post quantum cryptosystems with the end goal of standardization.

NIST also engaged the international cryptographic community with presentations and publications. Daniel Smith-Tone and Ray Perlner presented a paper at PQCrypto 2013, in addition to Dr. Smith-Tone speaking at the Joint Romanian Mathematical Society, and the Quantum Cryptanalysis Seminar in Schloss Dagstuhl, Germany. Yi-Kai Liu presented his research at QCrypt 2013, as well as giving a talk at the European Telecommunication Standard Institute (ETSI) Quantum-safe Crypto Workshop. Lily Chen also spoke at the ETSI Quantum-safe Crypto Workshop. Stephen Jordan delivered a keynote address at the 16th Workshop on Quantum Information Processing on a paper that was published in *Science* magazine. In FY 2013, Dr. Jordan also spoke about research at the Institute for Quantum Information and Matter, the Hughes Research Laboratory, and the Lorentz Center, as well as submitting some research papers for publication.

In FY 2014, NIST will continue to explore the security capacity of purported quantum-resistant technologies with the ultimate goal of uncovering the fundamental mechanisms necessary for efficient, trustworthy, and cost-effective information assurance in the post-quantum market. Upon the successful completion of this phase of the project, NIST will be prepared for possible standardization efforts in this area. NIST will consider hosting

a workshop on post-quantum cryptography to discuss practical steps towards this goal.

Contacts:

Email project Team: pqc@nist.gov

Dr. Dustin Moody
(301) 975-8136
dustin.moody@nist.gov

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

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

Dr. Daniel Smith-Tone
(502) 852-6010
daniel.smith@nist.gov

Dr. Yi-Kai Liu
(301) 975-6499
yi-kai.liu@nist.gov

NIST Beacon - A Prototype Implementation of a Randomness Beacon

NIST has implemented a public source of randomness. The prototype uses two independent, commercially available sources of randomness, each with an independent hardware entropy source.

The Beacon is designed to provide unpredictability, autonomy, and consistency. Unpredictability means that users cannot algorithmically predict bits before they are made available by the source. Autonomy means that the source is resistant to attempts by outside parties to alter the distribution of the random bits. Consistency means that a set of users can access the source in such a way that they are confident that they all receive the same random string.

The Beacon posts bit-strings in blocks of 512 bits every 60 seconds. Each such value is time-stamped and signed by NIST and includes the hash of the previous value to chain the sequence of values together. This prevents anyone, even the Beacon itself, from retroactively changing an output packet without being detected. The Beacon keeps all output packets and makes them available online at https://beacon.nist.gov/home.

Tables of random numbers have probably been used for multiple purposes at least since the Industrial Revolution. In the digital age, algorithmic random number generators have largely replaced those tables. The NIST Randomness Beacon expands the use of public randomness to multiple scenarios in which the latter methods cannot be used. The extra functionalities stem mainly from three features. First, the Beacon-generated numbers cannot be predicted before they are published. Second, the public, time-bound, and authenticated nature of the Beacon allows a user application to prove to anybody that it used truly random numbers not known before a certain point in time. Third, this proof can be presented offline and at any point in the future. For example, the proof could be mailed to a trusted third party, encrypted, and signed by an application, to be opened if needed and authorized.

Although commercially available physical sources of randomness are adequate as entropy sources for currently envisioned applications of the Beacon, NIST is working on developing a source of verifiably random sequences. Given that it is impossible to construct such sequences in any classical physical context, CSD is collaborating with the NIST Physical Measurement Laboratory (PML) to build a quantum source. The aim is to use quantum effects to generate sequences that are guaranteed to be unpredictable, even if an attacker has access to the random source. For more information on this collaboration, see http://www.nist.gov/pml/div684/random_numbers_bell_test.cfm.

As the bits posted by the Beacon are public, these are not to be used as secret values, such as cryptographic keys or seeds for random number generators used in the construction of cryptographic keys. NIST encourages the community-at-large to research and publish novel ways in which this tool can be used. Some examples of applications are unpredictable sampling, new authentication mechanisms, and secure multi-party computation. More details are available at http://beacon.nist.gov.

Contacts:

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

Dr. René Peralta
(301) 975-8702
rene.peralta@nist.gov

Privacy-Enhancing Cryptography Project

The privacy-enhancing cryptography project seeks to promote the use of communication protocols that do not unnecessarily reveal private information of communicating parties. There are many technical challenges in doing this, as it is typically hard to separate private data from general data (e.g., to convert a third-party-signed date-of-birth certificate into a certificate that a person is of voting age). Zero-knowledge (ZK) proof techniques and their variants can be used to accomplish this for a large class of assertions. These techniques allow one party to prove to another party that a given statement is true, without conveying any additional information apart from the fact that the statement is indeed true. Although many such ZK protocols are practical, adoption by industry is slow. CSD is following the progress of emerging technologies, such as fully homomorphic encryption (FHE). FHE could potentially solve a large class of

problems, by allowing computation on encrypted data without decryption. CSD has also shown that the NIST Randomness Beacon (discussed in the previous section) can be used as a primitive in secure multi-party computation, such as sealed-bid online auctions in which losing bids are never opened.

Team members continue to be in close collaboration with the NSTIC program and the Federal Cloud Credential Exchange (FCCX) project. In this context, CTG has served as evaluators and in technical support roles. Information about NSTIC and FCCX is available at http://www.nist.gov/nstic/.

Current communication security standards are primarily designed for two-party communication. Future protocols, such as those for identification, commercial transactions, and social media, will necessitate standards for three-party communications (e.g., two parties involved in a commercial transaction and a third party that serves as an enabler of some aspects of the transaction). This is particularly important if standards are to provide privacy protection. NIST has developed some basic protocols for this purpose. One such protocol allows for privacy-preserving identification with the aid of a mediator. In this protocol, the issuer of an assertion, such as "John Smith is an employee of the Department of Commerce," does not need to know who the consumer of the assertion is, yet it can encrypt the assertion with a key only known to that consumer (i.e., the mediator does not get to see the unencrypted assertion).

Contact:

Dr. René Peralta
(301) 975-8702
rene.peralta@nist.gov

Cryptography for Constrained Environments

Pervasive computing is an emerging technical area in which many highly constrained devices (e.g., limited resources, such as program space and RAM) are interconnected, typically communicating wirelessly with one another, and working in concert to accomplish some task. These systems apply to a wide variety of fields. Sample application areas include sensor networks, medical devices, distributed control systems, and the Smart Grid. Security can be very important in each of these areas. For example, an unauthorized party should not be able to take control of an insulin pump or the brakes on a car. There are also privacy concerns, particularly in the area of Health IT.

Because the majority of the current cryptographic algorithms were designed for desktop/server environments, many of these algorithms cannot operate under these constraints, or if they can be made to operate in these constrained environments, their performance is typically not acceptable. A particular problem is the use of asymmetric (public key) algorithms. These algorithms tend to be much more computational and resource-intensive and are not easily accommodated in such constrained environments.

As a result, CSD is currently focusing on studying the use of the NIST-approved symmetric-key algorithms in constrained environments. Symmetric-key algorithms can perform encryption for confidentiality, and can generate message authentication codes (MAC) for authenticity and integrity. NIST has implemented the Advanced Encryption Standard (AES) to provide both confidentiality and the AES-based message authentication code, CMAC mode, for authentication. Additionally, CTG has implemented the 256-bit version of the Secure Hash Algorithm (SHA-256) to provide a Hash-based Message Authentication Code (HMAC) for authentication. The emerging KECCAK algorithm has also been implemented – both the original 1600-bit permutation that won the hash competition (see the SHA-3 report above) and the reduced 800-bit permutation. It has been demonstrated that the KECCAK algorithm allows a more efficient construction for computing MACs than SHA-256, which requires the HMAC construction. CTG has also investigated other, non-NIST-approved algorithms for constrained environments.

CTG will continue to analyze the resource requirements and performance characteristics of these algorithms, and study their use as building blocks to perform other cryptographic functions beyond encryption.

Contact:

Mr. Lawrence Bassham
(301) 975-3292
lawrence.bassham@nist.gov

New Research Areas in Cryptographic Techniques for Emerging Applications

Stream Ciphers

Stream ciphers are symmetric-key cryptographic primitives that encrypt plaintext bits individually using a time-varying transformation. The performance advantages of dedicated stream ciphers make them more attractive than block ciphers in stream-cipher-type modes (e.g., AES counter mode) for some niche software and hardware applications. In 2004, the European Network of Excellence for Cryptology (ECRYPT) announced the ECRYPT Stream Cipher (eSTREAM) project with the goal of identifying new stream ciphers that offer some performance advantages over AES. The eSTREAM portfolio, published in 2012, includes: 1) four algorithms for software applications: HC-128, Rabbit, Salsa20/12 and Sosemanuk, and

2) three algorithms for hardware applications: Grain, Trivium and Mickey.

The primary focus of the project is to study the eSTREAM candidates and other commonly used stream ciphers for possible standardization. During FY 2013, three internal talks were given: *"Stream Ciphers for Constrained Environments," "Authenticated Encryption In Stream Ciphers," and "Stream Ciphers For Software Applications."* NIST researchers Meltem Sönmez Turan and Santanu Sarkar were two of the co-authors of "*A Chosen IV Related Key Attack on Grain-128*," published at the 18th Australasian Conference on Information Security and Privacy, ACISP 2013. Dr. Turan also published "*Related-Key Slide Attacks On Block Ciphers With Secret Components*" at the Second International Lightweight Cryptography for Security and Privacy workshop, LightSec 2013.

After comparing the security and performance of stream ciphers to block ciphers designed for constrained environments, CTG observed that the gate array requirements for block and stream ciphers are comparable, but stream ciphers have a better throughput/area performance characteristic. CTG currently believes that well-designed lightweight block ciphers may be more suitable than stream ciphers for constrained environments. This determination is based upon the following factors: 1) the maturity of literature on block ciphers; 2) the availability of better tools to analyze the security of block ciphers; 3) reduced round attacks on the stream cipher finalists; and 4) lack of flexible key sizes for stream ciphers.

In FY 2014, NIST will continue to study the security and performance of software-oriented stream ciphers and block ciphers designed for constrained environments.

Contacts:

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

Dr. Meltem Sönmez Turan
(301) 975-4391
meltem.turan@nist.gov

Circuit Research

Cryptographic primitives, such as encryption, digital signatures, and hashing, are implemented as electronic circuits for a wide class of applications. A variety of metrics is relevant to designing "good" circuits. In particular, minimizing the size and maximizing the throughput of a circuit closely translate into the combinatorial problem of designing circuits with few gates and short depth. The project team has shown that solving this design problem, even approximately, is "MAX-SNP Complete." In practice, this means that it is necessary to settle for heuristics that design "good" circuits, as opposed to provably optimal circuits. It also means that many basic questions are likely to remain unanswered for the foreseeable future, even if quantum computers are ever built. For example, it is unlikely that the minimum number of gates necessary to implement the AES can be found. In the 12 years since the approval of AES, successive improvements have roughly cut the gate count in half. The standard reference for the smallest published circuit for AES is from a study funded by the National Security Agency. CTG improved on this work significantly by designing combinatorial circuits that are smaller (meaning that they are likely to use less energy) and others that are of lower depth (meaning that they are likely to be faster). The general technique was issued a patent held jointly between NIST and the University of Southern Denmark.

CTG is also researching circuit-based security metrics for cryptographic functions. For a function to be secure (one-way), it must be the case that any circuit that implements it is sufficiently complex. In particular, a function is insecure if it can be implemented by a circuit containing too few Boolean AND gates. This security metric, namely the number of AND gates necessary and sufficient to implement a function, is referred to as its multiplicative complexity. When comparing two cryptographic functions, all other things being equal, the one with higher multiplicative complexity is preferable. Unfortunately, determining multiplicative complexity is extremely hard. Mathematicians attempted this in the 1970s, but the effort had been largely abandoned by the 1980s. CTG has been able to compute tight bounds for the multiplicative complexity of an important class of functions (the symmetric functions). This theory seems to have wide applicability and it points to exciting directions for both theoretical and applied research in security and cryptography.

A partial list of results includes:

- The construction of the smallest known circuits for multiplication in several small finite fields.
- The construction of the smallest known circuits for binary multiplication (i.e., multiplication of polynomials of degree *n* over the Galois Field with two elements).
- The construction of optimal circuits – with respect to multiplicative complexity – for all predicates on four bits. There are 65,536 such predicates. Surprisingly, the multiplicative complexity of all these functions turned out to be at most three.
- Circuits with small multiplicative complexity can be used to design more efficient multiparty computation protocols. Such circuits are useful for protocols that use either partially homomorphic schemes or fully homomorphic schemes. Some of the published circuits are being used as benchmarking tools in those areas.

- Significant advances have been made in heuristics for linear circuit complexity, and this is expected to yield improvements to the best-known circuits in this area for years to come.

Contact:

Dr. René Peralta
(301) 975-8702
rene.peralta@nist.gov

Applied Cryptography

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

FIPS 140-2, *Security Requirements for Cryptographic Modules*, defines the security requirements for the cryptographic modules that perform cryptographic operations. This standard is applicable to all federal agencies that use cryptography-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems), as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106, and the Federal Information Security Management Act of 2002, Public Law 107-347. The standard must be used in designing and implementing cryptographic modules that federal departments and agencies operate, or that are operated for them under contract.

The current version of the standard is FIPS 140-2. Draft FIPS 140-3, a revision proposed to supersede FIPS 140-2, has been developed. The draft revision of the standard adds new security requirements for cryptographic modules to reflect the latest advances in technology and security and to mirror other new or updated standards published by NIST in the areas of cryptography and key management. Additionally, software and firmware requirements are addressed in a new topic area while another new area specifying requirements to protect against noninvasive attacks is also provided.

The standard provides four increasing, qualitative levels of security, intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design, implementation and operation of a cryptographic module. These areas include cryptographic module specification; cryptographic module physical ports and logical interfaces; roles, authentication, and services; software security; operating environment; physical security; physical security – non-invasive attacks; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

The draft of FIPS 140-3 has had two rounds of public review. The resolutions to the public comments received on the second draft of FIPS 140-3 include: 1) a description of the assumed threat models (e.g., attacker's level of experience, expectations from the cryptographic module) for each of the four security levels; 2) an insertion of missing definitions for terms and acronyms; 3) changes to the Trusted Channel requirements; 4) the removal of the Trusted Role; 5) the inclusion of an identity-based authentication mechanism that would be allowed at Security Level (SL) 2; 6) the addition of a self-initiated cryptographic output capability and remote control capability; 7) the inclusion of additional integrity-technique requirements for the software components of a cryptographic module; 8) a restructure of the annexes and enhancement of the requirements for the allowed operator-authentication mechanisms; 9) an update of the list of the noninvasive attacks covered by the standard; and 10) an update of the requirements for the allowed modifiable operating environments.

During the process of addressing the public comments received on the second draft, CSD determined that additional feedback was required from the public to resolve gaps and inconsistencies among the comments received for particular sections of the second draft of FIPS 140-3. As a result, CSD requested additional public comments in August 2012 on several clearly identified sections.

During FY 2013, CSD discussed and addressed all comments received on the identified issues and prepared the updated draft FIPS 140-3 for a final internal review. The completion of the internal review and submission for approval by the Secretary of Commerce are expected in FY 2014.

http://csrc.nist.gov/groups/ST/FIPS140_3/

Contact:

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

Authentication

To support the Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, NIST developed SP 800-63, *Electronic Authentication Guideline*. Its subsequent revision, SP 800-63-1 (published at the end of FY 2012) significantly expanded the range of included technologies, such as Security Assertion Markup Language (SAML) assertions. The OMB memorandum defines four levels of authentication in terms of assurance about the validity of an asserted identity. This recommendation covers remote authentication of users (such as employees, contractors,

or private individuals) interacting with government IT systems over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions.

As more electronic service delivery systems that require authentication and identity management became available, large-scale enrollment and registration issues became a significant problem for agencies, particularly for health care. Enrollment and identity proofing result in much of the up-front cost to agencies of implementing online service delivery and can be a barrier to user adoption. SP 800-63-2, a revision with changes largely limited to identity proofing and credential issuance, was published at the end of FY 2013 and is available at http://csrc.nist.gov/publications/PubsSPs.html.

SP 800-63-2 is intended to facilitate more efficient and convenient user enrollment and identity proofing, mainly by exploiting the identity proofing already done for professional licensing, registration, or certification (e.g., for doctors, nurses, lawyers, professional engineers). SP 800-63-2 also reduces the number of cases where postal mailings are required to confirm addresses, saving expense and making registration easier and more immediate for users.

In FY 2014, NIST expects its authentication work to be driven by the needs of the ongoing rapid expansion of online service delivery, as experience accumulates and technology progresses. Efforts to develop accreditation programs for e-authentication have revealed problem areas in the text of the specifications, while the rapidly growing and evolving use of mobile devices with Internet access and new capabilities present both challenges and opportunities. Practical business models for large-scale registration and credential issuance seem to indicate that separate organizations should do both, and NIST has been urged to make a clearer delineation of these activities in a future revision of SP 800-63. Unattended biometric authentication is considered problematic for remote authentication in SP 800-63-2, but the relatively high quality and online video/audio capabilities of the current mobile devices, as well as the fingerprint readers in some mobile phones, all deserve fresh consideration. Level 4 identity proofing currently requires an in-person appearance, which is often both expensive for agencies and inconvenient and time consuming for registrants, particularly in rural or remote areas. A comment received during the public review of SP 800-63-2 urged allowing the use of secure kiosks with high-quality video, document scanners and biometric readers that would be linked to a human registration operator in a registration center, as a viable solution. While this was judged to be too complex to evaluate in the schedule for SP 800-63-2, the idea is intriguing and deserves a detailed consideration.

NIST, therefore, plans to actively consider another incremental revision to SP 800-63-2 in response to the issues noted above and other issues that can be dealt with in time to assist in the intense ongoing efforts to expand online services.

Contact:

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

Wireless Networks and Mobile Device Security

Today, wireless networks often provide connections for mobile devices using multiple and different radio technologies. In such a heterogeneous network, a mobile device may switch its between different wireless technologies. The procedure of conducting such a switch is called a “handover.” Inter-technology handover has brought many challenges to existing security solutions, such as the delays caused by access authentication for each handover. CSD has conducted intensive research in the security for media-independent handover (MIH) and has worked closely with the working group of IEEE 802.21 on security solutions for MIH services. The services specified in IEEE 802.21 include information service, event service, and command service. The security mechanisms were developed by Task Group A of IEEE 802.21 and specified in Amendment 2 of IEEE 802.21, which provide MIH message protection and accommodate proactive authentications.

However, the protection mechanisms specified in Amendment 2 of IEEE 802.21 are only applied to unicast messages; that is, the mechanisms protect messages between a point of service (PoS) and a mobile node. When the services provided by the pervasive heterogeneous networks are extended to other applications, such as Smart Grid applications, the MIH needs to be processed for a group of wireless nodes, such as smart meters, for the reliability of the services. For example, the information may need to be delivered to a group of smart meters. In this case, the multicast message is used to deliver the information. That is, the message is sent from one PoS to multiple wireless nodes. In some of the application environments, such as sensor networks, the groups are formed dynamically. That is, new nodes can be added to the group, and some nodes may need to be removed. Such groups are managed through multicast signals. The protection for multicast messages and group management signals becomes critical. In FY 2013, CSD has worked with IEEE 802.21 to develop security solutions for group management in Task Group D of IEEE 802.21. The solutions include the mechanisms to distribute group keys and for the protection of multicast messages. In FY 2014, CSD will continue to contribute to the development of the IEEE 802.21

Amendment on group management.

Contact:

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

Identity Management

Personal Identity Verification (PIV) and FIPS 201 Revision Efforts

Figure 8: Personal Identity Verification (PIV) and FIPS 201 Revision Efforts

In response to Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, was developed and was approved by the Secretary of Commerce in February 2005. HSPD-12 called for the creation of a new identity credential for federal employees and contractors. FIPS 201 is the technical specification for both the PIV identity credential and the PIV system that produces, manages, and uses the credential. Within NIST's Information Technology Laboratory (ITL), this work is a collaborative effort of the Information Access Division (IAD) and CSD. CSD activities in FY 2013 directly supported the revision and maintenance of the FIPS 201 standard. CSD performed the following activities during FY 2013 to revise the standard:

- Drafted and published the final release version of FIPS 201-2. FIPS 201-2 reflects the disposition of more than 1,000 comments received from over 40 organizations on the first public comment draft, and over 500 comments received from 36 organizations on the second public comment draft. NIST coordinated with the Office of Management and Budget (OMB), the United States Access Board, Office of Personnel Management (OPM), and other U.S. Government (USG) stakeholders before incorporating changes in the final release version of FIPS 201-2.
- Prepared and published a draft revision 4 of Special Publication (SP) 800-73 (SP 800-73-4), *Interfaces for Personal Identity Verification*. The update to the three-part SP details the new PIV Card capabilities introduced in FIPS 201-2 including Virtual Contact Interface (VCI), a secure channel protocol, an on-card biometric comparison mechanism and enforcement a minimum PIN length of six digits.
- Prepared and published a draft revision 4 of SP 800-78 (SP 800-78-4), *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The document has been modified to align with SP 800-73-4 (Draft), and includes the addition of new algorithms and key sizes for the secure messaging protocol and the addition of test requirements with the Cryptographic Algorithm Validation Program (CAVP) validation.
- Started drafting an update to SP 800-79, *Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCIs),* in order to incorporate changes required by FIPS 201-2.
- Started drafting updates to SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines,* and SP 800-85B, *PIV Data Model Test Guidelines*, in order to align these documents with FIPS 201-2, SP 800-73-4, and SP 800-78-4.
- To accommodate mobile devices, NIST started drafting SP 800-157, *Derived PIV Credentials*. As intended by FIPS 201-2, derived PIV credentials are part of the set of PIV credentials that can be provisioned directly to mobile devices to enable remote enterprise access from the device.

In FY 2014, CSD will be focusing on updating the relevant publications associated with FIPS 201-2, including developing a new publication, SP 800-156, *Representation of PIV Chain-of-Trust for Import and Export*. CSD will also continue to provide technical and strategic inputs to the PIV related initiatives.

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

Contacts:

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

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

Mr. Salvatore Francomacaro
(301) 975 6414
salvatore.francomacaro@nist.gov

Mr. Ketan Mehta
(301) 975-8405
ketan.mehta@nist.gov

PIV Program Test Cards

To facilitate the development of applications and middleware that support the PIV card, CSD developed a set of smart cards for testing. The initial work of developing the test cards was performed during FY 2011 and was completed during FY 2012. In late FY 2012, NIST began selling the test cards as NIST Special Database 33 (http://csrc.nist.gov/groups/SNS/piv/testcards.html).

Over the course of FY 2013, additional sets of test cards were created as the existing inventory of cards were sold. In addition, CSD has maintained a mailing list that has been used by individuals who have purchased the test cards to ask questions about the cards and to exchange advice on their use.

For further details on the PIV project, see the *Personal Identity Verification (PIV) and FIPS 201 Revision Efforts* section.

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

Figure 9: PIV Test Card

Contact:

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

NIST Personal Identity Verification Program (NPIVP)

The objective of the NIST Personal Identity Verification Program (NPIVP) is to validate PIV components for conformance to specifications in FIPS 201 and its companion documents. The two PIV components that come under the scope of NPIVP are PIV Smart Card Application and PIV Middleware. All of the tests under NPIVP are handled by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) Laboratories by the NIST NVLAP and are called accredited NPIVP test facilities. As of September 2013, there were nine such facilities.

In prior years, CSD published SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines*, to facilitate development of PIV Smart Card Application and PIV Middleware that conform to interface specifications in SP 800-73, *Interfaces for Personal Identity Verification*. CSD also developed an integrated toolkit called "PIV Interface Test Runner" for conducting tests on both PIV Card Application and PIV Middleware products, and provided the toolkit to accredited NPIVP test facilities.

NPIVP validation utilized the following versions and documents throughout FY 2013:

- SP 800-73-3, *Interfaces for Personal Identity Verification*
- SP 800-85A-2, *PIV Card Application and Middleware Interface Test Guidelines*

In FY 2013, two new PIV card application products were validated for conformance to SP 800-73-3 and received certificates, bringing the total number of NPIVP validated PIV Card application products to 36. Three PIV Middleware products were validated for conformance to SP 800-73-3 and received certificates, for a total number of 20 NPIVP-validated PIV Middleware products.

In addition, NPIVP is closely involved in ensuring that all changes in PIV companion documents, such as SP 800-73-3, SP 800-76-2, and SP 800-78-3, are fully reflected in the conformance test document SP 800-85A-2 as well as subsequently in the PIV Test Runner toolkit consequent on the expected publication of FIPS 201-2.

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

Contacts:

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

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

Cloud Computing and Virtualization

Cloud computing is a model defined in the NIST SP 800-145, *The NIST Definition of Cloud Computing*. The foundational technologies that facilitate the use of a computing infrastructure for cloud computing services is virtualization. At the core of a virtualized infrastructure is the virtualized host that provides abstraction of the hardware (e.g., CPU, memory) enabling multiple computing stacks (comprised of the operating system, middleware, and applications) to be run on a single physical machine. The efficiency of such a dynamic and distributed processing environment is counter-balanced by the interoperability, portability, and security challenges inherent to this computing environment. NIST is working in parallel on several projects introduced below that aim to accelerate the Federal Government's secure adoption of cloud computing by collaborating with standards bodies, public and private sector in developing security, interoperability and portability standards and guidance.

CSD Role in the NIST Cloud Computing Program

During FY 2013, the NIST Cloud Computing Team continued to promote the development of publications, national and international standards, and specifications in support of the USG's effective and secure use of cloud computing as well as providing technical guidance to USG agencies for secure and effective cloud computing adoption.. CSD supports many of the technical standards activities supported by the NIST Cloud Computing Program, with a particular focus on cloud computing security.

- Participated in the development of a revised SP 500-291, *NIST Cloud Computing Standards Roadmap*. The document, initially published in 2011, was updated in July 2013, and was incorporated into draft SP 500-293, *US Government (USG) Cloud Computing Technology Roadmap*.
- Participated in the update to the multi-part draft document SP 500-293, *US Government (USG) Cloud Computing Technology Roadmap (Vol. I, II, and III)* that defines and prioritizes USG requirements for interoperability, portability, and security for effective cloud computing adoption. It is anticipated that final versions of Volumes I and II of the SP 500-293 will be released by the end of the first quarter, FY 2014.
- Led the development of the draft SP 500-299, *NIST Cloud Computing Security Reference Architecture (SRA)*. It is anticipated that the final version of the document will be released by the end of the second quarter, FY 2014. SP 500-299 defines a modular framework that provides a formal model and a methodology for the secure adoption of cloud computing by applying a Cloud-adapted Risk Management Framework. The SRA is a security overlay to SP 500-292: *NIST Cloud Computing Reference Architecture*.
- Provided technical support to several Federal Chief Information Officer (CIO) Council committees, including the Cloud Computing Executive Steering Committee, Cloud Computing Advisory Council, the Information Security and Identity Management Workgroup, and the Web 2.0 working group.

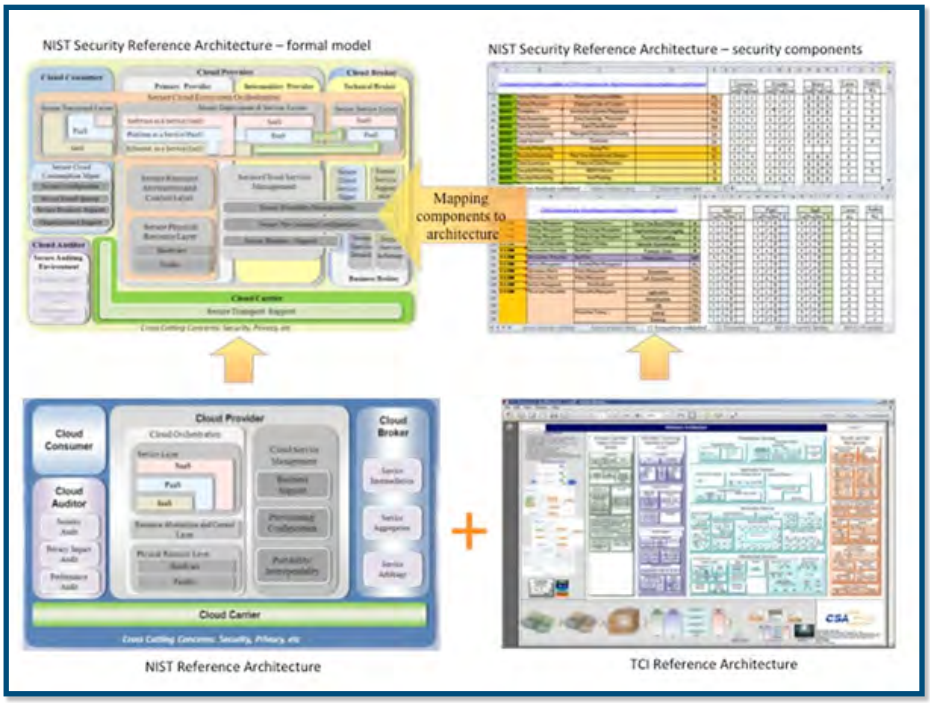


Figure 10: NIST Security Reference Architecture Diagram

CSD staff members contributed significantly to several NIST-hosted events:

- Sixth Cloud Computing Forum and Workshop: Cloud Computing and Big Data Forum, held in January 2013
- Seventh Cloud Computing Forum and Workshop: The Intersection of Cloud and Mobility Forum, initially scheduled for October 1-3, 2013, currently rescheduled

due to USG shutdown

- First Cloud Forensic Science Workshop, initially scheduled for October 3, 2013, also rescheduled due to USG shutdown.

In support of and advancement of USG cloud computing mandates, CSD staff members provided leadership for several public work groups operating under the NIST Cloud Computing Program. Through these working groups, CSD staff led the development of technical guidelines and recommendations that considered a close collaboration with public, private, academia and other stakeholders.

CSD staff chaired or co-chaired several significant cloud computing efforts in 2013:

- Chair of the NIST Cloud Computing Security Working Group focused the group on development of SP 500-299 (described above), and on key management research.
- Co-Chair, NIST Cloud Computing Forensic Science Working Group, led development of Digital Forensics Challenges in a cloud environment.
- Co-Chair, NIST Cloud Computing Standards Roadmap Working Group, led development of SP 500291, *USG Cloud Computing Standards Roadmap* (described above).
- Chair and Vice-Chair, INCITS CS1 (Cybersecurity) – U.S. Technical Advisory Group (TAG) to the ISO/IEC international committee JTC1/SC27 (IT Security Techniques) – that covers cloud computing taxonomy-related standards and cloud computing security standards.

CSD staff members participate in various standards development organizations, two of which are ISO/IEC JTC 1 Sub Committee 38 – Distributed Application Platforms and Services (SC 38) and ISO/IEC JTC 1 Sub Committee 27 – IT Security Techniques (SC 27). In SC 38, CSD acts as the co-convener for a collaborative ISO/ITU-T initiative on cloud computing taxonomy that includes work on *ISO/IEC 17788 – Information Technology – Cloud computing – Overview and Vocabulary*. Notably, the genesis for this international body of work is the widely accepted and used cloud computing definition found in SP 800-145, *NIST Definition of Cloud Computing*.

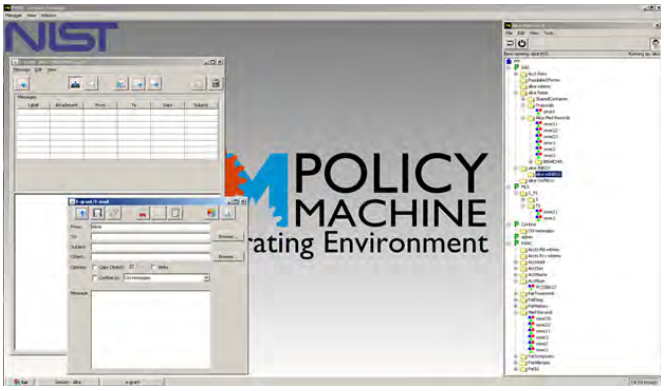
ISO/IEC 17788 is closely coordinated with another standards activity, ISO/IEC 17789 – *Information technology – Cloud Computing – Reference Architecture,* which is based on the widely used and accepted NIST publication, SP 500-292. Both ISO/IEC 17788 and 17789 are in the final stages of international balloting before final publication, which is anticipated in the first quarter of calendar year 2014.

CSD staff members are also actively participating in cloud computing security standards, primarily through SC 27, which is responsible for cloud computing security standards. CSD has provided technical contributions based on SP 500-299 and continues to advocate for secure, non-proprietary solutions.

In FY 2013, the CSD members of the NIST cloud computing team also presented the results of cloud computing research and development, introduced the standards and specifications under development, and provided status of the NIST Cloud Computing Program in a variety of conferences and workshops.

Policy Machine – Leveraging Access Control for Cloud Computing

Figure 11: Policy Machine operating environment



In FY 2013, CSD continued the research and development of a virtualization-based, enterprise-wide controlled delivery of data services for advanced cloud computing through Access Control. NIST and other members of an Ad Hoc INCITS working group are developing a three-part PM standard, under the title of "Next Generation Access Control" (NGAC), under three sub-projects:

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

The Policy Machine's architecture has been adopted by the ANSI/INCITS and is now available as ANSI INCITS 499 – *Information technology – Next Generation Access Control – Functional Architecture (NGAC–FA).*

Cryptographic Key Management Issues in Cloud Infrastructures

Many of the security capabilities associated with exercise of cloud service rely on cryptographic operations. The key management system (KMS) required to support cryptographic operations for the above tasks can be complex, due to differences in ownership and control of underlying infrastructures on which the KMS and the protected resources are located. CSD developed NISTIR 7956, *Cryptographic Key Management Issues & Challenges in Cloud Services* to discuss these critical issues.

Virtualization Security & Leveraging Virtualization for Security

CSD has been researching key areas in cloud and virtualization security producing the following papers:

"Security Assurance Requirements for Hypervisor Deployment Feature" published as part of the proceedings of the 7th International Conference on Digital Society. In FY 2014, CSD will consider feedback from public comments received and publish a (yet unnumbered) Special Publication titled *Secure Management Practices for Protection of Hypervisors*. In addition, security assurance requirements and security recommendations will be developed for components of virtualized infrastructure other than the hypervisor, such as the guest O/S, VM-based applications, and the virtual network..

Additional information about the NIST Cloud Computing Program is available at:

http://www.nist.gov/itl/cloud

http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsRoadmap

http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity

http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudForensics

Contacts for each project:

Computer Security Division Role in the NIST Cloud Computing Program
Dr. Michaela Iorga
Chair, Cloud Computing Security Workgroup
(301) 975-8431
michaela.iorga@nist.gov

Ms. Annie Sokol
Co-Chair, Cloud Computing Standards Roadmap
(301) 975-2006
annie.sokol@nist.gov

Mr. Daniel Benigni
Chair, INCITS CS1 (Cybersecurity) - US Technical Advisory Group (TAG) to the ISO/IEC international committee JTC1/SC27 (IT Security Techniques)
(301) 975-3279
dbenigni@nist.gov

Mr. Salvatore Francomacaro
Vice-Chair, INCITS CS1 (Cybersecurity) - US Technical Advisory Group (TAG) to the ISO/IEC international committee JTC1/SC27 (IT Security Techniques)
(301) 975-6414
salvatore.francomacaro@nist.gov

Policy Machine - Leveraging Access Control for Cloud Computing
Mr. David Ferraiolo
(301) 975-3046
david.ferraiolo@nist.gov

Mr. Serban Gavrila
(301) 975-4242
serban.gavrila@nist.gov

Cryptographic Key Management Issues in Cloud Infrastructures
Dr. Ramaswamy Chandramouli
(301) 975-5013
mouli@nist.gov

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

Virtualization Security & Leveraging Virtualization for Security
Dr. Ramaswamy Chandramouli
(301) 975-5013
mouli@nist.gov

Mobile Device Security

Smart phones have become both ubiquitous and indispensable for consumers and business people alike. Although these devices are relatively small and inexpensive, they can be used for voice calls, simple text messages, sending and receiving emails, browsing the web, online banking and ecommerce, social networking, and many functions once limited to laptop and desktop computers. Smart phones and tablet devices have specialized built-in hardware, such as photographic cameras, video cameras, accelerometers, Global Positioning System (GPS) receivers, and removable media readers. They also employ a wide range of wireless interfaces, including infrared, Wireless Fidelity (Wi-Fi), Bluetooth, Near Field Communications (NFC), and one or more types of cellular interfaces that provide network connectivity across the globe. Naturally, just as consumers and business people can realize productivity gains from these technologies, so can government agencies.

Like any new technology, smart phones present new capabilities, but also a number of new security and privacy challenges. As the pace of the technology life cycles continues to increase, current Information Assurance (IA) standards and processes must be updated and new technologies to allow government users to employ the latest technologies that consumers can use without sacrificing privacy and security.

NIST is conducting research in new software assurance methodologies for smart phone software (i.e., apps) and is working with industry to bridge the security gaps present with today's smart phones. NIST has developed an online beta Application Testing Portal (ATP) for Android that examines app functionality with respect to agency security and privacy guidelines. NIST is working closely with the Defense Advanced Research Projects Agency (DARPA) to transition this software assurance technology to other agencies and making the ATP software available to industry as open source.

Building on this expertise in mobile app software assurance, NIST researchers are developing platform-independent techniques for identifying mobile malware by analyzing mobile app network behavior. NIST researchers are also developing metrics for evaluating the effectiveness of mobile app security test tools.

Contacts:

Dr. Steve Quirolgico
(301) 975-8426
stephen.quirolgico@nist.gov

Dr. Jeffrey Voas
(301) 975-6622
jeff.voas@nist.gov

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

Strengthening Internet Security

USGv6: A Technical Infrastructure to Assist IPv6 Adoption

Internet Protocol (IP) Version 6 (IPv6) is an updated version of the current Internet Protocol, IPv4. The primary motivations for the development of IPv6 were to increase the number of unique IP addresses available for use and to handle the needs of new Internet applications and devices. In addition, IPv6 was designed with the following goals: increased ease of network management and configuration; expandable IP headers; improved mobility and security; and quality of service controls. IPv6 has been, and continues to be, developed and defined by the Internet Engineering Task Force (IETF).

FY 2012 was a significant year for the deployment of IPv6 in the United States Government. OMB's Memo of September 10, 2010, *Transition to IPv6*, required all government agencies to "upgrade public/external facing servers and services (e.g., web, email, Domain Name System (DNS), Internet Service Provider (ISP) services) to operationally use native IPv6 by the end of FY 2012." NIST worked with the USGv6 Task Force and with individual government agencies to achieve this goal. NIST developed an online monitor to demonstrate which high-level government domains have met this goal with respect to DNS services, email, web servers, and Domain Name System Security Extensions (DNSSEC). In FY 2013, NIST and OMB continued to use this monitor to measure USGv6 compliance with OMB's requirement.

FY 2014 will bring additional OMB IPv6 requirements. Agencies will "upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014." NIST is developing online diagnostic tools to help agencies verify compliance to this requirement.

The NIST IPv6 Test Program, whose goal is to provide assurance on IPv6 product conformance and interoperability, continues to operate. In FY 2014, NIST will continue to manage and evolve the USGv6 Test Program. The NIST program is a collaboration between CSD and the Advanced Networking Technology Division.

http://www.antd.nist.gov/usgv6

Contacts:

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

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

Access Control and Privilege Management

Access Control and Privilege Management Research

With the advance of current computing technologies and the diverse environments in which these technologies are used, security issues, such as situational awareness, trust management, preservation of privacy in access control, and privilege management systems, are becoming increasingly complex. Practical and conceptual guidance for these topics is needed.

In FY 2013, the following research was accomplished for this project: 1) unified enforcement mechanism of data services for use by a Policy Machine (PM) for enterprise computing environment, 2) enhanced the capabilities of the Access Control Policy Tool (ACPT), 3) researched a new fault-detection method for access control rule using Simulated Logic Circuit algorithms, 4) researched formal ABAC models, and completed the development of Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, which provides information of function components as well as enterprise consideration of ABAC.

CSD expects that this project will:

- Promote (or accelerate) the adoption of community computing that utilizes the power of shared resources and common trust management schemes
- Provide guidance in implementing access control models and mechanisms for standalone or enterprise systems
- Increase the security and safety of static (connected) distributed systems by applying the testing and verification tool for the access control policies
- Assist system architects, security administrators, and security managers whose expertise is related to access control or privilege policy in managing their systems, and in learning the limitations and practical approaches for their applications
- Provide accurate and efficient fault detection and correction technology for implementing access control rules and policies

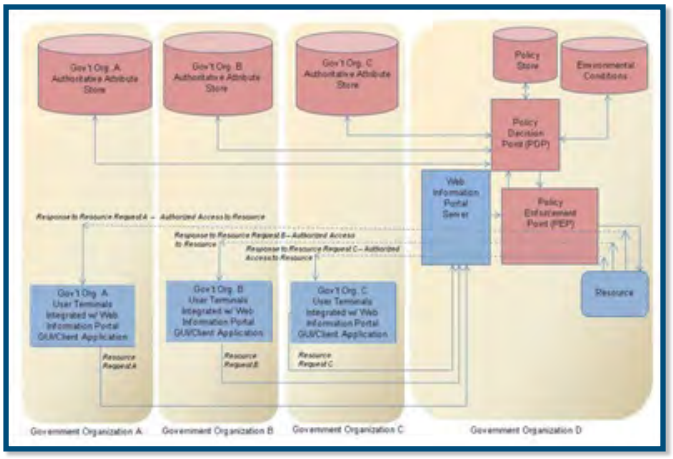


Figure 12: Access Control and Privilege Management

Contacts:

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

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

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

Conformance Verification for Access Control Policies

Access control systems are among the most critical network security components. Faulty policies, misconfigurations, or flaws in software implementation can result in serious vulnerabilities. The specification of access control policies is often a challenging problem. Often a system's privacy and security are compromised due to the misconfiguration of access control policies instead of the failure of cryptographic primitives or protocols. This problem becomes increasingly severe as software systems become more and more complex and are deployed to manage a large amount of sensitive information and resources organized into sophisticated structures. Identifying discrepancies between policy specifications and their properties (intended function) is crucial because correct implementation and enforcement of policies by applications is based on the premise that the policy specifications are correct. As a result, policy specifications must undergo rigorous verification and validation through systematic testing to ensure that the policy specifications truly encapsulate the desires of the policy authors.

To formally and precisely capture the security properties that access control should adhere to, access control models are usually written to bridge the rather wide gap in abstraction between policy and mechanism. Thus, an access control model provides unambiguous and precise expression as

well as reference for design and implementation of security requirements. Techniques are required for verifying whether an access control model is correctly expressed in the access controls policies and whether the properties are satisfied in the model. In practice, the same access control policies may express multiple access control models or express a single model in addition to extra access control constraints outside of the model. Ensuring the conformance of access control models and policies is a nontrivial and critical task.

Started in 2009, CSD developed a prototype system, Access Control Policy Tool (ACPT), which allows a user to compose, verify, test, and generate access control policies.

In FY 2013, ACPT was downloaded by 190 users and organizations. CSD performed prototype testing, enhanced the capability of ACPT by adding privilege inheritance algorithms, applied user cases of Attribute Based, Multi-Level, and Workflow access control models to test ACPT's performance, and compared to other formal method for performance and usability. CSD also produced a new user manual that explains new capabilities of ACPT. In addition, CSD published a research paper related to ACPT.

In FY 2014, CSD will continue testing, enhance the capability of ACPT by applying the tool for more complex access control policy combinations, provide model profiles, and improve user interfaces. CSD will also update ACPT based on user feedback and suggestions.

Figure 13: Conformance Verification

This project is expected to:

- Provide generic paradigm and framework of access control model/property conformance testing
- Provide templates for specifying access control rules in popular access control models such as Attribute Based, Multilevel, and Workflow models
- Provide tools or services for checking the security and safety of access control implementation, policy combination, and eXtensible Access Control Markup Language (XACML) policy generation
- Promote (or accelerate) the adoption of combinatorial testing for large-system (such as access control system) testing

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

Contacts:

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

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

Metrics for Evaluation of Access Control Systems (Real-Time Access Rule Fault Detection)

Specifying correct behaviors of Access Control (AC) policies is a challenging task, especially when an AC policy includes a large number of rules. Identifying discrepancies between AC policies and their intended functionalities is crucial because correct policy behaviors are based on the premise that the policies are correctly specified. Incorrect AC policies result in faults that not only leak but also disable access to information, and faults are especially difficult to detect without support of formal embedded models such as Multi-Level Security (MLS) and Chinese Wall.

Most research on AC model or policy verification techniques are focused on one particular model, and almost all of the research is in applied methods, which require the completed AC policies as the input for verification or test processes to generate fault reports. Even though correct verification is achieved and counterexamples may be generated along with found faults, those methods provide no information about the source of rule faults that might allow conflicts in privilege assignment, leakage of privileges, or conflict of interest permissions. The difficulty in finding the source of faults is increased especially when the AC rules are intricately covering duplicated variables to a degree of complexity. The complexity is due to the fact that a fault might not be caused by one particular rule; for example, rule *x* grants subject/attribute *s* access to object/attribute *o*, and rule *y* denies the group subject/attribute *g*, which *s* is a member of, access to object *o*. Such conflict can only be resolved by removing either rule *x* or *y*, or the *g* membership of *s* from the policy. But removing *x* or *y* affects other rules that depend on them (e.g., a member of subject group *g k* is granted access to object *o*), and removing *s*'s membership in *g* will disable *g*'s legitimate access to other objects/attributes through the

membership. Thus, it requires manually analyzing each rule in the policy in order to find the correct solution for the fault.

To address the issue, CSD researched the AC Rule Logic Circuit Simulation (ACRLCS) technique, which enables the AC authors to detect a fault when the fault-causing AC rule is added to the policy, so the fixing can be implemented in real time before adding other rules that further complicate the detecting effort. Rather than checking by retracing the interrelations between rules after the policy is completed, the policy author needs only check the newly added rule against previous "correct" ones. In ACRLCS, AC rules are represented in a Simulated Logic Circuit (SLC). The use of simulation may restrict ACRLCS implementation on a physical electronic circuit; however, the concept can be implemented and computed through simulated software.

In FY 2013, by using the Logic Circuit Simulation (LCS) software, CSD researched the SLC for the simulations of rule and inheritance assignments of AC privileges, formal AC model implementations, and multiple policy combinations. The result is published in the conference paper, *Real-Time Access Control Rule Fault Detection Using a Simulated Logic Circuit*.

In FY 2014, CSD is planning to further research the performance of the ACRLCS, and develop a basic reference implementation of the algorithm. Goals for the project include:

- Promote the concept of detecting AC policy faults in real time AC rule composing
- Provide an innovative method in specifying AC rules formed by Boolean logic expressions operated on variables of AC rules
- Provide techniques for preventing faults in enforcing fundamental security properties including Cyclic Inheritance, Privilege Escalation, and Separation of Duty
- Provide new methods for composing standard mandatory AC models such as Role-Based Access Control (RBAC) and MLS as well as some fundamental security properties

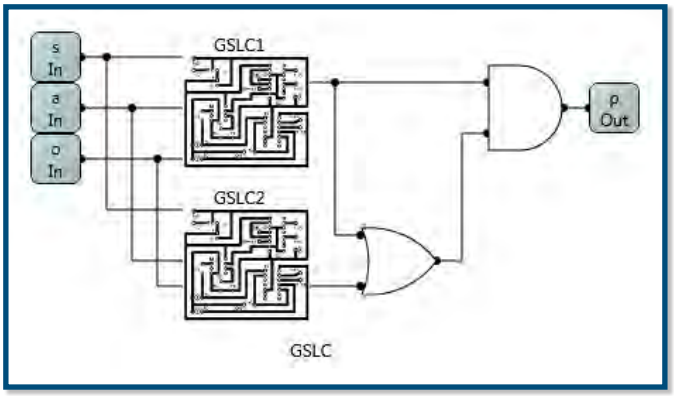


Figure 14: Real-time Access Control - Circuit

Contact:

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

Attribute Based Access Control

Attribute Based Access Control (ABAC) is a logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. ABAC represents a point on the spectrum of logical access control from simple access control lists to more capable role-based access (RBAC), and finally to a highly flexible method for providing access based on the evaluation of attributes.

There has not been a comprehensive effort to formally define or guide the implementation of ABAC within the Federal Government. This research provides considerations for using ABAC to improve information sharing within and among organizations while maintaining control of that information. The research serves a two-fold purpose; first, it aims to provide federal agencies with a definition of ABAC and a description of the functional components of ABAC. Second, it provides planning, design, implementation, and operational considerations for employing ABAC within a large enterprise with the goal of improving information sharing while maintaining control of that information.

In FY 2013, CSD completed the writing of SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. SP 800-162 includes terminology and basic understanding of ABAC; ABAC enterprise employment considerations during the initiation, acquisition/development, implementation/assessment, and operations and maintenance phases; and example to demonstrate how ABAC is implemented in a Web Information Portal. CSD also researched ABAC formal models, the result will be presented in a NISTIR, which describes a variety of characteristics and applications of ABAC formal models.

NIST conducted an Attribute Based Access Control Workshop, based on the SP 800-162, on July 17, 2013, in partnership with NSA and the National Cybersecurity Center of Excellence (NCCoE). About 100 individuals from government, industries, and academia/research attended the event. The workshop provided attendees an opportunity to identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop ABAC guidance; CSD updated SP 800-162 from the suggestions collected at the workshop.

In FY 2014, CSD will continue research of ABAC formal models as well as details and extended topics of ABAC capabilities, such as Attribute Engineering/Management, Integration with Identity Management, Federation, Situation Awareness (Real Time or Contextual) Mechanism, Policy Management, and Natural Language Policy translation to Digital Policy. The ABAC project will pursue the following objectives:

- Provide readers the terminology and basic understanding of ABAC
- Provide readers with an overview of the current state of logical access control, a working definition of ABAC, and an explanation of core and enterprise ABAC concepts
- Assist security policy makers in establishing a business case for ABAC implementation, and acquiring an interoperable set of capabilities
- Assist ABAC developers in developing the operational requirements, and overall enterprise architecture
- Assist ABAC administrators in establishing or refining business processes to support ABAC
- Promote adoption of ABAC for more secure and flexible method for information sharing in standalone or enterprise environment

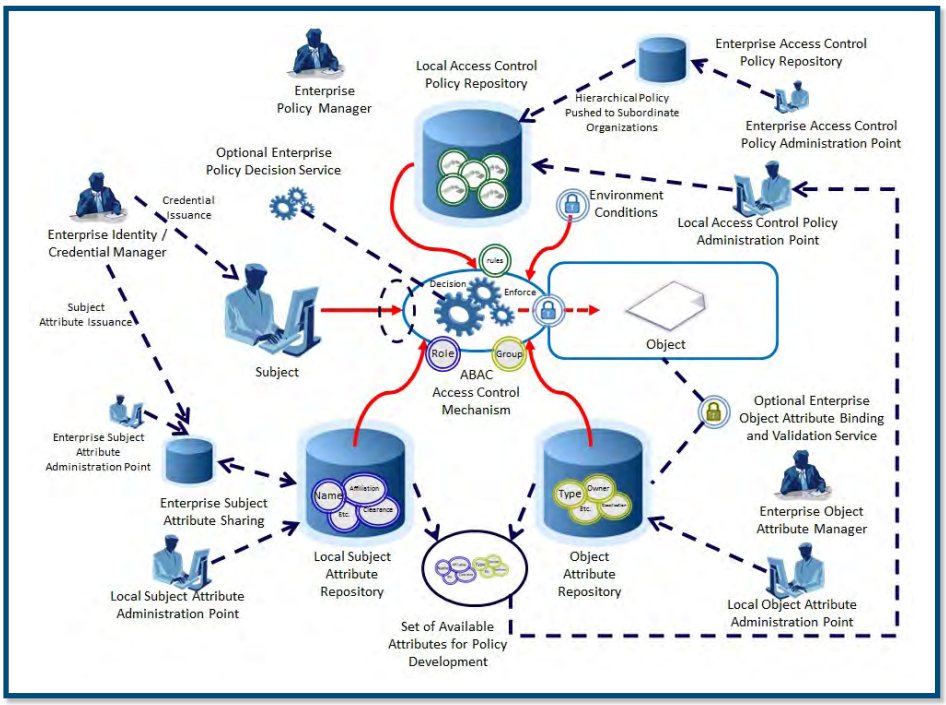


Figure 15: ABAC Access Control Mechanism Chart

http://csrc.nist.gov/projects/abac/

Contacts:

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

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

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

Advanced Security Testing and Measurements

Security Automation and Continuous Monitoring

IT organizations operate a diverse set of computing assets which access, route, store, and process information that is critical to the operations of businesses and the missions of government agencies. These IT environments are frequently reconfigured, and are under constant threat of attack. The wide variety of computing products, the speed of configuration change, and the diversity of threats require organizations to maintain situational awareness over their IT assets and to utilize this information to make risk-based decisions.

Security automation utilizes standardized data formats and transport protocols to enable data to be exchanged between business, operational, and security systems that support security processes by:

- Identifying IT assets
- Providing awareness over the operational state of computing devices
- Enabling security reference data to be collected from internal and external sources
- Supporting analysis processes that measure the effectiveness of security controls and provide visibility into security risks, enabling risk-based decision making

Commercial solutions built using security automation specifications enable the collection and harmonization of vast amounts of operational and security data into coherent, comparable information

streams to achieve situational awareness that informs timely and active management of diverse IT systems. Through the creation of reference data and guidance, and the international recognition of flexible, open standards, the NIST security automation program works to improve the interoperability, broad acceptance, and adoption of security automation solutions to address current and future security challenges, creating opportunities for innovation.

Specification, Standards, and Guidance Development

To support the overarching security automation vision, it is necessary to have specifications that describe the required interactions between systems, standards that document international consensus approaches, and guidance that informs product development and implementation. Through close work with partners in government, industry, and academia, NIST continues to facilitate the definition and development of security automation approaches that enable organizations to understand and manage IT security risks.

During FY 2013, NIST worked to build on previous security automation work by:

- Establishing working groups in standards development organizations to promote international consensus around standardized approaches
- Identifying and addressing gaps in the current specifications
- Evolving existing approaches to achieve greater scalability and impact
- Providing additional guidance on architectural, design, and analysis concerns
- Development and maintenance of tools and reference implementations

NIST is currently working with its partners in various standards development organizations, including the International Organization for Standardization (ISO), the Internet Engineering Task Force (IETF), the Forum of Incident Response and Security Teams (FIRST), and the Trusted Computing Group (TCG), to further mature and broaden adoption of security automation specifications, reference data, and techniques. This area of work is focused on evolving security automation specifications to integrate with existing transport protocols to provide for secure, interoperable exchange of security automation data. Additional work is focused on evolving security metrics and providing consensus guidance on security automation approaches. Through the definition and adoption of security automation standards and guidelines, IT vendors will be able to provide standardized security solutions to their customers. These solutions support continuous monitoring and automated, dynamic network defense capabilities based on analysis of data from operational and security data sources and the collective action of security components.

Security automation work has been focused in two areas: evolution and international adoption of the Security Content Automation Protocol (SCAP) and development of a Continuous Monitoring building block focused on secure software asset management capabilities. The following sections detail this work.

Security Content Automation Protocol (SCAP)

SCAP is a multipurpose protocol that provides an automated means to collect and assess the state of devices. SCAP supports automated vulnerability checking, verifying the installation of patches, checking security configuration settings, verifying technical control compliance, measuring security, and examining systems for indicators of compromise. SCAP uses the Extensible Markup Language (XML) to standardize the format and nomenclature by which security software products communicate information about software flaws, security configurations, and other aspects of device state. SCAP enables security automation content, also known as "SCAP content," to be expressed using standardized formats, identifiers, and scoring models. This content can be used by any tool that is conformant to the specifications, to collect and evaluate the state of software installed on a device.

SCAP has been widely adopted by major software and hardware manufacturers and has become a significant component of information security management and governance programs. SCAP-enabled tools are currently being used by the U.S. Government, critical infrastructure companies, academia, and other businesses, both domestically and internationally. Currently, CSD is leveraging SCAP in multiple areas, both to support its own mission and to enable other agencies and private sector entities to meet their goals. For CSD, SCAP is a critical component of the SCAP Validation Program, the National Vulnerability Database (NVD), and the National Checklist Program (NCP).

In September 2012, NIST published SP 800-126 Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, . That document describes the 11 component specifications composing SCAP.

SCAP 1.2 Specifications	
Specification	**Description**
Languages	
Extensible Configuration Checklist Description Format (XCCDF)	Used for authoring security checklists/benchmarks and for reporting results of evaluating them
Open Vulnerability and Assessment Language (OVAL)	Used for representing system configuration information, assessing machine state, and reporting assessment results
Open Checklist Interactive Language (OCIL)	Used for representing checks that collect information from people or from existing data stores populated by other data collection methods
Reporting Formats	
Asset Reporting Format (ARF)	Used to express information about assets and to define the relationships between assets and reports
Asset Identification	Used to uniquely identify assets based on known identifiers and other asset information
Enumerations	
Common Platform Enumeration (CPE)	A nomenclature and dictionary of hardware, operating systems, and applications; a method to identify applicability to platforms
Common Configuration Enumeration (CCE)	A nomenclature and dictionary of software security configurations
Common Vulnerabilities and Exposures (CVE)	A nomenclature and dictionary of security-related software flaws
Measurement and Scoring Systems	
Common Vulnerability Scoring System (CVSS)	Used for measuring the relative severity of software flaws
Common Configuration Scoring System (CCSS)	Used for measuring the relative severity of device security (mis-)configuration issues
Content and Result Integrity	
Trust Model for Security Automation Data (TMSAD)	Guidance for using digital signatures in a common trust model applied to security automation specifications

Since the release of SCAP 1.2, NIST has worked to improve guidance around the SCAP specifications by promoting broader international adoption of SCAP, encouraging the integration of SCAP into other standards, and by adapting SCAP to address specific gaps and challenges. The following work activities were performed during FY 2013:

NIST released draft NISTIR 7946, *CVSS Implementation Guidance*, which guides analysts scoring IT vulnerabilities using the CVSS Version 2.0. That document is the result of applying the CVSS specification to score over 50,000 vulnerabilities analyzed by the NVD. The report reviews the CVSS base metrics and provides guidance for difficult and/or unique scoring situations and assists vulnerability analysts with scoring particular types of vulnerabilities by identifying common keywords and phrases that often appear in vulnerability alerts. The report includes a collection of scored IT vulnerabilities from the NVD, a justification for each score provided, and a description of the NVD vulnerability scoring process.

NIST, in collaboration with industry partners in the IETF, established the Security Automation and Continuous Monitoring (SACM) working group, chartered in July 2013. The current scope of work for SACM includes identifying and/or defining the transport protocols and data formats needed to support the collection and evaluation of device state against expected values and standards for interacting with repositories of security automation content. The initial focus of the SACM working group is on identifying use cases, requirements, and architectural models to inform decisions about existing specifications and standards that can be referenced, required modifications or extensions to existing specifications and standards, and any gaps that need to be addressed. This working group provides a venue for advancing appropriate SCAP specifications into international standards and addressing identified gap areas.

For more information, please refer to:
http://datatracker.ietf.org/wg/sacm/charter/

Additionally, NIST collaborated with industry partners to revise the ISO/IEC 19770-2:2009 standard, *Information technology -- Software asset management -- Part 2: Software identification tag*, which establishes a specification for tagging software to support identification and management. This software identification (SWID) data model provides a mechanism for software publishers to provide authoritative identification, categorization, software relationship (e.g., dependency, bundling, and patch), file footprint details, and other software metadata for software they publish. This information enhances SCAP use cases by providing authoritative information for creation of CPE names, targeting of checklists, and associating software flaws to products based on a defect in a software library or executable.

NIST also worked with government and industry partners in the TCG to define a number of specifications related to the Trusted Network Connect (TNC) protocols. The first such publication is the TNC SCAP Messages for IF-M specification that supports carrying SCAP content and results over the TNC protocols. The second is the TNC Enterprise Compliance Profile (ECP) and related specifications that support the exchange of SWID data over the TNC protocols. The ECP enables collection of SWID data from a device for use by external tools to provide software inventory information. SCAP and SWID data collected using these mechanisms may be optionally used for network access control decision making, allowing device state to be evaluated when devices connect and on an ongoing basis thereafter.

For more information on these specifications, please visit:

http://www.trustedcomputinggroup.org/resources/tnc_scap_messages_for_ifm, and

http://www.trustedcomputinggroup.org/resources/tnc_endpoint_compliance_profile_specification.

Finally, NIST participated in two Forum of Incident Response and Security Teams (FIRST) Special Interest Groups (SIG). The CVSS SIG (CVSS-SIG) focused on defining CVSS Revision 3, which is intended to implement improvements to the scoring model based on community feedback. The CVSS-SIG plans to release a draft of the revision in early FY 2014, with a completed approved specification expected in the summer of 2014. The second SIG, the Vulnerability Reporting and Data eXchange SIG (VRDX-SIG), researches and recommends methods for identifying and exchanging vulnerability information across disparate vulnerability databases.

For more information, please visit:
http://www.first.org/global/sigs.

Through work with international SDOs, SCAP and related security automation capabilities are expected to evolve and expand in support of the growing need to define and measure effective security controls, assess and monitor ongoing aspects of information security, remediate noncompliance, and successfully manage systems in accordance with the Risk Management Framework described in SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

http://scap.nist.gov/

Contact:

Mr. David Waltermire
(301) 975-3390
david.waltermire@nist.gov

Continuous Monitoring

In September 2010, the Department of Homeland Security (DHS) released the *Continuous Asset Evaluation, Situational Awareness and Risk Scoring (CAESARS)* Reference Architecture Report. This report identifies commonality and strengths in the custom approaches used by civilian agencies to provide solutions that enable the continuous monitoring of IT systems. This report identifies "essential functional components of a security risk scoring system, independent of specific technologies, products, or vendors." It describes the use of security automation specifications, such as the SCAP, to enable continuous monitoring solutions.

In October 2010, the Federal Chief Information Officer Council's Information Security and Identity Management Committee's (ISIMC) subcommittee on Continuous Monitoring and Risk Scoring saw the need to create a technical initiative to expand upon the CAESARS architecture to better scale it to large enterprises (e.g., the entire U.S. Government). A team of researchers from the NSA Information Assurance Directorate (IAD), the DHS Federal Network Security CAESARS team, and NIST's Information Technology Laboratory (ITL) worked together to respond to this need. The draft CAESARS Framework Extension (CAESARS-FE) described by Draft NISTIR 7756, *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture*, is the output of this collaboration.

Draft NISTIR 7756 presents an enterprise continuous monitoring (ConMon) technical reference architecture that extends the framework provided by the DHS's CAESARS architecture. The primary goal of this effort is to enable enterprise ConMon by supporting the development and deployment of capabilities that support automated, enterprise-wide ConMon functions. The concepts, workflows, and subsystems presented in this document can be used by organizations seeking to establish federated queries, orchestration of data collection tasks, data analytics, and presentation and reporting capabilities across a diverse portfolio of security and IT products. CAESARS-FE supports IT operations and network defense capabilities, with compliance reporting as a byproduct of actual security monitoring and improvement. CAESARS-FE enables organizations to design, develop, and deploy ConMon capabilities by leveraging their existing security and IT tools while minimizing custom tool integration efforts. CAESARS-FE defines the requisite functionality needed to ensure the interoperability of vendor products while continuing to encourage security tool vendor participation and innovation.

To advance the state of the art in continuous monitoring capabilities and to further interoperability within commercially available tools, CSD is working within the international

standards development community to establish working groups and to author and comment on emerging technical standards in this area. The CAESARS-FE reference architecture will evolve as greater consensus is developed around interoperable, standards-based approaches that enable continuous monitoring of IT systems. In early FY 2014, CSD plans to release an update to NISTIR 7756 that provides additional guidance for development of ConMon architectures and solutions based on ongoing standards activities and feedback.

The NIST National Cybersecurity Center of Excellence (NCCoE) is also working to develop a series of ConMon building blocks that demonstrate cybersecurity solutions that apply across multiple industry sectors. The first building block, currently under development, proposes a standardized approach to software asset management, providing an organization with an integrated view of software throughout its lifecycle. The building block will support:

- Authorization and verification of software installation media – Verifies that the media is from a trusted software publisher and that the installation media has not been tampered with
- Software execution whitelisting – Verifies that the software is authorized to run and has not been tampered with
- Publication of installed software inventory – A device that securely communicates what software is installed to an organization-wide database
- Software inventory-based network access control – A device's level of access to a network is determined by what software is or is not present on the device and whether its patches are up to date

The building block document, *Continuous Monitoring Building Block: Software Asset Management,* can be viewed at http://csrc.nist.gov/nccoe/Building-Blocks/conmon.html. In FY 2014, the team will continue to develop this building block and to work with vendors to develop a solutions demonstration. Through this process, CSD provides publically available descriptions of the practical steps needed to implement the technical approaches defined by the building block.

Contact:

Mr. David Waltermire
(301) 975-3390
david.waltermire@nist.gov

Security Automation Reference Data

Through the NVD and the National Checklist Program (NCP), NIST is providing relevant and important reference data in the areas of vulnerability and configuration management. SCAP, and the programs that leverage it, are moving the information assurance industry towards being able to standardize communications, and the collection and storage of relevant data in standardized formats, and provide automated means for the assessment and remediation of systems for both vulnerabilities and configuration compliance.

National Vulnerability Database (NVD)

Security automation reference data is currently housed within the NVD. The NVD is the U.S. Government repository of security automation data based on security automation specifications. This data provides a standards-based foundation for the automation of software asset, vulnerability, and security configuration management; security measurement; and compliance activities. This data supports security automation efforts based on the SCAP. The NVD includes databases of security configuration checklists for the NCP, listings of publicly known software flaws, product names, and impact metrics. A formal validation program tests the ability of vendor products to use some forms of security automation data based on a product's conformance in support of specific enterprise capabilities.

SCAP defines the structure of standardized software flaws and security configuration reference data, also known as SCAP content. This reference data is provided by the NVD (http://nvd.nist.gov/).

The NVD is the U.S. Government repository of standards-based vulnerability management reference data. The NVD provides information regarding security vulnerabilities and configuration settings, vulnerability impact metrics, technical assessment methods, and references to remediation assistance and IT product identification data. As of October 2013, the NVD contained the following resources:

- Over 58,000 vulnerability advisories with an average of 8 new vulnerabilities added daily
- 52 SCAP-expressed checklists containing thousands of low-level security configuration checks that can be used by SCAP-validated security products to perform automated evaluations of system state
- 173 non-SCAP security checklists (e.g., English prose guidance and configuration scripts)
- 248 U.S. Computer Emergency Readiness Team (US-CERT) alerts, 2,771 US-CERT vulnerability summaries, and 8,140 SCAP machine-readable software flaw checks

- Product dictionary with over 79,000 operating system, application, and hardware name entries
- 42,954 vulnerability advisories translated into Spanish

NVD is hosted and maintained by NIST and is sponsored by the Department of Homeland Security's US-CERT.

The use of SCAP data by commercial security products, deployed in thousands of organizations worldwide, has extended NVD's effective reach. Increasing demand for NVD XML data feeds and SCAP-expressed content from the NVD website demonstrates increased adoption of SCAP.

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

Throughout FY 2013, NVD continued to provide access to vulnerability reference data and security checklists. CSD updated the NVD to support the latest CPE Naming specification, CPE 2.3, and produces the official CPE dictionary in multiple formats. NVD now hosts the list of configuration items, complementing the configuration checklist data already maintained. NVD data is substantially increasing the security of networks worldwide and it is a fundamental component of CSD's security automation infrastructure. CSD plans to update and improve the NVD in FY 2014 to include improvements in user navigation, addition of references to the SP 800-53 Revision 4 security controls content, and the ability to search, browse, and download common configuration enumeration (CCE) list data.

http://nvd.nist.gov

Contact:

Mr. Harold Booth
(301) 975-8441
harold.booth@nist.gov

Computer Security Incident Coordination

Recognizing that even well-engineered and administered computing systems are sometimes successfully attacked, it is important to establish and maintain processes and procedures to recover from attacks when defensive mechanisms are breached. NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide*, provides guidance on establishing and operating a Computer Security Incident Response Team (CSIRT). A wide-ranging attack may affect numerous organizations. When an attack has the potential to affect computing systems in multiple organizations, coordination among separate CSIRTs can make it possible to limit the damage caused by an attack, speed recovery operations, and maintain a higher level of operational security.

CSD is working with the Department of Homeland Security (DHS) to develop guidance on Computer Security Incident Coordination (CSIC). The goal of CSIC is to help diverse collections of organizations to effectively collaborate in the handling of computer security incidents. Effective collaboration raises numerous issues on how and when to share information between organizations, and in what form information should be shared. Because different organizations may have substantially different capabilities for responding to attacks, diagnosing causes, and handling sensitive attack-related information, guidance must provide a framework to help organizations interoperate despite their organizational differences.

This initiative will develop a NIST SP that provides guidance on how organizations can develop collaborative capabilities in advance of incidents in order to be prepared to operate swiftly and with coordination during incidents. The guidance will cover data handling considerations, such as sensitivity, data collection and retention practices, data standards, redaction, and use of tools such as anonymization. The guidance will help incident responders to understand when data can be shared, when it should not be shared, and when sharing is essential. A key element in the approach is the concept of an integrated, functionally-composed incident response team. The objective of a functionally-composed team is to enable each organization to contribute most in technical areas where that organization has higher relative levels of expertise and readiness, thus speeding incident detection, analysis, containment, eradication, and recovery.

In FY 2014, CSD plans to complete a Draft Special Publication providing guidance for Computer Security Incident Coordination and organize a workshop focused on the issues of incident coordination.

Contacts:

Mr. Lee Badger
(301) 975-3176
lee.badger@nist.gov

Mr. David Waltermire
(301) 975-3390
david.waltermire@nist.gov

Incident Handling Automation

In recent years, security threats to digital systems have become more prevalent and more sophisticated. While some security threats are generic in nature, others are targeted at specific organizations, assets, and missions. Although computer

security defenses may forestall many threats, not all can be prevented, and organizations must therefore develop incident handling capabilities. Incident handling encompasses a variety of tasks ranging from preparation prior to an incident, to timely detection and analysis of an incident, to recovery and repair from the effects of an incident, to post-incident learning and improvement. These tasks need to be performed both internally within specific organizations and externally via coordination across teams of collaborating organizations.

In the past year, NIST worked with the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) to develop Revision 2 of NIST Special Publication 800-61, *Computer Security Incident Handling Guide*. This document provides guidance on developing incident handling capabilities. The document explains the nature of incidents and incident handling processes, the structure and operation of Computer Security Incident Response Teams (CSIRT), and provides guidance on handling an incident and coordinating with other organizations.

SP 800-61 Revision 2 focuses primarily on manual (human) processes for incident handling and the effective use of human judgment, guided by applicable regulation and law, regarding which incident-related information is significant and which incident-related information may be shared. The growing volume of security threats, however, is driving the need for a more agile incident-handling framework that can operate at differing scales and speeds as required.

Working in concert with the DHS, NIST is expanding existing incident handling guidance to enable coordinated information sharing across disparate CSIRTs operating at differing scales and speeds. This work will include the analysis of standardized incident handling data models and the incorporation of these data models, as appropriate, into both CSIRT information sharing processes as well as incident/threat knowledge repositories. This work will describe how mature CSIRTs may operate in a diverse information-sharing network with both operational and strategic CSIRTs, as well as industry knowledge repositories. This may include selective use of security automation where applicable.

In FY 2014, this work will develop Draft SP 800-150, *Coordinated Computer Security Incident Handling Guidance*.

Contacts:

Mr. Lee Badger
(301) 975-3176
lee.badger@nist.gov

Mr. David Waltermire
(301) 975-3390
david.waltermire@nist.gov

National Checklist Program (NCP)

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

To facilitate development of security configuration checklists for IT products and to make checklists more organized and usable, NIST established the National Checklist Program (NCP) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, and also under the Cyber Security Research and Development Act, which tasks NIST to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government." In February 2008, revised Part 39 of the Federal Acquisition Regulation (FAR) was published. Paragraph (d) of section 39.101 states, "In acquiring information technology, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations available from the NIST website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated."

In Memorandum M-08-22, the Office of Management and Budget (OMB) mandated the use of SCAP-validated products for continuous monitoring of Federal Desktop Core Configuration (FDCC) compliance. The NCP strives to encourage and make simple agencies' compliance with these mandates.

The goals of the NCP are to:

- Facilitate development and sharing of checklists by providing a formal framework for checklist developers to submit checklists to NIST
- Provide guidance to developers to help them create standardized, high-quality checklists that conform to common operations environments
- Help developers and users by providing guidelines for making checklists better documented and more usable

- Encourage software vendors and other parties to develop checklists
- Provide a managed process for the review, update, and maintenance of checklists
- Provide an easy-to-use repository of checklists
- Encourage the use of automation technologies (e.g., SCAP) for checklist application

There are 225 checklists posted on the website; 52 of the checklists are SCAP-expressed and can be used with SCAP-validated products. In FY 2013, a total of 16 SCAP-expressed checklists were contributed to the NCP from other federal agencies and product vendors.

Organizations can use checklists obtained from the NCP website for automated security configuration patch assessment. NCP currently hosts SCAP checklists for Internet Explorer 9.0, Internet Explorer 10.0, Office 2010, Red Hat Enterprise Linux, Windows 7, Windows 8, Windows Server 2012, and other products.

To assist users in identifying automated checklist content, NCP groups checklists into tiers, from Tier I to Tier IV. NCP uses the tiers to rank checklists according to their automation capability. Tier III and IV checklists include SCAP content and have been validated by the SCAP content validation tool as conforming to the requirements outlined in SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP).* Tier IV checklists are considered production-ready and have been validated by NIST or a NIST recognized authoritative entity to ensure, to the maximum extent possible, interoperability with SCAP-validated products.

Tier III checklists use SCAP content to document security settings and should be compatible with SCAP-validated products. Tier II checklists document recommended security settings in a machine-readable, nonstandard format, such as a proprietary format or a product-specific configuration script. Tier I checklists are prose-based and contain no machine-readable content. Users can browse the checklists based on the checklist tier, IT product, IT product category, or authority, and also through a keyword search that searches the checklist name and summary for user specified terms. The search results show the detailed checklist metadata and a link to any SCAP content for the checklist, as well as links to any supporting resources associated with the checklist.

To assist checklist developers, the NCP provides both manual and automated interfaces to facilitate submission and maintenance processes. The manual interface consists of a web application that guides the submitter through the data entry process to ensure that all of the required information is submitted. The submission is validated upon review, and a report is returned to the submitting organization, verifying either acceptance or rejection based on the criteria requirements. For instance, Tier III and Tier IV checklists require validation using the SCAP Content Validation Tool (this tool is available for download via http://scap.nist.gov/revision/1.2/#tools).

The NCP is defined in SP 800-70 Revision 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, which can be found at http://csrc.nist.gov/publications/PubsSPs.html.

http://checklists.nist.gov

Contact:

Mr. Stephen Quinn
(301) 975-6967
stephen.quinn@nist.gov

United States Government Configuration Baseline (USGCB) / FDCC Baselines

The United States Government Configuration Baseline (USGCB) initiative creates security configuration baselines for information technology (IT) products widely deployed across the federal agencies. The project evolved from the Federal Desktop Core Configuration (FDCC) mandate originally described in a March 2007 memorandum from the U.S. White House Office of Management and Budget (Memorandum M-07-11). USGCB helps to improve information security and reduce overall IT operating costs by providing commonly accepted security configurations for major operating systems.

Through the National Checklist Program described in SP 800-70 Revision 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, a baseline submitter may express interest in submitting a candidate for use in the USGCB program.

CSD provides ongoing support for the USGCB automation content, including the creation of patch updates, assisting USGCB users in continuously monitoring and assessing security compliance of information systems. This ongoing monitoring element supports the Risk Management Framework described in SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

During FY 2013, a supplemental USGCB SCAP 1.0 content for Microsoft Windows XP, Vista and 7 was released to correct an issue with directory server performance caused by the existing USGCB content.

The USGCB Program will continue in FY 2014 to provide ongoing maintenance of the baseline artifacts and to consider additional applicable platforms.

Contact:

Mr. Stephen Quinn
(301) 975-6967
stephen.quinn@nist.gov

Apple OS X Security Configuration

CSD is working with Apple to develop secure system configuration baselines supporting different operational environments for Apple OS X, Version 10.8, Mountain Lion. These configuration guidelines will assist organizations with hardening OS X technologies and provide a basis for unified controls and settings for OS X workstations and for mobile system security configurations for federal agencies.

The configurations will be based on a collection of resources, including the existing NIST OS X configuration guidance, the OS X security configuration guide, the Department of Defense (DoD) OS X Recommended Settings, and the Defense Information Systems Agency (DISA) OS X Security Technical Implementation Guide (STIG). Our team is aggregating appropriately 400 initial settings, determining which settings will be included in the configuration baseline, and determining appropriate values for each included setting. As the desired configuration items are established, our team is developing shell scripts that apply the settings to an OS X 10.8 system. The settings are organized into three key baselines, which are appropriate for different environments:

- Enterprise baseline is appropriate for centrally managed, networked systems.
- Small Office Home Office baseline is appropriate for systems that are deployed remotely but need to connect to enterprise networks.
- Special Security Limited Functionality baseline is appropriate for systems where security requirements are more stringent and where the implementation of security safeguards is likely to reduce functionality.

SCAP, defined and discussed in other sections of this report, is used to express configuration settings and check system configuration compliance.

During FY 2013, CSD provided a block of initial settings to Apple and these settings are being posted for the Apple community on a periodic basis for public review, discussion, correction and agreement. Each setting will have a designated Common Configuration Enumeration (CCE) number, which will aid in long-term tracking of the setting. Once these settings are vetted and curated by Apple, these settings will be tested and included in the configuration baselines. In addition, CSD is producing a draft guideline, *Guide to Securing Apple OS X 10.8 Systems for IT Professionals*. This guidance, similar in structure to the NIST SP 800-68, *Windows XP Security Guide*, will provide detailed information about the security of Apple OS X 10.8, and will provide security configuration guidelines for the Apple OS X 10.8 operating system.

In FY 2014, CSD plans to complete the scripts for the remaining initial settings and post them to the Apple community for feedback. CSD will also continue the development of the draft *Guide to Securing Apple OS X 10.8 Systems for IT Professionals*; this documentation will then be made available for public comment.

Contacts:

Mr. Lee Badger
(301) 975-3176
lee.badger@nist.gov

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

Mr. Lawrence Keys
(301) 975-5482
lawrence.keys@nist.gov

Validation Programs

Security Content Automation Protocol (SCAP) Validation Program

The SCAP Validation Program performs conformance testing to ensure that products correctly implement SCAP as defined in SP 800-126 Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*. Conformance testing is necessary because SCAP is a complex specification consisting of eleven individual specifications that work together to support various use cases. A single error in product implementation could result in undetected vulnerabilities or policy noncompliance within agency and industry networks.

In FY 2013, CSD updated the SCAP Validation Program to support the testing of products against SCAP version 1.2. The division published NISTIR 7511 Revision 3, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*, which introduces a modular approach with respect to the platforms that vendors may support. Public validation test content was published , thus providing reference materials that support conformance testing by industry and end users. The SCAP 1.2 public test content provides vendors

with the materials required for quality assurance testing prior to entering formal SCAP testing by an NVLAP accredited SCAP lab. The SCAP Validation Program resources web page was introduced to provide the public with a centralized location for all resources and information necessary to prepare products for SCAP 1.2 validation. The resources provided include documentation, a list of Frequently Asked Questions (FAQ), the SCAP test content, and tools for validating and processing SCAP data streams. CSD updated the SCAP Content Validation Tool (SCAPVal), used for validating that data streams adhere to the SCAP specification, to include support for SCAP 1.2. The update for SCAP 1.2 included open source SCAP reference implementation tools that are used to process SCAP data streams.

End users may use the SCAP Validation Program resources page to learn more about the validation program and download reference materials. The program currently has seven independent laboratories accredited for SCAP 1.2 product testing and several products are undergoing testing.

The SCAP Validation Program will expand in FY 2014 to provide enhanced testing support and will focus on increased test coverage by SCAP reference implementation tools. Expansion plans also include improvements in automated testing capabilities.

http://scap.nist.gov/validation/

Contact:

Ms. Melanie Cook
(301) 975-5259
melanie.cook@nist.gov

Cryptographic Programs and Laboratory Accreditation

The Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP) were developed by NIST to support the needs of the user community for strong, independently tested, and commercially available cryptographic algorithms and modules. Through these programs, NIST works with private and governmental sectors and the cryptographic community to achieve security, interoperability, and assurance of correct implementation. The goal of these programs is to support the use of validated algorithms, and modules and to provide federal agencies with a security metric to use in procuring cryptographic modules. The testing carried out by independent third-party laboratories accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) and the validations performed by the CMVP and CAVP programs provide this metric. Federal agencies, industry, and the public can choose cryptographic modules and/or products containing cryptographic modules from the CMVP Validated Modules List and have confidence in the claimed level of security and assurance of correct implementation.

Cryptographic algorithm and cryptographic module testing and validation are based on underlying published standards . As federal agencies are required to use validated cryptographic modules for the protection of sensitive non-classified information, the validated modules and the validated algorithms that the modules contain represent the culmination and delivery of the division's cryptography-based work to the end user.

The CAVP and the CMVP are separate, collaborative programs based on a partnership between NIST's CSD and the Communication Security Establishment Canada (CSEC).. The CAVP and the CMVP validate algorithms and modules used in a wide variety of products, including secure Internet browsers, secure radios, smart cards, space based communications, munitions, security tokens, mobile phones, network and storage devices, and products supporting Public Key Infrastructure (PKI) and electronic commerce. A module may be a standalone product, such as a virtual private network (VPN) or smart card or it could be a module used in several products, such as a toolkit. As a result, a small number of modules may be incorporated within hundreds of products. The CAVP validates cryptographic algorithms that may be integrated in one or more cryptographic modules.

The CAVP and CMVP validation programs provide documented methodologies for conformance testing through defined sets of security requirements. For CAVP, the validation system documents are designed for each FIPS-approved and NIST-recommended cryptographic algorithm. See website for a listing. Security requirements for the CMVP are found in FIPS 140-2, *Security Requirements for Cryptographic Modules* and the associated test metrics and methods in *Derived Test Requirements for FIPS 140-2*. The four Annexes to FIPS 140-2 reference the underlying cryptographic algorithm standards or methods. The CMVP developed *Derived Test Requirements for FIPS 140-2* defines the test metrics and methods and ensures repeatability of tests and equivalency in results across the testing laboratories.

The CMVP reviews the cryptographic modules validation requests and, as a byproduct of the review, is attentive to emerging and/or changing technologies and the evolution of operating environments and complex systems during the module validation review activities. Likewise, the CAVP reviews the cryptographic algorithm validation requests submitted by the accredited laboratories. With these insights, the CAVP and CMVP can perform research and development on evolving test metrics and methods. Based on this research, the CAVP and CMVP publish Implementation Guidance to assist vendors,

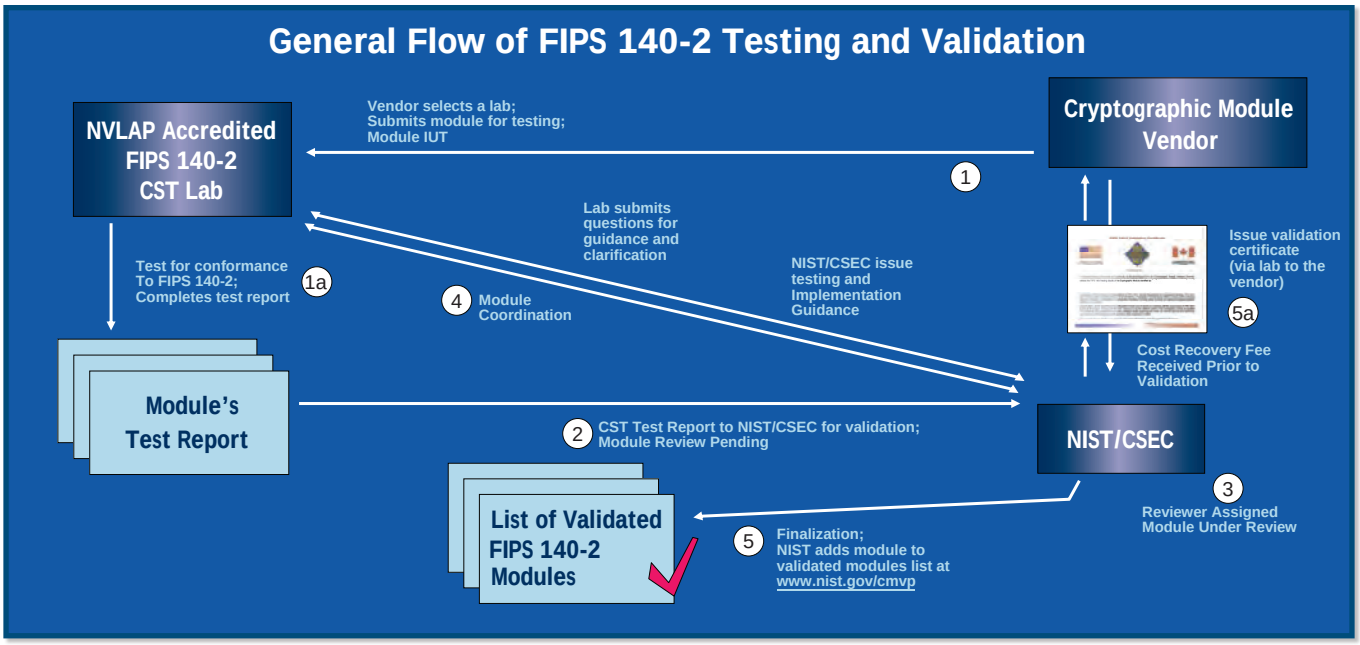


Figure 16: General Flow of FIPS 140-2 Testing and Validation

testing laboratories, and the user community. This guidance provides clarity, consistency of interpretation, and insight for successful conformance testing, validation, and revalidation.

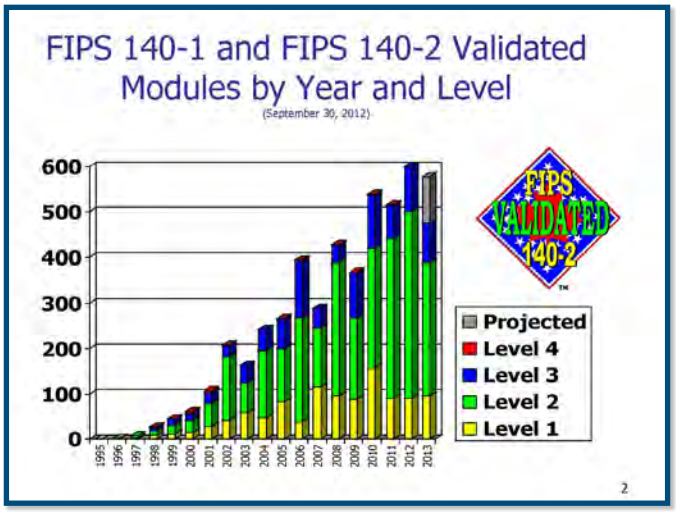


Figure 17: FIPS 140-1 and FIPS 140-2 Validated Modules by Year and Level

The unique position of the validation programs gives the CMVP the opportunity to acquire insight during the validation review activities and results in practical, timely, and up-to-date guidance that is needed by the testing laboratories and vendors to move their modules out to the user community in a timely and cost-effective manner and with the assurance of third-party conformance testing. This knowledge and insight provide a foundation for future standards development.

The CAVP and the CMVP have stimulated improved quality and security assurance of cryptographic modules. The latest set of statistics, which are collected quarterly from each of the testing laboratories, shows that 7% of the cryptographic algorithms and 35% of the cryptographic modules brought in for voluntary testing had security flaws that were corrected during testing. To date, over 2,004 cryptographic module validation certificates have been issued, representing over 4,811 modules that were validated by the CMVP. These modules have been developed by more than 425 domestic and international vendors.

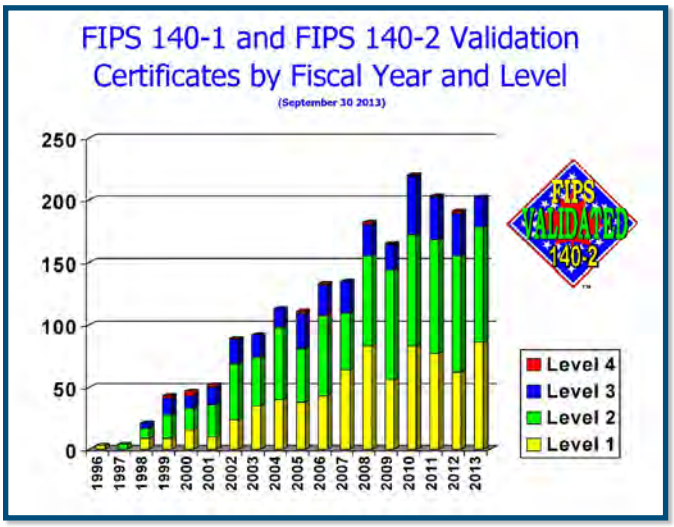


Figure 18: FIPS 140-1 and FIPS 140-2 Validation Certificates by Fiscal Year and Level

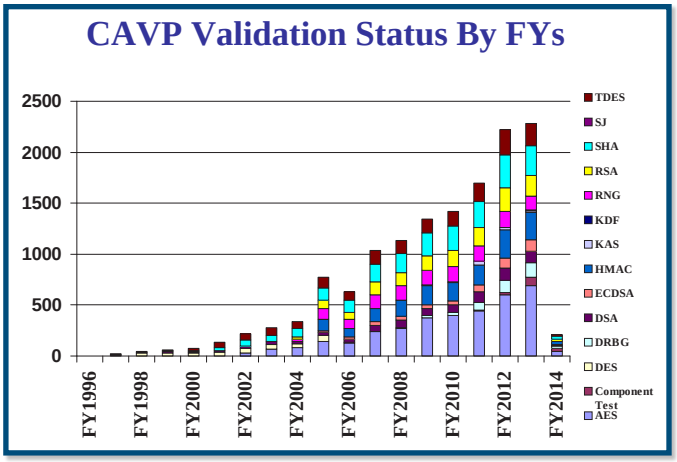


Figure 19: CAVP Validation Status by FYs

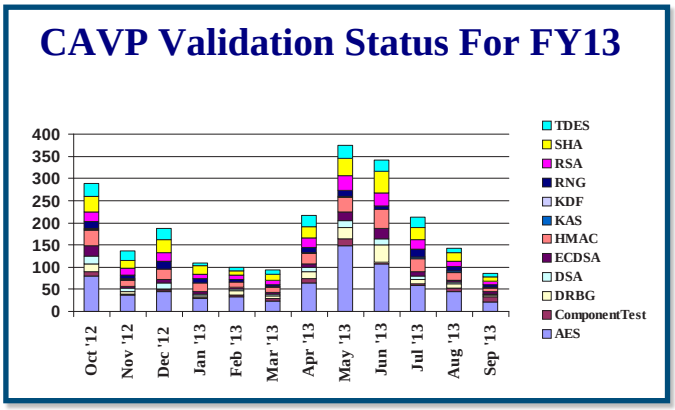


Figure 20: CAVP Validation Status for FY 2013

The CAVP issued 2,288 algorithm validations and the CMVP issued 191 module validation certificates in FY 2013. The number of algorithms and modules submitted for validation continues to grow, representing significant growth in the number of validations expected to be available in the future.

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

Contacts:

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

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

Automated Security Testing and Test Suite Development

NIST's CAVP utilizes the requirements and specifications of the algorithm FIPS and Special Publications (SPs) written by the Cryptography Technology Group (CTG) to develop algorithm test suites and automated security testing. The CAVP is responsible for providing assurance that the algorithms contained in modules are implemented correctly. The CAVP does this by designing and developing conformance testing for implementations of these algorithms.

CAVP Validated Implementation Actual Numbers

Updated As Wednesday, November 06, 2013

FiscalYear	AES	Comp.	DES	DSA	DRBG	ECDSA	HMAC	KAS	KDF	RNG	RSA	SHA	SJ	TDES	Total
FY1996	0	0	2	0	0	0	0	0	0	0	0	0	0	0	**2**
FY1997	0	0	11	6	0	0	0	0	0	0	0	7	2	0	**26**
FY1998	0	0	27	9	0	0	0	0	0	0	0	6	0	0	**42**
FY1999	0	0	30	14	0	0	0	0	0	0	0	12	1	0	**57**
FY2000	0	0	29	7	0	0	0	0	0	0	0	12	1	28	**77**
FY2001	0	0	41	15	0	0	0	0	0	0	0	28	0	51	**135**
FY2002	30	0	44	21	0	0	0	0	0	0	0	59	6	58	**218**
FY2003	66	0	49	24	0	0	0	0	0	0	0	63	3	73	**278**
FY2004	82	0	41	17	0	0	0	0	0	28	22	77	0	70	**337**
FY2005	145	0	54	31	0	14	115	0	0	108	80	122	2	102	**773**
FY2006	131	0	3	33	0	19	87	0	0	91	63	120	1	83	**631**
FY2007	238	0	0	63	0	35	127	0	0	137	130	171	1	136	**1038**
FY2008	271	0	0	77	4	41	158	0	0	137	129	191	0	122	**1130**
FY2009	373	0	0	71	23	33	193	6	0	142	143	224	1	138	**1347**
FY2010	399	0	0	70	31	39	179	12	0	150	155	239	0	142	**1416**
FY2011	440	7	0	102	79	68	201	34	0	148	183	255	0	177	**1694**
FY2012	599	24	0	121	122	92	283	20	3	157	231	323	1	248	**2224**
FY2013	689	85	0	106	145	113	276	12	9	132	208	293	0	217	**2285**
FY2014	48	28	0	9	22	6	26	0	1	2	22	30	0	17	**211**

Figure 21: CAVP Validated Implementation Actual Numbers

The conformance tests consist of a suite of validation tests for each approved cryptographic algorithm. These tests exercise the mathematical formulas and the algorithmic requirements detailed in the algorithm to assure that the detailed specifications are implemented correctly and completely. If the implementer deviates from or excludes any part of these instructions or requirements, the validation test will fail, indicating that the algorithm implementation does not function properly or is incomplete.

CAVP-developed validation tests are performed by accredited testing laboratories on a vendor's algorithm implementation using automated known-answer tests, which compare the result from a cryptographic operation with a specific input against the expected result. They provide a uniform way to assure that the cryptographic algorithm implementation adheres to the detailed specifications.

There are several types of validation tests, all designed to satisfy the testing requirements of the cryptographic algorithms and their specifications. These include, but are not limited to, Known-Answer Tests, Monte Carlo Tests, and Multi-Block Message Tests. The Known-Answer Tests are designed to examine the individual components of the algorithm by supplying known values to the variables and verifying the expected result. The Monte Carlo Test is designed to exercise the entire IUT. This test is designed to detect the presence of implementation flaws that are not detected with the controlled input of the Known-Answer Tests. The types of implementation flaws detected by this validation test include pointer problems, insufficient allocation of space, improper error handling, and incorrect behavior of the IUT. The Multi-Block Message Test (MMT) is designed to test the ability of the implementation to process multi-block messages, which require the chaining of information from one block to the next.

During the last few years, CSD has expanded its publications beyond only an algorithm's specification into how an algorithm should be used. Many of these requirements are outside the scope of the algorithm boundary and therefore cannot be tested at the algorithm level by the CAVP. Some of the requirements are within the scope of the CMVP while others are outside the scope of both the CAVP and the CMVP. In the case where the requirement is outside the scope of the CAVP and the CMVP, the fulfillment of the requirements is the responsibility of entities using, installing, or configuring applications or protocols that use the cryptographic algorithms. For example, depending on the design of a cryptographic module, it may not be possible for the module to determine whether a specific key is used for multiple purposes, a situation that is strongly discouraged.

The CAVP currently has algorithm validation testing for the following cryptographic algorithms:

Cryptographic Algorithm/Component	Special Publication or FIPS
Triple Data Encryption Standard (TDES)	SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, and SP 800-38A, *Recommendation for Block Cipher Modes of Operation–Methods and Techniques*
Advanced Encryption Standard (AES)	FIPS 197, *Advanced Encryption Standard*, and SP 800-38A
Digital Signature Standard (DSS)	FIPS 186-2, *Digital Signature Standard (DSS), with change notice 1*, dated October 5, 2001
	FIPS 186-4, *Digital Signature Standard (DSS)*, dated July 2013
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-2, *Digital Signature Standard (DSS), with change notice 1*, dated October 5, 2001 and ANSI X9.62
	FIPS 186-4, *Digital Signature Standard (DSS)*, dated July 2013 and ANSI X9.62
RSA algorithm	ANSI X9.31 and Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002
	FIPS 186-4, *Digital Signature Standard (DSS)*, dated July 2013 and ANSI X9.31 and Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002
Hashing algorithms SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256	FIPS 180-4, *Secure Hash Standard (SHS)*, dated March 2012
Random number generator (RNG) algorithms	FIPS 186-2 Appendix 3.1 and 3.2; ANSI X9.62 Appendix A.4
Deterministic Random Bit Generators (DRBG)	SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*
Counter with Cipher Block Chaining-Message Authentication Code (CCM) mode	SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*
Cipher-based Message Authentication Code (CMAC) Mode for Authentication	SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*

Galois/Counter Mode (GCM) GMAC Mode of Operation	SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, dated November 2007
XTS Mode of Operation	SP800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*, dated January 2010
Key Agreement Schemes and Key Confirmation	SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, dated March 2007
All of SP 800-56A except KDF	SP 800-56A All sections except Section 5.8 Key Derivation Functions for Key Agreement Schemes
SP 800-56A Section 5.7.1.2 ECC CDH function	SP 800-56A Section 5.7.1.2 Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECC CDH) Primitive Testing
Key-Based Key Derivation functions (KBKDF)	SP 800-108, *Recommendation for Key Derivation using Pseudorandom Functions*, dated October 2009
Application-Specific Key Derivation functions (ASKDF) (includes KDFs used by IKEv1, IKEv2, TLS, ANS X9.63-2001, SSH, SRTP, SNMP, and TPM)	SP 800-135 (Revision 1) *Recommendation for Existing Application Specific key Derivation Functions,* dated December 2011
Component test – ECDSA Signature Generation of hash value (This component test verifies the signing of a hash-sized input. It does not verify the hashing of the original message to be signed.)	FIPS 186-4, *Digital Signature Standard (DSS)*, dated July 2013 and ANSI X9.62
Component test – RSA PKCS#1 1.5 Signature Generation of encoded message EM (This component test verifies the signing of an EM. It does not verify the formatting of the EM.)	FIPS 186-4, *Digital Signature Standard (DSS)*, dated July 2013 and Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002
Component test – RSA PKCS#1 PSS Signature Generation of encoded message EM (This component test verifies the RSASP1 function.)	SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, August 2009, Section 7.1.2

In FY 2014, the CAVP expects to add algorithm validation testing for:

- SP 800-56C, *Recommendation for Key Derivation through Extraction-then-Expansion*, November 2011
- SP 800-132, *Recommendation for Password-Based Key Derivation Part 1: Storage Applications*, December 2010
- SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012
- SP 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013

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

Contacts:

Ms. Sharon Keller
(301) 975-2910
sharon.keller@nist.gov

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

ISO Standardization of Security Requirements for Cryptographic Modules

CSD has contributed to the activities of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), which issued ISO/IEC 19790, *Security Requirements for Cryptographic Modules*, on March 1, 2006, and ISO/IEC 24759, *Test Requirements for Cryptographic Modules*, on July 1, 2008. These efforts bring consistent testing of cryptographic modules to the global community.

ISO/IEC JTC 1/SC 27 WG 3 completed and published the revisions of both ISO/IEC 19790 and ISO/IEC 24759, for which Randall J. Easter of CSD is the editor. The revision of ISO/IEC 19790 was published August 15, 2012. ISO/IEC 19790:2012 was also adopted by the American National Standards Institute (ANSI). The revision of ISO/IEC 24759 was published January 31, 2014.

CSD's Randall J. Easter is the editor for three ISO/IEC documents. Work is nearing completion on the Technical Report document, ISO/IEC 30104 "*Physical Security Attacks, Mitigation Techniques and Security Requirements.*" A final draft of ISO/IEC 30104 was completed in December 2013 and circulated for national body comment.

Work is progressing on ISO/IEC 17825 "*Testing methods for the mitigation of non-invasive attack classes against cryptographic modules.*" The first committee draft of ISO/IEC 17825 was completed in December 2013 and circulated for

national body comment.

Work is progressing on a new standard document, ISO/IEC 18367 "*Cryptographic algorithms and security mechanisms conformance testing.*" The third working draft of ISO/IEC 18367 was completed in December 2013 and circulated for national body comment.

National body comments for the above four documents will be addressed at the 47th SC 27 WG 3 meeting to be held in Incheon, Korea, in October 2013.

CSD's contributions to the development of these international standards create a strong foundation for the adoption of and migration from currently used national standards. In particular, this adoption will promote the international harmonization for the implementation and testing of cryptographic algorithms and modules while accommodating individual country preferences in the choice of approved security functions.

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

Contact:

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

Cryptographic System Validation

Current validation programs focus on providing a known level of assurance for cryptographic algorithms and modules. These are used within the context of a larger system to provide cryptographic services as a method of protecting the data within the system. As information systems continue to become more complex, the methods used to implement cryptographic services have also increased in complexity. Problems with the use of cryptography are often introduced through the interaction of cryptographic components with the operating environment. This program seeks to specify how cryptographic components are used as part of a defined cryptographic system to solve problems with a measureable level of assurance, and to introduce automated methods of quantifying the level of assurance.

This program will begin the research required to define a reference cryptographic systems architecture and example use cases where cryptographic systems are built from known cryptographic components that cooperate through trust relationships to provide a measureable level of assurance. The architecture should begin at the lowest level with a hardware based root of trust, and each cryptographic component should be added in successive layers to provide assurance in a systematic way. This should allow the development of tests that would measure the correct implementation of cryptographic components as part of a larger system.

This program will perform research and experimentation in applicable technologies and techniques that will enable the efficient testing of the cryptographic capabilities of each layer, and continuous monitoring capabilities of each cryptographic component, providing the necessary interfaces to establish trust relationships with other cryptographic components. Techniques could include such items as:

- Embedding SCAP like data elements and standard interfaces to query those data elements during design and implementation of cryptographic components that would enable automated testing capabilities;
- Using cryptographic techniques to embed values into the module that would increase the verifiability and assurance that the module provides; and
- Using industry-based secure development techniques to increase the level of trust inherent in software modules starting with design and implementation.

Research into this area of cryptographic system validation holds the promise of automating the validation of all cryptographic components, providing a higher assurance with less manual effort by using SCAP-based ideas to embed data elements that instrument the test harnesses used to validate cryptographic systems. This would also provide the instrumentation that could be leveraged to enable a greater level of situational awareness and security measurement, and potentially to enable continuous monitoring of cryptographic systems.

Contact:

Mr. Michael Cooper
(301) 975-8077
michael.cooper@nist.gov

Technical Security Metrics

Security Risk Analysis of Enterprise Networks Using Attack Graphs

Protection of computer networks from malicious intrusions is critical to the economy and security of the nation. Vulnerabilities are regularly discovered in software applications, which are exploited to stage cyber attacks. System administrators need objective metrics to guide and justify decision making as they manage the security risk of enterprise networks. The objective of this research is to develop a standard model for security

risk analysis of computer networks. A standard model will enable us to answer questions such as "Are we more secure now than yesterday?" or "How does the security of one network configuration compare with another one?" Also, having a standard model to measure network security will allow users, vendors, and researchers to evaluate methodologies and products for network security in a coherent and consistent manner.

CSD has approached the challenge of network security analysis by capturing vulnerability interdependencies and measuring security based on how real attackers have penetrated networks. CSD's methodology for security risk analysis is based on attack graphs. CSD analyzes attack paths through a network, providing a probabilistic metric of the overall system risk. Through this metric, CSD analyzes trade-offs between security costs and security benefits.

Computer systems are vulnerable to both known and zero day attacks. Handling zero day vulnerabilities is inherently difficult due to their unpredictable nature. In FY 2013, CSD attempted to assess the risk of unknown attack patterns. CSD developed a new model "*k*-zero day safety" for zero day attacks. Existing algorithms for computing this metric are not scalable as they assume that a complete zero day attack graph has been generated. CSD has proposed a set of polynomial time algorithms for estimating *k*-zero day safety. CSD has authored a paper, "An Efficient Approach to Assessing the Risk of Zero-Day Vulnerabilities," that received the Best Paper Award at the tenth International Conference on Security and Cryptography (SECRYPT 2013), in Reykjavik, Iceland.

In FY 2014, CSD plans to apply attack graphs to study the effect of diversity for network defense. CSD also plans to publish the results as a NIST report and as white papers in conferences and journals.

http://csrc.nist.gov/groups/SNS/security-riskanalysis-enterprise-networks/

Contact:

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

Algorithms for Intrusion Measurement

Figure 22: Algorithms for Intrusion Measurement

The Algorithms for Intrusion Measurement (AIM) project, newly formed in FY 2013, furthers measurement science in the area of algorithms used in the field of intrusion detection. The team focuses on both new detection metrics and measurements of scalability (more formally algorithmic complexity). This analysis is applied to different phases of the detection lifecycle to include pre-emptive vulnerability analysis, initial attack detection, alert impact, alert aggregation/correlation, and compact log storage. In performing this work, the AIM project seeks to enhance our nation's ability to defend itself from network-borne attacks. Much of this scientific research is conducted in partnership with the Army Research Laboratory (ARL). ARL's participation helps focus the work on solving immediate critical problems facing U.S. Government networks. However, research solutions are made publicly available and are designed to be generally applicable to as many environments as possible.

In its first year, the AIM project initiated research in each stage of the detection lifecycle with a focus on graph theoretic approaches; it has already obtained several major results. For example, the project has advanced the state of the art in network scan detection, discovering and then thwarting circumvention attacks against a highly cited scan detection algorithm. A paper describing this approach, "Limitations to Threshold Random Walk Scan Detection and Mitigating Enhancements," was published at the First IEEE Conference on Communications and Network Security. Additionally, the project developed a hypergraph-based algorithm to use Hamming distance to aggregate security alert logs more than an order of magnitude faster than the previous state of the art, while providing enhanced aggregation.

In FY 2014, the AIM project will continue its scan detection work and publish its work on log aggregation. It will continue emerging research on log file compression and alert impact analysis. Newly initiated work will include investigation of

known-vulnerability based metrics for comparing the attack resistance of different networks or a single network over time.

Contacts:

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

Mr. Mark (Lee) Badger
(301) 975-3176
mark.badger@nist.gov

Automated Combinatorial Testing

Software developers often encounter failures that result from an unexpected interaction between components. NIST research has shown that most failures are triggered by one or two parameters and progressively fewer by three, four, or more parameters (see graph below), a relationship that is called the Interaction Rule. These results have important implications for testing. If all faults in a system can be triggered by a combination of *n* or fewer parameters, then testing all *n*-way combinations of parameters can provide very strong fault detection efficiency. These methods are being applied to software and hardware testing for reliability, safety, and security. CSD's focus is on empirical results and real-world problems.

Project highlights for FY 2013 included completion of a two-year Cooperative Research and Development Agreement (CRADA) with Lockheed Martin Corporation, showing approximately 20% reduction in software test development cost across a variety of projects; publication of the first textbook on combinatorial testing; release of an advanced tool for measuring combinatorial coverage of test sets (jointly with Centro Nacional de Metrología, Mexico); cooperative work with the National Aeronautics and Space Administration (NASA) Independent Verification and Validation (IV&V) Facility analyzing combinatorial coverage measurement for IV&V of space systems; lectures at conferences and research labs; and leading (jointly with IBM personnel) the IEEE Second International Conference on Combinatorial Testing, held with the International Conference on Software Testing.

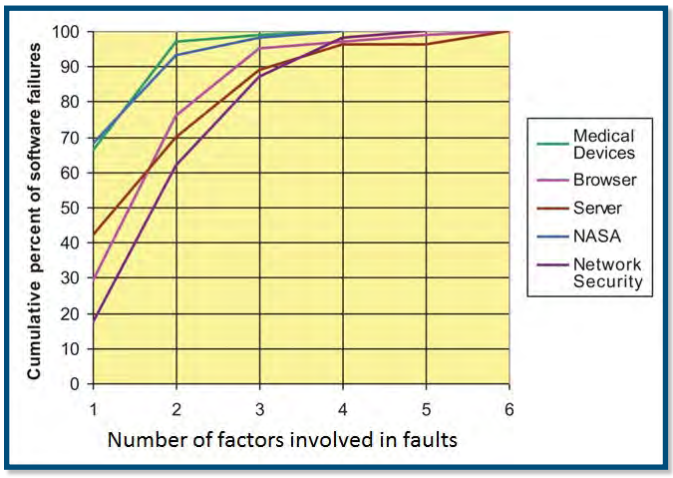


Figure 23: Interaction Rule

Technology transfer activities included publication of several technical papers; participation in the Maryland Technology Development Corporation (TEDCO) Technology Transfer Workshop; presentation of results of the work with Lockheed Martin; release of enhanced covering array, test prioritization, and fault location tools; plus seminars and lectures at several conferences, universities, and federal agencies.

Plans for FY 2014 include a second phase of a project with the NASA IV&V Facility to investigate integration of combinatorial coverage measurement methods in NASA IV&V practices; development of new methods and tools for very large covering arrays (hundreds of variables); lectures at conferences and research labs; and guiding development of a combinatorial software test development environment by graduate students at Carnegie Mellon University which will incorporate NIST software.

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

Contacts:

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

Dr. Raghu Kacker
(301) 975-2109
raghu.kacker@nist.gov

Hardware Roots of Trust

Modern computing devices consist of various hardware, firmware, and software components at multiple layers of abstraction. Many security and protection mechanisms are currently rooted in software that, along with all underlying components, must be trustworthy. A vulnerability in any of those components could compromise the trustworthiness of the security mechanisms that rely upon those components. Stronger security assurances may be possible by grounding security mechanisms in roots of trust.

Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.

A focus area for CSD's roots of trust research in FY 2013 was security for mobile devices. CSD worked with government and industry partners on guidelines on hardware-rooted security features in mobile devices. These guidelines focus on device

integrity, isolation, and protected storage features that are supported by roots of trust. Draft SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices*, was released for public comment in October 2012.

In FY 2014, CSD will release a revised draft of SP 800-164, based on the feedback received during the public comment period. In addition, CSD is working with the National Cybersecurity Center of Excellence (NCCoE) to encourage the adoption of stronger security technologies in mobile devices. Using draft SP 800-164 as a basis for an NCCoE building block activity, CSD and the NCCoE will invite mobile device, operating system, management software vendors, and application developers to study, demonstrate, and document how to use hardware-backed security solutions.

In FY 2013, CSD continued its work to protect fundamental system firmware, commonly known as Basic Input/Output System (BIOS). CSD has been working with key members of the computer industry on the use of roots of trust to improve the security of BIOS.

CSD will continue its efforts to secure BIOS and other critical firmware in FY 2014 and will finalize a Special Publication covering BIOS protections for server-class systems. CSD will also release an updated draft of SP 800-155, *BIOS Integrity Measurement Guidelines*, which will include additional guidelines for server-class systems and other boot firmware. In order to encourage the continued adoption of BIOS protections, CSD also plans to submit SP 800-147, *BIOS Protection Guidelines*, to ISO for standardization.

Contact:

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

Honors and Awards

Mr. Richard Kissel
U.S. Department of Commerce Bronze Medal

Mr. Kissel received a U.S. Department of Commerce Bronze Medal for raising small and medium-sized business (SMB) awareness of information security threats, vulnerabilities, and safeguards through implementation of NIST's SMB information security outreach program. As the program lead, Mr. Kissel worked collaboratively with the Small Business Administration and the FBI's InfraGard program to conduct information security training workshops for small businesses with a focus on the tools and techniques these businesses can apply directly. By empowering SMBs, which represent over 95% of all U.S. businesses, to better protect their information, the nation's overall information infrastructure is strengthened to enhance innovation, competitiveness, and economic security.

Mr. Jeremy Grant
Federal 100 Award

Jeremy Grant is a senior executive advisor for identity management at NIST. He leads the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office, which is working to foster a vibrant marketplace of identity solutions—provided by entities both private and public—that would enhance the security, convenience, and privacy of online transactions. *Federal Computer Week* included the following description in Mr. Grant's award: "Through his ability to facilitate dialogue and inspire action among NSTIC's complex and diverse community of stakeholders, he has helped foster NSTIC's vision and principles to produce marketable solutions and advanced innovation." Further details about the award are available at http://fcw.com/articles/2013/03/20/grant-jeremy.aspx.

FCW Federal 100 Awards

Three members of the Information Technology Laboratory and the Computer Security Division were named to the 2013 list of the top 100 government, industry and academic leaders in the Federal Government IT community. The award recognizes individuals who are making a difference in the way technology has transformed their agency or accelerated their agency's mission.

The Federal 100 Awards are sponsored by *Federal Computer Week*. Recipients are chosen by a panel of government and industry leaders. They were formally honored at a gala on March 20, 2013.

Mr. Jon Boyens
Federal 100 Award

Jon Boyens is a senior information technology security specialist in the Computer Security Division. As lead for NIST's Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) project, he identifies and evaluates technologies, tools, techniques, practices, and standards useful in managing risk to the ICT supply chain and co-leads the U.S. Government's efforts to develop ICT SCRM lifecycle processes and standards. *Federal Computer Week* included the following description in Mr. Boyens' award: "He led an integrated team that developed a set of standardized, repeatable practices to help federal agencies manage risks to their information and communications technology supply chain in the face of rapid technological evolution." Further details about the award are available at: http://fcw.com/articles/2013/03/20/boyens-jon.aspx.

Mr. Adam Sedgewick
Federal 100 Award

Senior Information Technology Policy Advisor Adam Sedgewick coordinates information technology projects with NIST's critical partners in the federal arena, including the Chief Information Officers' (CIO) Council, the Office of Management and Budget (OMB) and the National Security Staff. *Federal Computer Week* included the following description in Mr. Sedgewick's award: "[He] focused on government-wide impact while offering process improvements for the council's internal operations. He added tremendous substantive expertise gleaned from his experience as a cybersecurity and IT policy analyst on Capitol Hill. As senior IT policy adviser at NIST, he continues to shape the government-wide dialogue on cybersecurity reform." Further details about the award are available at http://fcw.com/articles/2013/03/20/sedgewick-adam.aspx.

Mr. Joshua Franklin & Ms. Kelley Dempsey

Government Information Security Leadership Award (GISLA)

Josh Franklin and Kelley Dempsey won the (ISC)² Government Information Security Leadership Award (GISLA) in the Process/ Policy Improvement category for their work on the Federal Mobile Security Baseline and the Mobile Computing Decision Framework. According to (ISC)², the award in this category is given to "An individual or team of senior-level U.S. federal government personnel…whose contribution to the development or implementation of any information security policy or process has significantly improved the security posture of a federal agency, department or government-wide within the last 12 months." Source: https://www.isc2.org/gisla/Default.aspx.

Dr. Ron Ross

Inaugural Lynn F. McNulty Information Security Leadership Tribute Award

National Institute of Standards and Technology (NIST) Fellow Ron Ross has been awarded the inaugural Lynn F. McNulty Tribute U.S. Government Information Security Leadership Award. The (ISC)² U.S. Government Advisory Board for Cyber Security (GABCS) announced the award on October 29, 2013, in recognition of Ross's "key role in establishing cybersecurity requirements for federal agencies for decades."

The award was established last year after the death of (ISC)² Fellow and IT security evangelist Lynn F. McNulty, CISSP. McNulty was considered by those in the community as the "pioneer" of government information security. The Tribute Award recognizes a member of the U.S. federal information security community who upholds McNulty's legacy as a visionary and innovator through outstanding service and commitment.

Ross worked with McNulty during the 1990s when McNulty was NIST's Associate Director of Computer Security.

"Ron's insight and leadership in producing a library of guidance publications over the past decade has greatly contributed to the advancement of information security in government and around the world," said Peter Gouldmann, CISSP, director of information risk programs, Office of Information Assurance, U.S. Department of State, and member, (ISC)² GABCS. "His highly collaborative approach, incorporating government and industry, has resulted in products that are being adopted and adapted for use on national security systems, transcending the unclassified and classified systems landscape."

Sources: https://www.isc2.org/GISLA-Lynn-McNulty-Award/defalt.aspx
http://www.nist.gov/itl/csd/ross-110513.cfm

This page is intentionally left blank.

FY 2013 Computer Security Division Publications

The Computer Security Division uses multiple NIST Technical Series to promulgate security standards, guidelines, recommendations, research, and additional background material. Those series include Federal Information Processing Standards (FIPS), NIST Special Publications (SPs), NIST Interagency or Internal Reports (NISTIRs) and Information Technology Laboratory (ITL) Bulletins. Links to these publications are available at http://csrc.nist.gov/publications.

Additionally, each year CSD staff authors numerous additional publications, including journal articles, conference papers, and other papers that are widely disseminated. They range from basic research to high-level summaries of CSD activities.

NIST Technical Series Publications – FIPS, Special Publications, NISTIRs, and ITL Bulletins

Below are lists of NIST Technical Series publications that CSD released as draft documents or as final publications during FY 2013 (from October 1, 2012 to September 30, 2013). Following the lists are abstracts and contact information for each publication.

DRAFT PUBLICATIONS		
Type & Number	**Publication Title**	**Draft Released Date**
Federal Information Processing Standards (FIPS)		
No draft FIPS were released in FY 2013.		

Special Publications (SPs)		
SP 800-164	*Guidelines on Hardware-Rooted Security in Mobile Devices*	*October 2012*
SP 800-162	*Guide to Attribute Based Access Control (ABAC) Definition and Considerations*	*April 2013*
SP 800-161	*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*	*August 2013*
SP 800-101 Revision 1	*Guidelines on Mobile Device Forensics*	*September 2013*
SP 800-90 Series (A Revision 1, B, and C)	*Random Bit Generators* ***A Revision 1:*** *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* ***B:*** *Recommendation for the Entropy Sources Used for Random Bit Generation* ***C:*** *Recommendation for Random Bit Generator (RBG) Constructions*	*September 2013*
SP 800-78-4	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification*	*May 2013*
SP 800-73-4	*Interfaces for Personal Identity Verification (3 Parts)* ***Part 1****- PIV Card Application Namespace, Data Model and Representation* ***Part 2****- PIV Card Application Card Command Interface* ***Part 3****- PIV Client Application Programming Interface*	*May 2013*
SP 800-63-2	*Electronic Authentication Guideline*	*February 2012*
SP 800-53 Revision 4	*Security and Privacy Controls for Federal Information Systems and Organizations*	*February 2013*
SP 800-52 Revision 1	*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*	*September 2013*
SP 800-38 G	*Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*	*July 2013*

NIST Interagency Reports (NISTIRs)		
NISTIR 7946	*CVSS Implementation Guidance*	*September 2013*
NISTIR 7924	*Reference Certificate Policy*	*April 2013*
NISTIR 7904	*Trusted Geolocation in the Cloud: Proof of Concept Implementation*	*December 2012*
NISTIR 7298 Revision 2	*Glossary of Key Information Security Terms*	*December 2012*

Final (Approved) Publications

Federal Information Processing Standards (FIPS)

Document Number	Publication Title	Publication Date
FIPS 201-2	*Personal Identity Verification (PIV) of Federal Employees and Contractors*	*August 2013*
FIPS 186-4	*Digital Signature Standard (DSS)*	*July 2013*

Special Publications (SPs)

Document Number	Publication Title	Publication Date
SP 800-165	*Computer Security Division 2012 Annual Report*	*June 2013*
SP 800-133	*Recommendation for Cryptographic Key Generation*	*December 2012*
SP 800-130	*A Framework for Designing Cryptographic Key Management Systems*	*August 2013*
SP 800-124 Revision 1	*Guidelines for Managing the Security of Mobile Devices in the Enterprise*	*June 2013*
SP 800-83 Revision 1	*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*	*July 2013*
SP 800-82 Revision 1	*Guide to Industrial Control Systems (ICS) Security*	*May 2013*
SP 800-81-2	*Secure Domain Name System (DNS) Deployment Guide*	*September 2013*
SP 800-76-2	*Biometric Specifications for Personal Identity Verification*	*July 2013*
SP 800-63-2	*Electronic Authentication Guideline*	*August 2013*
SP 800-56A Revision 2	*Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*	*May 2013*
SP 800-53 Revision 4	*Security and Privacy Controls for Federal Information Systems and Organizations*	*April 2013*
SP 800-40 Revision 3	*Guide to Enterprise Patch Management Technologies*	*July 2013*
SP 800-38F	*Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*	*December 2012*

NIST Interagency Reports (NISTIRs)

Document Number	Publication Title	Publication Date
NISTIR 7957	*Conformance Test Architecture and Test Suite for ANSI/NIST-ITL 1-2011 NIEM XML Encoded Transactions*	*September 2013*
NISTIR 7956	*Cryptographic Key Management Issues & Challenges in Cloud Services*	*September 2013*
NISTIR 7933	*Requirements and Conformance Test Assertions for ANSI/NIST-ITL 1-2011 Record Type 18 - DNA Record*	*May 2013*
NISTIR 7916	*Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop, April 23-24, 2012*	*February 2013*
NISTIR 7896	*Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition*	*November 2012*
NISTIR 7878	*Combinatorial Coverage Measurement*	*October 2012*
NISTIR 7817	*A Credential Reliability and Revocation Model for Federated Identities*	*November 2012*
NISTIR 7622	*Notional Supply Chain Risk Management Practices for Federal Information Systems*	*October 2012*
NISTIR 7511 Revision 3	*Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*	*January 2013*
NISTIR 7298 Revision 2	*Glossary of Key Information Security Terms*	*May 2013*

Final (Approved) Publications *(cont.)*	
ITL Bulletins	
Release Date	**Title of Bulletin**
September 2013	*NIST Opens Draft Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, For Review and Comment (Supplemental ITL Bulletin for September 2013)*
September 2013	*ITL Publishes Guidance on Preventing and Handling Malware Incidents*
August 2013	*ITL Publishes Guidance on Enterprise Patch Management Technologies*
July 2013	*ITL Issues Guidelines for Managing the Security of Mobile Devices*
June 2013	*ITL Updates Glossary of Key Information Security Terms*
May 2013	*ITL Publishes Security and Privacy Controls for Federal Agencies*
April 2013	*Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*
March 2013	*NIST to Develop a Cybersecurity Framework to Protect Critical Infrastructure*
January 2013	*Managing Identity Requirements for Remote Users of Information Systems to Protect System Security and Information Privacy*
December 2012	*Generating Secure Cryptographic Keys: A Critical Component of Cryptographic Key Management and the Protection of Sensitive Information*
November 2012	*Practices for Managing Supply Chain Risks to Protect Federal Information Systems*
October 2012	*Conducting Information Security-Related Risk Assessments: Updated Guidelines for Comprehensive Risk Management Programs*

Abstracts of NIST Technical Series Publications Released in FY 2013

The following sections provide abstracts and contact information for the draft and final FIPS, NIST SPs, and security-related NISTIRs listed in the previous section. These publications are available at http://csrc.nist.gov/publications.

Federal Information Processing Standards (FIPS)

FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

This standard specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and logical access to government information systems. The standard contains the minimum requirements for a federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive-12 (HSPD-12), including identity proofing, registration, and issuance. The standard also provides detailed specifications that will support technical interoperability among PIV systems of federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card.

Contacts:

Ms. Hildegard Ferraiolo
hildegard.ferraiolo@nist.gov

Dr. David Cooper
david.cooper@nist.gov

Mr. Salvatore Francomacaro
salvatore.francomacaro@nist.gov

Mr. Ketan Mehta
ketan.mehta@nist.gov

Ms. Annie Sokol
annie.sokol@nist.gov

FIPS 186-4, *Digital Signature Standard (DSS)*

This standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.

Contact:

Ms. Elaine Barker
elaine.barker@nist.gov

NIST Special Publications (SPs)

SP 800-165, *Computer Security Division 2012 Annual Report*

Title III of the E-Government Act of 2002, entitled the Federal Information Security Management Act (FISMA) of 2002, requires NIST to prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this law. The primary goal of the Computer Security Division (CSD), a component of NIST s Information Technology Laboratory (ITL), is to provide standards and technology that protects information systems against threats to the confidentiality, integrity, and availability of information and services. During FY 2013, CSD successfully responded to numerous challenges and opportunities in fulfilling that mission. Through CSD's diverse research agenda and engagement in many national priority initiatives, high-quality, cost-effective security and privacy mechanisms were developed and applied that improved information security across the Federal Government and the greater information security community. This annual report highlights the research agenda and activities in which CSD was engaged during FY 2013.

Contacts:

Mr. Patrick O'Reilly
patrick.oreilly@nist.gov

Mr. Kevin Stine
kevin.stine@nist.gov

Draft SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices*

Many mobile devices are not capable of providing strong security assurances to end users and organizations. Current mobile devices lack the hardware-based roots of trust that are increasingly built into laptops and other types of hosts. This document focuses on defining the fundamental security primitives and capabilities needed to enable more secure mobile device use. This document is intended to accelerate industry efforts to implement these primitives and capabilities. The guidelines in this document are intended to provide a baseline of security technologies that can be implemented across a wide range of mobile devices to help secure organization-issued mobile devices as well as devices brought into an organization, such as personally-owned devices used in enterprise environments (e.g., Bring Your Own Device (BYOD)).

Contacts:

Dr. Lily Chen
lily.chen@nist.gov

Mr. Joshua Franklin
joshua.franklin@nist.gov

Mr. Andrew Regenscheid
andrew.regenscheid@nist.gov

Draft SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

This document provides federal agencies with a definition of Attribute Based Access Control (ABAC). ABAC is a logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. This document also provides considerations for using ABAC to improve information sharing within organizations and between organizations while maintaining control of that information.

Contacts:

Dr. Vincent Hu
vhu@nist.gov

Mr. David Ferraiolo
david.ferraiolo@nist.gov

Mr. Rick Kuhn
rkuhn@nist.gov

Draft SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*

The Information and Communications Technology (ICT) supply chain is a complex, globally distributed system of interconnected networks that are logically long, with geographically diverse routes and multiple tiers of outsourcing. This system of networks includes organizations, people, processes, products, and services and the infrastructure supporting the system development life cycle, including research and development (R&D), design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement of an organization's ICT products (i.e., hardware and software) and services.

Today's ICT supply chains have increased complexity, diversity, and scale, while Federal Government information systems have been rapidly expanding in terms of capability and number, with an increased reliance on outsourcing and commercially available products. These trends have caused federal departments and agencies to have a lack of visibility and understanding throughout the supply chain of how the technology being acquired is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. This lack of visibility and understanding, in turn, has decreased the control federal departments and agencies have with regard to the decisions impacting the inherited risks traversing the supply chain and the ability to effectively manage those risks.

SP 800-161 provides guidance to federal departments and agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels in their organizations. SP 800-161

integrates ICT Supply Chain Risk Management (SCRM) into federal agency enterprise risk management activities by applying a multi-tiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance.

Contacts:

Mr. Jon Boyens
jon.boyens@nist.gov

Ms. Celia Paulsen
celia.paulsen@nist.gov

SP 800-133, *Recommendation for Cryptographic Key Generation*

Cryptography is often used in an information technology security environment to protect data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a cryptographic key. This Recommendation discusses the generation of the keys to be managed and used by the approved cryptographic algorithms.

Contacts:

Ms. Elaine Barker
elaine.barker@nist.gov

Dr. Allen Roginsky
allen.roginsky@nist.gov

SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*

This Framework for Designing Cryptographic Key Management Systems (CKMS) contains topics that should be considered by a CKMS designer when developing a CKMS design specification. For each topic, there are one or more documentation requirements that need to be addressed by the design specification. Thus, any CKMS that addresses each of these requirements would have a design specification that is compliant with this Framework.

Contact:

Ms. Elaine Barker
elaine.barker@nist.gov

SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*

Mobile devices, such as smart phones and tablets, typically need to support multiple security objectives: confidentiality, integrity, and availability. To achieve these objectives, mobile devices should be secured against a variety of threats. The purpose of this publication is to help organizations centrally manage the security of mobile devices. Laptops are out of the scope of this publication, as are mobile devices with minimal computing capability, such as basic cell phones. This publication provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their life cycles. The scope of this publication includes securing both organization-provided and personally-owned (bring your own device (BYOD)) mobile devices. [Supersedes SP 800-124.]

Contact:

Mr. Murugiah Souppaya
murugiah.souppaya@nist.gov

Draft SP 800-101 Revision 1, *Guidelines on Mobile Device Forensics*

Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is an evolving specialty in the field of digital forensics. This guide attempts to bridge the gap by providing an in-depth look into mobile devices and explaining technologies involved and their relationship to forensic procedures. This document covers mobile devices with features beyond simple voice communication and text messaging capabilities. This guide also discusses procedures for the validation, preservation, acquisition, examination, analysis, and reporting of digital information.

Contact:

Mr. Richard Ayers
richard.ayers@nist.gov

Draft SP 800-90 Series, *Random Bit Generators:*

Draft SP 800-90A Revision 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

This Recommendation specifies mechanisms for the generation of random bits using deterministic methods. The methods provided are based on hash functions, block cipher algorithms, or number theoretic problems.

Draft SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*

This Recommendation specifies the design principles and requirements for the entropy sources used by Random Bit Generators, and the tests for the validation of entropy sources. These entropy sources are intended to be combined with Deterministic Random Bit Generator mechanisms that are specified in SP 800-90A to construct Random Bit Generators, as specified in SP 800-90C.

Draft SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*

This Recommendation specifies constructions for the implementation of random bit generators (RBGs). An RBG may be a deterministic random bit generator (DRBG) or a non-deterministic random bit generator (NRBG). The constructed

RBGs consist of DRBG mechanisms as specified SP 800-90A and entropy sources as specified in SP 800-90B.

Contacts:

Ms. Elaine Barker
elaine.barker@nist.gov

Dr. John Kelsey
john.kelsey@nist.gov

SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. This publication provides recommendations for improving an organization's malware incident prevention measures. It also gives extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. [Supersedes SP 800-83.]

Contact:

Mr. Murugiah Souppaya
murugiah.souppaya@nist.gov

SP 800-82 Revision 1, *Guide to Industrial Control Systems (ICS) Security*

This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. [Supersedes SP 800-82.]

Contact:

Mr. Keith Stouffer
keith.stouffer@nist.gov

SP 800-81-2, *Secure Domain Name System (DNS) Deployment Guide*

The Domain Name System (DNS) is a distributed computing system that enables access to Internet resources by user-friendly domain names rather than IP addresses, by translating domain names to IP addresses and back. The DNS infrastructure is made up of computing and communication entities called Name Servers each of which contains information about a small portion of the domain name space. The domain name data provided by DNS is intended to be available to any computer located anywhere in the Internet. This document provides deployment guidelines for securing DNS within an enterprise. Because DNS data is meant to be public, preserving the confidentiality of DNS data is not a concern. The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit. This document provides extensive guidance on maintaining data integrity and performing source authentication. DNS components are often subjected to denial-of-service attacks intended to disrupt access to the resources whose domain names are handled by the attacked DNS components. This document presents guidelines for configuring DNS deployments to prevent many denial-of-service attacks that exploit vulnerabilities in various DNS components. [Supersedes SP 800-81 Revision 1.]

Contact:

Dr. Chandramouli (Mouli) Ramaswamy
mouli@nist.gov

Draft SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*

FIPS 201 defines requirements for the PIV lifecycle activities, including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS 201 also defines the structure of an identity credential that includes cryptographic keys. This document contains the technical specifications needed for the mandatory and optional cryptographic keys specified in FIPS 201, as well as the supporting infrastructure specified in FIPS 201 and the related SP 800-73, *Interfaces for Personal Identity Verification*, and SP 800-76, *Biometric Data Specification for Personal Identity Verification*, that rely on cryptographic functions.

Contacts:

Ms. Hildegard (Hildy) Ferraiolo
hildegard.ferraiolo@nist.gov

Dr. David Cooper
david.cooper@nist.gov

Mr. William Burr
william.burr@nist.gov

Mr. Tim Polk
william.polk@nist.gov

SP 800-76-2, *Biometric Specifications for Personal Identity Verification*

Homeland Security Presidential Directive HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, called for new standards to be adopted governing interoperable use of identity credentials to allow physical and logical access to Federal Government locations and systems. FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, was developed to define procedures and specifications for issuance and use of an interoperable

identity credential. This document, SP 800-76, is a companion document to FIPS 201. It describes technical acquisition and formatting specifications for the PIV system, including the PIV Card itself. It also establishes minimum accuracy specifications for deployed biometric authentication processes. The approach is to enumerate procedures and formats for collection and preparation of fingerprint, iris, and facial data, and to restrict values and practices included generically in published biometric standards. The primary design objective behind these particular specifications is to enable high performance and universal interoperability. The introduction of iris and face specifications into the current edition adds alternative modalities for biometric authentication and extends coverage to persons for whom fingerprinting is problematic. The addition of on-card comparison offers an alternative to PIN-mediated card activation as well as an additional authentication method.

Contacts:

Dr. Chandramouli (Mouli) Ramaswamy
mouli@nist.gov

Mr. Patrick Grother
patrick.grother@nist.gov

Draft SP 800-73-4, *Interfaces for Personal Identity Verification (3 Parts)*

Part 1- PIV Card Application Namespace, Data Model and Representation

Part 2- PIV Card Application Card Command Interface

Part 3- PIV Client Application Programming Interface

FIPS 201 defines the requirements and characteristics of a government-wide interoperable identity credential. FIPS 201 also specifies that this identity credential must be stored on a smart card. This document, SP 800-73, contains the technical specifications to interface with the smart card to retrieve and use the PIV identity credentials. The specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying a PIV data model, card edge interface, and application-programming interface. Moreover, this document enumerates requirements where the international integrated circuit card standards [ISO7816] include options and branches. The specifications go further by constraining implementers' interpretations of the normative standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.

Contacts:

Dr. Chandramouli (Mouli) Ramaswamy
mouli@nist.gov

Dr. David Cooper
david.cooper@nist.go

Ms. Hildegard (Hildy) Ferraiolo
hildegard.ferraiolo@nist.gov

Mr. Salvatore Francomacaro
salvatore.francomacaro@nist.gov

Mr. Ketan Mehta
ketan.mehta@nist.gov

SP 800-63-2, *Electronic Authentication Guideline*

This recommendation provides technical guidelines for federal agencies implementing electronic authentication and is not intended to constrain the development or use of standards outside of this purpose. The recommendation covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions. [Supersedes SP 800-63-1.]

Contacts:

Dr. Lily Chen
lily.chen@nist.gov

Mr. William Burr
william.burr@nist.gov

SP 800-56A Revision 2, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*

This recommendation specifies key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-Qu-Vanstone (MQV) key establishment schemes. [Supersedes SP 800-56A.]

Contacts:

Ms. Elaine Barker
elaine.barker@nist.gov

Dr. Lily Chen
lily.chen@nist.gov

Dr. Allen Roginsky
allen.roginsky@nist.gov

SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors (both intentional and unintentional). The security and privacy controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the Federal Government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of

security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and assurance helps to ensure that information technology component products and the information systems built from those products using sound system and security engineering principles are sufficiently trustworthy. [Supersedes SP 800-53 Revision 3.]

Contacts:

NIST FISMA Team
sec-cert@nist.gov

Dr. Ron Ross
rross@nist.gov

Mr. Arnold Johnson

Ms. Kelley Dempsey
kelley.dempsey@nist.gov

Draft SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*

Transport Layer Security (TLS) provides mechanisms to protect sensitive data during electronic dissemination across the Internet. This Special Publication provides guidance to the selection and configuration of TLS protocol implementations while making effective use of FIPS and NIST-recommended cryptographic algorithms, and requires that TLS 1.1 configured with FIPS-based cipher suites as the minimum appropriate secure transport protocol and recommends that agencies develop migration plans to TLS 1.2 by January 1, 2015. This publication also identifies TLS extensions for which mandatory support must be provided and other recommended extensions.

Contacts:

Ms. Kerry McKay
kerry.mckay@nist.gov

Mr. William (Tim) Polk
william.polk@nist.gov

SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. There are several challenges that complicate patch management. If organizations do not overcome these challenges, they will be unable to patch systems effectively and efficiently, leading to easily preventable compromises. This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. It provides an overview of enterprise patch management technologies and it also briefly discusses metrics for measuring the technologies effectiveness and for comparing the relative importance of patches. [Supersedes SP 800-40 Version 2.0.]

Contact:

Mr. Murugiah Souppaya
murugiah.souppaya@nist.gov

SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*

This publication describes cryptographic methods that are approved for key wrapping, i.e., the protection of the confidentiality and integrity of cryptographic keys. In addition to describing existing methods, this publication specifies two new, deterministic authenticated-encryption modes of operation of the Advanced Encryption Standard (AES) algorithm: the AES Key Wrap (KW) mode and the AES Key Wrap With Padding (KWP) mode. An analogous mode with the Triple Data Encryption Algorithm (TDEA) as the underlying block cipher, called TKW, is also specified, to support legacy applications.

Contact:

Dr. Morris Dworkin
morris.dworkin@nist.gov

Draft SP 800-38 G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*

This recommendation specifies three methods for format-preserving encryption, called FF1, FF2, and FF3. Each of these methods is a mode of operation of the AES algorithm, which is used to construct a round function within the Feistel structure for encryption.

Contact:

Dr. Morris Dworkin
morris.dworkin@nist.gov

NIST Interagency Reports (NISTIRs)

NISTIR 7957, *Conformance Test Architecture and Test Suite for ANSI/NIST-ITL 1-2011 NIEM XML Encoded Transactions*

The latest version of the ANSI/NIST-ITL standard was published in November 2011 (AN-2011). In addition to specifying Record Types in traditional encoding, the standard includes the specification of National Information Exchange Model (NIEM) Extensible Markup Language (XML) encoding and an associated schema. The Computer Security Division of NIST/ITL developed a Conformance Test Architecture (CTA) and Test Suite (CTS) called "BioCTS for AN-2011 NIEM XML" designed to test implementations of AN-2011 NIEM XML encoded transactions. Validating the XML files to a schema may indicate that the contained data is formatted correctly and individual values are within allowable ranges, assuming that the requirements for

that data have been documented in the schema file. However, schemas are not designed to test the internal consistency of implementations (i.e., testing for a relationship between two elements or structures within a transaction). These shortcomings of XML schema files for use in conformance testing necessitate that schemas be used only as a component of a complete testing solution. This complete solution (the test tool) ensures test coverage of requirements through a combination of schema validation and conformance tests of the data in the XML files. This document discusses the test software design including the XML Data Structures used and Classes implemented. It addresses the testing phases and the format of the test results; as well as the user interface and key usability features implemented in this version of the test tool. Details are provided on a modified schema that was required to be used in the tool in order to fully perform tests for all the requirements specified in the AN-2011 standard. Future development steps, including support for the new version of the ANSI/NIST-ITL standard under development, are also discussed.

Contacts:

Mr. Fernando Podio
fernando.podio@nist.gov

Mr. Dylan Yaga
dylan.yaga@nist.gov

Mr. Christofer McGinnis
christofer.mcginnis@nist.gov

NISTIR 7956, *Cryptographic Key Management Issues & Challenges in Cloud Services*

To interact with various services in the cloud and to store the data generated/processed by those services, several security capabilities are required. The publication considers a core set of features in the three common cloud services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The report identifies a set of security capabilities needed to exercise those features and the cryptographic operations they entail. An analysis of the common state of practice of the cryptographic operations that provide those security capabilities reveals that the management of cryptographic keys takes on an additional complexity in cloud environments compared to enterprise IT environments due to: (a) difference in ownership (between cloud Consumers and cloud Providers) and (b) control of infrastructures on which both the Key Management System (KMS) and protected resources are located. This document identifies the cryptographic key management challenges in the context of architectural solutions that are commonly deployed to perform those cryptographic operations.

Contacts:

Dr. Chandramouli (Mouli) Ramaswamy
mouli@nist.gov

Dr. Michaela Iorga
michaela.iorga@nist.gov

Draft NISTIR 7946, *CVSS Implementation Guidance*

This Interagency Report provides guidance to individuals scoring IT vulnerabilities using the Common Vulnerability Scoring System (CVSS) Version 2.0 scoring metrics. The guidance in this document is the result of applying the CVSS specification to score over 50,000 vulnerabilities analyzed by the National Vulnerability Database (NVD). An overview of the CVSS base metrics is first presented, followed by guidance for difficult and/or unique scoring situations. To assist vulnerability analysts, common keywords and phrases are identified and accompanied by suggested scores for particular types of software vulnerabilities. The report includes a collection of scored IT vulnerabilities from the NVD, alongside a justification for the provided score. Finally, this report contains a description of the NVD's vulnerability scoring process.

Contacts:

Mr. Joshua Franklin
joshua.franklin@nist.gov

Mr. Harold Booth
harold.booth@nist.gov

NISTIR 7933, *Requirements and Conformance Test Assertions for ANSI/NIST-ITL 1-2011 Record Type 18 - DNA Record*

CSD, in NIST's Information Technology Laboratory (NIST/ITL), develops conformance test architectures (CTA) and test suites (CTS) to support users that require conformance to selected biometric standards. Product developers as well as testing laboratories can also benefit from the use of these tools. This project supports the possible establishment of conformity assessment programs for biometrics and also supports NIST/ITL's Forensic Science Program by making conformance testing tools available that provide developers, users, and purchasers with increased levels of confidence in product quality and increases the probability of successful interoperability of biometrics and forensic data. One of the test tools is a CTA/CTS designed to test implementations of ANSI/NIST-ITL 1-2011 (AN-2011) *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information,* for selected Record Types based on 1,200 test assertions previously developed. As part of the process associated with the extension of the first version of BioCTS for AN-2011, NIST/ITL CSD's staff identified over 200 test assertions necessary to meet the conformance requirements for the AN-2011 Record Type 18- DNA Record. These test assertions are documented using the format specified in SP 500-295, *Conformance Testing Methodology for ANSI/NIST-ITL 1- 2011, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (Release 1.0).*

Contacts:

Mr. Fernando Podio
fernando.podio@nist.gov

Mr. Dylan Yaga
dylan.yaga@nist.gov

Mr. Christofer McGinnis
christofer.mcginnis@nist.gov

Draft NISTIR 7924, *Reference Certificate Policy*

The purpose of this document is to identify a baseline set of security controls and practices to support the secure issuance of certificates. This baseline was developed with publicly-trusted Certificate Authorities (CA) in mind. These CAs, who issue the certificates used to secure websites and sign software, play a particularly important role online. This document is formatted as a Reference Certificate Policy (CP). We expect different applications and relying party communities will tailor this document based on their specific needs. It was structured and developed so that the CP developer can fill in sections specific to organizational needs and quickly produce a suitable CP. This Reference CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.

Contacts:

Mr. Harold Booth
harold.booth@nist.gov

Mr. Andrew Regenscheid
andrew.regenscheid@nist.gov

NISTIR 7916, *Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop, April 23-24, 2012*

This publication contains the proceeding, abstracts, and present slides from the Cybersecurity in Cyber-Physical Systems Workshop of April 23-24, 2012. Some of the cyber-physical systems covered during the first day of the workshop included networked automotive vehicles, networked medical devices, semi-conductor manufacturing, and cyber-physical testbeds. Dr. Farnham Jahanian, National Science Foundation, was the keynote speaker on the first day of the workshop. Day two of the workshop covered the electric smart grid.

Contact:

Ms. Tanya Brewer
tanya.brewer@nist.gov

Draft NISTIR 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation*

This publication explains selected security challenges involving Infrastructure as a Service (IaaS) cloud computing technologies and geolocation. It then describes a proof of concept implementation that was designed to address those challenges. The publication provides sufficient details about the proof of concept implementation so that organizations can reproduce it if desired. The publication is intended to be a blueprint or template that can be used by the general security community to validate and implement the described proof of concept implementation.

Contacts:

Mr. Michael Bartock
michael.bartock@nist.gov

Mr. Murugiah Souppaya
murugiah.souppaya@nist.gov

NISTIR 7896, *Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition*

NIST opened a public competition on November 2, 2007 to develop a new cryptographic hash algorithm - SHA-3, which will augment the hash algorithms specified in FIPS 180-4, *Secure Hash Standard*. The competition was NIST's response to advances in the cryptanalysis of hash algorithms. NIST received 64 submissions in October 2008, and selected 51 first-round candidates on December 10, 2008; 14 second-round candidates on July 24, 2009; and 5 third-round candidates - BLAKE, Grøstl, JH, Keccak and Skein, on December 9, 2010, to advance to the final round of the competition. Eighteen months were provided for the public review of the finalists, and on October 2, 2012, NIST announced the winner algorithm of the SHA-3 competition – Keccak. This report summarizes the evaluation of the 5 finalists, and the selection of the SHA-3 winner.

Contacts:

Ms. Shu-jen Chang
shu-jen.chang@nist.gov

Mr. Ray Perlner
ray.perlner@nist.gov

Mr. William Burr
william.burr@nist.gov

Dr. Meltem Sönmez Turan
meltem.turan@nist.gov

Dr. John Kelsey
john.kelsey@nist.gov

Mr. Lawrence (Larry) Bassham
lawrence.bassham@nist.gov

NISTIR 7878, *Combinatorial Coverage Measurement*

Combinatorial testing applies factor covering arrays to test all *t*-way combinations of input or configuration state space. In some testing situations, it is not practical to use covering arrays, but any set of tests covers at least some portion of *t*-way combinations up to *t* [less than or equal to] *n*. This report describes measures of combinatorial coverage that can be used in evaluating the degree of *t*-way coverage of any test suite, regardless of whether it was initially constructed for combinatorial coverage.

Contact:

Mr. Rick Kuhn
rkuhn@nist.gov

NISTIR 7817, *A Credential Reliability and Revocation Model for Federated Identities*

A large number of Identity Management Systems (IDMS) are being deployed worldwide that use different technologies for the population of their users. With the diverse set of technologies, and the unique business requirements for organizations to federate, there is no uniform approach to the federation process. Similarly, there is no uniform method to revoke credentials or their associated attribute(s) in a federated community. In the absence of a uniform revocation method, this document seeks to investigate credential and attribute revocation with a particular

focus on identifying missing requirements. This document first introduces and analyzes the different types of digital credentials and recommends missing revocation-related requirements for each model in a federated environment. As a second goal, and as a by-product of the analysis and recommendations, this paper suggests a credential reliability and revocation service that serves to eliminate the missing requirements.

Contact:

Ms. Hildegard (Hildy) Ferraiolo
hildegard.ferraiolo@nist.gov

NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*

This publication provides a wide array of practices that, when implemented, will help mitigate supply chain risk to federal information systems. It seeks to equip federal departments and agencies with a notional set of repeatable and commercially reasonable supply chain assurance methods and practices that offer a means to obtain an understanding of, and visibility throughout, the supply chain.

Contacts:

Mr. Jon Boyens
jon.boyens@nist.gov

Ms. Celia Paulsen
celia.paulsen@nist.gov

NISTIR 7511 Revision 3, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*

This report defines the requirements and associated test procedures necessary for products to achieve one or more Security Content Automation Protocol (SCAP) validations. Validation is awarded based on a defined set of SCAP capabilities by independent laboratories that have been accredited for SCAP testing by the NIST National Voluntary Laboratory Accreditation Program (NVLAP).

Contacts:

Mr. David Waltermire
david.waltermire@nist.gov

Ms. Melanie Cook
melanie.cook@nist.gov

Mr. Stephen Quinn
stephen.quinn@nist.gov

NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms*

NIST has received numerous requests to provide a summary glossary for our publications and other relevant sources, and to make the glossary available to practitioners. As a result of these requests, this glossary of common security terms was extracted from FIPS, the SP 800 series, NISTIRs, and the Committee for National Security Systems Instruction 4009 (CNSSI-4009). This glossary includes most of the terms in the NIST publications. It also contains nearly all of the terms and definitions from CNSSI-4009. This glossary provides a central resource of terms and definitions most commonly used in NIST information security publications and in CNSS information assurance publications. For a given term, all definitions from NIST documents are not included – especially not from the older NIST publications. Since draft documents are not stable, those terms/definitions are not referenced. Each entry in the glossary points to one or more source NIST publications, and/or CNSSI-4009, and/or supplemental sources where appropriate. The NIST publications referenced are the most recent versions of those publications (as of the date of this document). [Supersedes NISTIR 7298 Revision 1 (February 2011)]

Contact:

Mr. Richard Kissel
richard.kissel@nist.gov

Additional Publications by CSD Authors

CSD authors actively contribute to the security community by authoring articles in the scholarly literature, participating in technical conferences, contributing to encyclopedias and other books, and publishing other "white papers" that fall outside the scope of NIST Technical Series publications described in the preceding section.

The following documents were published during FY 2013. For conference papers, the contributions listed below were accepted for conferences held during FY 2013; in some cases the final proceedings were not published until FY 2014. All NIST authors are identified using *italics*.

Links to the preprints and/or final publications of the documents below are available at http://csrc.nist.gov/publications.

Journal Articles

J. Boyar, P. Matthews and *R.C. Peralta*, "Logic Minimization Techniques with Applications to Cryptology," *Journal of Cryptology* 26(2), 280-312 (April 2013). doi:10.1007/s00145-012-9124-7.

A new technique for combinational logic optimization is described. The technique is a two-step process. In the first step, the non-linearity of a circuit { as measured by the number of non-linear gates it contains { is reduced. The second step reduces the number of gates in the linear components of the already reduced circuit. The technique can be applied to arbitrary combinational logic problems, and often yields improvements even after optimization by

standard methods has been performed. In this paper we show the results of our technique when applied to the S-box of the Advanced Encryption Standard (FIPS 197, *Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, 2001).

We also show that in the second step, one is faced with an NP-hard problem, the Shortest Linear Program (SLP) problem, which is to minimize the number of linear operations necessary to compute a set of linear forms. In addition to showing that SLP is NP-hard, we show that a special case of the corresponding decision problem is Max SNP-Complete, implying limits to its approximability.

Previous algorithms for minimizing the number of gates in linear components produced cancellation-free straight-line programs, i.e., programs in which there is no cancellation of variables in GF(2). We show that such algorithms have approximation ratios of at least 3/2 and therefore cannot be expected to yield optimal solutions to non-trivial inputs. The straight-line programs produced by our techniques are not always cancellation-free. We have experimentally verified that, for randomly chosen linear transformations, they are significantly smaller than the circuits produced by previous algorithms.

Q.H. Dang, "Changes in Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard," *Cryptologia* 37(1), 69-73 (2013). doi:10.1080/01611194.2012.687431.

This paper describes the changes between FIPS 180-3 and FIPS 180-4. FIPS 180-4 specifies two new secure cryptographic hash algorithms: SHA-512/224 and SHA-512/256; it also includes a method for determining initial value(s) for any future SHA-512-based hash algorithm(s). FIPS 180-4 also removes a requirement for the execution of the message length encoding operation.

D. Ferraiolo, *S. Gavrila*, and W. Jansen, "Enabling an Enterprise-wide, Data-centric Operating Environment," *Computer (IEEE)* 46(4), 94-96 (April 2013). doi:10.1109/MC.2013.130.

Although access control (AC) currently plays an important role in securing data services, if properly envisaged and designed, access control can serve a more vital role in computing than one might expect. The Policy Machine (PM), a framework for AC developed at NIST, was designed with this goal in mind. The PM has evolved beyond just a concept to a prototype implementation and is now being directed toward an open source project.

D. Maughan, *W.D. Newhouse* and T. Vagoun, "Introducing the Federal Cybersecurity R&D Strategic Plan," *The Next Wave - The National Security Agency's Review of Emerging Technologies* 19(4), 3-7 (2012).

In December 2011, the White House Office of Science and Technology Policy (OSTP) released the Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program —a framework for a set of coordinated federal strategic priorities and objectives for cybersecurity research. The release of this strategic plan marked an important milestone by the Federal Government's research community. It expresses an understanding of key causes of cybersecurity deficiencies and presents research themes with high potential to significantly improve the security of cyber systems and infrastructure. The strategic plan is a culmination of many efforts within the Federal Government, most notably by the Senior Steering Group for Cybersecurity R&D (CSIA R&D SSG), the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) of the Federal Networking and IT R&D (NITRD) Program, and by the Special Cyber Operations Research and Engineering Interagency Working Group (SCORE IWG).

C. McLeman and *D. Moody*, "Class Numbers via 3-Isogenies and Elliptic Surfaces," *International Journal of Number Theory* 9(1), 125-138 (February 2013). doi:10.1142/S179304211250128X.

We show that a character sum attached to a family of 3-isogenies defined on the fibers of a certain elliptic surface over Fp relates to the class number of the quadratic imaginary number field Q(\sqrt{p}). In this sense, this provides a higher-dimensional analog of some recent class number formulas associated to 2-isogenies of elliptic curves.

J.A. Montenegro, M.J. Fischer, J. Lopez and *R.C. Peralta*, "Secure Sealed-Bid Online Auctions Using Discreet Cryptographic Proofs," *Mathematical and Computer Modelling* 57(11-12), 2583-2595 (June 2013). doi:10.1016/j.mcm.2011.07.027.

This work describes the design and implementation of an auction system using secure multiparty computation techniques. Our aim is to produce a system that is practical under actual field constraints on computation, memory, and communication. The underlying protocol is privacy-preserving, that is, the winning bid is determined without information about the losing bids leaking to either the auctioneer or other bidders. Practical implementation of the protocol is feasible using circuit-based cryptographic proofs along with additively homomorphic bit commitment. Moreover, we propose the development of a Proof

Certificate standard. These certificates convey sufficient information to recreate the cryptographic proofs and verify them offline.

D. Moody and A.S. Zargar, "On Integer Solutions of x^4+y^4-2z^4-2w^4=0," *Notes on Number Theory and Discrete Mathematics* 19(1), 37-43 (2013).

In this article, we study the quartic Diophantine equation x^4+y^4-2z^4-2w^4=0. We find non-trivial integer solutions. Furthermore, we show that when a solution has been found, a series of other solutions can be derived. We do so using two different techniques. The first is a geometric method due to Richmond, while the second involves elliptic curves.

W.D. Newhouse, "Securing America's Digital Infrastructure Through Education," *The Next Wave - The National Security Agency's Review of Emerging Technologies* 19(4), 30-36 (2012).

This article provides an overview of the establishment of the National Initiative for Cybersecurity Education (NICE), its government structure, and it goals. Parallels are drawn between the strategic R&D thrust, Developing Scientific Foundations, described in "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program" published in December 2011 and NICE's awareness, education, and workforce efforts.

F.L. Podio, "Advances in Biometric Standardisation – Addressing Global Requirements for Interoperable Biometrics," *International Journal of Biometrics* 5(1), 5-19 (2013). doi:10.1504/IJBM.2013.05073.

The paper discusses the current status of biometric standards development activities, with a focus on international standards developments. Published standards, as well as standards under development or planned for the near future, are addressed. The work of Joint Technical Committee 1 of ISO and IEC Subcommittee 37 - Biometrics who is responsible for the development of a large portfolio of biometric standards in support of interoperability and data interchange is addressed. The work of two other JTC 1 Subcommittees, SC 17 Cards and personal identification and SC 27 - IT Security techniques who are also developing biometric standards within their scope of work is discussed. In many cases, the development of biometric standards impacts other standards developments including token-based, security, and telecommunication standards. Specific examples of this impact are provided. Standards activities performed in standards development bodies outside of ISO/IEC JTC 1 are also addressed. They include the work of ISO Technical Committee 68 – Financial Services – SC 2 – Security, and the International Telecommunication Union - Study Group 17- Security. Due to the large international impact and adoption, the development of the ANSI/NIST-ITL standards led by the Information Technology Laboratory of NIST is also addressed. Although a detailed discussion on biometric standards adoption is beyond the scope of this paper, a few examples of global and national biometric standards adoption for verification and identification applications are discussed.

S.M. Radack and *D.R. Kuhn*, "Protecting Wireless Local Area Networks (WLANs)," *IT Professional* 14(6), 59-61 (November-December 2012). doi:10.1109/MITP.2012.110.

This article summarizes the information that was presented in the February 2012 Information Technology Laboratory (ITL) bulletin, *Guidelines for Securing Wireless Local Area Networks (WLANs)*. The bulletin, which was noted by WERB in February 2012, was based on NIST Special Publication (SP) 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs): Recommendations of the National Institute of Standards and Technology*. The article summarizes the bulletin for a professional technical publication, and focuses on how organizations can implement sound security practices throughout the life cycles of their WLANs. Information is provided about access to SP 500-153, and to other NIST resources that are available to help organizations improve the security of wireless local area networks, the system development life cycle, and the management of risks to systems.

M. Sönmez Turan, "On the Nonlinearity of Maximum-length NFSR Feedbacks," *Cryptography and Communication* 4(3-4), 233-243 (December 2012). doi:10.1007/s12095-012-0067-5.

Linear Feedback Shift Registers (LFSR) are the main building block of many classical stream ciphers; however due to their inherent linearity, most of the LFSR-based designs do not offer the desired security levels. In the last decade, using Nonlinear Feedback Shift Registers (NFSR) in stream ciphers became very popular. However, the theory of NFSRs is not well-understood, and there is no efficient method that constructs a cryptographically strong feedback function with maximum period and also, given a feedback function it is hard to predict the period. In this paper, we study the maximum-length NFSRs, focusing on the nonlinearity of their feedback functions. First, we provide some upper bounds on the nonlinearity of the maximum-length feedback functions, and then we study the feedback functions having nonlinearity 2 in

detail. We also show some techniques to improve the nonlinearity of a given feedback function using cross-joining.

Conference Papers

M. Albanese, S. Jajodia, *A. Singhal* and L. Wang, "An Efficient Approach to Assessing the Risk of Zero-Day Vulnerabilities," *10th International Conference on Security and Cryptography (SECRYPT 2013)*, Reykjavik, Iceland, July 29-31, 2013.[To be published in a volume of Springer's *Communications in Computer and Information Science* series.]

*This paper received the Best Paper Award at SECRYPT 2013.

Computer systems are vulnerable to both known and zero-day attacks. Although known attack patterns can be easily modeled, thus enabling the development of suitable hardening strategies, handling zero-day vulnerabilities is inherently difficult due to their unpredictable nature. Previous research has attempted to assess the risk associated with unknown attack patterns, and a suitable metric to quantify such risk, the k-zero-day safety metric, has been defined. However, existing algorithms for computing this metric are not scalable, and must assume that complete zero-day attack graphs have been generated, which may be infeasible in practice for large networks. In this paper, we propose a set of polynomial algorithms for estimating the k-zero-day safety of possibly large networks efficiently, without pre-computing the entire attack graph. We validate our approach through experiments, and show that the proposed algorithms are computationally efficient and accurate.

S. Banik, S. Maitra, *S. Sarkar* and *M. Sönmez Turan*, "A Chosen IV Related Key Attack on Grain-128a," *18th Australasian Conference on Information Security and Privacy (ACISP 2013)*, Brisbane, Australia, July 1-3, 2013. In *Lecture Notes in Computer Science* 7959, *Information Security and Privacy*, C. Boyd and L. Simpson, eds., Springer, Berlin (2013) 13-26. doi:10.1007/978-3-642-39059-3_2.

Due to the symmetric padding used in the stream cipher Grain v1 and Grain-128, it is possible to find Key-IV pairs that generate shifted keystreams efficiently. Based on this observation, Lee et al. presented a chosen IV related Key attack on Grain v1 and Grain-128 at ACISP 2008. Later, the designers introduced Grain-128a having an asymmetric padding. As a result, the existing idea of chosen IV related Key attack does not work on this new design. In this paper, we present a Key recovery attack on Grain-128a, in a chosen IV related Key setting. We show that using around $\gamma \cdot 2^{32}$ (γ is a experimentally determined constant and it is sufficient to estimate it as 2^8) related Keys and $\gamma \cdot 2^{64}$ chosen IVs, it is possible to obtain $32 \cdot \gamma$ simple nonlinear equations and solve them to recover the Secret Key in Grain-128a.

J. Boyar, M. Find and *R. Peralta*, "Four Measures of Nonlinearity," *Eighth International Conference on Algorithms and Complexity (CIAC 2013)*, Barcelona, Spain, May 22-24, 2013. In *Lecture Notes in Computer Science* 7878, *Algorithms and Complexity*, P. G. Spirakis and M. Serna, eds., Springer, Berlin (2013) 61-72. doi:10.1007/978-3-642-38233-8_6.

Cryptographic applications, such as hashing, block ciphers and stream ciphers, make use of functions which are simple by some criteria (such as circuit implementations), yet hard to invert almost everywhere. A necessary condition for the latter property is to be "sufficiently distant" from linear, and cryptographers have proposed several measures for this distance. In this paper, we show that four common measures, nonlinearity, algebraic degree, annihilator immunity, and multiplicative complexity, are incomparable in the sense that for each pair of measures, μ1, μ2, there exist functions f1, f2 with μ1(f1) > _μ1(f2) but μ2(f1) < _μ2(f2). We also present new connections between two of these measures. Additionally, we give a lower bound on the multiplicative complexity of collision-free functions.

R. Chandramouli, "Security Assurance Requirements for Hypervisor Deployment Features," *Seventh International Conference on Digital Society (ICDS 2013)*, Nice, France, February 24-March 1, 2013, L. Berntzen and C-P Rückemann, eds., Xpert Publishing Services, Wilmington, Delaware (2013) 120-125.

Virtualized hosts provide abstraction of the hardware resources (e.g., CPU, Memory) enabling multiple computing stacks to be run on a single physical machine. The Hypervisor is the core software that enables this virtualization and hence must be configured to ensure security robustness for the entire virtualization infrastructure. Among the various combination of hypervisor types and hypervisor hardware platforms, we have chosen a reference architecture as the basis for our set of deployment features. For each deployment feature, this paper looks at the configuration options and analyzes the security implications of the options/deployment feature to derive a set of assurance requirements that are (a) provided by each of the configuration options or (b) are required for that deployment feature as a whole regardless of configuration options.

P. Cheng, L. Wang, S. Jajodia and *A. Singhal*, "Aggregating CVSS Base Scores for Semantics Rich Network Security Metrics," *2012 IEEE 31st Symposium on Reliable Distributed Systems (SRDS)*, Irvine, CA, United States, October 8-11, 2012, IEEE Computer Society, Washington, DC (2012) 31-40. doi:10.1109/SRDS.2012.4.

A network security metric is desirable in evaluating the effectiveness of security solutions in distributed systems. Aggregating CVSS scores of individual vulnerabilities provides a practical approach to network security metric. However, existing approaches to aggregating CVSS scores usually cause useful semantics of individual scores to be lost in the aggregated result. In this paper, we address this issue through two novel approaches. First, instead of taking each base score as an input, our approach drills down to the underlying base metric level where dependency relationships have well-defined semantics. Second, our approach interprets and aggregates the base metrics from three different aspects in order to preserve corresponding semantics of the individual scores. Finally, we confirm the advantages of our approaches through simulation.

V. C. Hu and K. Scarfone, "Real-Time Access Control Rule Fault Detection Using a Simulated Logic Circuit," *2013 International Conference on Social Computing (SocialCom)*, Washington, DC, September 8-14, 2013, IEEE Computer Society, Washington, DC (2013) 494-501. doi:10.1109/SocialCom.2013.76.

Access control (AC) policies can be implemented based on different AC models, which are fundamentally composed by semantically independent AC rules in expressions of privilege assignments described by attributes of subjects/attributes, actions, objects/attributes, and environment variables of the protected systems. Incorrect implementations of AC policies result in faults that not only leak but also disable access of information, and faults in AC policies are difficult to detect without support of verification or automatic fault detection mechanisms. This research proposes an automatic method through the construction of a simulated logic circuit that simulates AC rules in AC policies or models. The simulated logic circuit allows real-time detection of policy faults including conflicts of privilege assignments, leaks of information, and conflicts of interest assignments. Such detection is traditionally done by tools that perform verification or testing after all the rules of the policy/model are completed, and it provides no information about the source of verification errors. The real-time fault detecting capability proposed by this research allows a rule fault to be detected and fixed immediately before the next rule is added to the policy/model, thus requiring no later verification and saving a significant amount of fault fixing time.

R. Johnson, Z. Wang, A. Stavrou and *J. Voas*, "Exposing Software Security and Availability Risks For Commercial Mobile Devices," *Proceedings of the Annual Reliability and Maintainability Symposium, 2013 (RAMS'13)*, Orlando, Florida, January 28-31, IEEE, New York (2013) 1-7. doi:10.1109/RAMS.2013.6517735.

In this manuscript, we present our efforts towards a framework for exposing the functionality of a mobile application through a combination of static and dynamic program analysis that attempts to explore all available execution paths including libraries. We verified our approach by testing a large number of Android applications with our program to exhibit its functionality and viability. The framework allows complete automation of the execution process so that no user input is required. We also discuss how our static analysis program can be used to inform the execution of the dynamic analysis program. The program can serve as an extensible basis to fulfill other useful purposes such as symbolic execution, program verification, interactive debugger, and other approaches that require deep inspection of an Android application.

D.R. Kuhn, *I. Dominquez Mendoza*, *R.N. Kacker* and Y. Lei, "Combinatorial Coverage Measurement Concepts and Applications," *International Workshop on Combinatorial Testing 2013 (IWCT 2013)*, Luxembourg, March 22, 2013, IEEE Computer Society, Washington, DC (2013) 352-361. doi:10.1109/ICSTW.2013.77.

Combinatorial testing applies factor covering arrays to test all *t*-way combinations of input or configuration state space. In some testing situations, it is not practical to use covering arrays, but any set of tests covers at least some portion of *t*-way combinations up to *t* [less than or equal to] *n*. This report describes measures of combinatorial coverage that can be used in evaluating the degree of *t*-way coverage of any test suite, regardless of whether it was initially constructed for combinatorial coverage.

C. Liu, *A. Singhal* and D. Wijesekera, "Mapping Evidence Graphs to Attack Graphs," *IEEE International Workshop on Information Forensics and Security 2012 (WIFS 2012)*, Tenerife, Spain, December 2-5, 2012, IEEE Signal Processing Society, Piscataway, New Jersey (2012) 121-126. doi:10.1109/WIFS.2012.6412636.

Attack graphs compute potential attack paths from a system configuration and known vulnerabilities of a system. Evidence graphs model intrusion evidence and dependencies among them for forensic analysis. In this paper, we show how to map evidence graphs to attack graphs. This mapping is useful for application

of attack graphs and evidence graphs for forensic analysis. In addition to helping to refine attack graphs by comparing attack paths in both attack graphs and evidence graphs, important probabilistic information contained in evidence graphs can be used to compute or refine potential attack success probabilities contained in repositories like CVSS. Conversely, attack graphs can be used to add missing evidence or remove irrelevant evidence to build a complete evidence graph. In particular, when attackers use anti-forensics tools to destroy or distort evidence, attack graphs can help investigators recover the attack scenarios and explain the lack of evidence for missing steps. We illustrate the mapping using a database attack as a case study.

C. Liu, *A. Singhal* and D. Wijesekera, "Creating Integrated Evidence Graphs for Network Forensics," *Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics*, Orlando, FL, United States, January 28-30, 2013. In *IFIP Advances in Information and Communication Technology* 410, *Advances in Digital Forensics IX*, G. Peterson and S. Shenoi, eds., Springer, Berlin (2013) 227-241. doi:10.1007/978-3-642-41148-9_16.

Evidence Graphs model network intrusion evidence and their dependencies, which helps network forensics analysts collate and visualize dependencies. In particular, probabilistic evidence graph provide a way to link probabilities associated with different attack paths with available evidence. Existing work in evidence graphs assume that all evidence is available as one graph. We show how to merge different evidence graphs with or without the help of attack graphs. We show this by providing algorithms and a case study based on attacks on a fileserver and a database server in a lab network environment. An integrated evidence graphs that show all attacks launched toward a global network are more useful for forensics analysts and network administrators in searching for forensic evidence and safeguarding networks respectively.

R. Perlner and *D. Smith*, "A Classification of Differential Invariants for Multivariate Post-quantum Cryptosystems," *Fifth International Workshop on Post-Quantum Cryptography (PQCrypto 2013)*, Limoges, France, June 4-7, 2013. In *Lecture Notes in Computer Science* 7932, *A Classification of Differential Invariants for Multivariate Post-quantum Cryptosystems*, P. Gaborit, ed., Springer, Berlin (2013) 165-173. doi:10.1007/978-3-642-38616-9_11.

Multivariate Public Key Cryptography (MPKC) has become one of a few options for security in the quantum model of computing. Though a few multivariate systems have resisted years of effort from the cryptanalytic community, many such systems have fallen to a surprisingly small pool of techniques. There have been several recent attempts at formalizing more robust security arguments in this venue with varying degrees of applicability. We present an extension of one such recent measure of security against a differential adversary, which has the benefit of being immediately applicable in a general setting on unmodified multivariate schemes.

M. Sönmez Turan, "Related-Key Slide Attacks on Block Ciphers with Secret Components," *Second International Workshop on Lightweight Cryptography for Security and Privacy*, Gebze, Turkey, May 6-7, 2013. In *Lecture Notes in Computer Science* 8162, *Lightweight Cryptography for Security and Privacy*, G. Avoine and O. Kara, eds., Springer, Berlin (2013) 28-42. doi:10.1007/978-3-642-40392-7_3.

Lightweight cryptography aims to provide sufficient security with low area/power/energy requirements for constrained devices. In this paper, we focus on the lightweight encryption algorithm specified and approved in NRS 009-6-7:2002 by Electricity Suppliers Liaison Committee to be used with tokens in prepayment electricity dispensing systems in South Africa. The algorithm is a 16-round SP network with two 4-to-4 bit S-boxes and a 64-bit permutation. The S-boxes and the permutation are kept secret and provided only to the manufacturers of the system under license conditions. We present related-key slide attacks to recover the secret key and secret components using four scenarios; (i) known S-box and permutation with 2^48 time complexity using 2^16 + 1 chosen plaintexts; (ii) unknown S-box and known permutation with 2^55 time complexity using 2^22.71 + 1 chosen plaintexts; (iii) known S-box and unknown permutation with 2^48 time complexity using 2^16 + 1 chosen plaintexts and 2^12.28 adaptively chosen plaintexts; and finally, (iv) unknown S-box and permutation, with 2^48 time complexity using 2^22.71 + 1 chosen plaintexts and 2^31.29 adaptively chosen plaintexts. We also extend these attacks to recover the secret components in a chosen-key setting with practical complexities.

Books and Book Sections

D.R. Khun, *R.N. Kacker* and Y. Lei. *Introduction to Combinatorial Testing*. Boca Raton, Florida: CRC Press, 2013.

Combinatorial testing of software analyzes interactions among variables using a very small number of tests. This advanced approach has demonstrated success in providing strong, low-cost testing in real-world situations. Introduction to Combinatorial Testing presents a complete self-contained tutorial on advanced combinatorial testing methods for real-world software.

The book introduces key concepts and procedures of combinatorial testing, explains how to use software tools for generating combinatorial tests, and shows how this approach can be integrated with existing practice. Detailed explanations and examples clarify how and why to use various techniques. Sections on cost and practical considerations describe tradeoffs and limitations that may impact resources or funding. While the authors introduce some of the theory and mathematics of combinatorial methods, readers can use the methods without in-depth knowledge of the underlying mathematics.

Accessible to undergraduate students and researchers in computer science and engineering, this book illustrates the practical application of combinatorial methods in software testing. Giving pointers to freely available tools and offering resources on a supplementary website, the book encourages readers to apply these methods in their own testing projects.

White Papers

NIST Cloud Computing Public Security Working Group [M. Iorga], "Challenging Security Requirements for US Government Cloud Computing Adoption," National Institute of Standards and Technology, Gaithersburg, Maryland, November 27, 2012, 61 pp.

The Federal Cloud Strategy, February 8, 2010, outlines a federal cloud computing program that identifies program objectives aimed at accelerating the adoption of cloud computing across the Federal Government. NIST, along with other agencies, was tasked with a key role and specific activities in support of that effort, including the delivery of the NIST Cloud Computing Technology Roadmap and the publication of other Special Publications that address the reference architecture, definitions, and security aspects of cloud computing. In order to achieve adoption of cloud computing for the Federal Government, it is necessary to address the security and privacy concerns that federal agencies have when migrating their services to a cloud environment. To further exacerbate the situation, there are few documented details that directly address how to achieve some security aspects in a cloud environment. The purpose of this document is to provide an overview of the high-priority security and privacy challenges perceived by federal agencies as impediments to the adoption of cloud computing. The document provides descriptions of the existing mitigations to these security and privacy impediments. If no mitigations are listed, then ongoing efforts that could lead to mitigations are described. In the cases where no ongoing efforts were identified, the document makes recommendations for possible mitigation or references existing best practices.

C. Paulsen and *J. Boyens*, "Summary of the Workshop on Information and Communication Technologies Supply Chain Risk Management, National Institute of Standards and Technology, October 15-16, 2012," National Institute of Standards and Technology, Gaithersburg, Maryland, July 10, 2013, 21 pp.

There is a great demand from federal departments and agencies for supply chain risk management (SCRM) guidance. This document is a summary of a workshop held October 15-16, 2012 to broadly engage all stakeholders in an effort to set a foundation for NIST's future work on Information and Communication Technologies SCRM.

Opportunities to Engage with CSD and NIST

Guest Research Internships at NIST

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

Ms. Donna Dodson
(301) 975-8443
donna.dodson@nist.gov

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

Details at NIST for Government or Military Personnel

Opportunities are available at NIST for 6- to 24-month details at NIST in CSD. Qualified individuals should contact CSD, provide a statement of qualifications, and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring agency; however, in some cases, agency salary costs may be reimbursed by NIST. For further information, contact:

Ms. Donna Dodson
(301) 975-8443
donna.dodson@nist.gov

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

Federal Computer Security Program Managers' Forum (FCSPM)

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:

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

Visit the FCSPM Forum website:

http://csrc.nist.gov/groups/SMA/forum/membership.html

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:

Ms. Donna Dodson
(301) 975-8443
donna.dodson@nist.gov

Funding Opportunities at NIST

NIST funds industrial and academic research in a variety of ways. The Small Business Innovation Research Program funds R&D proposals from small businesses; see www.nist.gov/sbir. CSD also offers other grants to encourage work in specific fields: precision measurement, fire research, and materials science. Grants/awards supporting research at industry, academia, and other institutions are available on a competitive basis through several different Institute offices.

For general information on NIST grants programs, please contact:

Mr. Christopher Hunton
(301) 975-5718
christopher.hunton@nist.gov

Funding opportunity information:

http://www.nist.gov/director/ocfo/grants/grants.cfm

Acknowledgments

The editor, Patrick O'Reilly of the Computer Security Division, wishes to thank his colleagues in the Computer Security Division, who provided write-ups on their 2013 project highlights and accomplishments for this annual report (their names are mentioned after each project write-up). The editor would also like to acknowledge Barbara Guttman, Kevin Stine, Jim Foti (ITL, NIST), Greg Witte, Chris Johnson and Doug Rike (G2) for reviewing and providing valuable feedback for this annual report. The Editor also would like to thank Lorie Richards (Facilities Services Division, Creative and Printing Service, NIST) for designing the cover and final layout of our division's annual report. Finally, the editor would like to thank Joshua Franklin and Michaela Iorga (Computer Security Division, ITL, NIST) for their input with the 2013 annual report cover design.

This page is intentionally left blank.

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