COMPUTER SECURITY DIVISION

ANNUAL REPORT 2014

NIST SPECIAL PUBLICATION 800-176

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

NIST SPECIAL PUBLICATION 800-176

COMPUTER SECURITY DIVISION

ANNUAL REPORT 2014

PATRICK O'REILLY, EDITOR
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

CO-EDITORS:
Larry Feldman
Greg Witte
G2, Inc.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM
http://dx.doi.org/10.6028/NIST.SP.800-176

AUGUST 2015

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 Director

DISCLAIMER: ANY MENTION OF COMMERCIAL PRODUCTS IS FOR INFORMATION ONLY; IT DOES NOT IMPLY NIST RECOMMENDATION OR ENDORSEMENT, NOR DOES IT IMPLY THAT THE PRODUCTS MENTIONED ARE NECESSARILY THE BEST AVAILABLE FOR THE PURPOSE.

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SPECIAL PUBLICATION 800-176
NATL. INST. STAND. TECHNOL. SPEC. PUB., 107 PAGES (AUGUST 2015) CODEN: NSPUE2**

TABLE OF CONTENTS

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, transparent, and collaborative manner that enlists broad 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 globally.

The need for cybersecurity standards and best practices that address interoperability, usability and privacy continues to be critical for the Nation. CSD continues 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, roots of trust, identity and access management, advanced security testing and measurement, cyber-physical systems, and public safety networks.

Trust is crucial to the broad adoption of our standards and guidelines, including our cryptographic standards and guidelines. To ensure that our cryptography resources have been developed according the highest standard of inclusiveness, transparency and security, NIST initiated a formal review of our cryptographic standards development efforts in 2014. We documented and solicited public comment on the principles and rigorous processes we use to engage stakeholders and experts in industry, academia, and government to develop and revise these standards. We anticipate a final report in 2015 that will serve as a basis for our future standards development and revision efforts.

Increasing the trustworthiness and resilience of the IT infrastructure is a significant undertaking that requires a substantial investment in the architectural design and development of our systems and networks. A disciplined and structured set of systems security engineering processes that starts with and builds on well-established international standards provides an important starting point. Draft Special Publication 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*, issued in May 2014, helps organizations to develop a more defensible and survivable information technology infrastructure. This resource, coupled with other NIST standards and guidelines, contributes to systems that are more resilient in the face of cyber attacks and other threats.

Strong partnerships with diverse stakeholders are vital to the success of our technical programs. In February 2014, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity as directed in Executive Order 13636. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. Its approach helps owners and operators of critical infrastructure to manage cybersecurity-related risk. Collaborations continue as NIST works with stakeholders from across the country and around the world. 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.

Active engagement with diverse stakeholders continues to be critical to our success. In the federal space, 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. Our cybersecurity awareness, training, and education programs also exemplify the importance of engagements with academic institutions, federal agencies, small and medium businesses and others to increase awareness and enhance the overall cybersecurity posture of the Nation.

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 strengthening these relationships as we lead the development and practical application of scalable and sustainable information security standards and practices.

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.

Matthew Scholl
Acting Division Chief

COMPUTER SECURITY DIVISION (CSD) ORGANIZATION

MATTHEW SCHOLL

Acting Chief and, Deputy Chief,
Computer Security Division

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

INTRODUCTION TO CSD'S FIVE GROUPS

The Computer Security Division's computer scientists, mathematicians, IT specialists, support 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:

The Cryptographic Technology Group's (CTG) 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. The 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 FY 2014, the 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, the CTG worked with industry partners to promote the use of NIST-approved cryptographic methods.

The NIST cryptographic standards' program standardizes cryptographic primitives, algorithms, schemes, and guidelines in Federal Information Processing Standards (FIPSs), NIST Special Publications (SPs), and NIST Interagency or Internal Reports (NISTIRs). The NIST standardized cryptographic tools have been adopted as standards by standards-setting organizations, such as the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), and the Trusted Computing Group (TCG), and have been implemented on a variety of platforms.

In FY 2014, in response to public concerns about NIST cryptographic standards -in particular, the DUAL_EC_DRBG, a deterministic random number generator specified in SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*—NIST initiated a review of the cryptographic standards development process. The CTG summarized the development process for each cryptographic standard and provided materials and presentations to the NIST Visiting Committee on Advanced Technology (VCAT) and a NIST Committee of Visitors (COV), consisting of experts invited by the VCAT, to conduct the review. A summary for this review is provided in the Cryptographic Standards and Guidelines Process Review section of this annual report.

CTG researchers were highly engaged and productive in several critical cryptographic areas, such as post-quantum cryptography, elliptic curve cryptography, privacy-enhancing cryptography, and lightweight cryptographic schemes for constrained environments. The CTG has collaborated with many universities internationally, and research results were published in the major cryptography conferences and journals. The CTG also held workshops and conferences, as well as hosted guest researchers.

Several guidelines on cryptographic applications were published in various areas, such as key management, Internet protocols, and trusted platforms. The CTG contributed to other CSD cybersecurity projects, such as the Smart Grid and Personal Identity Verification (PIV) standards. The CTG also worked closely with the Security Testing, Validation, and Measurement Group of the CSD on FIPS 140-2, *Security Requirements for Cryptographic Modules*, the Cryptographic Algorithm Validation Program (CAVP), and the Cryptographic Module Validation Programs (CMVP).

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 of systems, to the design and analysis of next-generation, leap-ahead security capabilities. Computer security depends fundamentally on the level of trust of 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, and to testing

tools that identify 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, guidelines, and other documentary resources.

Collaborating extensively with government, academia, and the private sector, 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.

In FY 2014, collaborators and the associated collaborations have included Carnegie Mellon University (test development environment), Johns Hopkins Applied Physics Lab (practical application of combinatorial coverage measurement tool), the University of Texas at Arlington (covering array generation algorithm), Mexico's Centro Nacional de Metrología (constraints for a 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 University of Texas Dallas and East Carolina University (safety-critical systems testing), the National Science Foundation (cybersecurity metrics and assurance building), the National Security Agency (secure software tool chain competition development), and the Department of Homeland Security (incident coordination).

SCMG accomplishments include updates to the Advanced Combinatorial Testing System (ACTS) software and documentation, and the NIST Biometrics Conformance Test Software (BioCTS) 2014 biometric conformance testing tool and test assertions.

GROUP MANAGER:

Mr. Mark (Lee) Badger
(301) 975-3176
lee.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 identifying emerging and high-priority technologies, and on developing security solutions that will have a high impact on the U.S. critical infrastructures. The group conducted 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. In addition, the group worked 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 investigated the security concerns associated with such areas as mobile devices, cloud computing and virtualization, identity management, access control and authorization management, and software assurance. SSAG's research helps to meet federal information security requirements that may not be fully addressed by existing technology. The group collaborated 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;
- Published several Personal Identity Verification documents;
- Methods for achieving comprehensive policy enforcement and data interoperability across enterprise data services; and
- Test methods for mobile device (smart phone) application security.

In particular, the SSAG released an open-source reference implementation of ANSI/INCITS 499, *Next Generation Access Control.* The group also published SP 800-162, *Attribute Based Access Control (ABAC) Definition and Considerations*, providing the first authoritative definition of ABAC. In support of the Federal Government's mobile security initiatives, the group published SP 800-163, *Vetting the Security of Mobile Applications*, to provide

agencies with guidelines on how to test mobile applications for government use. In support of the Federal Government's cloud computing initiatives, the group led the NIST Security Working Group that published the *NIST Cloud Computing - Security Reference Architecture*. In support of the recently revised FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* six PIV-related 800-series SPs were revised. In addition to these, draft SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials,* was published to guide the implementation and deployment of PIV credentials for mobile devices.

To improve access to new technologies, the group also 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 the 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, Cyber Physical and Industrial Control Systems, Health Information Technology, and the National Public Safety Broadband Network. The group produces standards and guidelines through the Federal Information Security Management Act (FISMA) implementation program 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 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 the 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 infrastructures, and other application areas. The STVMG supports the testing and validation of cryptographic modules and the cryptographic algorithms specified in NIST standards. These cryptographic modules and algorithms enable products and systems to provide security services, such as confidentiality, integrity authentication, and source 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

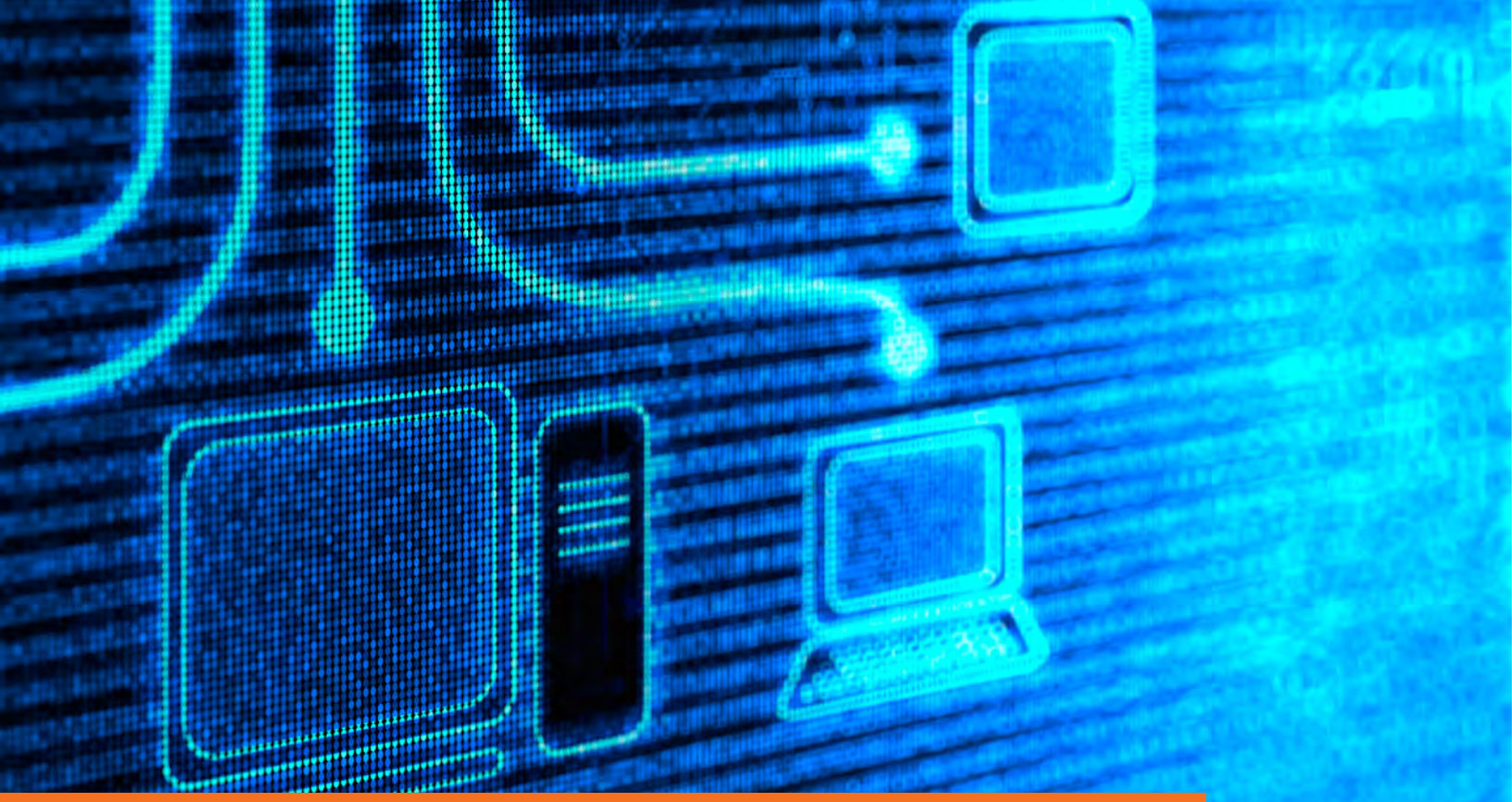
products meet established security requirements and use only tested and validated cryptographic modules and algorithms.

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 the validations awarded.

GROUP MANAGER:

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

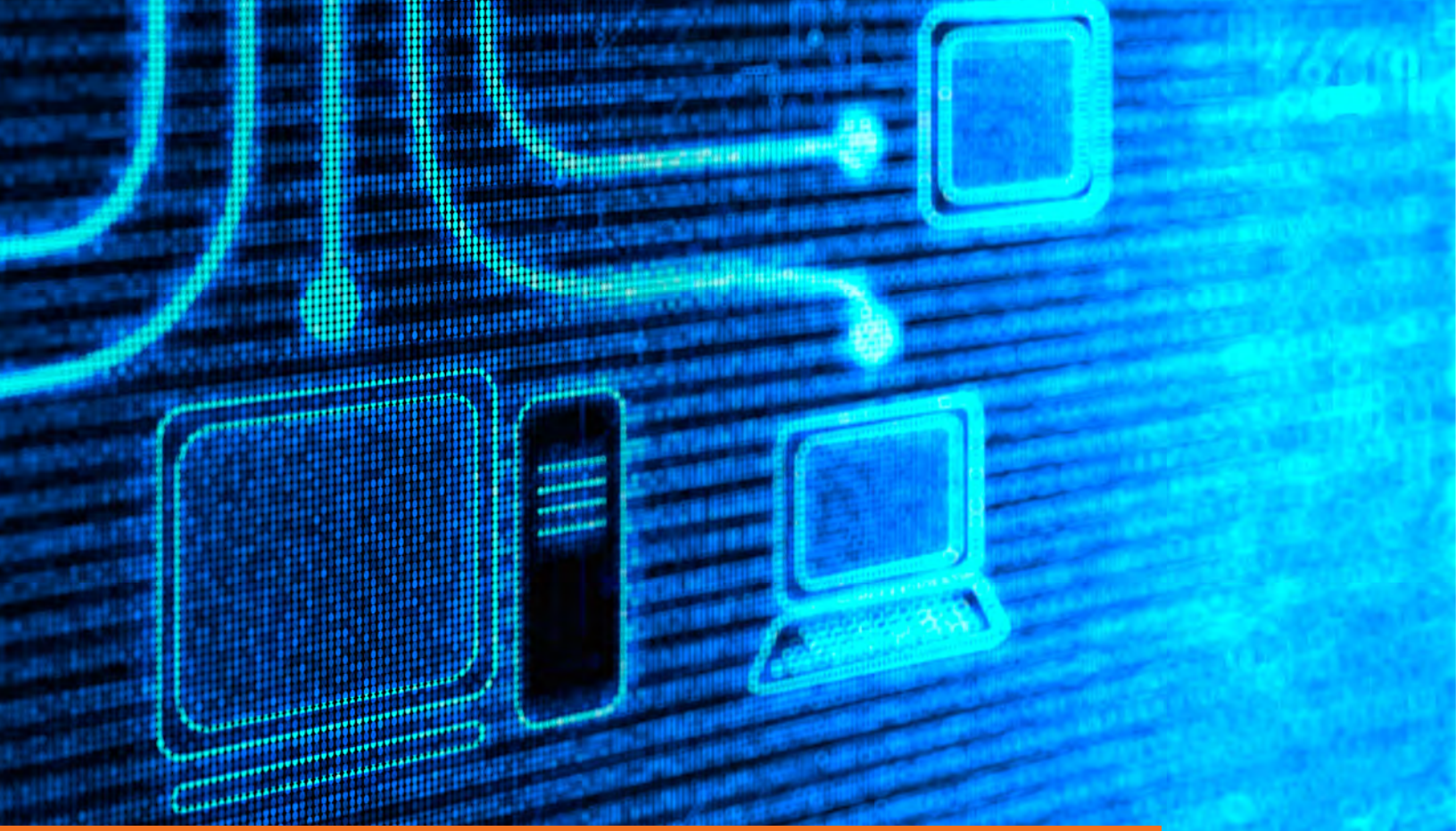


THE COMPUTER SECURITY DIVISION IMPLEMENTS THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

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 2014, the CSD addressed its FISMA responsibilities through the following activities:

- Issued a draft Federal Information Processing Standard (FIPS): FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions,* which specifies the Secure Hash Algorithm-3 (SHA-3) family of functions on binary data. Each of the SHA-3 functions is based on an instance of the Keccak algorithm that NIST selected as the winner of the SHA-3 Cryptographic Hash Algorithm Competition.
- Issued 23 draft and final NIST Special Publications (SPs) that provide management, operational, and technical security guidelines in areas such as application whitelisting, attribute-based access control, personal identity verification and derived credentials, key management, BIOS protection, mobile device forensics, secure communications protocol implementations, third-party mobile application vetting, supply chain risk management practices, role-based cybersecurity training, industrial control systems security, systems security engineering, and security and privacy controls assessments.
- Issued 13 draft and final NIST Interagency or Internal Reports (NISTIRs) on a variety of topics, including smart grid cybersecurity, personal identity verification, Common Vulnerability Scoring System (CVSS) implementation, cloud computing forensics; identity management in Public Safety mobile networks, replication device cybersecurity, automated access management using Secure Shell, and the development process for NIST cryptographic standards and guidelines.
- 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 2014, this collaboration produced updated guidelines for assessing security and privacy controls employed in federal information systems and organizations.
- Provided assistance to agencies and the private sector through many outreach programs, including the National Initiative for Cybersecurity Education (NICE), the Federal Information Systems Security Educators' Association (FISSEA), and the Federal Computer Security Managers' Forum.
- Conducted workshops, awareness briefings, and outreach to CSD customers to ensure the 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; cyber physical systems; cryptographic key management; safeguarding health information; secure hash algorithms; supply-chain risk management; improving critical infrastructure cybersecurity; broad computer security awareness, training, education, and outreach events; and cybersecurity innovation forums.
- Engaged with international standards bodies in a variety of areas, including promoting a broader international adoption of security automation specifications. Additionally, NIST's CSD continued to lead, the Cryptographic Module Validation Program (CMVP), in conjunction with the Government of Canada's Communications Security Establishment. 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 2014 annual report and released it as a NIST SP. CSD annual reports from fiscal years 2003 through 2014 are available on the Computer Security Resource Center (CSRC) at http://csrc.nist.gov/publications/PubsTC.html#AnnualReports.



PROGRAM AND PROJECT ACHIEVEMENTS FOR FISCAL YEAR 2014

PROGRAM AND PROJECT ACHIEVEMENTS FOR FY 2014

In FY 2014, 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 infrastructures. The following sections describe the 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 its critical infrastructure, the President issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity,* in February 2013. This EO directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices – for reducing cybersecurity risks to critical infrastructures.

The Cybersecurity Framework provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help owners and operators of critical infrastructures and other interested entities identify, assess, and manage cybersecurity-related risk, while protecting business confidentiality, individual privacy, and civil liberties.

In FY 2014, NIST continued to work with a diverse stakeholder community to develop the Framework through an open public process. This process included:

- Preparing a Preliminary Cybersecurity Framework for official public review and comment;
- Hosting a workshop at the North Carolina State University in Raleigh, North Carolina to gather input on the Preliminary Cybersecurity Framework;
- Issuing the Cybersecurity Framework in February 2014 as directed in the Executive Order;
- Publishing a companion Cybersecurity Framework Roadmap detailing high-priority areas that should be addressed in order to improve future versions of the Framework; and
- The release of a formal Request for Information (RFI), seeking feedback on awareness, experiences with the Framework, and related activities to support the use of the Framework.

Since the release of the Framework, NIST's primary goal has been to raise awareness of the Framework and encourage its use as a tool to help industry sectors and organizations manage cybersecurity risks. NIST has strengthened its collaboration with critical-infrastructure owners and operators, industry leaders, government partners, and other stakeholders, building on interactions over the previous year that were crucial to the Framework's development.

In FY 2015, NIST will continue to conduct stakeholder outreach and will work collaboratively with them to further understand stakeholder needs regarding tools and resources to enable a more effective use of the Framework. NIST will conduct additional public workshops, including a forum hosted by the Florida Center for Cybersecurity (FC2) located at the University of South Florida in Tampa on October 29-30, 2014. Periodic updates will be provided and additional events announced through the Framework website.

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

CSD WORK IN NATIONAL AND INTERNATIONAL STANDARDS

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

Figure 1 (below) shows many of the national and international standards-developing organizations (SDOs) involved in cybersecurity standardization. CSD participates in many cybersecurity standards' activities in many of these organizations, either in leadership positions or as editors and contributors, including the BioAPI Consortium; the Bluetooth Special Interest Group (SIG): Bluetooth Security Expert Group (BT-SEG); the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T); various groups within the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF); the North American Security Products Organization (NASPO); the Trusted Computing Group (TCG); and Accredited Standards Committee X9, Inc. (X9) (e.g. Financial Industry Standards X9F). Many of CSD's publications have been the basis for both national and international standards projects.

The following write-ups discuss the CSD's standards activities in conjunction with the InterNational Committee for Information Technology Standards (INCITS) Technical Committee Cyber Security (CS1), where CSD's Dan Benigni served as the Chair and U.S. Head of Delegation to subcommittee SC 27, and CSD's Sal Francomacaro served as the 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 representation by one member per country. The scope of ISO covers the standardization in all fields except electrical and electronic engineering standards, which are the responsibility of the International Electrotechnical Commission (IEC).

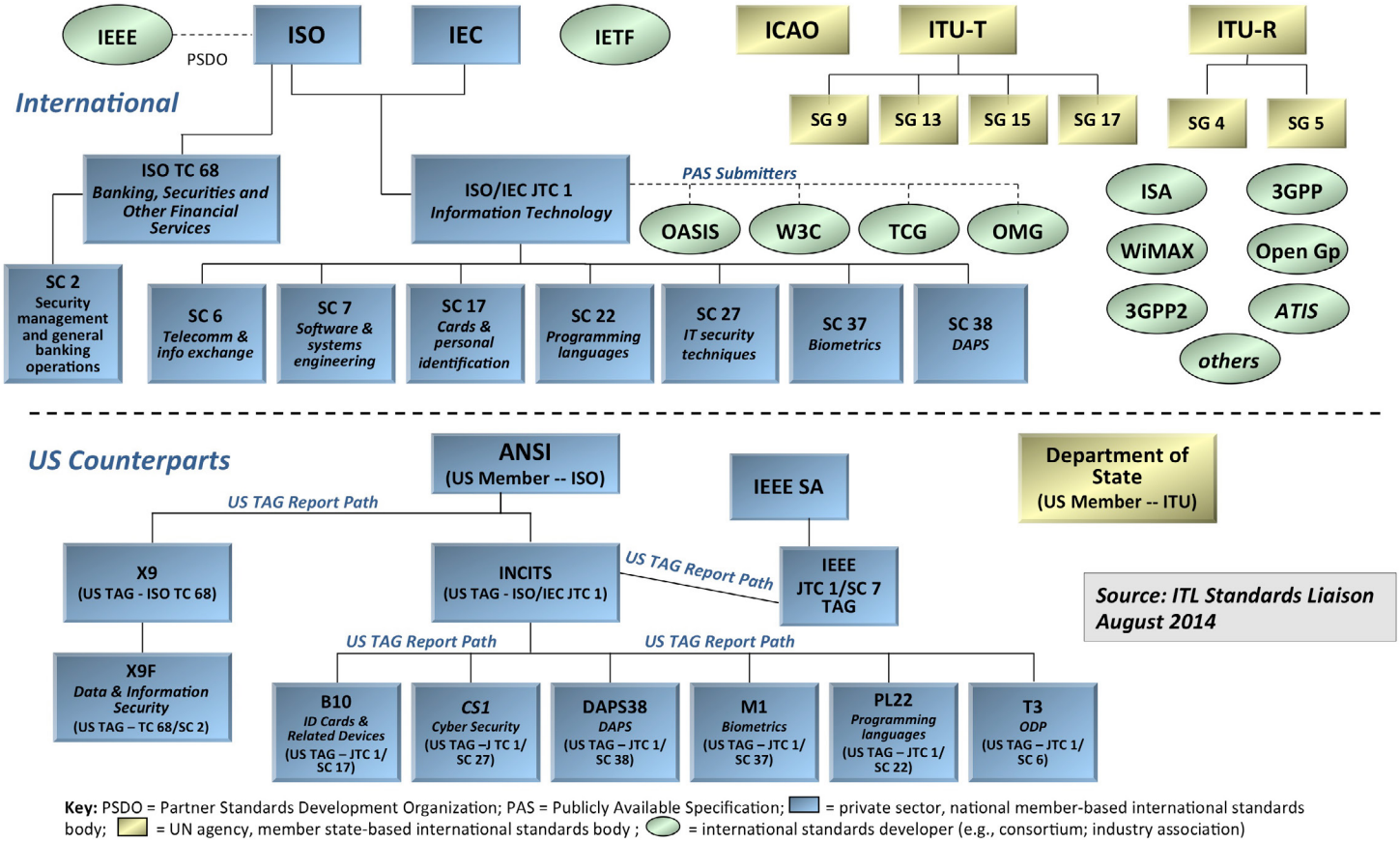


Figure 1: SDOs involved in Cybersecurity

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. (http://www.iec.ch/about/)

Joint Technical Committee 1 (JTC 1) was formed by ISO and IEC to be responsible for international standardization in the field of Information Technology (http://www.iso.org/iso/jtc1_home.html). It develops, maintains, promotes, and facilitates the IT standards required by global markets, meeting business and user requirements concerning:

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

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; and
- SC 37 – Biometrics (Note: Fernando Podio, NIST CSD, served as 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, and
- SC 38 – Distributed application platforms and services (DAPS).

The American National Standards Institute (ANSI)

ANSI is a private, nonprofit (501(c)(3)) organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system, and facilitates the development of American National Standards (ANSs) 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 U.S. 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 CSD, Chair, Sal Francomacaro, NIST CSD, Vice Chair, and NIST Principal Voting Member);
- E22 – Item Authentication;
- M1 – Biometrics (Fernando Podio, NIST CSD, Chair);
- T3 – Open Distributed Processing (ODP);
- T6 – Radio Frequency Identification (RFID) Technology;
- GIT1 – Governance of IT; and
- 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 an identity management framework, role-based access control, and single sign-on; and
- Privacy technologies, including a privacy framework, privacy reference architecture, privacy infrastructure, anonymity and credentials, and specific privacy-enhancing technologies.

The scope of CS1 explicitly excludes the areas of cybersecurity standardization, which is presently under development in INCITS B10, M1, T3, T10, and T11, as well as other standard groups, such as the Alliance for Telecommunications Industry Solutions (ATIS), the IEEE, the IETF, the Travel Industry Association of America (TIAA), and 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; U.S. 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, co-editors, or in other SC 27 leadership positions. Currently, over a dozen CS1 members are serving as SC 27 document editors or co-editors on various standards projects.

All input from CS1 is processed through INCITS to ANSI, then to SC 27. It is also a conduit for getting U.S.-based new work item proposals and U.S.-developed national standards into the international SC 27 standards development process. 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 JTC 1 SC 27 in a consistent, efficient, and timely manner.

NIST's CSD contributes to many of CS1's national and international IT security standards efforts through its membership on CS1, where Dan Benigni served as the nonvoting chair and Sal Francomacaro 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 100 current international standards projects. During FY 2014, eighteen new standards were published in SC 27, and all of them have been recommended by CS1 for adoption as U.S. national standards.

CSD's Role in Cybersecurity Standardization

CSD's cybersecurity research also plays a direct role in the Cybersecurity Standardization efforts of CS1 at the national level. The following is a description of the national-level progress achieved during FY 2014 by CSD and CS1.

The NIST Policy Machine research and development has resulted in three ongoing national standards projects in CS1 in the early stages of development. They include:

- *Next Generation Access Control –Functional Architecture (NGAC-FA),* project number INCITS 499-2013, was published in FY 2013 and is recently beginning an early revision;
- *Next Generation Access Control – Generic Operations & Abstract Data Structures (NGAC-GOADS).* Serban Gavrila, NIST CSD, is the editor. The project is assigned project number 2195-D, and the document (planned for publication in FY 2015) is out for second public review; and
- *Next Generation Access Control -Implementation Requirements, Protocols and API Definitions (NGAC-IR-PADS).* Project number is 2193-D has been assigned.

Dan Benigni also served as cybersecurity standards coordinator in CSD.

CONTACT:

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

(Editor Note: Mr. Dan Benigni led this program until his recent retirement.)

Identity Management Standards within INCITS B10 and ISO JTC1/SC17

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 the interoperability of Identification Cards and Related Devices. CSD has contributed and provided valuable feedback to many INCITS B10 standards in the development process. In addition, CSD also participates in the B10.12 committee. The B10.12 committee develops interoperable standards for Integrated Circuit Cards with Contacts, and it is the US TAG (Technical Advisory Group) for the international ISO/IEC JTC 1 SC 17 Working Groups 4 and 11. During FY 2014, Mr. Salvatore Francomacaro, a CSD staff member; served as the U.S. Head of delegation to ISO/IEC JTC 1 SC 17 WG4 and WG11.

CSD provides technical and editorial support in the development of national and international standards. Specifically, a CSD staff member 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. During FY 2014, INCITS 504 Parts 1 and 2 have started an amendment process to better align them with the new NIST SP 800-73-4 (PIV) specifications.

CSD staff also provided significant input to standards of major interest to U.S. government agencies and U.S. markets. CSD played a role in 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 2015, the INCITS B10 committee, along with the active collaboration of CSD staff, plans to:

- Publish Part 3 of INCITS 504;
- Complete the amendment process for INCITS 504 Part 1 and 2; and
- Contribute to the publication of several revisions of the ISO/IEC 7816 family of standards (all relevant to FIPS 201 specifications).

CSD staff will continue to actively support relevant ID management standard initiatives, such as ISO/IEC 19286 (Integrated Circuit Card (ICC) protocols and services ensuring privacy) and ISO/IEC 18328 (ICC managed Devices).

CSD's investment in these activities is motivated by new technical ideas that emerge from these ISO 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 National Strategy for Trusted Identities in Cyberspace (NSTIC). ISO/IEC 24727 aims to create an interoperability framework that increases the resilience and scalability of identity management solutions and to foster 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 a 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; and
- Conducting FISMA outreach to public and private-sector organizations.

During FY 2014, CSD continued to strengthen 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 (JTF) Transformation Initiative. The JTF partners continue to develop and update key cybersecurity guidelines for protecting federal information and information systems as part of 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 began work with the General Services Administration (GSA) Federal Risk and Authorization Management Program (FedRAMP) to develop a high-impact security control baseline overlay for FedRAMP cloud systems in accordance with NIST standards and guidelines.

In FY 2014, CSD worked on the following three initiatives:

- **Risk Management Guidelines:** SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* provides organizations with the security controls necessary to appropriately strengthen their information systems and the environments in which those systems operate, and with a process for selecting the appropriate controls, which contributes to systems that are resilient in the face of attacks and other threats. This "Build It Right" strategy is reinforced with the May 2014 publication of the Initial Public Draft (IPD) of SP 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*. The implementation of SPs 800-53 and 800-160, combined with the implementation of SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* and SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations,* provide organizations with near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.
- **Guidelines for a Role-Based Information Security Training Model:** SP 800-16, *A Role-Based Model for Federal Information Technology/Cybersecurity Training,* describes a process for developing information technology/cybersecurity role-based training. Its primary focus is to provide a comprehensive, yet flexible, methodology for the development of training courses or modules for personnel who have been identified as having significant information technology/cybersecurity responsibilities within agencies. Agencies can use SP 800-16 to tailor the Role-Based Security Training to meet the needs of their own organization.
- **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 an effective implementation of the NIST RMF. In addition, CSD conducted outreach activities with academic institutions, providing information on NIST's security standards and guidelines, exploring new areas of cybersecurity research and development, and serving on cybersecurity advisory panels.

In FY 2014, CSD completed the following activities:

- Published the IPD of SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal*

Information Systems and Organizations, and began public comment adjudication;

- Published errata versions of SPs 800-37 Revision 1 and 800-53 Revision 4 to make necessary clarifications and ensure consistency with subsequently published/revised NIST SPs and new/updated federal policy requirements;
- Published *Supplemental Guidance on Ongoing Authorization* to assist federal agencies in transitioning from the static point-in-time information system security assessment and authorization model to the dynamic, near real-time ongoing assessment and authorization model;
- Collaborated with the Department of Homeland Security (DHS) to develop a multiple-volume *Interagency Report on Automation Support for Ongoing Assessments,* which is based on NIST standards and guidelines; and
- Continued the development of a preliminary draft of SP 800-18 Revision 2, *Guide for Developing Security Plans for Federal Information Systems and Organizations.*

In FY 2015, CSD intends to:

- Finalize SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations;*
- Publish an errata update to SP 800-53 Revision 4;
- Begin the automation of the SP 800-53 revision and public comment process in support of more timely updates to counter threats and keep up with technological advancements;
- Finalize SP 800-16, *A Role-Based Model for Federal Information Technology / CyberSecurity Training;*
- Finalize SP 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems;*
- Publish the IPD of SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations;*
- Begin the development of 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; and
- Continue to support federal agencies in the effective implementation of the NIST RMF.

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

CONTACTS:

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

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

NIST's CSD supports the development of biometric conformance-testing methodology standards and other conformity-assessment efforts through active technical participation in the development of these standards and the development of associated conformance-test architectures and test suites. These test tools are developed to promote the adoption of these standards and to support users that require conformance to selected biometric standards, product developers and testing labs. CSD's project team contributes to the development of biometric standards and leads the InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1 – *Biometrics* and International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1 Subcommittee (SC) 37 – *Biometrics* standards bodies. The CSD plans to continue this work in FY 2015.

The development of the two versions of the Biometric Conformance Test Software (BioCTS) continued. "BioCTS for ANSI/NIST" (which targets biometric transactions based on the NIST SP 500-290, and SP 500-290 Revision 1 - *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information)* received enhanced testing features for XML files, as well as updates to begin supporting the revision of SP 500-290; for more information see: http://www.nist.gov/itl/iad/ig/ansi_standard.cfm. "BioCTS for ISO/IEC" (which targets several ISO/IEC biometric data interchange formats and profiles) received updates to add additional conformance test suites (CTSs) for selected PIV Profiles of biometric data formats (as specified in

SP 800-76-2), as well as support for ISO/IEC 19794-4:2011 Amendment 2, which is an XML encoding for the finger image data format. The latest versions of BioCTS were released in September 2014, together with documentation and sample data.

Intensive research was performed to study the feasibility of implementing the existing conformance-testing tools within a cloud-computing setting. This research was conducted on an Apache Hadoop platform, investigating implementation requirements, benefits and potential applications for biometric conformance testing. To progress the work beyond the original goal of research, the development of a solution was performed, resulting in a working implementation of an existing CSD BioCTS CTS (developed in Microsoft C#) being incorporated into a Linux and Java-based Apache Hadoop MapReduce job. This work successfully overcame several initial implementation problems, and resulted in a release package and methodology for using BioCTS software in Apache Hadoop (for more information on Apache Hadoop see: https://hadoop.apache.org/). The process, problems, and methods used to overcome them were presented at Global Identity Summit 2014. BioCTS Web, an ASP.NET Web application that runs existing BioCTS CTSs, was updated to support more testing suites. For more information on BioCTS in the Cloud, see: http://www.nist.gov/itl/csd/biometrics/biocts_cloud.cfm.

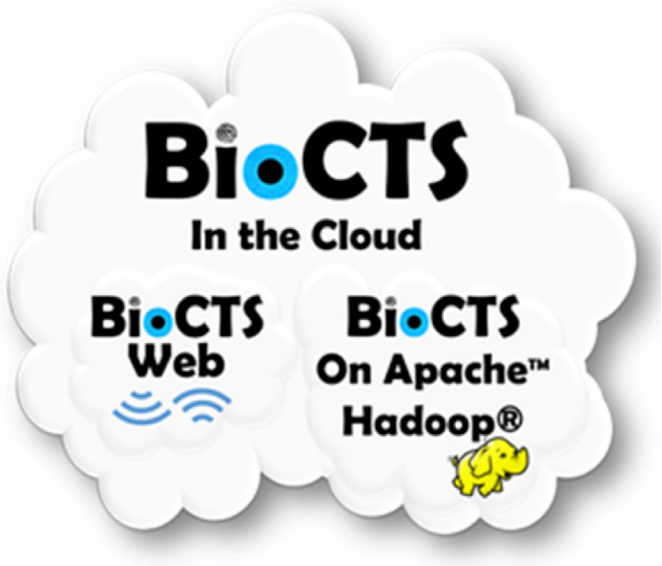


Figure 2: BioCTS in the Cloud

In addition to the conformance test tools, additional supporting tools were developed and released to benefit users of the test tools. They include a Data Extractor, which allows users to extract data from an ANSI/NIST-ITL formatted file; a Directory Hash Summary program, which allows users to generate a SHA-256 hash value for every file within the a given directory recursively; and enhanced statistical features within BioCTS for both versions of BioCTS. In addition, advanced editing features were incorporated in BioCTS for ANSI/NIST.

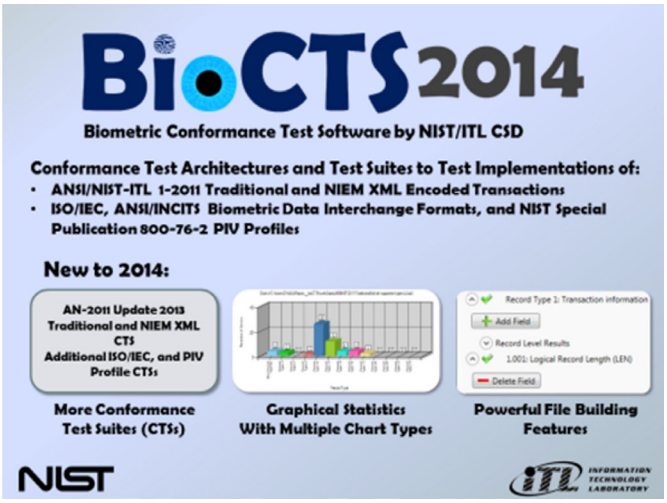


Figure 3: Biometric Conformance Test Software by CSD

The BioCTS software installer files, as well the ancillary tools and sample data can be downloaded from: http://www.nist.gov/itl/csd/biometrics/biocta_download.cfm.

A number of technical contributions towards the development of ANSI/NIST and international standards were submitted. They included technical contributions on international biometric data interchange formats and their associated conformance testing methodologies, as well as on the SP 500-290 Revision 1 and the associated NIEM XML Schema. A member of the project team, Dylan Yaga, CSD, received the INCITS Standards Service Award for his technical excellence, performance and dedication towards supporting the development of biometric standards. (Further details of Dylan's award is located in the Honors and Awards section of this annual report - page 77.)

Outreach efforts in FY 2014 in support of biometric standards development and conformity assessment included contributions on the test tools to the standards developers (in support of ongoing development projects), and presentations on ANSI/NIST and international biometric standards and related conformity assessment activities. The work included the development of technical publications,

the review of research papers for external publications, and participation in conference program committees. This effort included participation in the program development of the Global Identity Summit conference (previously the Biometric Consortium Conferences), which was held September 16-18, 2014, in Tampa, Florida. The conference included nearly 1500 attendees from 30 countries representing government, industry, and academia. NIST's CSD supported a booth at the conference's technical exposition and a member of the project team (Dylan Yaga) presented material regarding the conformance test tool development project. Over 140 speakers participated in the program.

Global Identity Summit conference program including released presentations:
http://www.biometrics.org/bc2014/program.pdf

BioCTS 2014 - Biometric Conformance Test Tool Downloads:
http://www.nist.gov/itl/csd/biometrics/biocta_download.cfm

CONTACT:

Mr. Dylan Yaga
(301) 975-6004
dylan.yaga@nist.gov

(Editor Note: Mr. Fernando Podio led this program until his recent retirement.)

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 2014, the NITRD Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG) monthly meetings provided an opportunity to learn and share information about ongoing research related to the themes and thrusts expressed in the Strategic Plan for the Federal Cybersecurity Research and Development. NIST's CSD briefed the IWG on initiatives in privacy engineering, combinatorial testing, android application testing, cyber-physical systems, big data, the National Initiative for Cybersecurity Education (NICE), and usability.

With the NITRD CSIA Senior Steering Group, CSD participated in the dialogue and planning that resulted in the creation of the National Privacy Research Forum to address concerns about privacy that were voiced in recent President's Council of Advisors on Science and Technology (PCAST) reports and to develop a strategic plan for privacy R&D in FY 2015.

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 and reports to the National Science & Technology Council's Committee on Homeland & National Security.

CONTACT:

Mr. Bill Newhouse
(301) 975-2869
william.newhouse@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 continued to support the EAC in finalizing changes to 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

that 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 the technologies used in current UOCAVA voting processes, including vote-by-mail, online voter registration, electronic ballot delivery, and online ballot marking.

Finally, CSD began working with NIST's Systems and Software Division (SSD) to explore applying software assurance concepts to electronic voting systems. The initial work in this area applies the Common Weakness Enumeration (CWE) list of software weaknesses to voting systems. The CWE was used to assist in the categorization of reported vulnerabilities within voting voting-system security security-analysis reports. Additionally, the vulnerabilities within the CWE are being mapped to the Voluntary Voting System Guidelines (VVSG)—both the current and upcoming standard.

Proposed plans for FY 2015, NIST will continue researching the applicability of software assurance concepts to electronic voting systems and continue to support efforts to improve the voting process for UOCAVA voters. Additionally, 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 the secure use and sharing of health information. HIT 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 CSD continued its HIT security outreach efforts in FY 2014. NIST and the Department of Health and Human Services' (DHHS) Office for Civil Rights (OCR) co-hosted the seventh annual HIPAA Security Rule conference, *Safeguarding Health Information: Building Assurance through HIPAA Security,* in September 2014 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 and panel discussions covered a variety of security management and technical assurance topics, including:

- Updates on the OCR audit and enforcement programs;
- Use of the NIST Cybersecurity Framework in the healthcare sector;
- Safeguarding data using cryptographic technologies and strong identity and access management;
- Strategies for engaging the executive leadership to privacy and security risks; and
- Case studies on safeguarding patient information, and lessons learned for health data breaches.

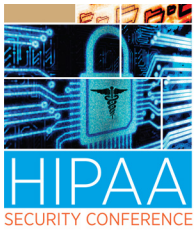
Keynote addresses were delivered by Darren Dworkin, Senior Vice President of Enterprise Information Systems and Chief Information Officer (CIO) of Cedars-Sinai Health System, and Daniel Solove, the John Marshall Harlan Research Professor of Law at the George Washington University Law School.

In FY 2015, NIST CSD will continue to work with diverse healthcare stakeholders, including partners in government and industry, to identify opportunities to strengthen the sector's cybersecurity risk management efforts by using the NIST Cybersecurity Framework. As part of its continued outreach efforts, NIST CSD also plans to co-host the eighth 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)

Information and communication technologies (ICT) rely on a complex, globally distributed, and interconnected supply-chain ecosystem that is long, has geographically diverse routes, and consists of multiple tiers of outsourcing. In addition, 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 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 that 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. Figure 4 (below) shows how ICT supply-chain risk may be derived from adversarial or non-adversarial threats, as well as external or internal vulnerabilities. The likelihood of an event and the potential impact of an event are also key factors.

This project seeks to provide federal agencies with a standardized, repeatable, and feasible toolkit of technical and intelligence resources to strategically manage supply-chain risk throughout the entire lifecycle of systems, products and services.

In FY 2014, CSD reviewed and addressed comments from the initial public draft of SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* 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

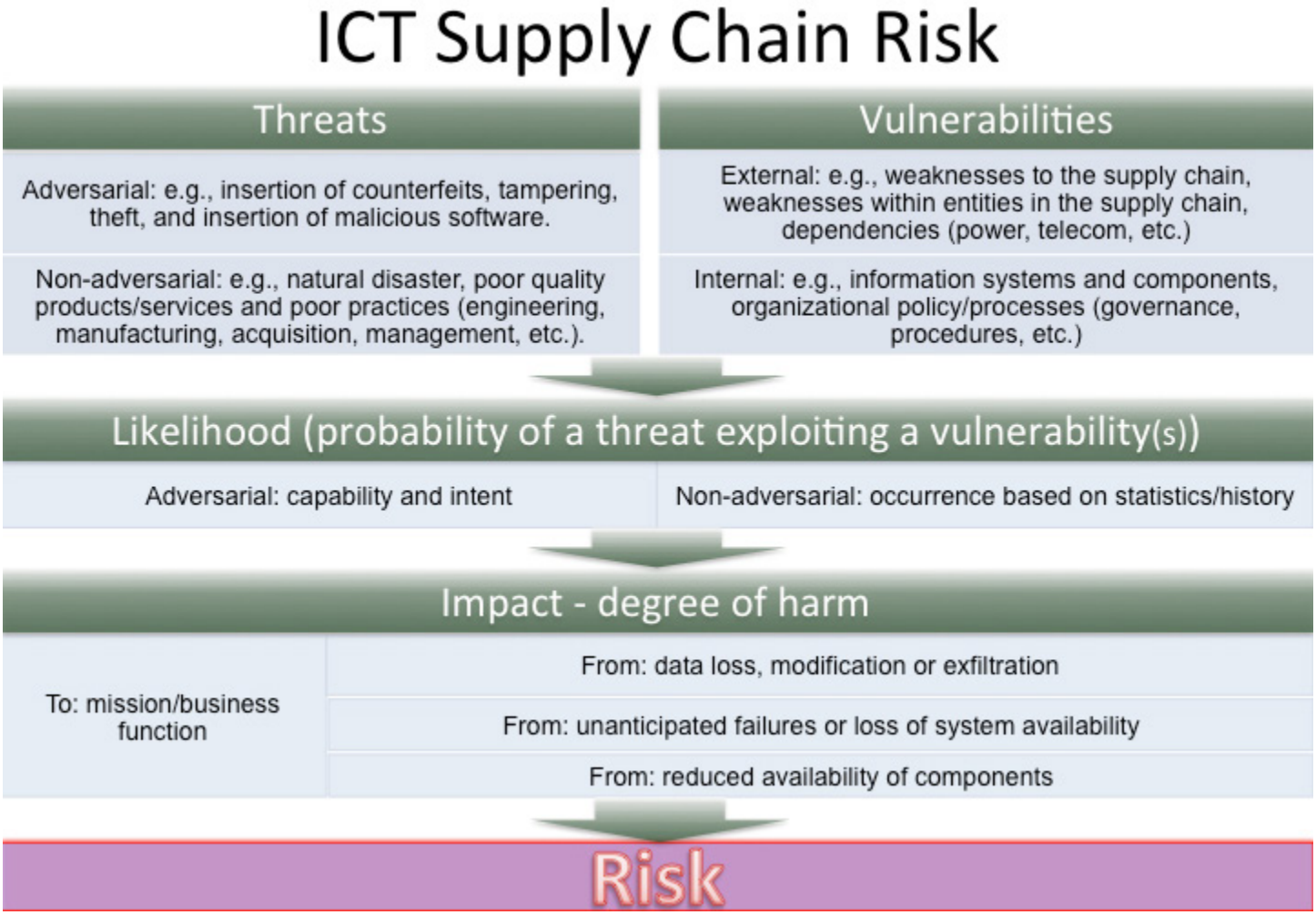


Figure 4: ICT Supply Chain Risk

the unified information security framework. A second public draft of the document was published in June 2014.

In June 2014, the University of Maryland Supply Chain Management Center of the R. H. Smith School of Business completed the fourth phase of a multi-year research project through a NIST grant awarded in 2013. Previous phases of the project resulted in the development of a Cyber Risk Portal where users can conduct ICT supply-chain risk self-assessments and gain access to a number of resources. This phase of the project deployed wide-scale testing of the portal and made improvements to the security infrastructure and applications.

NIST awarded the University of Maryland Supply Chain Management Center an additional grant in 2014 to define an effective engagement model that will enable representatives of stakeholder organizations to come together in person and online to learn how to map and manage their critical ICT supply-chain risks using the portal-based tool set. The project will be completed in April 2015.

In FY 2015, CSD will:

- Publish SP 800-161;
- Research and develop tools and guidance to help agencies effectively conduct criticality analysis and other aspects needed to manage supply-chain risk;
- 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
- Begin researching best practices and developing an organizational strategy for supply-chain risk management in response to the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity.*

ICT SCRM Team email: scrm-nist@nist.gov

CONTACTS:

Mr. Jon Boyens
(301) 975-5549
jon.boyens@nist.gov

Ms. Celia Paulsen
(301) 975-5981
celia.paulsen@nist.gov

NATIONWIDE PUBLIC SAFETY BROADBAND NETWORK (NPSBN) CYBERSECURITY

Source: http://www.pscr.gov/

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 the 3rd Generation Partnership Project's (3GPP) 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 to be used by public safety officials, vendors, and other interested parties for interacting with the nationwide network. NIST is also directed to conduct research and development that supports the acceleration and advancement of the nationwide network.

In FY 2014, CSD supported the joint National Telecommunications and Information Administration (NTIA) and NIST Public Safety Communications Research (PSCR) program (http://www.pscr.gov) with efforts in public-safety mobile-application security, identity management, and enabling cybersecurity capabilities on the PSCR 700 MHz LTE demonstration network located in Boulder, Colorado. In February 2014, CSD, in cooperation with the Association of Public-Safety Communications Officials (APCO) International and FirstNet, held a half-day workshop titled "*Public Safety Mobile Application Security*

Requirements". The outcome of that workshop is captured in Draft NISTIR 8018, *Public Safety Mobile Application Security Requirements Workshop Summary.* At PSRC's Annual Public Safety Broadband Stakeholder Conference in June 2014, CSD organized and moderated a panel titled "Mobile Applications Security for Public Safety".

CSD developed Draft NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks,* that provides a brief introduction to identity management, summarizes existing guidance (including OMB-04-04, *E-Authentication Guidance for Federal Agencies*; Homeland Security Presidential Directive 12 (HSPD12): *Policy for a Common Identification Standard for Federal Employees and Contractors;* and NIST SP 800-63-2, *Electronic Authentication Guideline*), and describes possible identity tokens/credentials that could be supported by mobile devices.

CSD participated in the standards development process for LTE technology within the 3rd Generation Partnership Project (3GPP) supporting security requirements for public safety that are related to Proximity Services (ProSe), Group Communication System Enablers (GCSE), and Mission Critical Push-To-Talk (MCPTT). In addition, CSD broadened its scope within the Internet Engineering Task Force (IETF) to include efforts related to public safety.

In FY 2015, CSD will continue representing public safety in international standardization efforts, such as the IETF and 3GPP. CSD will work to implement and exercise cybersecurity capabilities in the PSCR 700 MHz LTE demonstration network, conduct research into mobile authentication solutions to support the different public-safety disciplines, and investigate mobile application-security services to support the security requirements of public-safety mobile applications. CSD will continue to engage the public-safety communications community by organizing workshops and conferences; and participating in events such as APCO's Annual Meeting, PSRC's Annual Public Safety Broadband Stakeholder Conference, and the International Wireless Communications Expo (IWCE).

CONTACTS:

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

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

SECURITY OF CYBER-PHYSICAL SYSTEMS (CPS)

Cyber-Physical Systems (CPS) will provide the next generation of "smart," co-design and co-engineered interacting networks of physical and computational components. CPS is commonly used in the nation's critical infrastructure and includes systems in the electric grid, manufacturing, healthcare, and transportation sectors. Composed of heterogeneous, potentially distributed components and systems, CPS provides a promise of increased efficiency and interaction between the digital and physical worlds. However, assuring that these emerging and evolving systems are reliable, robust, resilient, trustworthy, secure, and that they protect the privacy of information poses a unique cybersecurity challenge.

CPS present unique challenges, including the need for integration with legacy components and allowance for emerging technologies, and real-time response in support of extremely high availability, predictability, and reliability. Cybersecurity is an important crosscutting discipline that is critical to the safe and resilient design, development and operation of CPS. Addressing the opportunities and challenges of CPS requires a broad collaboration to develop a common foundation to work from, including a consensus definition, vocabulary, reference architecture, and a shared understanding of the essential roles of timing, cybersecurity and data interoperability. CSD is researching the cybersecurity needs of the broader landscape of CPS, by leveraging CSD's expertise in cybersecurity in different domains and applications of CPS (such as industrial control systems, smart grid, hardware-enabled security, and embedded systems).

In June 2014, NIST established the CPS Public Working Group (PWG), which is open to all, to foster and capture inputs from those involved in CPS, both nationally and globally. CSD is working in collaboration with NIST's Engineering Laboratory (EL) Smart Grid and Cyber-Physical Systems Program Office, NIST's Physical Measurement Laboratory Time and Frequency Division, ITL's Software and Systems Division and ITL's Advanced Networking Technologies Division to lead a public-private working group of government, academia, and industry stakeholders. The CPS PWG consists of five technical subgroups:

- Definition, Vocabulary, and Reference Architecture;
- Use Cases;
- Cybersecurity and Privacy;
- Data Interoperability; and
- Timing and Synchronization.

Each subgroup consists of co-leads from academia, industry and NIST. CSD co-leads the Cybersecurity and Privacy subgroup focused on identifying strategies for cybersecurity and privacy in CPS, and will work collaboratively with the other subgroups to ensure that cybersecurity is included as a design principle during development.

In 2015, the CPS PWG will publish an integrated Framework that includes the work of the five technical subgroups and begin work on a CPS Technology Roadmap, which will identify opportunities for a coordinated effort on key technical challenges. The CPS PWG deliverables will be technology and business-model neutral, and freely available online and intended for open use by all stakeholders.

Additionally, in 2015, CSD, in conjunction with NIST's Engineering Laboratory, Intelligent Systems Division, will finalize SP 800-82 Revision 2, *Guide to Industrial Control Systems Security*. CSD will also 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.

http://www.nist.gov/cps/
http://www.nist.gov/cps/cpspwg.cfm

CONTACTS:

Ms. Victoria Yan Pillitteri
(301) 975-8542
victoria.pillitteri@nist.gov

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

SMART GRID CYBERSECURITY

Figure 5: Smart Meter

The major elements of the smart grid are: information technology, industrial control systems/operational technology, and the communications infrastructure. The infrastructure is 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.

SGIP
SMART GRID INTEROPERABILITY PANEL

The Smart Grid Interoperability Panel (SGIP) became a membership-supported organization in January 2013. The SGIP Cybersecurity Working Group (CSWG) was renamed the Smart Grid Cybersecurity Committee (SGCC), and continues to be led by a NIST representative in support of responsibilities identified in the Energy Independence and Security Act of 2007. The SGCC chair is a voting member of the SGIP Technical Committee, and serves as an ex-officio Director of the Board. In addition, the SGIP SGCC continues to include 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.

In 2014, the SGCC contributed to the update of NISTIR 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity,* which was published in September, following a public comment period and comment resolution by the SGCC members. 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. In addition to the revision of NISTIR 7628, the SGCC have focused on developing documents to be published through SGIP on cybersecurity risk management, a User's Guide for NISTIR 7628, cloud computing for the smart grid, and a mapping between NISTIR 7628 and the *Framework for Improving Critical Infrastructure Cybersecurity.* Work in these areas is completed through SGCC subgroups, which are created and disbanded on an as-needed basis.

The SGCC also continues to support 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 including cybersecurity in future revisions and in the implementation of the standards. CSD supports the SGCC in assessing the security of the 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 NIST 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.

Future activities include working with the SGIP Committees, Domain Expert Working Groups, and Priority Action Plans to integrate cybersecurity into their work efforts. Additionally, the SGIP SGCC will continue to collaborate with industry, academia, other working groups, and government agencies to address the cybersecurity needs for the smart grid.

In FY 2015, CSD will continue to support the SGCC in the evaluation of the cryptographic methods used in standards, practices, guidelines, and other technical documents for inclusion in the SGIP CoS. 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.nist.gov/smartgrid
http://www.sgip.org

CONTACTS:

Ms. Victoria Yan Pillitteri
(301) 975-8542
victoria.pillitteri@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 been the lead for the National Initiative for Cybersecurity Education (NICE) since its inception in 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."

NICE is an initiative that enhances the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cybersecurity skills, and knowledge of our nation's students and workforce.

NIST's CSD is leading the NICE initiative working from the strengths and energy of more than 20 federal departments and agencies leveraging each of their relationships with academia and industry sectors to ensure coordination, cooperation, focus, public engagement, technology transfer and sustainability. NIST will highlight these activities, engage various stakeholder groups and create forums for sharing information and leveraging best practices.

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

- Developing planning documents and building consensus on the strategy and implementation activities of NICE;
- Utilizing a newly established public-private working group to make progress towards NICE's goals;
- Promoting the use of data-driven initiatives within NICE;
- Facilitating cross-functional cooperation among federal departments and 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 workforce and education; and
- Coordinating with other federal initiatives and efforts related to NICE.

The NICE leadership team attended many events, symposia, forums, competitions, educational outreach meetings, and workshops to promote the activities within NICE. The team continued its leadership of the Office of Personnel Management (OPM) Cross-Agency Priority Goal: "Closing Skills Gap" for IT/Cybersecurity focused on reducing cybersecurity workforce gaps and supported the goals of the White House's Ready to Work initiative.

In FY 2015, CSD will continue to promote the coordination of existing and future cybersecurity education, training, and workforce activities. The Fifth annual NICE Workshop will take place on November 5-6, 2014 in Columbia, Maryland (http://csrc.nist.gov/nice/events.html). The CSD will also identify opportunities to extend and integrate the NICE focus on cybersecurity workforce, education, and training within NIST Special Publications and informational reports while promoting the value of the National Cybersecurity Workforce Framework (NCWF) and the forthcoming Department of Defense Cyberspace Workforce Strategy as resources that address cybersecurity workforce needs.

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

CONTACTS:

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

Dr. Ernest McDuffie (retired)
FY 2014 NICE Lead

Computer Security Resource Center (CSRC)

The CSRC, CSD's website, is one of the most visited websites at NIST. CSRC encourages the 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 2014, CSRC had more than 54 million page views and downloads.

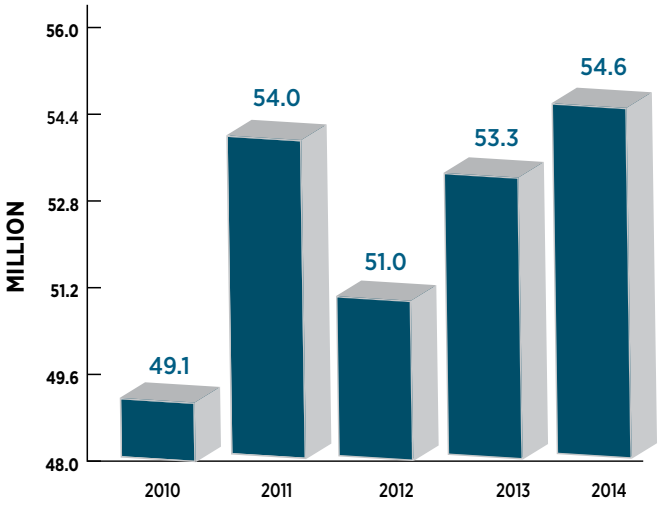


Figure 6: CSRC Website Visitors For Past 5 Years

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.

In addition to CSRC, CSD maintains a publication announcement mailing list. This free e-mail list notifies subscribers about publications that have been posted to the CSRC website, along with announcing new CSD-sponsored events and important news or announcements. The e-mail list is a valuable tool for more than 56 000 subscribers from the Federal Government, industry, academia, and individuals with a personal interest in IT security worldwide. Individuals who are interested in subscribing to this list should visit http://csrc.nist.gov/publications/subscribe.html for more information.

During FY 2014, the CSRC underwent what the CSD terms as "Quick Fixes" to the CSRC website. These "Quick Fixes" will improve the overall navigation experience on CSRC. The CSRC homepage was streamlined by providing hot topics (these hot topics are the most popular projects/programs that have webpages), updated references in the Useful Resources section, and an improved News and Events section. The homepage was condensed to reduce the amount of scrolling on the page. Another improvement made to the CSRC website was the dropdown menus, which appear on all pages. In previous years, the division's projects/programs listings were placed under the division's group layout. Now, the projects/programs listings are under their own category (Ex. Education & Outreach category, a project falling under this category: Small and Medium-Sized Business (SMB) Outreach). The CSRC team created an A to Z listing of the webpages for all of CSD's projects/programs in order to ease the finding of a particular area.

Plans for FY 2015 for the CSRC website will include moving the CSRC website to a content management system (CMS). Moving to a CMS is expected to improve the website's functionality.

Questions on the website can 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 1100 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's CSD serves as the Secretariat of the Forum, providing necessary administrative and logistical support. Patricia Toth 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. The Forum also holds bimonthly meetings and an annual two-day conference to discuss current issues and developments of interest to those responsible for protecting sensitive (unclassified) federal systems.

Topics of discussion at Forum meetings in FY 2014 included briefings from various federal agencies on Controlled Unclassified Information (CUI) Implementation Activities, Cross Agency Priority (CAP) Goals, Automated Assessment Practicals, Automated Assessment Concepts Supporting Information Security Continuous Monitoring (ISCM), NIST's Role in Ongoing Assessments, Ongoing Authorization Clarifying and Amplifying Guidance, and the National Cybersecurity Framework.

This year's annual two-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, Department of State, National Security Council, Department of Homeland Security (DHS), and NIST. Technical sessions included briefings on updates from NIST Computer Security Division (CSD), FedRAMP Overview and Security Processes, Supply Chain Risk Management, Ongoing Authorization, Fiscal Service's Risk-Based ISCM Strategy, Derived PIV Credentials, Cybersecurity Training, Incident Response, White House Initiatives, FY 2015 FISMA Metrics and recent updates to the FISMA publications.

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:

Ms. Patricia Toth
Chair
(301) 975-5140
ptoth@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 NIST for information system security professionals to assist federal agencies in meeting their information system's security awareness, training, and education responsibilities. FISSEA strives to elevate the general level of information system 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 system security professionals, professional trainers and educators, and managers responsible for information system 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. To become a FISSEA member; 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's CSD assists FISSEA with its operations by providing staff support for several of its activities and by being FISSEA's host agency.

FISSEA membership in 2014 spanned federal agencies, industry, military, contractors, state governments, academia, the press, and foreign organizations in a total of ten countries. The 700 federal agency members represent 89 agencies from the executive and legislative branches of government.

The 27th Annual FISSEA Conference occurred March 18-20, 2014, at NIST. Approximately 180 information system security professionals and trainers attended from federal agencies, academia, and industry.

This year's theme was, "*Partners in Performance: Shaping the Future of Cybersecurity Awareness, Education, and Training.*" The program team solicited presentations that reflected current projects, trends, and future initiatives 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 National Initiative for Cybersecurity Education (NICE) activities.

Keynote presentations were given by: Dr. Ron Ross, NIST Fellow, CSD; Ambassador Karen Kornbluh, Executive Vice President of External Affairs for Nielsen, former U.S. Ambassador to the Organization for Economic Cooperation and Development (OECD); and Ms. Linda Cureton, Chief Executive Officer and Founder of Muse Technologies, Inc. (former NASA CIO).

Presenters represented NIST, DHS, DOS, NSA, NASA, IRS, private industry and academia. Attendees had an opportunity to visit fifteen vendors on the second day. A Government Best Practice Poster and Demonstration session was held on the third day, which provided an opportunity for agencies to share and tell about their specific awareness and

2014 FISSEA Educator of the Year Award: Sam Maroon, FITSI Foundation / Wounded Warrior Cyber Combat Academy

training programs. In addition, there was a panel discussion of former FISSEA Educator of the Year recipients - influential leaders who have demonstrated a superior level of expertise, effectiveness, and dedication to the advancement of the information system security awareness, training and education profession. They discussed their best and worst ideas for improving cybersecurity programs, shared significant activities, and answered questions.

The FISSEA Educator of the Year Award was established to recognize and honor a contemporary who is making special efforts to create, build, manage, or inspire an information system security awareness, training, or education program. This year's Educator of the Year award was presented to Sam Maroon, Federal IT Security Institute (FITSI) Foundation/ Wounded Warrior Cyber Combat Academy. The nomination letter recommending him for this award made the following statements: "*Mr. Maroon deserves this award for his unflagging work supporting this country's injured servicemen and women in transitioning them to the cyber battlefield through the Wounded Warrior Cyber Combat Academy. … He has donated at least 300 hours of his own personal time…*" The full nomination letters are posted on the FISSEA website.

FISSEA conference events also included announcing the winners of FISSEA contests and awarding prize drawings. 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 2014 FISSEA Awareness, Training and Education Contest are:

- Poster Winner: Alexis Benjamin – Department of State, Office of Computer Security;
- Website Winner: Emma Gilli, Daisy Karaiosifoglou, Dan Acuff, and Nicole Rousseau – United Technologies Corporation;
- Motivational Item Winner: Kimberly Conway, Sara Fitzgerald, and Steven Van Brackle – Food and Drug Administration;
- Newsletter Winner: Jane Moser – Employment and Social Development Canada; and
- Role-Based Training Winner: Susan Farrand, Supply Chain Risk Management Resource Center, DOE.

Peers Choice Award winners voted on at the March Conference:

- Poster Winner: Deborah Coleman – Department of Education OCIO Information Assurance Services;
- Website Winner: Kimberly Conway, Sara Fitzgerald, Steven Van Brackle – Food and Drug Administration;
- Motivational Item Winner: Nicole Rousseau – United Technologies Corporation;
- Newsletter Winner: Kimberly Conway, Sara Fitzgerald, Steven Van Brackle – Food and Drug Administration; and
- Role-Based Training Winner: Susan Farrand – Supply Chain Risk Management Resource Center, Department of Energy.

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 2015 FISSEA conference is planned for March 24-25, 2015, 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 Information Security and Privacy Advisory Board (ISPAB) is a federal advisory committee with specific statutory objectives to identify emerging managerial, technical, administrative, and physical safeguard issues related to information security and privacy. The Board was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board (CSSPAB) within the Department of Commerce. The CSSPAB was chartered in May 1988 in accordance with the Federal Advisory Committee Act, as amended, 5 U.S.C., App. In December 2002, Public

Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002, Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-4) amended the statutory authority of the Board and renamed it the Information Security and Privacy Advisory Board.

Since the inception of this Advisory Board in 1987, ISPAB successfully renewed its charter with proper authority every two years. The legislative history for Public Law 100-235 and Public Law 107-347 underscores that Congress intended that the Board be a continuing body. The Board plays a central and unique role in providing the government with expert advice concerning information security and privacy issues that may affect federal information systems. 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: 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.

Congress indicated the long-term need for the Board by setting the term of Board members at a minimum of four years. The charter (http://csrc.nist.gov/groups/SMA/ispab/documents/ispab_charter_2014-2016.pdf) requires that the NIST Director appoint the Chairman and all twelve members of the Board. They are selected for their preeminence in the information technology industry or related disciplines.

The Charter also stipulates that Board members be selected from three main categories, with each category providing four members. Category 1 includes members from outside the Federal Government who are 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 who are eminent in the field of information technology, or related

Annual ISPAB Board Photo
(Left to Right): Ed Roback, Annie Sokol, Greg Garcia, Gale Stone, Peter Weinberger, Matt Thomlinson (Chair), Dave Cullinane, Chris Boyer, Matt Scholl, Kevin Fu, John Centafont, and Toby Levin

disciplines. Category 3 includes experienced information system managers from the Federal Government, including those with experience in information security and privacy, at least one of whom should be from the National Security Agency. The categorization of Board members is intended to meet ISPAB's statutory objectives. 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.

Presently, the ISPAB Chairperson is Matt Thomlinson, Senior Vice President, Microsoft Security, who assumed the chair in October 2012. He is supported by the following Board members:

- Julie Boughn, (formerly from Center for Medicare & Medicaid, Innovation Centers for Medicare & Medicaid Services (CMS));
- Christopher Boyer, AT&T;
- John Centafont, National Security Agency (NSA);
- David Cullinane, Security Starfish, LLC;
- Kevin Fu, The University of Michigan;
- Gregory Garcia, Financial Services Sector Coordinating Council (FSSCC);
- Toby Levin, Retired (formerly from U.S. Department of Homeland Security);
- Edward Roback, U.S. Department of Treasury;
- Gale Stone, Social Security Administration; and
- Peter Weinberger, Google, Inc.

During FY 2014, ISPAB held three meetings, all in Washington D.C:

- December 19-20, 2013 – this meeting was to replace the meeting scheduled for October 10-12, 2013 that was cancelled due to a government shutdown;
- March 12-14, 2014; and
- June 11-13, 2014.

During the December 2013 meeting, the Board developed a FY 2014 work plan. The resulting plan included the following areas of focus:

- Coordination with Office of Management and Budget (OMB), and other federal agencies, such as National Security Agency (NSA) and U.S. Department of Homeland Security (DHS), on all matters relating to information security and privacy;
- Cybersecurity technical transfer and implementation interests, considering items of particular note to individual industry sectors;
- Updates from the Privacy and Civil Liberties Oversight Board (PCLOB);
- Updates from NIST's CSD regarding cybersecurity and cryptographic work;
- Updates regarding embedded software security, including medical device security;
- Considerations surrounding Trusted Internet Connections, DHS Enhanced Cybersecurity Services (ECS) and special needs for critical infrastructures;
- Procurement and requirements to reduce supply-chain risk;
- Cross-Agency Priority Goals (CAP Goals) for cybersecurity;
- Information sharing with a focus on information security and privacy;
- Updates regarding FISMA, the related security controls (SP 800-53), and FedRAMP; and
- Updates of other critical NIST publications.

In addition to the work-plan focus areas, the Board also considered the following topics during FY 2014:

- Internet of Things (IOT);
- Cryptography and NIST Cryptography processes;
- Transportation Sector and Vehicle-to-Vehicle Communication;
- GAO reports relating to information security and privacy;
- Big Data and Privacy;
- Controlled Unclassified Information (CUI) Program;
- Federal Cloud Credential Exchange (FCCX) and the NSTIC; and
- National Cybersecurity Center of Excellence (NCCoE) Updates.

The presenters at each Board meeting were leaders and experts representing private industry; academia; federal agency CIOs, IGs and CISOs.

Copies of the current list of members and their biographies, the Board's charter and past Board activities are located at http://csrc.nist.gov/groups/SMA/ispab. Information on ISPAB Meetings is published in Federal

Register Notices at least 16 days prior to the meeting. Those interested in receiving meeting notices and other notices relating to NIST work in information security and privacy may email their name, affiliation, and address to Annie Sokol at the address below.

CONTACT:

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

Small and Medium Size Business (SMB) Cybersecurity Workshop 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 small and medium-size businesses (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 the 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 cybersecurity training workshops for small businesses. These workshops provide an overview of cybersecurity threats, vulnerabilities, and corresponding protective tools and techniques, with a special emphasis on information that small business personnel can apply directly.

In FY 2014, NIST, in collaboration with the FBI and the SBA, focused on implementing a three-year renewal of the co-sponsorship agreement that governs this cybersecurity workshop outreach program.

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

CONTACT:

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

(Editor Note: Mr. Richard Kissel led this program until his recent retirement.)

CRYPTOGRAPHIC STANDARDS PROGRAM

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

NIST opened a public competition in 2007 to develop a new cryptographic hash algorithm, SHA-3, to augment the hash algorithms specified in the *Secure Hash Standard*, FIPS 180-4. The competition ended on October 2, 2012 when NIST announced the selection of Keccak as the winning algorithm for standardization as the new SHA-3 Standard. NIST consulted with the Keccak designers and the cryptographic community, and then developed a SHA-3 standardization plan, which was presented at numerous cryptography conferences in 2013, and posted at the NIST hash website, indicated below, for public feedback.

On May 28, 2014, NIST CSD announced Draft FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, in the Federal Register (79 FR 30549) and requested comments. The announcement also proposed a revision of the Applicability Clause (#6) of the Announcement Section of FIPS 180-4, *Secure Hash Standard*, to allow the use of hash algorithms specified in either FIPS 180-4 or FIPS 202 for federal applications that require a cryptographic hash algorithm. The revision was necessary because the original text in FIPS 180-4 mandates the use of hash algorithms specified in FIPS 180-4 only. The other sections of FIPS 180-4 remain unchanged. The ninety-day public comment period for Draft FIPS 202 and the revision in FIPS 180-4 ended on August 26, 2014.

The CSD also hosted a SHA-3 workshop at the University of California, Santa Barbara, on August 22, 2014 to obtain feedback on the proposed SHA-3 Standard, and on additional modes of operation based on SHA-3 that are being considered for standardization. Approximately 75 participants from around the world attended the workshop.

The CSD received much feedback throughout the year, especially during the week of the workshop. Official comments received on Draft FIPS 202 and on the revision of the Applicability Clause of FIPS 180-4 are posted at http://csrc.nist.gov/groups/ST/hash/sha-3/fips-202-public-comments-aug2014.html. CSD is in the process of addressing these comments, and incorporating them, as appropriate, in the final versions of FIPS 202 and FIPS 180-4, to be approved by the Secretary of Commerce. NIST will announce the final approval by the Secretary in the Federal Register.

Information about the SHA-3 standardization effort is available at:
http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html.

CONTACT:

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

Random Number Generation (RNG)

Random numbers are required for the 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 (American National Standard (ANS) 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, CSD 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 in January 2012 to include additional capabilities identified during the development of Part 4 of ANS X9.82.

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 could contain a backdoor, namely, the Dual_EC_DRBG, which is based on the use of elliptic curves. This weakness could allow attackers to successfully predict the secret cryptographic keys that form the foundation for the assurances provided by security products. CSD immediately published an ITL Bulletin (September 2013, visit the CSRC ITL Bulletins page http://csrc.nist.gov/publications/PubsITLSB.html) 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. In April 2014, another public comment period was held on a revision of SP 800-90A that removed the Dual_EC_DRBG from the document. An additional public comment period was held in late 2014 that included additional changes suggested during the April 2014 comment period.

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 the initial drafts were made available for public comment in 2012. 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. These documents have undergone further changes as a result of the public comments and discussions with industry representatives. Updated drafts will be provided for another public comment period in early FY 2015.

CONTACTS:

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

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

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

Dr. Kerry McKay
(301) 975-4969
kerry.mckay@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 same key is used to reverse the transformation and recover the original block of data. A cryptographic technique that is constructed from a block cipher is called a mode of operation.

NIST's CSD is developing AES modes of operation for format-preserving encryption (FPE), based on proposals that were submitted from the private sector. A format can be a sequence of decimal digits, such as a credit card number or a social security number (SSN); formats can also be defined for other sets of characters besides decimal digits. FPE produces ciphertext with the same format as the corresponding plaintext, so that, for example, an encrypted SSN still looks like a valid SSN. FPE is expected to facilitate the retrofitting of encryption to existing applications. For example, FPE could be applied to database systems, so that the sensitive data could be targeted for encryption without disrupting the underlying data fields/pathways.

Draft SP 800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption,* which was released for public comment in July 2013, included three methods for FPE called FF1, FF2, and FF3. These methods are modes of operation of the AES that are intended to support a security strength of 128 bits or more.

As part of the public review of Draft SP 800-38G and as part of its routine consultation with other agencies, NIST was advised by the National Security Agency that the FF2 mode in the draft could not support 128 bits of security strength for some use cases. NIST independently confirmed this assessment, and in June 2014, NIST's CSD announced its intention to remove FF2 from the document.

The FF2 mode was designed for the payment card industry and submitted for NIST's consideration in 2011 by VeriFone Systems, Inc. NIST's analysis does not imply any practical vulnerability for the implementations of FF2 in the payment card industry. Nevertheless, in order for FF2 to meet NIST's security requirements for other potential applications, VeriFone Systems, Inc. has indicated that it will submit a revised proposal for NIST CSD to review. Meanwhile, CSD expects to finalize SP 800-38G with FF1 and FF3 in FY 2015.

CONTACT:

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

Key Management

NIST's CSD continues to provide guidelines on cryptographic key management for the Federal Government, and to coordinate with other national and international organizations, industry, and academia.

SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, was first published in August 2009. This publication specifies approved methods for automated key establishment using Rivest, Shamir, Adleman (RSA) key-transport and key-agreement schemes. In an RSA key-transport scheme, one party (called the sender) generates a key to be used in subsequent communications and sends it to another party (called the receiver), encrypted using the receiver's public key. In a key-agreement scheme, two parties contribute information that is used by each party to compute a shared secret, which is then used to derive a key that is known by both parties. The 2009 version approved the use of 1024- and 2048-bit keys for both key-transport and key-agreement schemes, and in the case of the key-agreement schemes, specified two approved methods for key derivation, both using an approved hash function. SP 800-56B has been revised to remove the use of 1024-bit keys because they no longer provide adequate protection for federal information, and to approve the use of 3072-bit keys. This revision also includes the approval of additional key-derivation methods specified in SP 800-56C, *Recommendation for Key Derivation through Extraction-then-Expansion*, and SP 800-135, *Recommendation for Existing Application-Specific Key Derivation Functions*, and the use of Hash-based Message Authentication Code (HMAC), as well as a hash function, during the key-derivation process. HMAC is specified in FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*. The revision of SP 800-56B was published in September 2014.

SP 800-57, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, was first published in 2009. This document addresses the key-management issues of currently available cryptographic mechanisms, including the use of Public Key Infrastructures (PKI) and several commonly used security protocols. A revision of this document was provided for public comment in May 2014 that updated the guidance provided in the 2009 version, included an additional section on the Secure Shell

(SSH) protocol and removed the 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 final version of SP 800-57, Part 3 will be published in early 2015.

SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*, is under development to provide guidance on the CKMSs to be used by the Federal Government. This document provides refinements of the requirements for CKMS designers that are specified in SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*. SP 800-152 also provides requirements and recommendations for the service providers of CKMSs used by federal agencies and their contractors, as well as guidance for the federal agencies in selecting a CKMS that supports the security and management policies of those agencies. A draft of this document was provided for public comment in FY 2013, and a workshop was held in March 2013 to discuss the draft. A second draft has been under development throughout FY 2014 to address the received comments and issues raised at the workshop. This draft will be available for public comment in December 2014.

A new NIST publication is under development that provides 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 2015.

Additional key-management work to be conducted in FY 2015 includes revisions to the following publications:

- SP 800-56A, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*: This revision will align SP 800-56A more closely with SP 800-56B, including the addition of 3072-bit keys for the finite-field Diffie-Hellman key-agreement schemes.
- SP 800-57 Part 1, *Recommendation for Key Management: Part 1: General:* The revision will include an update of the approved key sizes for cryptographic algorithms, and reference the new SHA-3 hash functions specified in FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*.
- SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths:* This document will be revised to include references to the SHA-3 hash functions and to update guidance on the continued use of cryptographic algorithms and key sizes by the Federal government.

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

Transport Layer Security

SP 800-52 Revision 1, *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. In September 2013, CSD announced Draft SP 800-52 Revision 1. Changes to the document were made based on comments received during the public comment period, which ended in mid-December 2013. The final version of SP 800-52 Revision 1 was published in April 2014.

SP 800-52 Revision 1 is a significant update to the original guidance and includes recommendations providing higher levels of security. 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 Internet Engineering Task Force (IETF) is actively developing extensions that can be used to add functionality to TLS. The CSD's Cryptographic Technology Group (CTG) will review updates and additions to the TLS protocol in the second half of FY 2015. If there are changes that should be incorporated into SP 800-52, the development of a new revision will begin.

CONTACTS:

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

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

CRYPTOGRAPHIC RESEARCH

Post-Quantum Cryptography

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break the existing infrastructure of public-key cryptography. The focus of the Post Quantum Cryptography project is to identify candidate quantum-resistant systems that are secure against both quantum and classical computers, as well as the impact that such post-quantum algorithms will have on current protocols and security infrastructures.

In FY 2014, CSD researchers 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.

CSD staff also engaged the international cryptographic community with presentations and publications. Presentations were made at the *2014 Conference on Theory of Quantum Computation, Communication, and Cryptography, CRYPTO 2014,* and *PQCrypto 2014 Conference*. CSD staff were invited to give talks at *QCrypt 2014*, and at the *PQCrypto 2014 Conference*. A CSD staff member gave a course on quantum algorithms. CSD staff helped organize the joint NIST-University of Maryland Workshop on Quantum Information and Computer Science. CSD also contributed to the European Telecommunications Standards Institute whitepaper on quantum-safe cryptography. The CSD also hosted two leading experts in the field, Dr. Jintai Ding and Dr. Vadim Lyubashevsky, for extended visits.

In FY 2015, the CSD 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, CSD will be prepared for possible standardization efforts in this area. The CSD will hold a workshop on cybersecurity in a post-quantum world in March of 2015.

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

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

Privacy-Enhancing Cryptography

The privacy-enhancing cryptography project seeks to promote the use of communication protocols that do not reveal unneeded private information of the 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 indicating 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. However, even though many such ZK protocols are practical, adoption by industry is slow. CSD's CTG is also 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. CTG has also shown that the NIST Randomness Beacon (discussed below) 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 work in collaboration with the National Strategy for Trusted Identities in Cyberspace (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. CTG believes that 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. CTG 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 cannot see the unencrypted assertion).

CONTACT:

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

Cryptographic Standards and Guidelines Process Review

In September 2013, news reports about leaked classified documents raised concerns over the trustworthiness of the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG), which is included in SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. In response to these concerns, NIST initiated an internal review, reopened public comment on SP 800-90A, and invited an independent review of its standards development processes.

As a first step, NIST's CSD solicited public comments to obtain feedback on the following: the processes used to develop standards, and the mechanisms used to engage experts in industry, academia and government to develop them. As part of this process, the team compiled information about the principles, processes and procedures that drive NIST cryptographic standards development efforts. This supports guidance to help the public understand how such standards are developed. This information was published in draft NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process.*

NIST's federal advisory committee, the Visiting Committee on Advanced Technology (VCAT), was asked to review NIST's cryptographic standards program. The VCAT formed a Committee of Visitors (COV) with invited experts from standards organizations, industry, and the cryptographic research community to assist in this review. During three meetings in April and May 2014, the COV reviewed NIST's cryptographic standards development process, including the events that led up to the inclusion of the Dual_EC_DRBG in SP 800-90A; the development of the SP 800-38 series of block cipher modes; and the selection and status of the recommended elliptic curves in FIPS 186-4, the *Digital Signature Standard*. As part of the review, the COV provided recommendations for process improvement, as well as some specific technical considerations and criteria for NIST's cryptographic standards and processes.

Based on the COV's recommendations, the VCAT produced a report detailing recommendations for NIST's cryptographic standards program. The VCAT recommendations called for NIST to increase its staff of cryptography experts and implement more explicit processes for ensuring openness and transparency to strengthen its cryptography efforts.

NIST has posted the full VCAT report, including the individual recommendations from the COV, on the NIST website, as well as the briefing documents provided to assist in the review.

NIST CSD is working to implement the recommendations of the VCAT. In response to comments received from the public, and the recommendations from the VCAT and COV, NIST CSD is working on a revision to NISTIR 7977 that will provide more detailed processes and procedures. These additions will ensure that there is a clear record of the contributions to NIST standards and guidelines, and will establish a maintenance process that ensures that publications remain current. Additionally, NIST will continue to strengthen capabilities with new hires, guest researchers, contracts and external collaborations with researchers, industry and standards organizations. Finally, NIST CSD will work with the cryptographic community to evaluate other technical concerns raised by the VCAT's review and take appropriate remediating actions.

http://www.nist.gov/director/vcat/index.cfm

http://www.nist.gov/director/vcat/cryptographic-standards-guidelines-process.cfm

CONTACT:

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

NEW RESEARCH AREAS IN CRYPTOGRAPHIC TECHNIQUES FOR EMERGING APPLICATIONS

Circuit Complexity Research

Cryptographic functions, such as encryption, digital signatures, and hashing, are implemented as electronic circuits for a wide class of applications. In practice, it is important to be able to minimize the size of these circuits. This problem is closely related to designing small combinational circuits. These circuits use only binary AND, XOR and NEGATION gates, i.e. multiplication, addition, and "+1" in arithmetic modulo 2. A combinational circuit on four variables is depicted below. The project team has shown that finding optimal combinational circuits 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. The CSD's CTG has developed and implemented new heuristics for the circuit minimization problem. Two patents have been granted related to this work, the last one in FY 2014. These are held jointly between NIST and the University of Southern Denmark.

CSD's 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. 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. In the process, the CTG research team developed tools that have wide applicability for both theoretical and applied research in security and cryptography.

Multiparty computation is a technique that allows a group of people to compute a function of their inputs without revealing the inputs themselves. Examples of this are: i) holding an election; ii) conducting closed-bid auctions in which only the winning bid is determined; iii) proving to a third party that an entity's encrypted attributes satisfy some requirement, such as "over 21 and (US citizen or Canadian citizen)". The protocols that solve multiparty computation problems often encrypt bits using arithmetic modulo 2. The complexity of such protocols largely depends on the number of multiplications required – hence, the importance of expressing functions as circuit computations with few multiplication (AND) gates. Some of the published circuits are now the standard reference for benchmarking tools in multiparty computation.

A partial list of new results consists of:

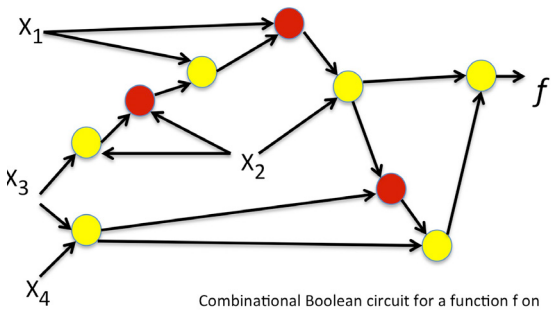
- The construction of the smallest known circuits for multiplication in several small finite fields;
- The construction of the smallest known circuits for the multiplication of polynomials of degree *n* over the Galois Field with two elements (for small values of *n*); and
- The construction of optimal circuits - with respect to the 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.

Additionally, our circuits use no more than seven non-linear gates (XOR, XNOR). This is quite hard. Consider the following predicate (arithmetic is modulo 2):

$$f = x_1 + x_2 + x_3 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_3x_4.$$

Computing the last term requires three multiplications. So it is quite surprising that the full expression can be computed using only three multiplications; however, this has been shown to be the case for f and all other predicates on four bits. The circuit depicted below computes f using 3 multiplications and 6 additions.

- A proof that the maximum multiplicative complexity of predicates on five bits (there are more than 4 billion such predicates) is four. The proof is constructive, meaning the circuits can actually be built. This result appears in the proceedings of the *Third International Workshop on Lightweight Cryptography for Security & Privacy (Springer-Verlag)*.



Combinational Boolean circuit for a function f on inputs (x_1,x_2,x_3,x_4). The red nodes are AND gates, the yellow nodes are XOR gates.

Figure 7: Combinational Boolean Circuit

The page http://cs-www.cs.yale.edu/homes/~peralta/CircuitStuff/CMT.html contains many of our results.

CONTACT:

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

Cryptography for Constrained Environments

There are several emerging areas in which highly constrained devices are interconnected, typically communicating wirelessly with one another, and working in concert to accomplish some task. Examples of these areas include: sensor networks, healthcare, distributed control systems, the Internet of Things, cyber physical systems, and the smart grid. Security and privacy can be very important in all of these areas. Because the majority of current cryptographic algorithms were designed for desktop/server environments, many of these algorithms do not fit into the constrained resources. If current algorithms can be made to fit into the limited resources of constrained environments, their performance is typically not acceptable.

CSD's Cryptographic Technology Group (CTG) is studying the use of the NIST-approved symmetric-key algorithms in constrained environments. CTG has developed microcontroller implementations of the Advanced Encryption Standard (AES) to provide both confidentiality and the AES-based message authentication code, Cipher-based Message Authentication Code (CMAC), 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. SHA-3, as specified in Draft FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, and a variant of KECCAK using an 800-bit permutation has also been implemented. CTG has demonstrated that SHA-3 allows a more efficient construction for computing Message authentication codes (MACs) than the HMAC construction, which is required when using SHA-256. CTG has also investigated other, non-NIST-approved algorithms for constrained environments.

CTG has also begun to examine applications in constrained environments to determine whether NIST should develop a lightweight encryption standard. CTG has talked with industry experts to understand challenges, limitations, and work from other standardization bodies in this area. Also, CTG has had internal discussions on additional considerations for a lightweight standard, as restrictions on its use would be necessary in order to prevent the adoption of a lightweight cipher where the strong protection of AES is required.

CTG is preparing a report that describes the current state and challenges in target application areas, and provides a survey of lightweight primitives, including block and stream ciphers that have been proposed for constrained environments. CTG researchers also studied efficient implementations of the Boolean functions used in lightweight primitives and published *Multiplicative Complexity of Boolean Functions on Four and Five Variables* at the *Third International Workshop on Lightweight Cryptography for Security & Privacy* (LightSec 2014).

In FY 2015, CTG will continue to analyze the resource requirements and performance characteristics of lightweight primitives, and study their use as building blocks to perform various cryptographic objectives. Additionally, CTG will investigate specific application areas in order to determine functionality and resource requirements in the area of cryptography for constrained environments.

CONTACTS:

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

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

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

NIST Randomness Beacon

NIST has implemented a source of public randomness. The prototype, called the Beacon, 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 all, 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 these 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, only 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.

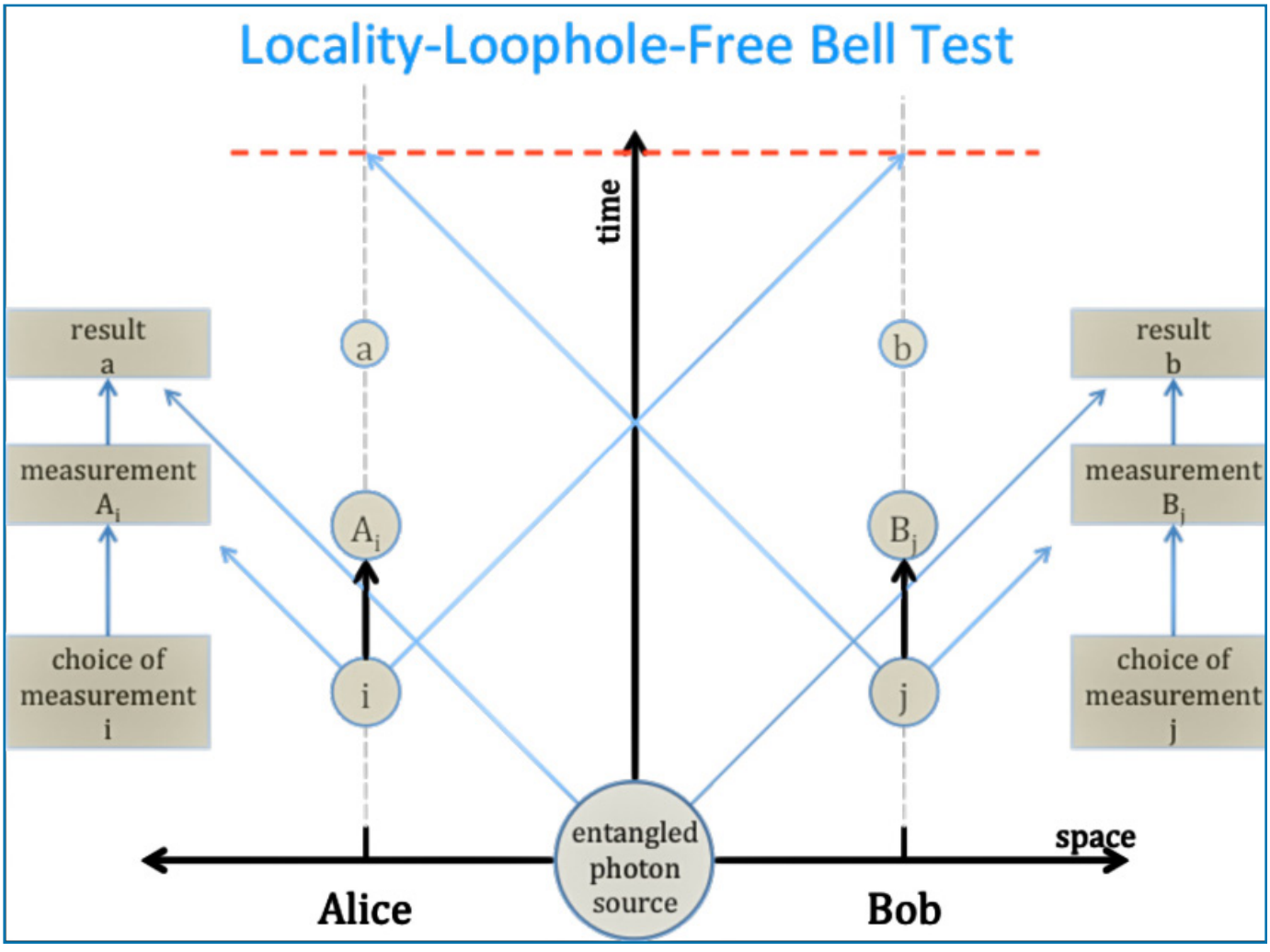


Figure 8: A Space-time Diagram Illustrating a Locality-loophole-free Bell Test

Since the bits posted by the Beacon are public, these bits 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. To learn more about the NIST Randomness Beacon project, please visit the project's website at: http://beacon.nist.gov.

CONTACT:

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

Wireless and Mobile 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 connection between different wireless technologies. The procedure for conducting such a switch is called a "handover." Media-independent handover (MIH) is a set of services specified in IEEE 802.21 to assist the handover. 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 by a group of wireless nodes, such as smart meters, for balancing the network load and for reliability. In this case, the information may need to be delivered to a group of smart meters using a multicast message, which is used to deliver the information. That is, the message is sent from one point-of-service (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 in the group may need to be removed. Such groups are managed through multicast signals.

Amendment 2 of IEEE 802.21 provides protection mechanisms for unicast messages, that is, mechanisms that protect messages between a PoS and a single mobile node. However, the protection for multicast messages and group management signals is critical. In FY 2014, CSD has worked with IEEE 802.21 to develop security solutions for group management in Task Group D of IEEE 802.21. The solutions, specified in IEEE 802.21 Amendment 4, include the mechanisms to distribute group keys and for the protection of multicast messages. A draft of Amendment 4 has been approved through sponsor ballot. In FY 2015, CSD will continue to contribute to a broader scope of IEEE 802 wireless standards.

CONTACT:

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

VALIDATION PROGRAMS

Federal agencies, industry, and the public rely on many of the standards and specifications supported by NIST's CSD. Poor implementations of these standards or specifications may render a particular product insecure, potentially placing sensitive information at risk. CSD operates several validation programs that help provide a level of assurance that products meet established security requirements and conform to published specifications. To that end, the Security Testing, Validation, and Measurement Group (STVMG) develops test suites and test methods; provides implementation guidance and technical support to industry forums; and conducts education, training, and outreach programs.

STVMG's validation programs work together with independent 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 programs described below validate the implementation under test. The CSD subsequently publishes lists of the validations awarded on public websites.

Cryptographic System Validation

Current validation programs focus on providing a known level of assurance for cryptographic algorithms and modules. These modules 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 that has been provided.

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 the 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

Cryptographic Programs and Laboratory Accreditation

The Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP) were developed in collaboration between NIST and the Communications Security Establishment (CSE) of Canada to support the respective federal user communities for strong, independently tested, and commercially available cryptographic algorithms and modules. Through these programs, NIST and CSE work with international government, public and private sectors as a part of the cryptographic community to achieve standards-based security and assurance of correct implementation. The goal of these programs is to provide federal agencies with a security metric to use in procuring and deploying cryptographic modules and promote the use of validated algorithms and modules by industry and the public. 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 CAVP and CMVP 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 published NIST 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 CSD's cryptography-based work to the end user.

The CAVP and the CMVP are separate collaborative programs. The CAVP and the CMVP validate algorithms and modules, respectively, that are used in a wide variety of products, including Internet browsers, radios, smart cards, space-based communications, munitions, security tokens, mobile phones, network and storage devices, and products supporting the 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 embedded in many products, such as a cryptographic-based 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.

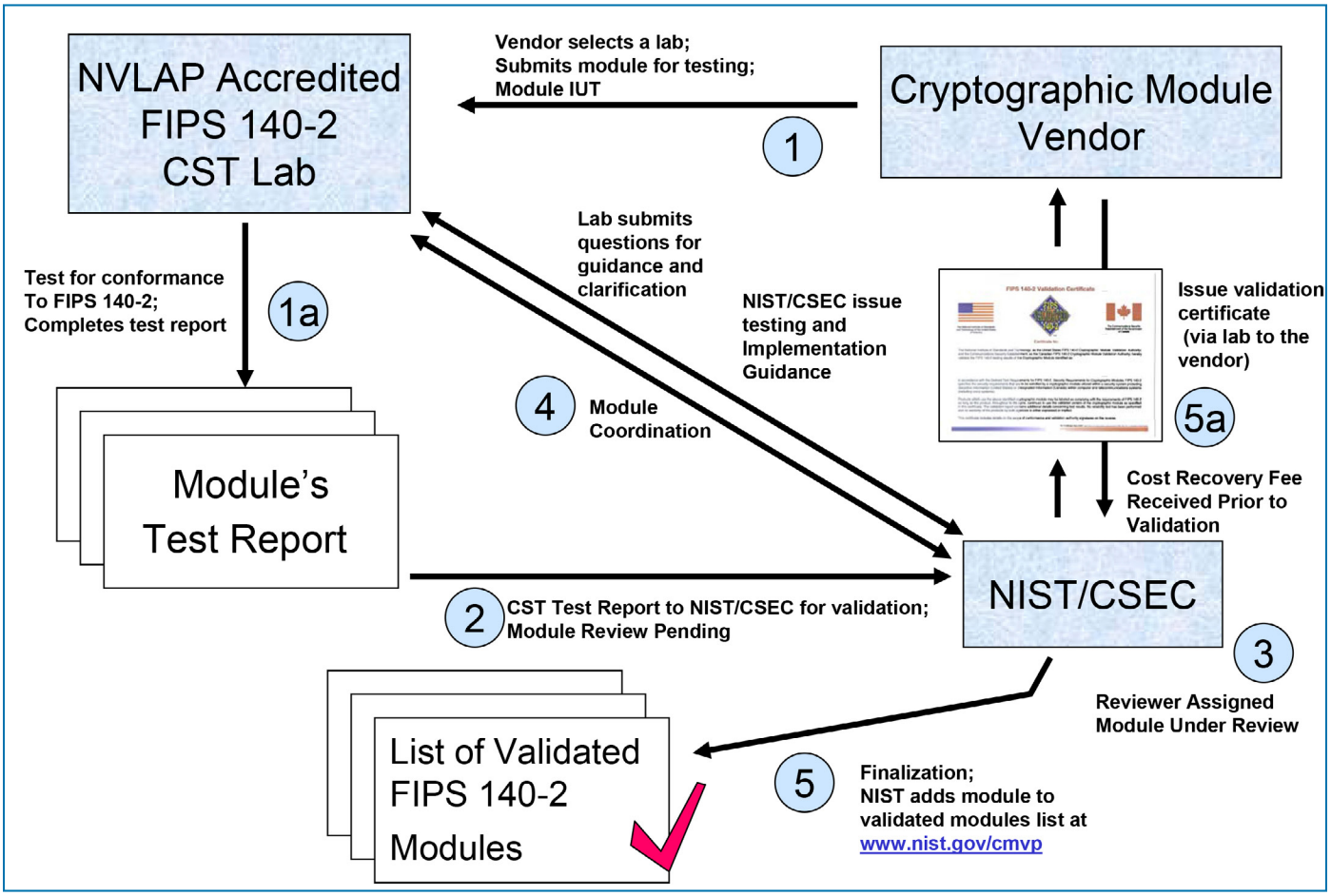


Figure 9: General Flow of FIPS 140-2 Testing and Validation

The CAVP and CMVP validation programs provide documented methodologies for conformance testing through defined sets of security requirements. For the CAVP, the validation system documents are designed for each FIPS-approved and NIST-recommended cryptographic algorithm. See the website for a listing (see http://csrc.nist.gov/groups/STM/cavp/). 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, Security Requirements for Cryptographic Modules* (DTR). The four Annexes to FIPS 140-2 reference the underlying cryptographic algorithm standards or methods. The CMVP-developed *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Validation Program* (IG) provides programmatic and implementation guidance across all of the referenced documents. The information provided in the DTR and IG documents ensures the repeatability of tests and the equivalency in results across the testing laboratories. The Implementation Guidance provides clarity, consistency of interpretation, and insight for successful conformance testing, validation, and revalidation.

The unique position of the validation programs gives the CAVP and 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 current and future standards and tools development.

The CMVP reviews the cryptographic module validation requests from the testing laboratories and, as a byproduct of the review, is attentive to emerging and/or changing technologies. These insights into the evolution of operating environments and complex systems allow, the CMVP to perform research and development on evolving test metrics and methods and future requirements for cryptographic modules. This research is used to assist developers of cryptographic modules, testing laboratories, and the user community when developing new standards.

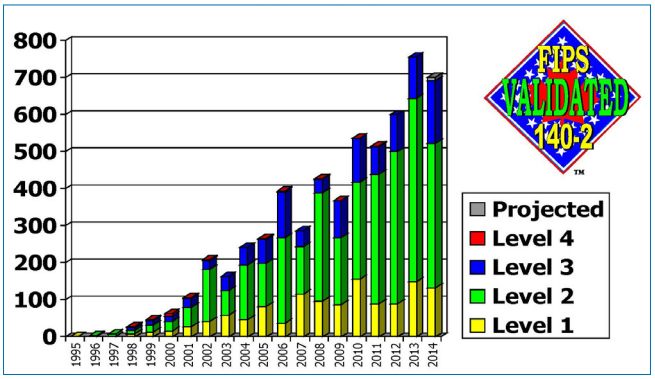


Figure 10: FIPS 140-1 and FIPS 140-2 Validated Modules by Calendar Year and Level

The CAVP and the CMVP have stimulated improved quality and security assurance of cryptographic algorithm implementations and modules. The latest set of statistics, which are collected quarterly from each of the testing laboratories, shows that 5 % (dropped from 7 % in FY 2013) of the cryptographic algorithms and 54 % (increased from 35 % in FY 2013) of the cryptographic modules brought in for voluntary testing had security flaws that were corrected during testing. By the end of FY 2014, the CMVP had validated and issued a total of 2258 cryptographic module validation certificates that represent 5785 modules. These modules have been developed by more than 475 domestic and international vendors. Likewise, to date, the CAVP has issued approximately 15 963 validations, representing the algorithm validations of approximately 17 approved algorithms.

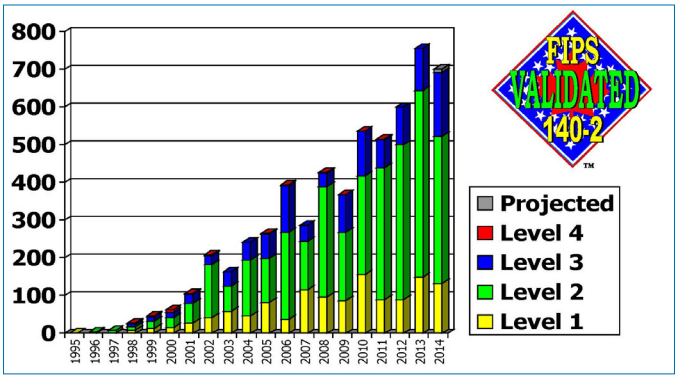


Figure 11: FIPS 140-1 and FIPS 140-2 Validation Certificates by Fiscal Year and Level

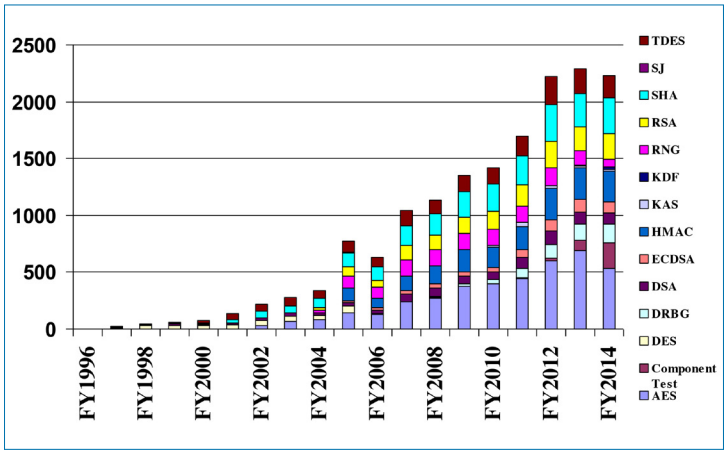


Figure 12: CAVP Validation Status by FYs

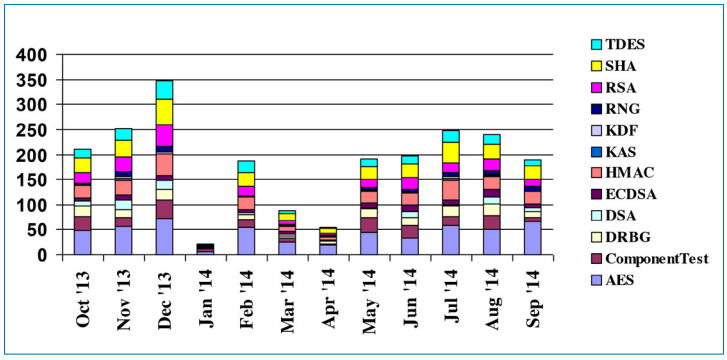


Figure 13: CAVP Validation Status for FY 2014

The CAVP issued approximately 2200 algorithm validations in FY 2014. Included in this total, is the 3000th Advanced Encryption Standard (AES) validation, a significant milestone for the CAVP. The CMVP issued 191 module validation certificates in FY 2014. 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:
Dr. Apostol Vassilev
(301) 975-3221
apostol.vassilev@nist.gov

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

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	1	54	31	0	14	115	0	0	108	80	122	2	102	**774**
FY2006	131	1	3	33	0	19	87	0	0	91	63	120	1	83	**632**
FY2007	238	5	0	63	0	35	127	0	0	137	130	171	1	136	**1043**
FY2008	271	7	0	77	4	41	158	0	0	137	129	191	0	122	**1137**
FY2009	373	2	0	71	23	33	193	6	0	142	143	224	1	138	**1349**
FY2010	399	2	0	70	31	39	179	12	0	150	155	239	0	142	**1418**
FY2011	440	11	0	102	79	68	201	34	0	148	183	255	0	177	**1698**
FY2012	599	24	0	121	122	92	283	20	3	157	231	323	1	248	**2224**
FY2013	691	88	0	106	145	113	276	12	9	132	208	293	0	217	**2290**
FY2014	535	223	0	95	167	96	276	14	23	63	225	314	0	195	**2226**
Total	**4000**	**364**	**331**	**882**	**571**	**550**	**1895**	**98**	**35**	**1293**	**1569**	**2516**	**19**	**1840**	**15963**

Figure 14: CAVP Validated Implementation Actual Numbers

Automated Security Testing and Test Suite Development

The Cryptographic Algorithm Validation Program (CAVP), a collaborative program between NIST and the Communications Security Establishment (CSE) of Canada, utilizes the requirements and specifications of NIST standards (i.e., FIPS and Special Publications), to develop algorithm validation test suites and automated security testing. The CAVP is responsible for providing assurance that the cryptographic algorithm implementations contained in cryptographic modules are implemented according to the specifications in the standards. The CAVP accomplishes this by designing and developing conformance testing specific to each cryptographic algorithm.

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

The cryptographic algorithm validation tests designed and developed by the CAVP are performed by independent third-party laboratories accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). The laboratory works with vendors to validate their cryptographic algorithm implementations. The suite of validation tests for each algorithm ensures the repeatability of tests and the equivalency in results across the testing laboratories.

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. Negative testing is also performed by supplying known incorrect values to assure that the implementation recognizes values that are not allowed. The Monte Carlo Test is designed to exercise the entire implementation under test (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, the CTG has expanded its publications to not only contain the algorithm's specifications, but also to include requirements on an algorithm's use. Many of these usage requirements do not fall within the scope of the CAVP because the CAVP focuses on the correctness of the instructions within the algorithm's boundary. If these additional algorithm usage requirements are not considered applicable to the algorithm's implementation, they cannot be tested at the algorithm level by the CAVP, but may be tested by the Cryptographic Module Validation Program (CMVP) if the requirements are considered applicable to the cryptographic module. However, some of these usage requirements may be considered to be outside the scope of both the algorithm implementation and cryptographic module. In this latter case, 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, *Recommendation for Block Cipher Modes of Operation–Methods and Techniques*
Digital Signature Standard (DSS)	FIPS 186-2, *Digital Signature Standard (DSS), with change notice 1*
	FIPS 186-4, *Digital Signature Standard (DSS)*
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-2, *Digital Signature Standard (DSS), with change notice 1* and ANS X9.62
	FIPS 186-4, *Digital Signature Standard (DSS),* and ANS 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),* 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)*
Random number generator (RNG) algorithms	FIPS 186-2 Appendix 3.1 and 3.2; ANS X9.62 Appendix A.4
Deterministic Random Bit Generators (DRBG)	SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

Cryptographic Algorithm/Component	Special Publication or FIPS
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*
XTS Mode of Operation	SP 800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*
Key Wrapping	SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*
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, Key Derivation Functions for Key Agreement Schemes: All sections except Section 5.8
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*
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*
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),* and ANS 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),* 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 2015, 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; and
- 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 by providing ISO-equivalent standards representing NIST FIPS 140-2, *Security Requirements for Cryptographic Modules* and *Derived Test Requirements [DTR] for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*.

ISO/IEC JTC 1/SC 27 WG 3 completed and published revisions of ISO/IEC 19790:2006 and ISO/IEC 24759:2008, for which Randall J. Easter of NIST's CSD was the principal editor. The revision of ISO/IEC 19790 was published on August 15, 2012. The revision of ISO/IEC 24759 was published on January 31, 2014. Both ISO/IEC standards were also adopted by the American National Standards Institute (ANSI). The two ISO/IEC revisions were developed with international support and the collaboration of governments, industry and academia. The NIST CMVP and the NVLAP-accredited testing laboratories worked closely with ISO in the standards revision.

ISO/IEC 19790:2012 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. This international standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life-protecting data, personal identity information, and sensitive information used by a government) and a diversity of application environments (e.g. a guarded facility, an office,

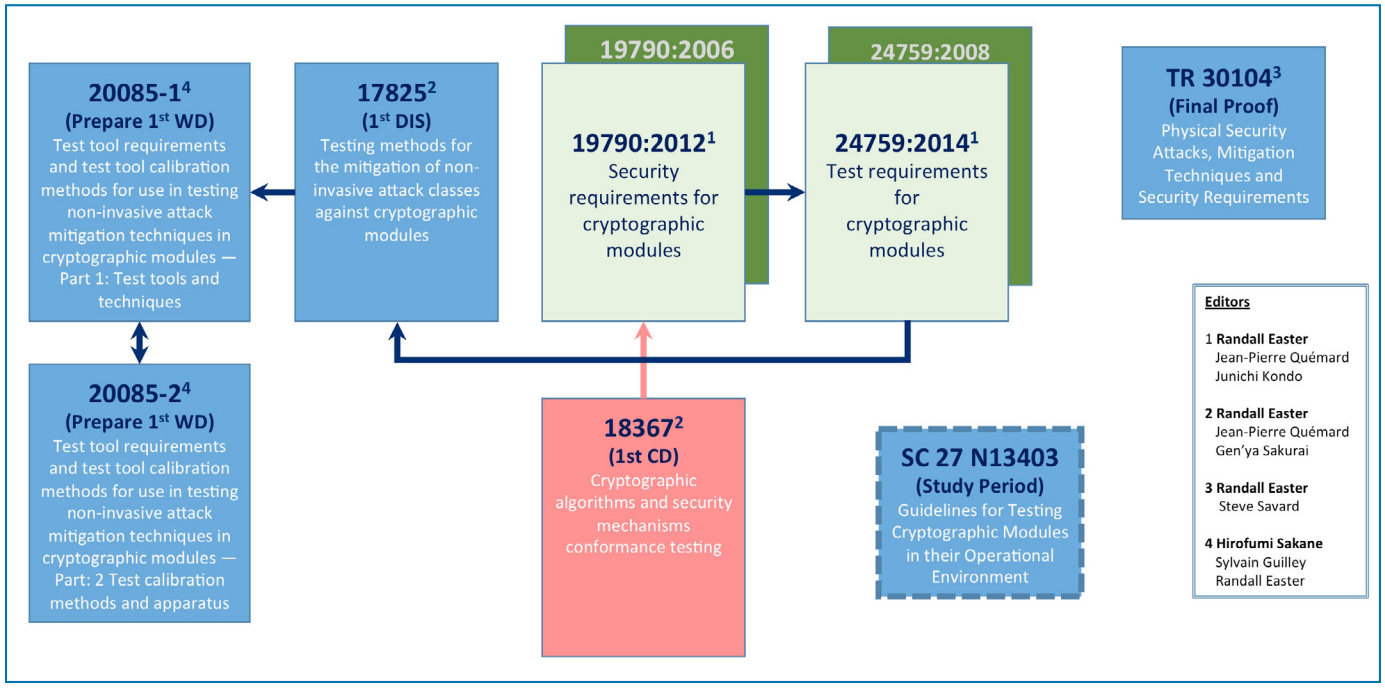


Figure 15: Cryptographic Module Testing – ISO Standards

removable media, and a completely unprotected location). The overall security rating of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilized and for the security services that the module is to provide.

The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; the operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

CSD's Randall J. Easter is the principal editor of the following draft ISO/IEC documents:

- ISO/IEC 17825, *Testing methods for the mitigation of non-invasive attack classes against cryptographic modules;*
- ISO/IEC 18367, *Cryptographic algorithms and security mechanisms conformance testing;* and
- ISO/IEC TS 30104, *Physical Security Attacks, Mitigation Techniques and Security Requirements.*

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. Randy Easter
(301) 975-4641
randall.easter@nist.gov

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 collection of eleven individual specifications that work together to support various use

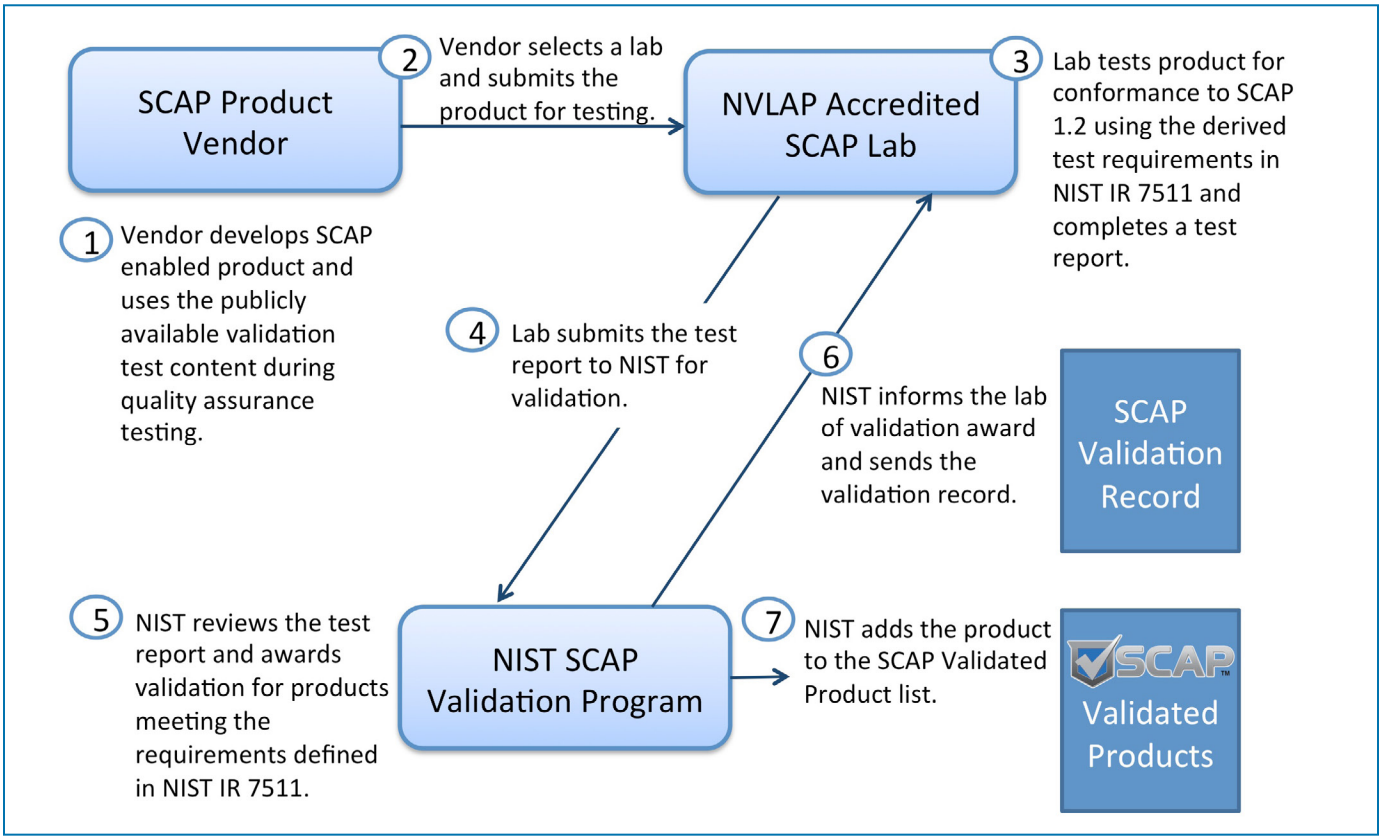


Figure 16: SCAP 1.2 Validation Process

cases. A single error in product implementation could result in undetected vulnerabilities or policy noncompliance within an organization's networks.

The test requirements for SCAP 1.2 are defined in NISTIR 7511 Revision 3, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements.* In general, vendors may opt for product validation for one or more SCAP capabilities or operating systems. Currently, the program offers testing on Microsoft Windows and Red Hat Enterprise Linux platforms. The validation process starts when a vendor voluntarily submits an SCAP-enabled product to a NVLAP-accredited laboratory. Once the lab completes product testing, and all validation requirements are met, the lab submits a test report to the SCAP Validation Program for review. NIST reviews the test report and will award a validation if all requirements have been met. Once a validation is awarded, the SCAP Validation Record is sent to the lab, and the newly validated product is posted on the SCAP Validated Products web page.

The SCAP Validation Program resources web page (http://scap.nist.gov/validation) was introduced in FY 2013, and was updated in FY 2014 to provide the public with a centralized location for all resources and information necessary for preparing products for SCAP 1.2 validation. Resources include documentation, a list of Frequently Asked Questions (FAQ), the SCAP validation-test content, and tools for validating and processing SCAP data streams. The SCAP validation-test content should be used by vendors for quality assurance testing prior to entering formal SCAP testing with an NVLAP accredited laboratory. The open-source tools that are available for download may be used by SCAP content authors for testing SCAP source content. The SCAP Content Validation Tool (SCAPVal) may be used to determine if the content conforms to the SCAP specification. Open-source SCAP reference implementation tools, such as the SCAP Reference Implementation Tool, may be used to process SCAP data streams.

End users may use information on the SCAP Validation web page to learn about SCAP validation and find products that have been awarded validations. The validation records that are posted on the SCAP Validated Products page state the product version that was tested in the laboratory, along with details about the validation, such as the tested platforms, SCAP capabilities, the validation test suite version, and the lab that performed the product test.

In FY 2014, five products successfully completed testing and were awarded validations. Several products are in various stages of validation testing and are expected to be awarded validations in FY 2015. The current list of SCAP 1.2 validated products may be found on the SCAP Validated Products list at https://nvd.nist.gov/SCAP-Validated-Tools/.

In FY 2015, the SCAP Validation Program plans to provide enhanced testing support and will focus on validation test content for new operating systems. 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

IDENTITY MANAGEMENT

Personal Identity Verification (PIV) and FIPS 201 Revision Efforts

Figure 17: Government Employees Use PIV Cards for Facility Access

In response to Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors,* 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 2014 directly supported the recently revised FIPS 201-2 by updating the relevant publications associated with FIPS 201-2 and by developing two new publications. CSD performed the following activities during FY 2014 in support of HSPD-12:

- Published Draft NISTIR 7863, *Cardholder Authentication for the PIV Digital Signature Key*. The document provides clarification for the requirement in FIPS 201-2 that a PIV cardholder perform an explicit user action prior to each use of the digital signature key stored on the card.
- Published two new draft documents to accommodate e-authentication with mobile devices:
  - Draft SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, defines the technical details for implementing and deploying derived PIV credentials on mobile devices, such as smart phones and tablets. As intended by FIPS 201-2, a derived PIV credential is a PIV credential that can be provisioned directly to a mobile device to enable remote enterprise access from the device.
  - Draft NISTIR 7981, *Mobile, PIV, and Authentication,* analyzes and summarizes various current and near-term options for remote authentication with mobile devices that leverage both the investment in the PIV infrastructure and the unique security capabilities of mobile devices.
- Completed the comment resolution of Draft SP 800-73-4, *Interfaces for Personal Identity Verification*, and published a revised draft. The three-part SP details the new PIV Card capabilities introduced in FIPS 201-2, including a Virtual Contact Interface (VCI), a secure channel protocol, an on-card biometric comparison mechanism and an enforcement of a minimum PIN length of six digits.
- Completed the comment resolution of Draft SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* and published a revised draft. The document has been modified to align with Draft SP 800-73-4, 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.
- Published Draft SP 800-79, *Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCIs)*. The draft document incorporates changes required by FIPS 201-2, including a new set of issuer controls for Derived PIV Credentials Issuers.
- Prepared Draft SP 800-85A-4, *PIV Card Application and Middleware Interface Test Guidelines,* and published Draft SP 800-85B-4, *PIV Data Model Test Guidelines*, in order to align these documents with FIPS 201-2, SP 800-73-4, and SP 800-78-4.
- As the NIST PIV Validation Authority, completed the transition phase from FIPS 201-1 to FIPS 201-2 for validated PIV Card Applications and PIV Middleware.
- Created additional sets of test cards for the inventory of PIV test cards. These test cards are available for purchase and facilitate the development of applications and middleware that support the PIV card (see http://csrc.nist.gov/groups/SNS/piv/testcards.html).

In FY 2015, CSD will continue to focus on updating the relevant publications associated with FIPS 201-2, including developing two new publications: SP 800-156, *Representation of PIV Chain-of-Trust for Import and Export,* and SP 800-166, *Guidelines for Testing Derived Personal Identity Verification (PIV) Credentials.* 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

NIST Personal Identity Verification Program (NPIVP) & Revisions to FIPS 201-2 Companion Documents

The objective of the NIST Personal Identity Verification Program (NPIVP) is to validate PIV components for conformance to the specifications in FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, and its companion documents. The two PIV components that come under the scope of NPIVP are the PIV Smart Card Application and the PIV Middleware. NPIVP test facilities that perform the two types of tests are the Cryptographic and Security Testing (CST) Laboratories that have been accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). As of September 2014, there were nine such facilities.

The interface specifications for the PIV Smart Card Application and PIV Middleware are found in a FIPS 201-associated document, namely, SP 800-73 (the latest published version SP 800-73-3) - *Interfaces for Personal Identity Verification*. The conformance tests for these specifications are detailed in SP 800-85A (the latest published version is SP 800-85A-2) - *PIV Card Application and Middleware Interface Test Guidelines.* To implement these tests and to generate conformance test reports, CSD also developed an integrated toolkit called "PIV Interface Test Runner," which conducts tests on both PIV Card Application and PIV Middleware products, and provides the toolkit to accredited NPIVP test facilities.

In 2014, CSD's activity focused on the transitioning of PIV Card Application and PIV Middleware products from FIPS 201-1 to FIPS 201-2 compliance. Coordinating with the test facilities, FIPS 201-1 products were identified and placed on the Removed Products List (RPL). Nine PIV card application products and fifteen PIV middleware products were affected. With this change, there are 27 NPIVP validated PIV card application products, and five PIV Middleware products listed.

In addition, NPIVP is closely involved in ensuring that all changes in PIV companion documents, such as SP 800-73-4, SP 800-76-2, *Biometric Specifications for Personal Identity Verification*, and SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* are fully reflected in the updated versions of the conformance test documents, SP 800-85A and SP 800-85B, as well as in the "PIV Interface Test Runner" toolkit. Currently, the NPIVP team is guiding the development of the "PIV Interface Test Runner" toolkit for validating PIV Card application and PIV Middleware products for conformance to the specifications in SP 800-73-4, SP 800-76-2 and SP 800-78-4.

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

RESEARCH IN EMERGING TECHNOLOGIES

Cloud Computing and Virtualization

The model for Cloud Computing is defined in SP 800-145, *The NIST Definition of Cloud Computing*. The foundational technology that facilitates 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 an abstraction of the hardware (e.g., CPU, memory) that enables 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's CSD is working in parallel on several projects (introduced below) that aim to accelerate the Federal Government's adoption of secure cloud computing by collaborating with standards bodies, and public and private sectors 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 United States Government's (USG) 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. Activities included the following:

- Led the development of the draft SP 500-299, *NIST Cloud Computing Security Reference Architecture (SRA)*. 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 (CRMF). The SRA is a security overlay to SP 500-292, *NIST Cloud Computing Reference Architecture*. During FY 2014, the draft document was completed, posted for public comments, and the received comments were addressed.
- Co-led the development of the NISTIR 8006, *Cloud Forensics Challenges*.

- Led the development of an internal draft document, *Cloud-adapted Risk Management Framework: Guide for Applying the Risk Management Framework to Cloud-based Federal Information Systems*. The document introduces a cloud customer-centric approach to applying the risk management framework to cloud-based information systems. This internal draft has not yet been released for public comment; it is currently planned for future publication in the NIST SP 800 series.
- Led the research and development of the data that constitutes the foundation of an internal draft document, *Security and Privacy Controls for Cloud-based Federal Information Systems*. The document will provide a cloud overlay of NIST SP 800-53 Revision 4 security controls for cloud-based ecosystems. This internal draft has not yet been released for public comment; it is currently planned for future publication in the NIST SP 800 series.

CSD staff members:

- Organized and contributed to the seventh NIST Cloud Computing Forum and Workshop: *The Intersection of Cloud and Mobility Forum*, March 25-27, 2014; and,
- Organized and contributed to the first *NIST Cloud Computing Forensic Science Workshop*, March 24, 2014.

In support of USG cloud-computing mandates, CSD staff members provided leadership for several public cloud working groups operating under the NIST Cloud Computing Program. These working groups focus on meeting the high priority requirements contained in SP 500-293, *U.S. Government Cloud Computing Technology Roadmap.*

CSD staff chaired or co-chaired several significant cloud computing efforts in 2014:

- Co-Chaired the NIST Cloud Computing Security Working Group. Led the group on the development of the SP 500-299, *NIST Cloud Computing Security Reference Architecture;* SP 800-163, *Cloud-adapted Risk Management Framework: Guide for Applying the Risk Management Framework to Cloud-based Federal Information Systems;* SP 800-174, *Security and Privacy Controls for Cloud-based Federal Information Systems* (all three described above); and on researching cryptographic key-management challenges in cloud ecosystems.
- Co-Chaired the NIST Cloud Computing Forensic Science Working Group. Led the development of NISTIR 8006, *NIST Cloud Computing Forensics Challenges.*
- Co-Chaired the NIST Cloud Computing Interoperability and Portability Working Group. Addressed issues facing cloud computing with respect to interoperability and portability, standards, and common and functional terminologies. The goal is to develop guidance and best practices for cloud-computing interoperability and portability that best enable business necessities, such as the ability to exchange, use and reuse information/data in a cloud environment.
- Co-editor for ISO/IEC AWI 19941 *Information technology – Cloud computing – Interoperability and Portability.* This is an effort to develop a standard that focuses on defining the types of cloud-computing interoperability and portability; the relationship and interactions between interoperability and portability; the contexts where interoperability and portability are relevant in cloud computing, with respect to the cloud-computing reference architecture; and the common terminology and concepts used to describe interoperability and portability, particularly as they relate to cloud services.
- Chair and Vice-Chair of INCITS CS1 (Cybersecurity) – U.S. Technical Advisory Group (TAG) to the ISO/IEC international committee JTC1/SC27 (IT Security Techniques). This group is concerned with the development of cloud-computing taxonomy-related standards and cloud computing security standards.

CSD staff members participated 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 publication of *ISO/IEC 17788 – Information Technology – Cloud computing – Overview and Vocabulary*, and *ISO/IEC 17789 Information technology – Cloud computing – Reference Architecture.* These standards are a joint collaborative work between ITU-T and ISO, and they are approved to be available at no charge. 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.*

There are three new standards under development:

- ISO/IEC 19086 Information Technology - *Cloud Computing - Service Level Agreement (SLA) Framework.* This international standard has three parts, where Part 1 specifies an overview of SLAs for cloud services, identification of the relationship between the master service agreement and the SLA, SLA concepts and requirements that can be used to build SLAs, and terms

and metrics commonly used in SLAs for cloud services. This standard is for the benefit and use of both the provider and customer. Part 2 specifies a model and metrics for describing and measuring properties of the concepts and components in 19086. This standard is for the benefit and use of both the provider and customer, and Part 3 specifies core conformance requirements for SLAs for cloud services for ISO/IEC 19086.

- ISO/IEC 19941 *Information Technology - Cloud Computing – Interoperability and Portability.* This international standard specifies cloud-computing interoperability and portability types; the relationship and interactions between these two aspects; and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services.
- ISO/IEC 19944 I*nformation Technology - Cloud Computing - Data and their Flow across Devices and Cloud Services.* This International Standard defines the reference architecture for mobile-to-cloud ecosystems, while providing the necessary structure that allows for data-flow transparency between portable devices and the cloud services ecosystem.

CSD staff members are also actively participating in the development of cloud-computing security standards, primarily through INCITS CS1, SC 27, which is responsible for cloud-computing security standards for ISO. CSD has provided technical contributions based on SP 500-299 and continues to advocate for secure, non-proprietary solutions. There is a continued contribution to a number of cloud-related standards, including the recently approved international standard, ISO/IEC 27018, *Information technology – Security techniques – Code of practice for protection of personal identifiable information (PII) in public clouds acting as PII processors,* ISO/IEC WD 27036-4, *Information technology – Information security for supplier relationships – Part 4: Guidelines for security of Cloud services,* and the commencement of a study period on cloud components, controls and capabilities.

In FY 2014, the CSD members of the NIST cloud-computing team continued research in key areas of cloud security, cloud interoperability and portability, cloud metrics, cloud services, and cloud SLAs. They also presented the results of cloud-computing research and development, introduced the standards and specifications under development, and provided the status of the NIST Cloud-Computing Program in a variety of domestic and international conferences and workshops. CSD staff continues to engage industry and federal agencies for inputs and collaborative work through working groups, publications, and networking.

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:

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
2014 Chair, INCITS CS1 (Cybersecurity) - U.S. Technical Advisory Group (TAG) to the ISO/IEC international committee JTC1/SC27 (IT Security Techniques)
(For 2015 – contact Mr. Salvatore Francomacaro – contact information below)

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

Policy Machine – Leveraging Access Control for Cloud Computing

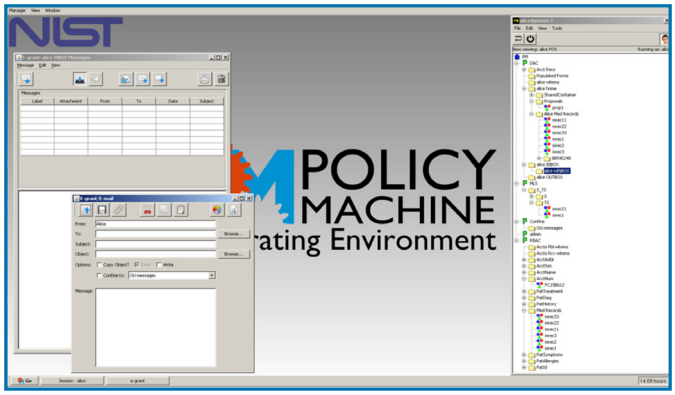


Figure 18: Policy Machine Operating Environment

In FY 2014, CSD continued the research and development of a virtualization-based, enterprise-wide controlled delivery of data services for advanced cloud computing through Access Control. This included the publication of a detailed Policy Machine specification as NISTIR 7987, *Policy Machine: Features, Architecture, and Specification*, in May 2014. The team also published a description of the benefits and an approach of the Policy Machine's integration of Access Control and Data Services as a conference paper, *On the Unification of Access Control and Data Service*, in the proceedings of the IEEE 15th International Conference of Information Reuse and Integration, August 2014. In addition, CSD released its reference implementation of the Policy Machine as open source (available at GitHub).

NIST and other members of an Ad Hoc INCITS working group are developing a three-part Policy Machine 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;* and
- Project 2195–D: *Next Generation Access Control – Generic Operations & Abstract Data Structures.*

The Policy Machine's architecture was the basis for the NGAC work within INCITS. An initial standard from this work was published in 2013 and is now available from the ANSI e-standards store as INCITS 499 – *NGAC Functional Architecture (NGAC–FA).* The standard resulting from Project 2195–D: *NGAC Generic Operations & Abstract Data Structures (NGAC-GOADS),* has begun the approval process, and is expected to reach the second Public Review stage in the summer of 2015.

In FY 2015, CSD plans to issue a new version of its open-source distribution to reflect new features and enhanced performance, and publish a NISTIR 7987 revision to reflect greater consistence with NGAC's suite of standards.

http://csrc.nist.gov/pm/

CONTACTS:

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

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

Virtualization Security & Leveraging Virtualization for Security

In FY 2014, CSD continued its research in key areas of cloud and virtualization security by producing two conference papers and one SP:

- **Conference Papers:** *"Analysis of Protection Options for Virtualized Infrastructures in Infrastructure as a Service Cloud "* and *"Deployment-driven Security Configuration for Virtual Networks;"* and
- **Special Publication:** SP 800-125A, *Security Recommendations for Hypervisor Deployment (*submitted for public comment).

The focus of research for FY 2015 in the area of Virtualized Infrastructures is two-pronged. The first approach will focus on identifying the security requirements for various use cases involved in offering cloud services using virtualized infrastructures and analyzing the protection options to meet those security requirements in terms of their features, security strengths and architectural foundation. The second approach will focus on deriving secure configuration operations in a specific area of virtualized infrastructure – t*he Virtual Network* – leveraging state-of-the-art architectural paradigms, such as the Software-defined network (SDN). The security recommendations for Hypervisor deployment will cover two areas: one based on architectural choices, and the other based on configuration parameters. For developing the configuration parameters that form the basis of security recommendations, the following approach will be adopted:

- The baseline functions of the hypervisor will be identified along with their associated interfaces and threat sources; and

- The protection measures against those threats will then form the security recommendations for hypervisor deployment. The security recommendations will cover all known implementations of baseline functions, making them applicable across multiple hypervisor designs.

CONTACT:

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

MOBILE 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 e-commerce, 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 businesses 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 adopted to allow government users to employ the latest technologies that consumers can use without sacrificing privacy and security.

NIST is conducting research in software-assurance methodologies for smart phone software (i.e., applications, commonly referred to as "apps") and is working with other government agencies and industry to bridge the security gaps present with today's smart phones. For example, NIST developed an app-vetting system and framework for managing an organization's app-vetting process with respect to the organization's security and privacy policies and requirements. This system was used by the Defense Advanced Research Projects Agency (DARPA) to vet apps prior to being deployed on thousands of military mobile devices for use in the current U.S. war theater, the 2013 Presidential Inauguration, and the 2014 Boston Marathon.

NIST's work in mobile security has earned the 2014 Government Computer News (GCN) award for Information Technology Excellence and the 2013 U.S. Department of Commerce Gold Medal Award. For FY 2015, NIST will continue to develop and transition mobile security-related technologies, publish guidance on issues of mobile security, and provide mobile security expertise to industry and other government agencies.

CONTACTS:

Dr. Steve Quirolgico
(301) 975-8426
steveq@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 the 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 (USG). 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 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.

Additional OMB IPv6 requirements were mandated for FY 2014. Agencies were required to "upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use IPv6 by the end of FY 2014." NIST developed 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 2015, NIST will continue to manage and evolve the USGv6 Test Program and to help federal agencies fulfill OMB mandates and monitor compliance to those mandates. 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 2014, the following research was accomplished for this project:

- Enhanced the unified enforcement mechanism of data services for use by a Policy Machine (PM) for an enterprise computing environment;
- Enhanced the capabilities of the Access Control Policy Tool (ACPT);
- Implemented a fault-detection method for an access control rule using Simulated Logic Circuit algorithms;
- Studied formal Attribute-Based Access Control (ABAC) models;
- Published the SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations,* which provides information for function components, as well as an enterprise consideration of ABAC;
- Studied an Access Control scheme for Big Data Processing; and
- Studied an assurance mechanism for ABAC attributes.

In FY 2015, CSD will continue the above research, and present the most updated results in CSD's CSRC website. 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 for 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; and
- Provide accurate and efficient fault detection and correction technology for implementing access control rules and policies.

See Figure 19 on next page for chart of 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

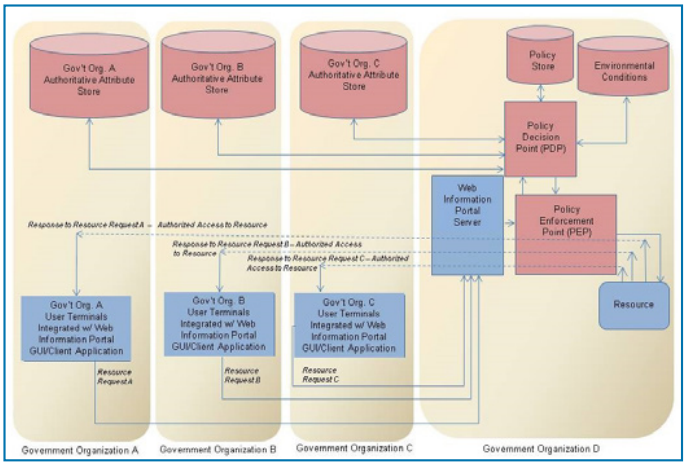


Figure 19: Access Control and Privilege Management

Conformance Verification for Access-Control Policies

To formally and precisely capture the security properties that access control (AC) 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 a reference for design and implementation of security requirements. Techniques are required for verifying whether an access-control model is correctly expressed in the access-control policies and whether the properties are satisfied in the model.

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 when faults were found, those methods provide no information about the source of 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. 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 fix 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 to 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 2014, CSD accomplished the following:

- Researched the ACRLCS, and implemented a prototype access control rule composing system - the Access Control Rule Logic Circuit Simulation System;
- Worked with industrial and academic organizations in exploring new capabilities that helped to improve the usability of the AC tools (ACPT and ACRLCS);
- Enhanced the capability of ACPT by improving user interfaces and adding privilege inheritance and multiple policy combination algorithms;
- Performed prototype testing; and
- ACPT was downloaded by 277 users and organizations.

In FY 2015, CSD is planning to conduct further research on the new capabilities and enhance performance of the ACPT and ACRLCS.

Figure 20: Conformance Verification

This project is expected to:

- Provide a 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 the Attribute Based, Multilevel, and Workflow models;
- Provide tools or services for checking the security and safety of an 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 testing (such as an access control system);
- 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; and
- Provide new methods for composing standard mandatory AC models, such as Role-Based Access Control (RBAC) and Multi-Level Security (MLS), as well as some fundamental security properties.

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

Attribute-Based Access Control

Attribute-Based Access Control (ABAC) is a logical access control methodology where an authorization to perform a set of operations is determined by evaluating the 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 addition to the core concept (i.e. definition and consideration), ABAC research includes technologies such as attribute assurance, attribute engineering/management, identity system integration, attribute federation, situational awareness (real time or contextual) mechanism, policy management, and natural-language policy translation to digital policy.

In FY 2014, CSD published 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 an 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 that will describe a variety of characteristics and applications of ABAC formal models. CSD also started research on the Attribute Assurance of ABAC in partnership with the National Security Agency (NSA), the National Strategy for Trusted Identities in Cyberspace (NSTIC), and the National Cybersecurity Center of Excellence (NCCoE); CSD developed a white paper based on the mechanism for defining the levels of assurance of ABAC attributes, as well as collecting use cases, current standards, and engineering experiences through a Request for Information (RFI) and working with ABAC user/commercial product communities.

In FY 2015, CSD will continue the research of ABAC formal models, as well as details and extended topics of ABAC capabilities, such as Attribute Assurance, ABAC implementation examples, and ABAC standards. The ABAC project will pursue the following objectives:

- Provide readers with the terminology and a 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 the 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; and
- Promote the adoption of ABAC for a more secure and flexible method for information sharing in a standalone or enterprise environment.

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

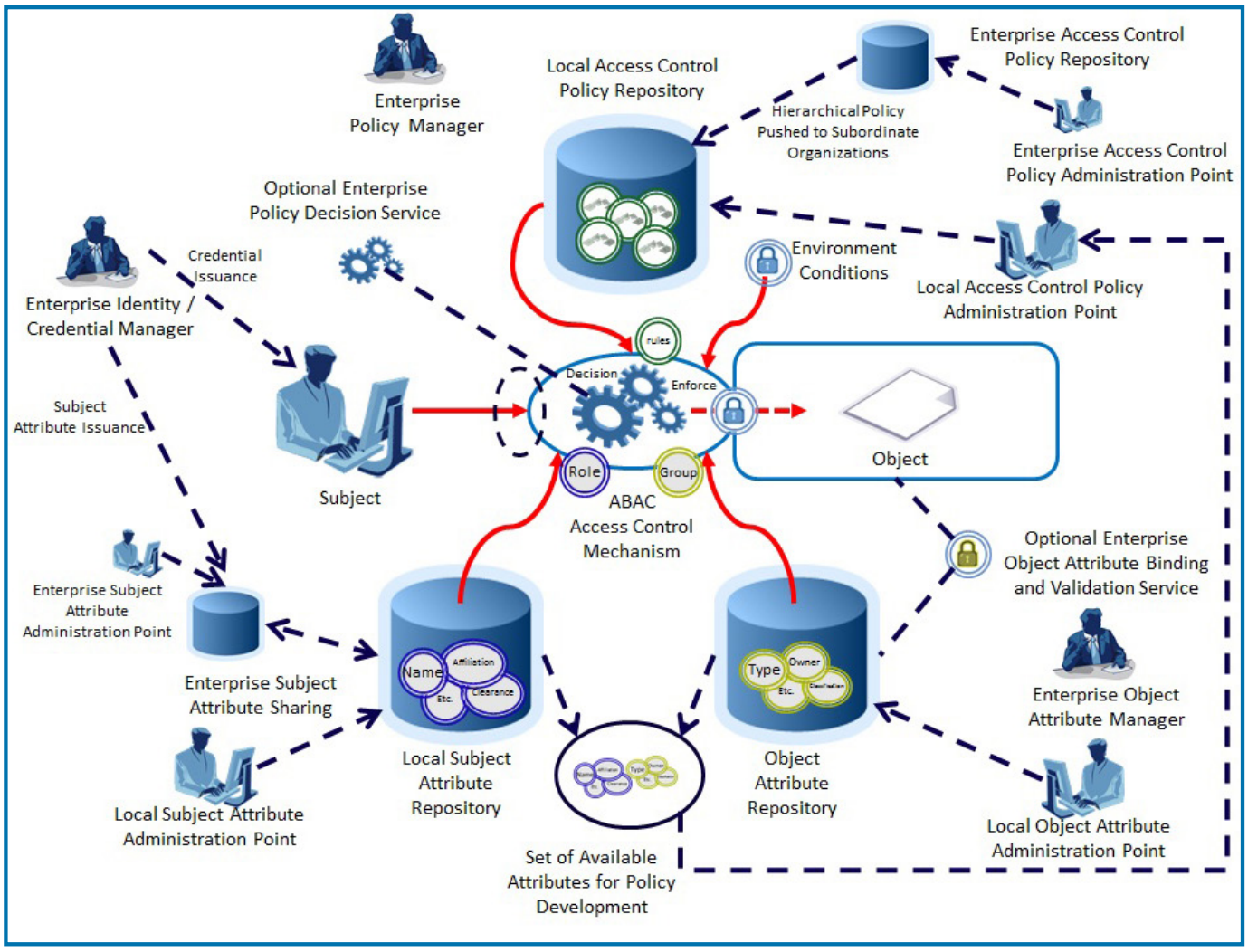


Figure 21: ABAC Access Control Mechanism Chart

ADVANCED SECURITY TESTING AND MEASUREMENTS

Security Automation and Continuous Monitoring

IT organizations operate a diverse set of computing assets that 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; and
- 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 allows 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 developers and implementers. Through close work with partners in government, industry, and academia, NIST CSD continues to facilitate the definition and development of security automation approaches that enable organizations to understand and manage IT security risks.

During FY 2014, CSD worked to build on previous security automation work by:

- Participating in 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; and
- The development and maintenance of tools and reference implementations.

CSD 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 the 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 the 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 the 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: the evolution and international adoption of the Security Content Automation Protocol (SCAP), and the 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 a 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, CSD 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. See Table on next page.

Since the release of SCAP 1.2, CSD has worked to improve guidance around the SCAP specifications by promoting a broader international adoption of SCAP, encouraging the integration of SCAP into other standards, and by adapting SCAP to address specific gaps and challenges. The sections describe work activities performed during FY 2014.

CSD has continued its collaboration with industry partners in the IETF Security Automation and Continuous Monitoring (SACM) working group. This working group provides a venue for advancing appropriate SCAP specifications into international standards and addressing identified gap areas. 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 a device state against the expected values and standards for interacting with repositories of security-automation content. Over the past twelve months, the SACM working group has been working 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.

The working group has been developing the following Internet drafts:

INTERNET DRAFT	PURPOSE
https://datatracker.ietf.org/doc/draft-ietf-sacm-terminology/	Definition of the common terminology used within a number of working-group documents.
https://datatracker.ietf.org/doc/draft-ietf-sacm-use-cases/	Description of use cases and related capabilities to guide the development of requirements, architecture, and specifications for data models and transports.
https://datatracker.ietf.org/doc/draft-ietf-sacm-requirements/	Listing architectural and specification requirements for SACM specifications.

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

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

Additionally, CSD 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 defines a mechanism for software publishers to provide authoritative identification, categorization, software relationship (e.g., dependency, bundling, and patch), executable and library footprint details, and other metadata for software that they publish. This information enhances the SCAP use cases by providing authoritative information for the creation of Common Platform Enumeration (CPE) names, the targeting of checklists, and associating software flaws to products based on a defect in a software library or executable.

CSD 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 the 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 the 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, CSD has worked with the Forum of Incident Response and Security Teams (FIRST) by participating in two 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 is currently working on the CVSS revision, which will be released in FY 2015. 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*. Standards that are developed and published by these SDOs will be considered for inclusion in future revisions of SCAP.

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 CSD 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, an 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 with the IETF SACM working group to develop data-model and transport standards to support enterprise continuous monitoring. The CAESARS-FE reference architecture will evolve as consensus is developed within SACM around interoperable, standards-based approaches that enable continuous monitoring of IT systems. CSD is working to complete an update to NISTIR 7756 that provides additional guidance for the 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—The ability to verify that software media is from a trusted publisher and that the integrity of the installation media has been maintained;
- Software-execution whitelisting—The execution environment verifies that the software to be executed, is authorized for execution, and that the executable file(s) and any associated shared libraries have not been tampered with;
- Publication of an installed software inventory—When connected to an authorized network, a device's full or updated software inventory is securely reported to an external configuration-management database that aggregates the software inventory of multiple devices for further analysis; and
- Software inventory-based network access control—Control access to network resources at the time of a connect operation, based on the published, installed-software inventory. Access to network resources can be limited if software is outdated or patches are not installed in accordance with digital policies.

When used together, these capabilities enable the enterprise-wide management of the software that is allowed to be installed and executed. The collected information will also provide software-version information to support license, vulnerability and patch management needs. If historic software-inventory information is maintained, retroactive analysis techniques can be applied on this data to determine historic vulnerable conditions in support of incident-response and recovery processes. Finally, using the collected software inventory, network access can be controlled, enabling the device to be connected to a remediation network, if necessary, so that the appropriate software changes can be made before allowing the device full access to the operational network.

The building-block document, *Continuous Monitoring Building Block: Software Asset Management*, can be viewed at http://nccoe.nist.gov/content/continuous-monitoring. In early FY 2015, the team will publish an update to the building-block document and will begin work with vendors to develop a solutions demonstration. Through this process, CSD provides publicly 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 National Vulnerability Database (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 to provide an 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/).

As of October 2014, the NVD contained the following resources:

- Over 65 000 vulnerability advisories, with an average of 40 new vulnerabilities added daily;
- 56 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 the system state;
- 197 non-SCAP security checklists (e.g., English prose guidance and configuration scripts);
- 248 U.S. Computer Emergency Readiness Team (US-CERT) alerts; 3690 US-CERT vulnerability summaries; and 10 286 SCAP machine-readable software flaw checks;
- A product dictionary with over 97 000 operating system, application, and hardware name entries; and
- 50 038 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 (i.e., mechanisms that provide updated data from data sources) and SCAP-expressed content from the NVD website demonstrates an increased adoption of SCAP.

The 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.

During FY 2014, the NVD infrastructure has been significantly changed to improve responsiveness and availability and to position the NVD for future improvements, which will be coming soon. NVD now hosts the SP 800-53 Revision 4 security controls content and will host the SP 800-53A Revision 4 content when that publication becomes final. NVD data is substantially increasing the security of networks worldwide, and it is a fundamental component of CSD's security automation infrastructure. CSD plans for the NVD in FY 2015 include improvements in the organization and layout of the NVD to assist new users in locating content, the addition of visualization options of the NVD data for security researchers, and an implementation of the forthcoming release of the Common Vulnerability Scoring System (CVSS) version 3 specifications from FIRST.

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 for responding to and recovering from attacks. SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, provides guidance that helps organizations establish and operate a Computer Security Incident Response Team (CSIRT). When an attack has the potential to affect computing systems in multiple organizations, information sharing and coordination among organizations can make it possible to reduce the impact of the 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 each organization may have substantially different capabilities for responding to attacks, diagnosing causes, and handling sensitive incident-related information, guidance is needed to help organizations interoperate despite these organizational differences.

The CSIC initiative is focused on the development of a Special Publication (SP) that provides guidance on how organizations can establish information sharing and coordination capabilities in advance of incidents in order to be prepared to operate swiftly and with coordination during incidents. The guidance covers information sharing architectures; risk-informed incident response capabilities; data privacy and sensitivity; data collection and retention

practices; and the use of open standards for information exchange, redaction, and guidance on how an organization can establish, participate in, and maintain coordination and information-sharing relationships.

The CSIC guidance will help incident responders, network defenders, and operations personnel consider what information could be shared, the circumstances under which sharing is permitted, whom it can be shared with, and how the information should be protected. One of the key objectives of information sharing and coordination is to enable organizations to harness the collective knowledge and experience of their sharing partners to enhance protective measures, speed incident detection, augment analysis capabilities, and enhance containment, eradication, and recovery processes.

In early FY 2015, CSD plans to release a Draft SP that provides guidance for Computer Security Incident Coordination. After the public comment period for the draft, a final version of the publication will be prepared and released later in the fiscal year.

CONTACTS:

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

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

Mr. Christopher Johnson
(301) 975-3247
christopher.johnson@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 the development of security configuration checklists for IT products and to make checklists more organized and usable, NIST's CSD 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 Cybersecurity 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 assist federal agencies with these mandates.

The goals of the NCP are to:

- Facilitate the 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 operation 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; and
- Encourage the use of automation technologies (e.g., SCAP) for checklist application.

There are 253 checklists posted on the website (http://checklists.nist.gov); 120 of the checklists, addressing 48 platforms, are SCAP-expressed and can be used with SCAP-validated products. The majority of the SCAP-expressed checklists have been posted in the past three years, demonstrating continual use and adoption of this automated means of expressing checklist content.

Organizations can use checklists obtained from the NCP website for automated security configuration patch assessment. The 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 these checklists into tiers, from Tier I to Tier IV. The 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 interoperability with SCAP-validated products to the maximum extent possible.

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 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 periodic 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.* It also supports the Core functions of the Cybersecurity Framework, providing USGCB users with settings that protect digital assets and enable detection of suspicious activity.

During FY 2015, the USGCB Program will continue to provide ongoing maintenance of the baseline artifacts and to consider additional applicable platforms.

The USGCB's team email address is: usgcb@nist.gov.

CONTACT:

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

Apple OS X Security Configuration

CSD is working with Apple Incorporated 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). The project team is aggregating 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, the 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:

- The Enterprise baseline is appropriate for centrally managed, networked systems.
- The Small Office Home Office baseline is appropriate for systems that are deployed remotely, but need to connect to enterprise networks.
- The 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 were posted for the Apple community on a periodic basis for public review, discussion, correction and agreement. Each setting has a designated Common Configuration Enumeration (CCE) number, which aids in long-term tracking of the setting. Once these settings are vetted by Apple, the settings will then 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 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 all users of the Apple OS X 10.8 operating system.

During FY 2014, a majority of all proposed settings were scripted. The corresponding spreadsheet batches have been sent to Apple for feedback; approximately 230 settings are now completed. Settings have also been implemented on OS X 10.9, when possible. Work on the draft guideline, *Guide to Securing Apple OS X 10.8 Systems for IT Professionals,* was temporarily suspended while configuration setting research was performed, but will be resumed in FY 2015.

In FY 2015, CSD plans to finish scripting the few remaining OS X settings. The draft publication, *Guide to Securing Apple OS X 10.8 Systems for IT Professionals* will also be completed and made available for public comment. One of the script's three profiles will be deployed on select CSD systems to test the extended use of a system with a specific profile applied. CSD plans to continue improving the script after all settings are implemented.

CONTACTS:

Mr. Mark Trapnell
(301) 975-4091
mark.trapnell@nist.gov

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

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

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

TECHNICAL SECURITY METRICS

Security Risk Analysis of Enterprise Networks Using Attack Graphs

The protection of computer networks from malicious intrusions is critical to the economy and security of the nation. Vulnerabilities are regularly discovered in software applications that 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 NIST 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 2014, CSD attempted to model network diversity for evaluating the resilience of networks against zero-day attacks. CSD developed a formal model for network diversity as a security metric for evaluating the robustness of networks against potential zero-day attacks. CSD has proposed a new metric based on the least and average attacking effort. CSD has authored a paper, "Modeling Network Diversity for Evaluating the Robustness of Networks against Zero- Day Attacks," that was presented at the 19th European Symposium on Research in Computer Security (ESORICS), Wroclaw, Poland, September 7-11, 2014.

In FY 2015, CSD plans to develop new techniques and metrics to detect stealthy attacks on Cloud Computing using Bayesian Networks. 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-risk-analysis-enterprise-networks/

CONTACT:

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

Algorithms for Intrusion Measurement

The Algorithms for Intrusion Measurement (AIM) project furthers measurement science in the area of the algorithms used in the field of intrusion detection. The team focuses on both new detection metrics and measurements of scalability (more formally called algorithmic complexity). This analysis is applied to different phases of the detection lifecycle to include preemptive vulnerability analysis, initial attack detection, alert impact, alert aggregation/correlation, and compact log storage. In performing this work, the AIM project seeks to enhance the nation's ability to defend itself from network-borne attacks. This scientific research is conducted in partnership with the Army Research Laboratory (ARL) and the University of Maryland. ARL's participation helps focus the work on solving immediately 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 FY 2014, the AIM project completed research pertaining to several stages of the detection lifecycle through the application of graph theoretic approaches: security log compression, alert aggregation, and network threat propagation. The project team accomplished the following:

- The research team enabled significantly tighter compression for security logs, compared to using standard compression algorithms alone, and accomplished it using less processing time. The invention was a lightweight packing process that takes advantage of the restricted semantics and regular format of certain kinds of log files to render them substantially more amenable to compression with standard algorithms (research published by the Military Communications Conference, 2014). The team achieved a reduction of compressed file sizes to as little as 21 % of that of maximally compressed files without packing, and reduced overall compression times up to 64 %.
- To aid in the human analysis of such intrusion and security logs, the team designed an efficient approach to visually compress groups of related logs (as opposed to the previous work that reduced the actual size on a disk). The team designed a user-adjustable log aggregation approach using varying Hamming distances to quickly and losslessly aggregate alerts (research published by the International Journal of Network Security and its Applications). The result is a reduction in the cognitive load on analysts by minimizing the overall number of alerts and the number of data elements that need to be reviewed in order for an analyst to evaluate the set of original alerts.
- The research team addressed the problem of determining how far an attack may have spread in a network when a perimeter incursion has been detected. To accomplish this, the team created metrics and an algorithm for bounding the scope of network ingress attacks using the network tainting invention (research published by IEEE Conference on Software Security and Reliability, 2014). This approach provides an efficient means by which to stage and prioritize network forensics examinations.

In FY 2015, the AIM project will work on measuring Internet resilience to attacks by colluding countries, the

detection of persistent and stealthy network scanning, and efficient representations and algorithms for modeling and defending attack paths within a network.

CONTACT:

Mr. Peter Mell
(301) 975-5572
peter.mell@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 the 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 2014 included the publication of a report on a two-year Cooperative Research and Development Agreement (CRADA) with Lockheed Martin Corporation, showing approximately a 20 % reduction in software test development cost across a variety of projects, with a 20 % to 50 % improvement in test coverage; the development of a parallel algorithm for fault location, demonstrated on 22 000 variables; nine invited lectures at conferences and research labs; leading (jointly with IBM personnel) the IEEE Third International Conference on Combinatorial Testing, held with the International Conference on Software Testing; and a joint project with Carnegie Mellon University developing an advanced test environment that incorporates combinatorial methods.

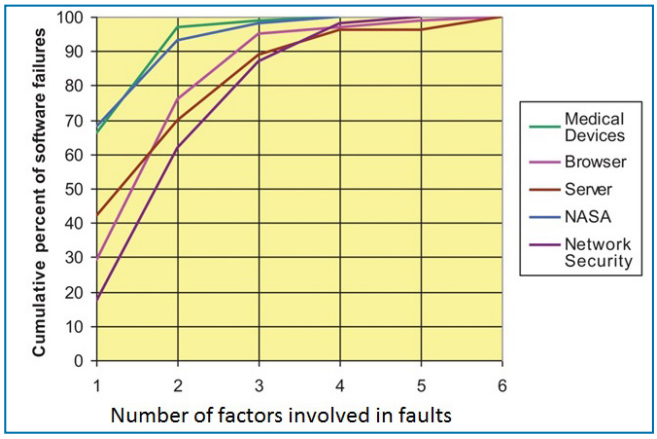


Figure 22: Interaction Rule

Technology transfer activities included the publication of several technical papers; a presentation of the results of the work with Lockheed Martin; a 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 2015 include a follow-up project with the NASA IV&V Facility to investigate the integration of combinatorial coverage measurement methods in NASA Independent Verification and Validation (IV&V) practices; the release of test a development environment as an open source project (jointly with Carnegie Mellon University); lectures at conferences and research labs; and a joint development of enhanced fault location tools with Johns Hopkins University Applied Physics Lab.

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

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

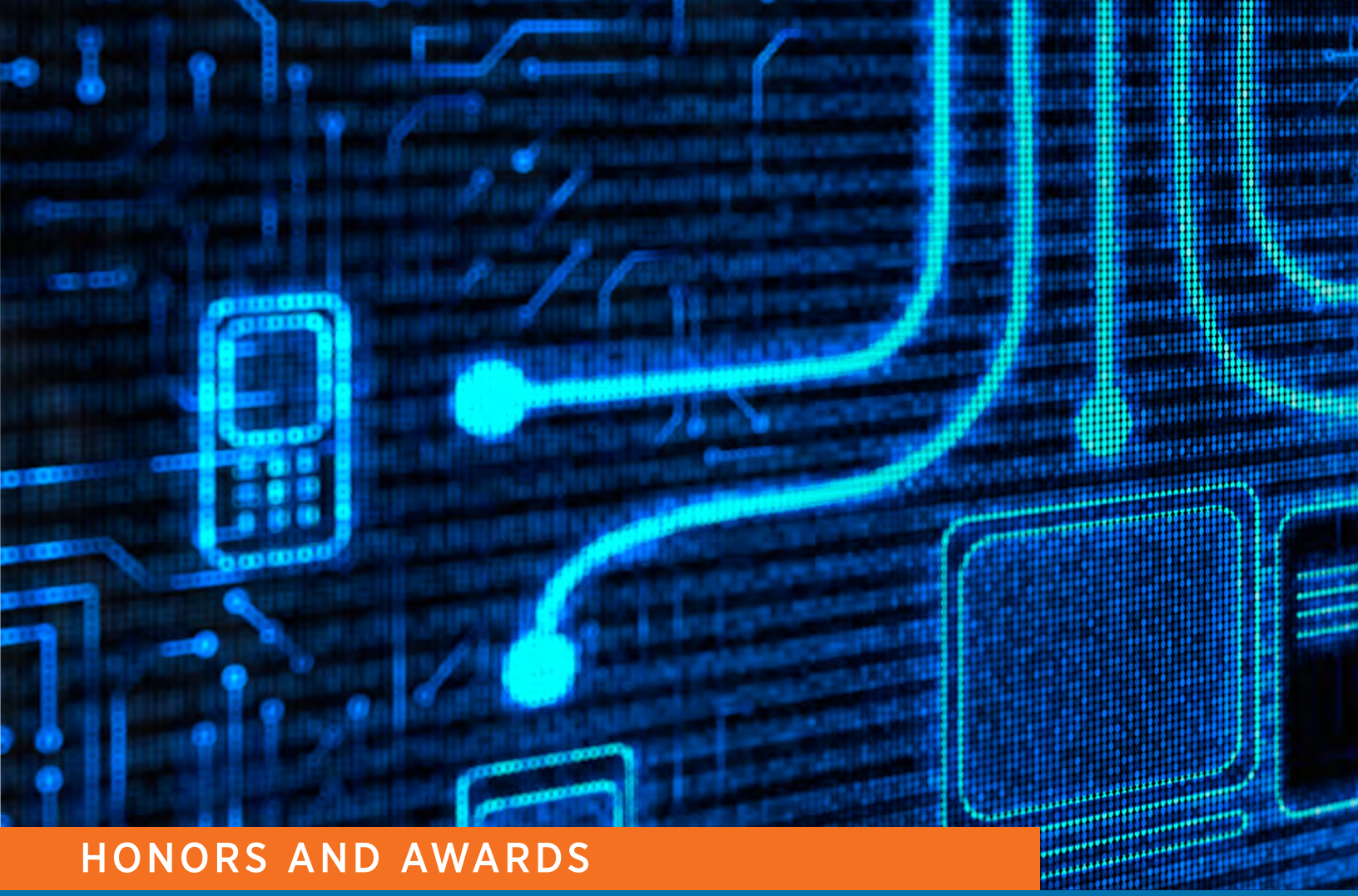
NIST CSD's work aims to encourage the use of roots of trust in computers to provide stronger security assurances. A focus area for this work has been securing mobile devices, using roots of trust to provide device integrity, data and application isolation, and protected storage. As part of this work, CSD is revising SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices,* based on the public comments that were received on the draft. A revised draft will be released in FY 2015.

Meanwhile, the draft guideline is being used as the basis for an effort 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 foundational document, the NCCoE and CSD developed the *Mobile Device Security for Enterprises* building block, which will demonstrate commercially available technologies that provide protection to both organization-issued and personally owned mobile platforms. The NCCoE will invite mobile device, operating system, and management software vendors, as well as application developers, to participate in this building block activity and demonstrate how their technologies could be used together to meet existing security requirements.

The CSD also continued its work to protect platform firmware in FY 2014. Boot firmware, commonly known as the Basic Input/Output System (BIOS), is a critical firmware component, due to its unique and privileged position within modern computing architectures. CSD has been working with key members of the computer industry on the use of roots of trust to improve the security of BIOS. In order to encourage the continued adoption of BIOS protections, The CSD submitted SP 800-147, *BIOS Protection Guidelines,* to ISO for international standardization. CSD will continue these standards efforts in FY 2015, and conduct research on protections for other critical platform firmware.

CONTACT:

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



HONORS AND AWARDS

Department of Commerce Gold Medal Award

Tom Karygiannis, Stephen Quirolgico, and Jeffrey Voas (CSD)

Additional recipients of this award were:
Brian Antonishek, Anthony Downs, Lisa Fronczek, Craig Schlenoff, and Brian Weiss
(all from the NIST Engineering Laboratory, Intelligent Systems Division)

From Left to Right: Secretary of Commerce Penny Pritzker, Brian Weiss, Craig Schlenoff, Brian Antonishek, Anthony Downs, Lisa Fronczek, Stephen Quirolgico, Jeff Voas, Tom Karygiannis, and Patrick Gallagher, NIST Director

The NIST team led a multi-organizational effort (NIST/George Mason University/DARPA) that developed innovative methods for security, testing, and evaluation of hardware and software to securely deploy off-the-shelf smartphones and applications in military field operations. NIST introduced software assurance methods, power and reliability analysis techniques, and standards-based cryptographic solutions that empowered the USG to securely deploy modified commercial solutions, reduce development costs, enhance the combat capability of U.S. troops, and save U.S. soldiers' lives.

Department of Commerce Gold Medal Award

Sheila Frankel (CSD)

Additional recipients of this award were:
Mark Carson, Douglas Montgomery, Stephen Nightingale, Darrin Santay,
(all from the Information Laboratory (ITL), Advanced Network Technologies Division)

From Left to Right: Secretary of Commerce Penny Pritzker, Darren Santay, Stephen Nightingale, Mark Carson, Doug Montgomery, Sheila Frankel, Patrick Gallagher, NIST Director

The group is recognized for technical leadership and innovation in the development and execution of the USGv6 Program that enabled the U.S. Government to meet aggressive OMB milestones for the adoption of IPv6 technologies. The team developed the critical standards, acquisition profiles, accreditation and testing programs, test suites, procurement guides, security guides, and operational test and measurement tools necessary to significantly improve the maturity of commercial IPv6 products and to guide the USG in their acquisition, deployment, and secure use. The NIST USGv6 Program provided a vital catalyst to the Internet industry and established the USG as a world leader in ensuring the continued growth and continuity of the Internet.

Department of Commerce Bronze Medal Award

Richard Kissel, CSD

Mr. Kissel is recognized 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 percent 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.

Stuart Katzke, Gallery of Distinguished Scientists, Engineers and Administrators

Dr. Katzke was recognized for his outstanding contributions in the field of cybersecurity, including his role as the founding director of NIST's Computer Security Division. He was honored as a nationally and internationally recognized leader in the development of cybersecurity standards during his tenure at NIST ITL from 1975 through 1999, and again during 2001 through 2008.

Naomi Lefkovitz, FierceGovernment IT "Fierce 15" Awardee

Ms. Lefkovitz is the Senior Privacy Policy Adviser for the NIST ITL. She was recognized as an innovator for her work in privacy and identity management, including her diligent support of privacy considerations for the National Strategy for Trusted Identities in Cyberspace (NSTIC). She represented the challenging and sensitive considerations to safeguard the privacy of individuals, while supporting several important information security and risk management initiatives, including the *Framework for Improving Critical Infrastructure Cybersecurity*. More information about this award is available from: http://www.fiercegovernmentit.com/special-reports/fiercegovernmentits-2013-fierce-15.

Kevin Stine, FierceGovernment IT "Fierce 15" Awardee

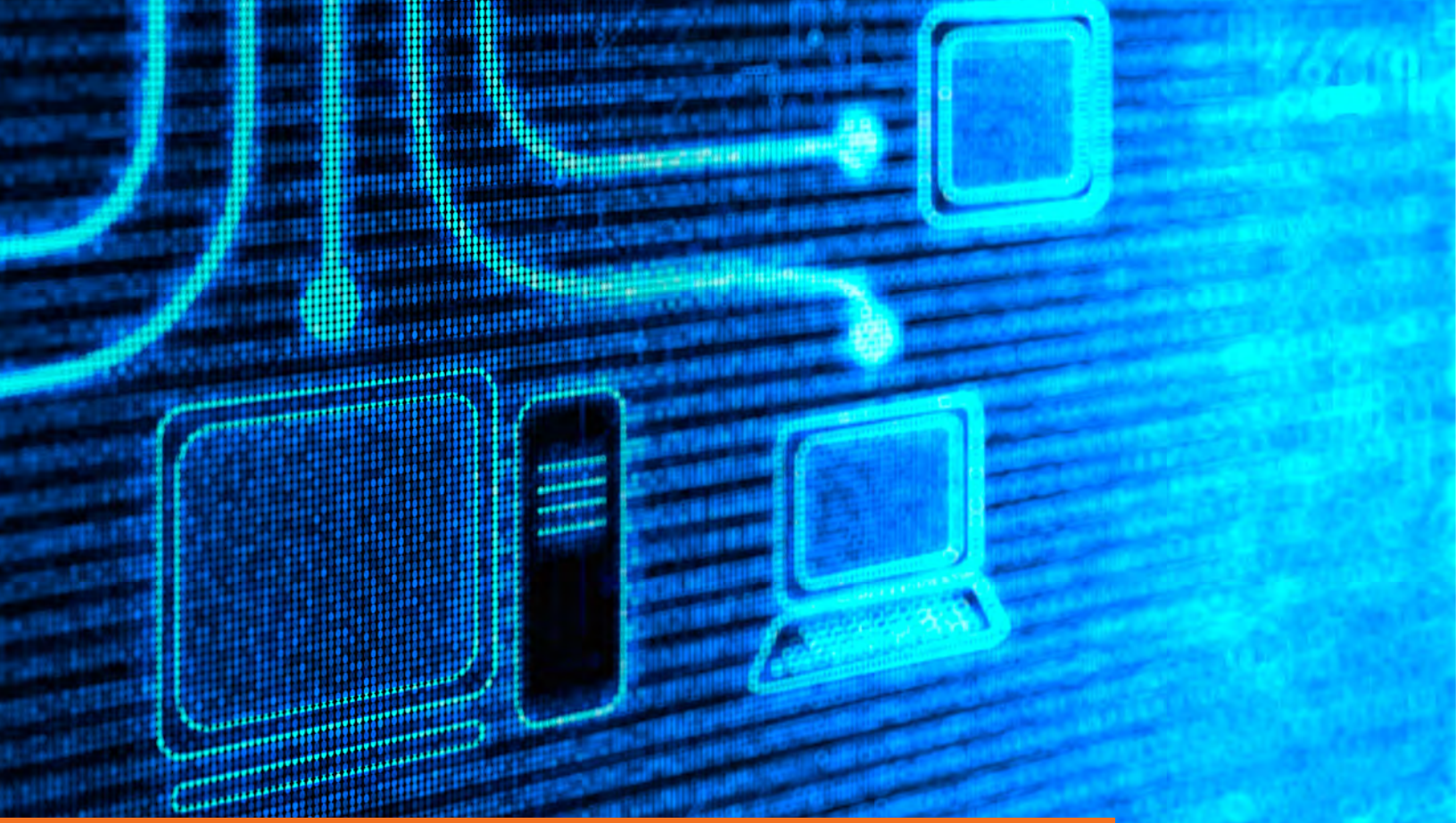
The Fierce 15 award is designed to recognize genuine groundbreaking innovation in IT. Mr. Stine was recognized as an innovator in the Federal Government and, with Naomi Lefkovitz's award from previous page, demonstrated ITL's commitment to creativity and innovation. The award recognized those orchestrating "some of the most progressive projects underway in government and work tirelessly to make government more efficient, service- and mission-oriented, and accountable." Mr. Stine was specifically awarded for his work in developing the *Framework for Improving Critical Infrastructure Cybersecurity*. His leadership of a global collaboration with public and private sector operators of critical infrastructure, and the subsequent open public review and comment process, represent CSD's synergistic approach. More information about this award is available from: http://www.fiercegovernmentit.com/special-reports/fiercegovernmentits-2013-fierce-15.

Matthew Scholl, Federal 100 Award

Matthew Scholl was recognized for his strategic direction and leadership of several initiatives, including the *Framework for Improving Critical Infrastructure Cybersecurity*, Digital Government Strategy, and Federal cross-agency priority goals on cybersecurity. Federal Computer Week recognized his work enabling "the secure configuration of all government Windows-based desktop computers, [increasing] security of credit card transactions worldwide, and [establishment of] industry tools to effectively implement and monitor secure configurations." The Federal 100 Awards are presented to leaders who have played pivotal roles that affect how the Federal Government acquires, develops and manages IT. Mr. Scholl was recognized as exemplifying that spirit through his successful leadership in CSD, including efforts to transform continuous security monitoring by expanding the use of automated tools. More information about this recognition is available from: http://fcw.com/articles/2014/03/10/fed100_scholl-matthew.aspx.

Dylan Yaga, 2014 InterNational Committee for Information Technology Standards (INCITS) Service Award

Mr. Yaga received the 2014 InterNational Committee for Information Technology Standards (INCITS) Service Award. This is an honorary award presented to participants who have provided outstanding service to the INCITS organization through committee work or duties. INCITS recognized his numerous contributions to the INCITS/M1 - Biometrics standards community, his detailed review of requirements in the biometric data interchange format standards and associated conformance testing methodology projects. His contributions to the first and second generation of data format standards have improved and promoted the successful development of national and international biometric standards. More information about this award is available from: http://www.incits.org/news-events/annual-awards.



COMPUTER SECURITY DIVISION PUBLICATIONS

Computer Security Division Publications

During FY 2014, CSD staff authored a significant number of computer/information security-related guidelines, recommendations, and research through the NIST technical series, journal articles, conference papers, and other published documents.

In the NIST technical series, CSD solicited public comments on forty draft publications, including one FIPS, 28 SPs and 11 NISTIRs. The FIPS had a 90-day comment period, while the other publications averaged 45 days. In particular, Draft NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process* (discussed in this annual report in the Cryptographic Standards and Guidelines Process Review section), sought feedback on the NIST mechanisms used to engage experts in industry, academia and government to develop cryptographic standards.

Nine SPs and four NISTIRs were issued as final publications, including new documents, revisions or updated revisions. CSD also continued to have its work published monthly in ITL Bulletins, which summarize the various publications and projects occurring across CSD. Those interested in being notified of new and draft publications may visit http://csrc.nist.gov and subscribe to email alerts.

Seeking to expand the availability of its publications in formats besides PDFs, CSD began converting some of its newer and most-downloaded publications into the .EPUB format, which is commonly used by e-book readers on mobile platforms. More than 28 e-books were posted during FY 2014 on the Computer Security Resource Center (CSRC) publications pages, http://csrc.nist.gov/publications/.

Publications are available for download from CSRC (http://csrc.nist.gov/), and FIPS (http://csrc.nist.gov/publications/PubsFIPS.html), SPs (http://csrc.nist.gov/publications/PubsSPs.html) and NISTIRs (http://csrc.nist.gov/publications/PubsNISTIRs.html) issued since mid-2012 have been posted on a server maintained by the NIST Library and assigned Digital Object Identifiers (DOIs). During FY 2014, Google Scholar began crawling the NIST Library server, resulting in significantly greater exposure and availability of CSD's technical series publications. The following lists the CSD-authored FIPS, SPs and NISTIRs that were most-downloaded during FY 2014:

Top 10 Most-Downloaded CSD publications in NIST Technical Series (i.e., FIPS, SP 800s, NISTIRs, and ITL Bulletins):

- SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations;*
- FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors;*
- SP 800-30 Revision 1, *Guide for Conducting Risk Assessments;*
- NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms;*
- FIPS 186-4, *Digital Signature Standard (DSS);*
- SP 800-82 Revision 1, *Guide to Industrial Control Systems (ICS) Security;*
- SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations;*
- SP 800-63-2, *Electronic Authentication Guideline;*
- SP 800-165, *2012 Computer Security Division Annual Report;* and
- SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

Top 3 FIPS:

- FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors;*
- FIPS 186-4, *Digital Signature Standard (DSS);* and
- FIPS 140-2, *Security Requirements for Cryptographic Modules.*

Top 3 NISTIRs:

- NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms;*
- NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems;* and
- NISTIR 7896, *Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition.*

Top 3 ITL Bulletins:

- December 2013, *The National Vulnerability Database (NVD): Overview;*
- February 2014, *Framework for Improving Critical Infrastructure Cybersecurity;* and
- June 2014, ITL *Forensic Science Program.*

Additionally, CSD shares its ongoing research efforts through other publications, such as journal articles, conference papers, books and other whitepapers. Although these publications can be found through NIST's Publications Portal (http://www.nist.gov/publication-portal.cfm), in FY 2014 CSD began posting a bibliography of those documents on CSRC (http://csrc.nist.gov/publications/articles/), including links to preprints and the final publications. During FY 2014, more than 25 such documents were published, and are listed in the next section (FY 2014 Computer Security Division Publications) of this annual report. Notably, the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0,* described earlier in this annual report, was downloaded more than 34 000 times.

CSD also dipped into its archives and posted a new page on CSRC, http://csrc.nist.gov/publications/history/nissc/, with full-text copies of proceedings from its 23 computer security conferences, held from 1979-2000 under various names: *National Information Systems Security Conference* (NISSC; 1995-2000), *National Computer Security Conference* (NCSC; 1985-1994), D*OD/NBS Computer Security Conference* (1984) and *Seminar on the DOD Computer Security Initiative* (1979-1983).

In FY 2015, besides expanding its library of available e-books, CSD intends to greatly improve the publication search, browse capabilities on CSRC, and provide additional details and cross references for each publication.

CONTACT:

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

FY 2014 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 FIPS, NIST SPs, NISTIRs and Information Technology Laboratory (ITL) Bulletins. Links to these publications are available at http://csrc.nist.gov/publications.

Additionally, each year CSD staff author 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, SPs, NISTIRs, and ITL Bulletins

Below are lists of NIST Technical Series publications that CSD released as draft documents or as final publications during FY 2014 (from October 1, 2013 to September 30, 2014). Following the lists are abstracts and contact information for each publication.

DRAFT PUBLICATIONS

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)		
Publication Number	***Publication Title***	***Draft Released Date***
FIPS 202	*SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*	May 2014

SPECIAL PUBLICATIONS (SPs)		
Publication Number	***Publication Title***	***Draft Released Date***
SP 800-167	*Guide to Application Whitelisting*	August 2014
SP 800-163	*Technical Considerations for Vetting 3rd Party Mobile Applications*	August 2014
SP 800-161 (Second Draft)	*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*	June 2014
SP 800-160	*Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*	May 2014
SP 800-157	*Guidelines for Derived Personal Identity Verification (PIV) Credentials*	March 2014
SP 800-152	*A Profile for U.S. Federal Cryptographic Key Management Systems*	January 2014
SP 800-90A Revision 1 (Second Draft)	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*	April 2014
SP 800-85B-4	*PIV Data Model Conformance Test Guidelines*	August 2014
SP 800-82 Revision 2	*Guide to Industrial Control Systems (ICS) Security*	May 2014
SP 800-79-2	*Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*	June 2014
SP 800-78-4	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification*	May 2014
SP 800-73-4	*Interfaces for Personal Identity Verification*	May 2014
SP 800-57 Part 3, Revision 1	*Recommendation for Key Management: Application-Specific Key Management Guidance*	May 2014
SP 800-56B Revision 1	*Guidelines for Derived Personal Identity Verification (PIV) Credentials*	March 2014 (Approved as Final: September 2014)
SP 800-53A Revision 4	*Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*	July 2014
SP 800-53 Revision 4, Appendix H	*International Information Security Standards: Security Control Mappings for ISO/IEC 27001 and 15408*	August 2014
SP 800-16 Revision 1 (Second Draft) (Third Draft)	*A Role-Based Model For Federal Information Technology/ CyberSecurity Training*	 October 2013 March 2014

NIST INTERAGENCY OR INTERNAL REPORTS (NISTIRs)		
Publication Number	***Publication Title***	***Draft Released Date***
NISTIR 8023	*Risk Management for Replication Devices (RDs)*	September 2014
NISTIR 8018	*Public Safety Mobile Application Security Requirements Workshop Summary*	July 2014
NISTIR 8014	*Considerations for Identity Management in Public Safety Mobile Networks*	July 2014
NISTIR 8006	*NIST Cloud Forensic Science Challenges*	June 2014
NISTIR 7981	*Mobile, PIV, and Authentication*	March 2014
NISTIR 7977	*NIST Cryptographic Standards and Guidelines Development Process*	February 2014
NISTIR 7966	*Security of Automated Access Management Using Secure Shell (SSH)*	August 2014
NISTIR 7924 (Second Draft)	*Reference Certificate Policy*	May 2014
NISTIR 7863	*Cardholder Authentication for the PIV Digital Signature Key*	December 2013
NISTIR 7628 Revision 1	*Guidelines to Smart Grid CyberSecurity*	October 2013 (Approved as Final September 2014)

FINAL APPROVED PUBLICATIONS

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)
NO FINAL APPROVED FIPS RELEASED DURING FY 2014.

SPECIAL PUBLICATIONS (SPs)		
Publication Number	***Publication Title***	***Publication Date***
SP 800-170	*Computer Security Division 2013 Annual Report*	June 2014
SP 800-168	*Approximate Matching: Definition and Terminology*	May 2014
SP 800-162	*Guide to Attribute Based Access Control (ABAC) Definition and Considerations*	January 2014
SP 800-147B	*BIOS Protection Guidelines for Servers*	August 2014
SP 800-101 Revision 1	*Guidelines on Mobile Device Forensics*	May 2014
SP 800-56B Revision 1	*Guidelines for Derived Personal Identity Verification (PIV) Credentials*	September 2014
SP 800-53 Revision 4 [Errata]	*Security and Privacy Controls for Federal Information Systems and Organizations*	April 2013 (original release date); updated January 15, 2014

SPECIAL PUBLICATIONS (SPs) (cont.)		
Publication Number	***Publication Title***	***Publication Date***
SP 800-52 Revision 1	*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*	April 2014
SP 800-37 Revision 1 [Errata]	*Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*	February 2010 (original release date); updated June 5, 2014

NIST INTERAGENCY OR INTERNAL REPORTS (NISTIRs)		
Publication Number	***Publication Title***	***Publication Date***
NISTIR 7987	*Policy Machine: Features, Architecture, and Specification*	May 2014
NISTIR 7946	*CVSS Implementation Guidance*	April 2014
NISTIR 7849	*A Methodology for Developing Authentication Assurance Level Taxonomy for Smart Card-based Identity Verification*	March 2014

ITL BULLETINS	
Publication Date	***Bulletin Title***
September 2014	*Release of NIST Interagency Report 7628 Revision 1, Guidelines for Smart Grid Cybersecurity*
August 2014	*Policy Machine: Towards A General-Purpose, Enterprise-Wide Operating Environment*
July 2014	*Release of NIST Interagency Report 7946, CVSS Implementation Guidance*
June 2014	*ITL Forensic Science Program*
May 2014	*Small and Medium-Size Business Information Security Outreach Program*
April 2014	*Release of NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
March 2014	*Attribute Based Access Control (ABAC) Definition and Considerations*
February 2014	*Framework for Improving Critical Infrastructure Cybersecurity*
January 2014	*A Profile of the Key Management Framework for the Federal Government*
December 2013	*The National Vulnerability Database (NVD): Overview*
November 2013	*ITL Releases Preliminary Cybersecurity Framework*
October 2013	*ITL Updates Federal Information Processing Standard (FIPS) for Personal Identity Verification (PIV) of Federal Employees and Contractors*

ABSTRACTS OF NIST TECHNICAL SERIES PUBLICATIONS RELEASED IN FY 2014

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.

FIPS

DRAFT FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*

This standard specifies the *Secure Hash Algorithm-3 (SHA-3)* family of functions on binary data. Each of the SHA-3 functions is based on an instance of the KECCAK algorithm that NIST selected as the winner of the SHA-3 Cryptographic Hash Algorithm Competition. This Standard also specifies the KECCAK-p family of mathematical permutations, including the permutation that underlies KECCAK, in order to facilitate the development of additional permutation-based cryptographic functions.

The SHA-3 family consists of four cryptographic hash functions, called SHA3-224, SHA3-256, SHA3-384, and SHA3-512, and two extendable-output functions (XOFs), called SHAKE128 and SHAKE256.

Hash functions are components for many important information security applications, including 1) the generation and verification of digital signatures, 2) key derivation, and 3) pseudorandom bit generation. The hash functions specified in this Standard supplement the SHA-1 hash function and the SHA-2 family of hash functions that are specified in FIPS 180-4, *The Secure Hash Standard.*

Extendable-output functions are different from hash functions, but it is possible to use them in similar ways, with the flexibility to be adapted directly to the requirements of individual applications, subject to additional security considerations.

CONTACTS:

Dr. Morris Dworkin
morris.dworkin@nist.gov

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

NIST SPs

SP 800-170, *Computer Security Division 2013 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

SP 800-168, *Approximate Matching: Definition and Terminology*

Approximate matching is a promising technology for designed to identify similarities between two digital artifacts. It is used to find objects that resemble each other or to find objects that are contained in another object. This can be very useful for filtering data for security monitoring, digital forensics, or other applications.

CONTACTS:

Mr. Douglas White
Software and Systems Division, ITL
douglas.white@nist.gov

Ms. Barbara Guttman
Software and Systems Division, ITL
barbara.guttman@nist.gov

DRAFT SP 800-167, *Guide to Application Whitelisting*

An application whitelist is a list of applications and application components that are authorized to be used in an organization. Application whitelisting technologies use whitelists to control which applications are permitted to execute on a host. This helps to stop the execution of malware, unlicensed software, and other unauthorized software. This publication is intended to assist organizations in understanding the basics of application whitelisting. It also explains planning and implementation for whitelisting technologies throughout the security deployment lifecycle.

CONTACTS:

Mr. Adam Sedgewick
adam.sedgewick@nist.gov

Mr. Murugiah Souppaya
murugiah.souppaya@nist.gov

DRAFT SP 800-163, *Technical Considerations for Vetting 3rd Party Mobile Applications*

Today's commercially available mobile devices (e.g., smart phones, tablets) are handheld computing platforms with wireless capabilities, geographic localization, cameras, and microphones. Similar to computing platforms such as desktops and laptops, the user experience with a mobile device is tied to the software apps and the tools and utilities available. The purpose of this document is to provide guidance for vetting 3rd party software applications (apps) for mobile devices. Mobile app vetting is intended to assess a mobile app's operational characteristics of secure behavior and reliability (including performance) so that organizations can determine if the app is acceptable for use in their expected environment.

CONTACTS:

Dr. Jeff Voas
jeff.voas@nist.gov

Dr. Stephen Quirolgico
stephen.quirolgico@nist.gov

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. Richard (Rick) Kuhn
kuhn@nist.gov

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

Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies decreased visibility into, understanding of, and control over how the technology that they acquire 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 publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. This publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on supply chain risk assessment and mitigation activities.

CONTACTS:

Mr. Jon Boyens
jon.boyens@nist.gov

Ms. Celia Paulsen
celica.paulsen@nist.gov

DRAFT SP 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*

This publication addresses the actions necessary for developing a more defensible and survivable IT infrastructure—including the component products, systems, and services that compose the infrastructure. It starts with and builds upon well-established International Standards for systems and software engineering published by the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronic Engineers (IEEE), and infuses systems security engineering techniques, methods, and practices into those systems/software engineering processes. The ultimate objective is to address cybersecurity issues from a stakeholder requirements and protection needs perspective and to use already established organizational processes to ensure such requirements/needs are addressed early in the life cycle of the system.

CONTACT:

Dr. Ron Ross
rross@nist.gov

DRAFT SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*

This recommendation provides technical guidelines for the implementation of standards-based, secure, reliable, interoperable PKI-based identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV Card. The scope of this document includes requirements for initial issuance, maintenance and termination of these credentials, certificate policies and cryptographic specifications, technical specifications for permitted cryptographic token types and the command interfaces for the removable implementations of such cryptographic tokens.

CONTACTS:

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

Mr. David Cooper
david.cooper@nist.gov

Mr. Salvatore Francomacaro
salvatore.francomacaro@nist.gov

Mr. Andy Regenscheid
andrew.regednscheid@nist.gov

DRAFT SP 800-152, *A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)*

This *Profile for U.S. Federal Cryptographic Key Management Systems (FCKMSs)* contains requirements for their design, implementation, procurement, installation, configuration, management, operation, and use by U.S. federal organizations. The Profile is based on SP 800-130, *A Framework for Designing Cryptographic Key Management Systems (CKMS).*

CONTACT:

Ms. Elaine Barker
elaine.barker@nist.gov

SP 800-147B, *BIOS Protection Guidelines for Servers*

Modern computers rely on fundamental system firmware, commonly known as the Basic Input/Output System (BIOS), to facilitate the hardware initialization process and transition control to the hypervisor or operating system. Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the PC architecture. The guidelines in this document include requirements on servers to mitigate the execution of malicious or corrupt BIOS code. They apply to BIOS firmware stored in the BIOS flash, including the BIOS code, the cryptographic keys that are part of the Root of Trust for Update, and static BIOS data. This guide is intended to provide server platform vendors with recommendations and guidelines for a secure BIOS update process.

CONTACT:

Mr. Andy Regenscheid
andy.regenscheid@nist.gov

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 the 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 (Rick) Ayers
Software and Systems Division, ITL
richard.ayers@nist.gov

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 either hash functions, block cipher algorithms or number theoretic problems.

CONTACTS:

Ms. Elaine Barker
elaine.barker@nist.gov

Dr. John Kelsey
john.kelsey@nist.gov

DRAFT SP 800-85B-4, *PIV Data Model Test Guidelines*

FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* describes a variety of data model components as a part of the PIV logical credentials. Such components include biometric elements in the form of fingerprint information and facial imagery and security elements such as electronic keys, certificates, and signatures. FIPS 201 incorporates by reference NIST SP 800-73-4 *Interfaces for Personal Identity Verification,* which specifies elements related to the PIV card interface, NIST SP 800-76 *Biometric Specifications for Personal Identity Verification*, which specifies the biometric requirements, and NIST SP 800-78 *Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* which specifies acceptable cryptographic algorithms and key sizes for PIV systems.

A robust testing framework and guidelines to provide assurance that a particular component or system is compliant with FIPS 201 and supporting standards should exist to build the necessary PIV infrastructure to support common unified processes and systems for government-wide use. NIST developed test guidelines in two parts. The first part addresses test requirements for the interface to the PIV card, which are provided in NIST SP 800-85A *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-3 Compliance).* The second part provides test requirements for the PIV data model and is provided in this document. This document specifies the derived test requirements, and the detailed test assertions and conformance tests for testing the PIV data model.

CONTACTS:

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

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

Mr. Ketan Mehta
ketan.mehta@nist.gov

DRAFT SP 800-82 Revision 2, *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.

CONTACTS:

Mr. Keith Stouffer
keith.stouffer@nist.go

Ms. Suzanne Lightman
suzanne.lightman@nist.gov

Ms. Vicky Pillitteri
victoria.pillitteri@nist.gov

DRAFT SP 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*

The purpose of this SP is to provide appropriate and useful guidelines for assessing the reliability of issuers of PIV Cards and Derived PIV Credentials. These issuers store personal information and issue credentials based on OMB policies and on the standards published in response to HSPD-12 and therefore are the primary target of the assessment and authorization under this guideline. The reliability of an issuer is of utmost importance when one organization (e.g., a federal agency) is required to trust the identity credentials of individuals that were created and issued by another federal agency. This trust will only exist if organizations relying on the credentials issued by a given organization have the necessary level of assurance that the reliability of the issuing organization has been established through a formal authorization process.

CONTACTS:

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

Ms. Hildegard (Hildy) Ferraiolo
hildegard.ferraiolo@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:

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

Ms. Donna Dodson
donna.dodson@nist.gov

Ms. Hildegard Ferraiolo
hildegard.ferraiolo@nist.gov

Dr. David Cooper
david.cooper@nist.gov

DRAFT SP 800-73-4, *Interfaces for Personal Identity Verification*

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 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. Ramaswamy (Mouli) Chandramouli
mouli@nist.gov

Dr. David Cooper
david.cooper@nist.gov

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

Mr. Salvatore Francomacaro
salvatore.francomacaro@nist.gov

Mr. Ketan Mehta
ketan.mehta@nist.gov

DRAFT SP 800-57 Part 3, Revision 1, *Recommendation for Key Management: Application-Specific Key Management Guidance*

SP 800-57 provides cryptographic key management guidance. It consists of three parts. Part 1 provides general guidance and best practices for the management of cryptographic keying material. Part 2 provides guidance on policy and security planning requirements for U.S. government agencies. Finally, Part 3 provides guidance when using the cryptographic features of current systems.

CONTACTS:

Ms. Elaine Barker
elaine.barker@nist.gov

Mr. Quynh Dang
quynh.dang@nist.gov

SP 800-56B Revision 1, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*

This recommendation specifies key-establishment schemes using integer factorization cryptography, based on ANS X9.44, *Key Establishment Using Integer Factorization Cryptography*, which was developed by the Accredited Standards Committee (ASC) X9, Inc.

CONTACTS:

Ms. Elaine Barker
elaine.barker@nist.gov

Dr. Lily Chen
lily.chen@nist.gov

Dr. Dustin Moody
dustin.moody@nist.gov

DRAFT SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*

This publication provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST SP 800-53 Revision 4. The procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security control assessments and privacy control assessments that support organizational risk management processes and that are aligned with the stated risk tolerance of the organization. Information on building effective security assessment plans and privacy assessment plans is also provided along with guidance on analyzing assessment results.

CONTACT:

NIST FISMA Team
Joint Task Force Transformation Initiative
sec-cert@nist.gov

SP 800-53 Revision 4 (Updated), *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.

CONTACT:

NIST FISMA Team
Joint Task Force Transformation Initiative
sec-cert@nist.gov

DRAFT SP 800-53 Revision 4 Appendix H, *International Information Security Standards: Security Control Mappings for ISO/IEC 27001 and 15408*

This update to Appendix H was initiated due to the 2013 revision to ISO/IEC 27001, which occurred after the final publication of SP 800-53 Revision 4. In addition to considering the new content in ISO/IEC 27001 for the mapping tables, new mapping criteria were employed in conducting the mapping analysis. The new criteria are intended to produce more accurate results—that is, to successfully meet the mapping criteria, the implementation of the mapped controls should result in an equivalent information security posture. While mapping exercises may by their very nature, include a degree of subjectivity, the new criteria attempts to minimize that subjectivity to the greatest extent possible.

CONTACT:

NIST FISMA Team
Joint Task Force Transformation Initiative
sec-cert@nist.gov

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 SP 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 SP also identifies TLS extensions for which mandatory support must be provided and other recommended extensions.

CONTACTS:

Dr. Kerry McKay
kerry.mckay@nist.gov

Mr. Tim Polk
william.polk@nist.gov

SP 800-37 Revision 1 (Updated), *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*

The purpose of SP 800-37 Revision 1 is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

CONTACT:

NIST FISMA Team
Joint Task Force Transformation Initiative
sec-cert@nist.gov

DRAFT SP 800-16 Revision 1 (Second & Third Drafts), *A Role-Based Model for Federal Information Technology / Cybersecurity Training*

Meeting security responsibilities and providing for the confidentiality, integrity, and availability of information in today's highly networked environment can be a difficult task. Each individual that owns, uses, relies on, or manages information and information technology (IT) systems must fully understand their specific security responsibilities. This includes ownership of the information and the role individuals have in protecting information. Information that requires protection includes information they own, information provided to them as part of their work and information they may come into contact with.

This document describes information technology/cybersecurity role-based training for the Federal Departments and Agencies and Organizations (Federal Organizations) and contractor support in these roles. Its primary focus is to provide a comprehensive, yet flexible, training methodology for the development of training courses or modules for personnel who have been identified as having significant information technology/cybersecurity responsibilities. This document is intended to be used by Federal information technology/cybersecurity training personnel and their contractors to assist in designing role-based training courses or modules for Federal Organizations personnel and contractors who have been identified as having significant responsibilities for information technology/cybersecurity. This publication should also be read, reviewed, or understood at a fairly high level by several audiences including the Organizational Heads through the leadership chain to the individual. Some of the titles include, but not limited to, the IT Managers, Senior Agency Information Security Officer (SAISO), Certified Information Systems Security Officer (CISSO), Information Systems Security Officer (ISSO), Information Assurance Manager (IAM), and Program Manager (PM).

CONTACT:

Ms. Patricia Toth
ptoth@nist.gov

NISTIRs

DRAFT NISTIR 8023, *Risk Management for Replication Devices (RDs)*

This publication provides guidance on protecting the confidentiality, integrity, and availability of information processed, stored, or transmitted on replication devices (RDs). It suggests appropriate countermeasures in the context of the System Development Life Cycle. A security risk assessment template is also provided to help organizations determine the risk associated with replication devices.

CONTACTS:

Ms. Kelley Dempsey
kelley.dempsey@nist.gov

Ms. Celia Paulsen
celia.paulsen@nist.gov

DRAFT NISTIR 8018, *Public Safety Mobile Application Security Requirements Workshop Summary*

This document captures the input received from the half-day workshop titled "Public Safety Mobile Application Security Requirements" organized by the Association of Public-Safety Communications Officials (APCO) International, in cooperation with FirstNet and the Department of Commerce and held on February 25, 2014. This first-of-its-kind workshop was attended by public safety practitioners, mobile application developers, industry experts, and government officials who contributed their experience and knowledge to provide input in identifying security requirements for public safety mobile applications.

CONTACTS:

Mr. Nelson Hastings
nelson.hastings@nist.gov

Ms. Barbara Guttman
Software and Systems Division
barbara.guttman@nist.gov

Mr. Michael Ogata
Software and Systems Division
michael.ogata@nist.gov

DRAFT NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*

This document analyzes approaches to identity management for public safety networks in an effort to assist individuals developing technical and policy requirements for public safety use. These considerations are scoped into the context of their applicability to public safety communications networks with a particular focus on the nationwide public safety broadband network (NPSBN) based on the Long Term Evolution (LTE) family of standards. A short background on identity management is provided alongside a review of applicable federal and industry guidance. Considerations are provided for identity proofing, selecting tokens, and the authentication process. While specific identity management technologies are analyzed, the document does not preclude other identity management technologies from being used in public safety communications networks.

CONTACTS:

Mr. Nelson Hastings
nelson.hastings@nist.gov

Mr. Joshua Franklin
joshua.franklin@nist.gov

DRAFT NISTIR 8006, *NIST Cloud Computing Forensic Science Challenges*

This document summarizes the research performed by the members of the NIST Cloud Computing Forensic Science Working Group, and aggregates, categorizes and discusses the forensics challenges faced by experts when responding to incidents that have occurred in a cloud-computing ecosystem. The challenges are presented along with the associated literature that references them. The immediate goal of the document is to begin a dialogue on forensic science concerns in cloud computing ecosystems. The long-term goal of this effort is to gain a deeper understanding of those concerns (challenges) and to identify technologies and standards that can mitigate them.

CONTACTS:

NIST Cloud Computing Forensic Science Working Group (NIST)
Dr. Michaela Iorga
nistir8006@nist.gov
michaela.iorga@nist.gov

NISTIR 7987, *Policy Machine: Features, Architecture, and Specification*

The ability to control access to sensitive data in accordance with policy is perhaps the most fundamental security requirement. Despite over four decades of security research, the limited ability for existing access control mechanisms to enforce a comprehensive range of policy persists. While researchers, practitioners and policy makers have specified a large variety of access control policies to address real-world security issues, only a relatively small subset of these policies can be enforced through off-the-shelf technology, and even a smaller subset can be enforced by any one mechanism. This report describes an access control framework, referred to as the Policy Machine (PM), which fundamentally changes the way policy is expressed and enforced. The report gives an overview of the PM and the range of policies that can be specified and enacted. The report also describes the architecture of the PM and the properties of the PM model in detail.

CONTACTS:

Mr. David Ferraiolo
david.ferraiolo@nist.gov

Mr. Serban Gavrila
serban.gavrila@nist.gov

DRAFT NISTIR 7981, *Mobile, PIV, and Authentication*

The purpose of this document is to analyze various current and near-term options for remote electronic authentication from mobile devices that leverage both the investment in the PIV infrastructure and the unique security capabilities of mobile devices, such as smart phones and tablets.

CONTACTS:

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

Dr. David Cooper
david.cooper@nist.gov

Mr. Andy Regenscheid
andrew.regenscheid@nist.gov

Mr. Salvatore (Sal) Francomacaro
salvatore.francomacaro@nist.gov

DRAFT NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process*

This document describes the principles, processes and procedures that drive cryptographic standards development efforts. This draft document will be revised based on the feedback received during the public comment period, and the revised publication will serve as basis for NIST's future standards development efforts. It will also serve as the basis for the review of NIST's existing body of cryptographic standards and guidelines.

CONTACTS:

Dr. Lily Chen
lily.chen@nist.gov

Mr. Andy Regenscheid
andrew.regenscheid@nist.gov

DRAFT NISTIR 7966, *Security of Automated Access Management Using Secure Shell (SSH)*

Hosts must be able to access other hosts in an automated fashion, often with very high privileges, for a variety of reasons, including file transfers, disaster recovery, privileged access management, software and patch management, and dynamic cloud provisioning. This is often accomplished using the Secure Shell (SSH) protocol. The SSH protocol supports several mechanisms for authentication, with public key authentication being recommended for automated access with SSH. Management of automated access requires proper provisioning, termination, and monitoring processes, just as interactive access by normal users does. However, the security of SSH-based automated access has been largely ignored to date. This publication assists organizations in understanding the basics of SSH automated access management in an enterprise, focusing on the management of SSH access tokens.

CONTACT:

Mr. Murugiah Souppaya
murugiah.souppaya@nist.gov

NISTIR 7946, *CVSS Implementation Guidance*

This NISTIR 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

DRAFT NISTIR 7924 (Second Draft), *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 (CAs) in mind. These CAs, who issue the certificates used to secure websites using TLS and verify the authenticity of software, play a particularly important role online. This document 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. Andy Regenscheid
andrew.regenscheid@nist.gov

DRAFT NISTIR 7863, *Cardholder Authentication for the PIV Digital Signature Key*

FIPS 201-2 requires explicit user action by the Personal Identity Verification (PIV) cardholder as a condition for use of the digital signature key stored on the card. This document clarifies the requirement for explicit user action to encourage the development of compliant applications and middleware that use the digital signature key.

CONTACTS:

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

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

Dr. David Cooper
david.cooper@nist.gov

NISTIR 7849, *A Methodology for Developing Authentication Assurance Level Taxonomy for Smart Card-based Identity Verification*

Smart cards (smart identity tokens) are now being extensively deployed for identity verification for controlling access to Information Technology (IT) resources as well as physical resources. Depending upon the sensitivity of the resources and the risk of wrong identification, different authentication use cases are being deployed. Assignment of authentication strength for each of the use cases is often based on: (a) the total number of three common orthogonal authentication factors – What You Know, What You Have and What You are, and (b) the entropy associated with each factor chosen. The objective of this paper is to analyze the limitation of this approach and present a methodology for assigning authentication strengths based on the strength of pair wise bindings between the five entities involved in smart card based authentications – the card (token), the token secret, the card holder, the card issuer, and the person identifier stored in the card. The rationale for the methodology is based on the following three observations: (a) The form factor of the smart identity token introduces some threats of misuse; (b) the common set of credentials objects provisioned to a smart card embody bindings to address those threats and (c) the strength of an authentication use case should therefore be based on the number and type of binding verifications that are performed in the constituent authentication mechanisms. The use of the methodology for developing an authentication assurance level taxonomy for two real world smart identity token deployments is also illustrated.

CONTACT:

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

NISTIR 7628 Revision 1, *Guidelines for Smart Grid CyberSecurity*

This three-volume report, Guidelines for Smart Grid Cybersecurity, presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of Smart Grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information presented in this report as guidance for assessing risk and identifying and applying appropriate security requirements. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

CONTACTS:

The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee

Ms. Tanya Brewer
tanya.brewer@nist.gov

Ms. Vicky Pillitteri
vicky.pillitteri@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 2014. For conference papers, the contributions listed below were either i) accepted for a conference held during FY 2014, or ii) accepted for a conference held prior to FY 2014 with a final proceeding published in FY 2014 (and not listed in an earlier CSD Annual Report). All NIST authors of a publication are identified using *italics*.

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

Journal Articles

I. Bojanova and *D.R. Kuhn,* "IT Pro Conference on Information Systems Governance," *IT Professional* 16(4), 4-6 (July/August 2014). doi: 10.1109/MITP.2014.55.

> Approximately 100 IT professionals participated in the 2014 IT Pro Conference on Information Systems Governance, held at NIST on May 22, 2014 (www.computer.org/itproconf). Information systems governance focuses on properly managing IT resources to achieve organizational goals. The conference was designed to bring together IT professionals from industry, government, and academia to discuss new challenges in information systems and share ways of overcoming such challenges. Sponsored by IEEE, NIST, and Noblis, the conference featured three keynotes and 12 presentations, focusing on the following key questions: 1) How can we get the most value from IT while still delivering successful projects and reliable information systems and infrastructure? 2) How can we secure critical systems while keeping pace with advances in technology? and 3)What changes are on the horizon for technology and business leaders?

R. Bryce and *D.R. Kuhn,* "Software Testing," *Computer (IEEE Computer)* 47(2), 21-22 (February 2014). doi: 10.1109/MC.2014.45.

> [Guest editor introduction to a special issue presenting papers focused on important problems within the Software Testing community.]

W. Burr, H. Ferraiolo and *D. Waltermire,* "NIST and Computer Security," *IT Professional* 16(2), 31-37 (March-April 2014). doi: 10.1109/MITP.2013.88.

> The U.S. NIST's highly visible work in four key areas—cryptographic standards, role-based access control, identification card standards, and security automation—has and continues to shape computer and information security at both national and global levels. This article is part of a special issue on NIST contributions to IT.

F. Izadi, F. Khoshnam, *D. Moody* and A.S. Zargar, "Elliptic Curves Arising from Brahmagupta Quadrilaterals," *Bulletin of the Australian Mathematical Society* 90(1), 47-56 (August 2014). doi: 10.1017/S0004972713001172.

> A Brahmagupta quadrilateral is a cyclic quadrilateral whose sides, diagonals, and area are all integer values. In this article, we characterize the notions of Brahmagupta, introduced by K. R. S. Sastry, by means of elliptic curves. Motivated by these characterizations, we use Brahmagupta quadrilaterals to construct infinite families of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ having ranks (at least) 4, 5, and 6. Furthermore, by specializing we give examples from these families of specific curves with rank 9.

R. Kissel, "Avoiding Accidental Data Loss," *IT Professional* 15(5), 12-15 (September-October 2013). doi: 10.1109/MITP.2013.75.

> Does your organization have systematic procedures to remove sensitive data from obsolete equipment, or do you use a somewhat ad hoc process for the cleanup and disposal of old gear? Careless disposal of data storage hardware has led to costly and embarrassing incidents for organizations that discovered too late that their control over media sanitization was inadequate. The guidelines presented here will help organizations review their sanitization procedures and develop a more sound process if needed.

R. Marin-Lopez, F. Bernal-Hidalgo, S. Das, *L. Chen* and Y. Ohba, "A New Standard for Securing Media-Independent Handover: IEEE 802.21a," *IEEE Wireless Communications* 20(6), 82-90 (December 2013). doi: 10.1109/MWC.2013.6704478.

> When enabling handover between different radio interfaces (e.g., handover from 3G to Wi-Fi), reducing network access authentication latency and securing handover related signaling messages are major challenging problems, amongst many others. The IEEE 802 Local Area Network (LAN)/ Metropolitan

Area Network (MAN) Standards committee has recently finished its standardization work in this area by defining the IEEE standard 802.21a-2012. The mechanisms introduced in this standard are aimed to protect the IEEE standard 802.21-2008 messages and services and to reduce handover latency by introducing the concept of proactive authentication. We provide a comprehensive survey of this standard and describe how the defined mechanisms can be used to reduce the overall latency during handover between access networks using heterogeneous radio interfaces.

E. McDuffie and V.P. Piotrowski, "The Future of Cybersecurity Education," *Computer (IEEE Computer)* 47(8), 67-69 (August 2014). doi: 10.1109/MC.2014.224.

By fostering public-private partnerships in cybersecurity education, the U.S. government is motivating federal agencies, industry, and academia to work more closely together to defend cyberspace.

P. Mell and R. Harang, "Reducing the Cognitive Load on Analysts through Hamming Distance Based Alert Aggregation," *International Journal of Network Security & Its Applications (IJNSA)* 6(5), 35-50 (September 2014).

Previous work introduced the idea of grouping alerts at a Hamming distance of 1 to achieve alert aggregation; such aggregated meta-alerts were shown to increase alert interpret-ability. However, a mean of 84 023 daily Snort alerts were reduced to a still formidable 14 099 meta-alerts. In this work, we address this limitation by investigating several approaches that all contribute towards reducing the burden on the analyst and providing timely analysis. We explore minimizing the number of both alerts and data fields by aggregating at Hamming distances greater than 1. We show how increasing bin sizes can improve aggregation rates. And we provide a new aggregation algorithm that operates up to an order of magnitude faster at Hamming distance 1. Lastly, we demonstrate the broad applicability of this approach through empirical analysis of Windows security alerts, Snort alerts, netflow records, and DNS logs.

V.Y. Pillitteri, "NIST Cybersecurity Framework Addresses Risks to Critical Infrastructure," *ei Magazine* 19 (6), 20-21 (June 2014).

On February 12, 2014, President Obama issued a statement that, "[c]yber threats pose one the gravest national security dangers that the United States faces. To better defend our nation against this systemic challenge, one year ago I signed an Executive Order directing the Administration to take steps to improve information sharing with the private sector, raise the level of cybersecurity across our critical infrastructure, and enhance privacy and civil liberties." That Executive Order, E.O. 13636, *Improving Critical Infrastructure Cybersecurity,* directed the National Institute of Standards and Technology (NIST) to develop a voluntary, risk-based Cybersecurity Framework ("Framework")—based on existing industry standards and best practices—to help organizations manage cybersecurity risk. The resulting Framework was created through a yearlong collaboration between government and industry.

A.L. Roginsky, K. Christensen and M. Mostowfi, "Delay Behavior of On-Off Scheduling: Extending Idle Periods," *Applied Mathematics & Information Sciences* 7(6), 2123-2136 (November 2013). doi: 10.12785/amis/070603.

On-off scheduling of systems that have the ability to sleep can be used to extend system idle periods and enable greater opportunities for energy savings from sleeping. In this paper, we achieve a theoretical understanding of the delay behavior of on-off scheduling as it may apply to communications links and other systems capable of sleeping. We consider a single-server coalescing queue with a scheduler that schedules on-off periods for the server in order to extend idle periods of the downstream link. At the start of an off period (duration T_{off}) the server stops serving jobs immediately if idle, or after processing a job already in service. Service of any queued and arriving jobs begins at the start of the next on period (duration T_{on}). On and off periods are fixed. We solve for the scheduling queue behavior as a function of T_{off}, T_{on}, interarrival time t, service time x, and time of first arrival g for periodic job arrivals. Results are closed form and have both theoretical and practical significance.

A.T. Vassilev and *T.A. Hall*, "The Importance of Entropy to Information Security," *Computer (IEEE Computer)* 47(2), 78-81 (February 2014). doi: 10.1109/MC.2014.47.

The strength of cryptographic keys is an active challenge in academic research and industrial practice. In this paper, we discuss the entropy as fundamentally important concept for generating hard-to-guess, i.e., strong, cryptographic keys and outline the difficulties in generating and estimating the available entropy for cryptographic needs. We consider traditional entropy estimation in cryptographic applications and motivate the development of new spectral techniques for estimation.

L. Wang, S. Jajodia, *A. Singhal,* P. Cheng and S. Noel, "*k*-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities," *IEEE Transactions on Dependable and Secure Computing* 11(1), 30-44 (January-February 2014). doi: 10.1109/TDSC.2013.24.

> By enabling a direct comparison of different security solutions with respect to their relative effectiveness, a network security metric may provide quantifiable evidences to assist security practitioners in securing computer networks. However, research on security metrics has been hindered by difficulties in handling zero day attacks exploiting unknown vulnerabilities. In fact, the security risk of unknown vulnerabilities has been considered as something unmeasurable due to the less predictable nature of software flaws. This causes a major difficulty to security metrics, because a more secure configuration would be of little value if it were equally susceptible to zero day attacks. In this paper, we propose a novel security metric, *k*-zero day safety, to address this issue. Instead of attempting to rank unknown vulnerabilities, the described metric counts how many such vulnerabilities would be required for compromising network assets; a larger count implies more security since the likelihood of having more unknown vulnerabilities available, applicable, and exploitable all at the same time will be significantly lower. We formally define the metric, analyze the complexity of computing the metric, devise heuristic algorithms for intractable cases, and finally demonstrate through case studies that applying the metric to existing network security practices may generate actionable knowledge.

L. Wilbanks, *D.R. Kuhn* and W. Chou, "IT Risks," *IT Professional* 16(1), 20-21 (January-February 2014). doi: 10.1109/MITP.2014.7.

> Risk management is a common phrase when managing information, from the Chief Information Security Officer (CISO) to the programmer. We acknowledge that risk management is the identification, assessment and prioritization of risks and reflects how we manage uncertainty. These are some areas of risk that we have come to accept, their mitigation strategies are part of our development, part of our everyday work. Most IT professionals would agree that IT is good at identifying and managing the risks. But is that really the case or has risk management/mitigation become a buzz word for us?

Conference Papers

R. Chandramouli, "Analysis of Protection Options for Virtualized Infrastructures in Infrastructure as a Service Cloud," *Fifth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2014)*, Venice, Italy, May 25-29, 2014, pp. 37-43.

> Infrastructure as a Service (IaaS) is one of the three main cloud service types where the cloud consumer consumes a great variety of resources such as computing (Virtual Machines or VMs), virtual network, storage and utility programs (DBMS). Any large-scale offering of this service is feasible only through a virtualized infrastructure at the service provider. At the minimum, this infrastructure is made up of resources such as Virtualized hosts together with associated virtual network and hardware/software for data storage An IaaS's consumer's total set of interactions with these resources constitute the set of use cases for IaaS cloud service. These use cases have associated security requirements and these requirements are met by protection options enabled by available security solutions/technologies. The purpose of this paper is to analyze these protection options from the viewpoint of: (a) Security functionality they can provide and (b) the architecture that governs their deployment, so that IaaS consumers can decide on the most appropriate security configuration for their VM instances depending upon the profile of the applications running in them.

I. Dominguez, *D.R. Kuhn, R.N. Kacker,* and Y. Lei, "CCM: A Tool for Measuring Combinatorial Coverage of System State Space" [poster], *2013 ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM 2013)*, Baltimore, Maryland, October 10-11, 2013, p. 291. doi: 10.1109/ESEM.2013.44.

> This poster presents some measures of combinatorial coverage that can be helpful in estimating residual risk related to insufficient testing of rare interactions, and a tool for computing these measures.

D. Ferraiolo, S. Gavrila and W. Jansen, "On the Unification of Access Control and Data Services," *15th IEEE Conference on Information Reuse and Integration (IRI 2014)*, San Francisco, California, August 13-15, 2014, pp. 450-457. doi: 10.1109/IRI.2014.7051924.

> A primary objective of enterprise computing (via a data center, cloud, etc.) is the controlled delivery of data services (DS). Typical DSs include applications such as email, workflow, and records management, as well as system level features, such as file and access

control management. Although access control (AC) currently plays an important role in imposing control over the execution of DS capabilities, AC can be more fundamental to computing than one might expect. That is, if properly designed, a single AC mechanism can simultaneously implement, control, and deliver capabilities of multiple DSs. The Policy Machine (PM) is an AC framework that has been designed with this objective in mind. This paper describes the PM features that provide a generic AC mechanism to implement DS capabilities, and comprehensively enforces mission tailored access control policies across DSs.

L. Ghandehari, J. Czerwonka, Y. Lei, S. Shafiee, *R.N. Kacker* and *D.R. Kuhn*, "An Empirical Comparison of Combinatorial and Random Testing," *Third International Workshop on Combinatorial Testing (IWCT 2014),* in *Proceedings of the Seventh IEEE International Conference on Software, Testing, Verification and Validation (ICST 2014),* Cleveland, Ohio, March 31 - April 4, 2014, pp. 68-77. doi: 10.1109/ICSTW.2014.8.

Some conflicting results have been reported on the comparison between *t*-way combinatorial testing and random testing. In this paper, we report a new study that applies *t*-way and random testing to the Siemens suite. In particular, we investigate the stability of the two techniques. We measure both code coverage and fault detection effectiveness. Each program in the Siemens suite has a number of faulty versions. In addition, mutation faults are used to better evaluate fault detection effectiveness in terms of both number and diversity of faults. The experimental results show that in most cases, *t*-way testing performed as good as or better than random testing. There are few cases where random testing performed better, but with a very small margin. Overall, the differences between the two techniques are not as significant as one would have probably expected. We discuss the practical implications of the results. We believe that more studies are needed to better understand the comparison of the two techniques.

J. Hagar, *D.R. Kuhn, R.N. Kacker* and T. Wissink, "Introducing Combinatorial Testing in a Large Organization: Pilot Project Experience Report" [poster], *Third International Workshop on Combinatorial Testing (IWCT 2014),* in *Proceedings of the Seventh IEEE International Conference on Software, Testing, Verification and Validation (ICST 2014),* Cleveland, Ohio, March 31 - April 4, 2014, p. 153. doi: 10.1109/ICSTW.2014.70.

This poster gives an overview of the experience of eight pilot projects, over two years, applying combinatorial testing in a large aerospace organization. While results varied across the different pilot projects, overall it was estimated that CT would save roughly 20 % of testing cost, with 20 % to 50 % improved test coverage.

D.R. Kuhn, *R.N. Kacker* and Y. Lei, "Estimating Fault Detection Effectiveness" [poster], *Third International Workshop on Combinatorial Testing (IWCT 2014),* in *Proceedings of the Seventh IEEE International Conference on Software, Testing, Verification and Validation (ICST 2014),* Cleveland, Ohio, March 31 - April 4, 2014, p.154. doi: 10.1109/ICSTW.2014.69.

A *t*-way covering array can detect *t*-way faults; however, they generally include other combinations beyond *t*-way as well. For example, a particular test set of all 5-way combinations is shown capable of detecting all seeded faults in a test program, despite the fact that it contains up to 9-way faults. This poster gives an overview of methods for estimating fault detection effectiveness of a test set based on combinatorial coverage for a class of software. Detection effectiveness depends on the distribution of *t*-way faults, which is not known. However based on past experience one could say for example the fraction of 1-way faults is F_1 = 60 %, 2-way faults F_2 = 25 % F_3 = 10 % and F_4 = 5 %. Such information could be used in determining the required strength *t*. It is shown that the fault detection effectiveness of a test set may be affected significantly by the *t*-way fault distribution, overall, simple coverage at each level of *t*, number of values per variable, and minimum *t*-way coverage. Using these results, we develop practical guidance for testers.

C. Liu, *A. Singhal* and D. Wijesekera, "A Model Towards Using Evidence from Security Events for Network Attack Analysis," *11th International Workshop on Security in Information Systems (WOSIS 2014),* Lisbon, Portugal, April 27, 2014. doi: 10.5220/0004980300830095.

Constructing an efficient and accurate model from security events to determine an attack scenario for an enterprise network is challenging. In this paper, we discuss how to use evidence obtained from security events to construct an attack scenario and build an evidence graph. To achieve the accuracy and completeness of the evidence graph, we use Prolog inductive and abductive reasoning to correlate evidence by reasoning the causality, and use an anti-forensics database and a corresponding attack graph to find the missing evidence. In addition, because the constructed scenario and supplied evidence might

need to stand up in the court of law, the federal rules of evidence are also taken into account to predetermine the admissibility of the evidence.

P.M. Mell and R. Harang, "Limitations to Threshold Random Walk Scan Detection and Mitigating Enhancements," *2013 IEEE Conference on Communications and Network Security (CNS),* Washington, DC, October 14-16, 2013, pp. 332-340. doi: 10.1109/CNS.2013.6682723.

This paper discusses limitations in one of the most widely cited single source scan detection algorithms: threshold random walk (TRW). If an attacker knows that TRW is being employed, these limitations enable full circumvention allowing undetectable high speed full horizontal and vertical scanning of target networks from a single Internet Protocol address. To mitigate the discovered limitations, we provide three enhancements to TRW and analyze the increased cost in computational complexity and memory. Even with these mitigations in place, circumvention is still possible but only through collaborative scanning (something TRW was not designed to detect) with a significant increase in the required level of effort and usage of resources.

P.M. Mell and R. Harang, "Using Network Tainting to Bound the Scope of Network Ingress Attacks," *Eighth International Conference on Software Security and Reliability (SERE 2014),* San Francisco, California, June 30-July 2, 2014, pp. 206-215. doi: 10.1109/SERE.2014.34.

This research describes a novel security metric, network taint, which is related to software taint analysis. We use it here to bound the possible malicious influence of a known compromised node through monitoring and evaluating network flows. The result is a dynamically changing defense-in-depth map that shows threat level indicators gleaned from monotonically decreasing threat chains. We augment this analysis with concepts from the complex networks research area in forming dynamically changing security perimeters and measuring the cardinality of the set of threatened nodes within them. In providing this, we hope to advance network incident response activities by providing a rapid automated initial triage service that can guide and prioritize investigative activities.

M. Sönmez Turan, R. Peralta, "The Multiplicative Complexity of Boolean Functions on Four and Five Variables," *Third International Workshop on Lightweight Cryptography for Security & Privacy (LightSec 2014),* Istanbul, Turkey, September 1-2, 2014. In *Lecture Notes in Computer Science* 8898, *Lightweight Cryptography for Security and Privacy,* T. Eisenbarth and E. Öztürk, eds., Berlin: Springer, 2015, pp. 21-33. doi: 10.1007/978-3-319-16363-5_2.

A generic way to design lightweight cryptographic primitives is to construct simple rounds using small nonlinear components such as 4x4 S-boxes and use these iteratively (e.g., PRESENT and SPONGENT). In order to efficiently implement the primitive, efficient implementations of its internal components are needed. Multiplicative complexity of a function is the minimum number of AND gates required to implement it by a circuit over the basis (AND, XOR, NOT). It is known that multiplicative complexity is exponential in the number of input bits *n*. Thus it came as a surprise that circuits for all 65 536 functions on four bits were found which used at most three AND gates. In this paper, we verify this result and extend it to five-variable Boolean functions. We show that the multiplicative complexity of a Boolean function with five variables is at most four.

L. Wang, M. Zhang, S. Jajodia, *A. Singhal* and M. Albanese, "Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks," *19th European Symposium on Research in Computer Security (ESORICS 2014),* Wroclaw, Poland, September 7-11, 2014. In *Lecture Notes in Computer Science* 8713, *Computer Security – ESORICS 2014,* M. Kutyłowski and J. Vaidya, eds., Berlin: Springer, 2014, pp. 494-511. doi: 10.1007/978-3-319-11212-1_28.

The interest in diversity as a security mechanism has recently been revived in various applications, such as Moving Target Defense (MTD), resisting worms in sensor networks, and improving the robustness of network routing. However, most existing efforts on formally modeling diversity have focused on a single system running diverse software replicas or variants. At a higher abstraction level, as a global property of the entire network, diversity and its impact on security have received limited attention. In this paper, we take the first step towards formally modeling network diversity as a security metric for evaluating the robustness of networks against potential zero day attacks. Specifically, we first devise a biodiversity-inspired metric based on the effective number of distinct resources. We then propose two complementary diversity metrics, based on the least and the average attacking efforts, respectively. Finally, we evaluate algorithm and metrics through simulation.

Books and Book Sections

Y. Cheng, J. Deng, J. Li, S. DeLoach, *A. Singhal* and X. Ou, "Metrics of Security," *Cyber Defense and Situational Awareness,* edited by A. Knott, C. Wang and R.F. Erbacher *(Advances in Information Security* 62), Berlin: Springer, 2014, pp. 263-295. doi: 10.1007/978-3-319-11391-3_13.

Discussion of challenges and ways of improving Cyber Situational Awareness dominated our previous chapters. However, we have not yet touched on how to quantify any improvement we might achieve. Indeed, to get an accurate assessment of network security and provide sufficient Cyber Situational Awareness (CSA), simple but meaningful metrics—the focus of the Metrics of Security chapter—are necessary. The adage, "what can't be measured can't be effectively managed," applies here. Without good metrics and the corresponding evaluation methods, security analysts and network operators cannot accurately evaluate and measure the security status of their networks and the success of their operations. In particular, this chapter explores two distinct issues: (i) how to define and use metrics as quantitative characteristics to represent the security state of a network, and (ii) how to define and use metrics to measure CSA from a defender's point of view.

White Papers

K. Dempsey, R. Ross and *K. Stine,* "Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management," NIST, Gaithersburg, Maryland, June 2014, 13 pp.

Office of Management and Budget (OMB) Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems,* reminds federal agencies that, "our nation's security and economic prosperity depend on ensuring the confidentiality, integrity and availability of federal information and information systems," and directs NIST to "publish guidance establishing a process and criteria for agencies to conduct ongoing assessments and authorization." The following guidance clarifies and amplifies current NIST guidance on security authorization contained in Special Publications 800-37, 800-39, 800-53, 800-53A, and 800-137.

K. Dempsey, G. Witte and D. Rike, "Summary of NIST SP 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations," NIST, Gaithersburg, Maryland, February 19, 2014, 13 pp.

The white paper provides an overview of SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* which was published April 30, 2013.

"Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0," NIST, Gaithersburg, Maryland, February 12, 2014, 41 pp.

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats take advantage of the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security at risk. To better protect these systems, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* on February 12, 2013. The Executive Order established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. The Framework enables organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

Smart Grid Interoperability Panel, Smart Grid Cybersecurity Committee *(NIST contributors include V.Y. Pillitteri and T.L. Brewer),* "Cybersecurity User's Guide to the Guidelines for Smart Grid Cybersecurity (NISTIR 7628 Vol. 1 2010)," February 26, 2014, 30 pp.

> While the NISTIR 7628 document covers many significant cybersecurity topics, this User's Guide is focused primarily on the application of NISTIR 7628 Volume 1 in the context of an organization's cybersecurity risk management practices. The User's Guide provides an end-to-end implementation guide for an organization's Smart Grid cybersecurity activities, and references the Department of Energy Electricity Subsector Cybersecurity Risk Management Process to provide the cybersecurity risk management framework and organizational structure needed before system-specific controls identified in NISTIR 7628 can be applied. The User's Guide was developed with significant involvement by utilities.

ACRONYMS

3GPP	3rd Generation Partnership Project
ABA	American Bar Association
ABAC	Attribute Based Access Control
AC	Access Control
ACPT	Access Control Policy Tool
ACRLCS	AC Rule Logic Circuit Simulation
ACTS	Advanced Combinatorial Testing System
AES	Advanced Encryption Standard
AIM	Algorithms for Intrusion Measurement
AMI	Advanced Metering Infrastructure
ANS	American National Standards
ANSI	American National Standards Institute
API	Application programming interface
ARF	Asset Reporting Format
ARL	Army Research Laboratory
ASC	Accredited Standards Committee
ATIS	Alliance for Telecommunications Industry Solutions
BioCTS	Biometrics Conformance Test Software
BIOS	Basic Input/Output System
CAC	Common Access Card
CAESARS	Continuous Asset Evaluation, Situational Awareness and Risk Scoring
CAESARS-FE	CAESARS Framework Extension
CAs	Certificate Authorities
CAVP	Cryptographic Algorithm Validation Program
CCE	Common Configuration Enumeration
CCEVS	Common Criteria Evaluation and Validation Scheme
CCSS	Common Configuration Scoring System
CERT	Computer Emergency Readiness Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CKMS	Cryptographic Key Management System
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CNCI	Comprehensive National Cybersecurity Initiatives
CNSS	Committee on National Security Systems
ConMon	Continuous monitoring
CP	Certificate Policy
CPE	Common Platform Enumeration
CPS	Cyber-Physical Systems
CRADA	Cooperative Research and Development Agreement
CRMF	Cloud-adapted Risk Management Framework
CS1	Cyber Security 1
CSD	Computer Security Division
CSIA	Cyber Security and Information Assurance
CSIC	Computer Security Incident Coordination
CSIRT	Computer Security Incident Response Team
CSPs	Critical Security Parameters
CSRC	Computer Security Resource Center
CST	Cryptographic and Security Testing
CSWG	Cyber Security Working Group
CTAs	Conformance Test Architectures
CTG	Cryptographic Technology Group
CTSs	Conformance Test Suites
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DARPA	Defense Advanced Research Projects Agency
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DHHS	Department of Health and Human Services
DISA	Defense Information Systems Agency
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOD	Department of Defense
DOE	Department of Energy

DRBG	Deterministic random bit generator
DSS	Digital Signature Standard
EAC	Election Assistance Commission
ECDSA	Elliptic Curve Digital Signature Algorithm
ECP	Enterprise Compliance Profile
EL	Engineering Laboratory
EO	Executive Order
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCCX	Federal Cloud Credential Exchange
FDCC	Federal Desktop Core Configuration
FedRAMP	Federal Risk and Authorization Management Program
FHE	fully homomorphic encryption
FIPS	Federal Information Processing Standard
FIRST	Forum of Incident Response and Security Teams
FirstNet	First Responder Network Authority
FISMA	Federal Information Security Management Act
FISSEA	Federal Information Systems Security Educators' Association
FITSI	Federal IT Security Institute
FPE	format-preserving encryption
FVAP	Federal Voting Assistance Program
FY	Fiscal Year
GAO	Government Accountability Office
GCM	Galois/Counter Mode
GCSE	Group Communication System Enablers
GICS	Generic Identity Command Set
GPS	Global Positioning System
GSA	General Services Administration
HAVA	Help America Vote Act
HIT	Health information technology
HMAC	Hash-based Message Authentication Code
HSPD-12	Homeland Security Presidential Directive-12
IA	Information Assurance
IaaS	Infrastructure as a Service
IAD	Information Access Division
IAD	Information Assurance Directorate
IAWG	Identity Assurance Working Group
ICS	Industrial Control Systems
ICT	Information and Communications Technologies
IEEE	Institute of Electrical and Electronics Engineers
INCITS	InterNational Committee for Information Technology Standards
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IR	Interagency or Internal Report
ISP	Internet Service Provider
IT	information technology
ITL	Information Technology Laboratory
IUT	Implementation under test
IV&V	Independent Verification and Validation
ISPAB	Information Security and Privacy Advisory Board
ISIMC	Information Security and Identity Management Committee's
ISO	International Organization for Standardization
ISA	International Society of Automation
ITI	the Information Technology Industry
IWG	Interagency Working Group
JTC 1	Joint Technical Committee 1
LTE	Long-Term Evolution
MACs	Message authentication codes
MIH	Media-independent handover
MMT	Multi-Block Message Test

MLS	Multi-Level Security
NASA	National Aeronautics and Space Administration
NCCoE	National Cybersecurity Center of Excellence
NCP	National Checklist Program
NFC	Near Field Communications
NGAC-FA	Next Generation Access Control – Functional Architecture
NGAC-GOADS	Next Generation Access Control – Generic Operations & Abstract Data Structures
NGAC-IRPADS	Next Generation Access Control-Implementation Requirements, Protocols and API Definitions
NICCS	National Initiative for Cybersecurity Careers and Studies
NICE	National Initiative for Cybersecurity Education
NIEM	National Information Exchange Model
NISTIR	NIST Interagency or Internal Report
NITRD	Networking and Information Technology Research and Development
NNLT	NIST NICE Leadership Team
NPIVP	NIST Personal Identity Verification Program
NPSBN	National Public Safety Broadband Network
NSA	National Security Agency
NSTIC	National Strategy for Trusted Identities in Cyberspace
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
NVLAP	National Voluntary Laboratory Accreditation Program
OCIL	Open Checklist Interactive Language
OCR	Office for Civil Rights
ODNI	Office of the Director of National Intelligence
ODP	Open Distributed Processing
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OVAL	Open Vulnerability and Assessment Language
PCI	Payment Card Industry
PIV	Personal Identity Verification
PIV-I	PIV-Interoperable
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PLC	Programmable Logic Controllers
PM	Policy Machine
PML	Physical Measurement Laboratory
PoS	Point of service
PSCR	Public Safety Communications Research
RBAC	Role-Based Access Control
RBGs	Random bit generators
R&D	Research and development
RFI	Request for Information
RFID	Radio Frequency Identification
RMF	Risk Management Framework
RNG	Random number generation
RPL	Removed Products List
RSA	Rivest, Shamir, Adleman
SACM	Security Automation and Continuous Monitoring
SBA	Small Business Administration
SC	Subcommittee
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCAPVal	SCAP Content Validation Tool
SCMG	Security Components and Mechanisms Group
SCORE	Special Cyber Operations Research and Engineering
SCRM	Supply Chain Risk Management
SDO	Standards Developing Organizations
SEW	Social, Economic, and Workforce

SGCC	Smart Grid Cybersecurity Committee
SGIP	Smart Grid Interoperability Panel
SHS	Secure Hash Standard
SIG	Special Interest Groups
SLC	Simulated Logic Circuit
SMBs	Small and medium-size businesses
SNIA	Storage Networking Industry Association
SOIG	Security Outreach and Integration Group
SP	Special Publications
SRA	Security Reference Architecture
SSAG	Secure Systems and Applications Group
SSP	Sensitive Security Parameters
STIG	Security Technical Implementation Guide
STVMG	Security Testing, Validation, and Measurement Group
SWGDE	Scientific Working Group on Digital Evidence
SWID	Software identification
TAG	Technical Advisory Group
TCG	Trusted Computing Group
TDEA	Triple Data Encryption Algorithm
TGDC	Technical Guidelines Development Committee
TIAA	Travel Industry Association of America
TLS	Transport Layer Security
TMSAD	Trust Model for Security Automation Data
TNC	Trusted Network Connect
TS	Technical Specification
UOCAVA	Uniformed and Overseas Citizens Voting Act
USG	U.S. Government
USGCB	United States Government Configuration Baseline
USNC	United States National Committee
VCI	Virtual Contact Interface
VMs	Virtual Machines
VPN	Virtual private network
VRDX-SIG	Vulnerability Reporting and Data eXchange SIG
VVSG	Voluntary Voting System Guidelines
Wi-Fi	Wireless Fidelity
XACML	eXtensible Access Control Markup Language
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language

OPPORTUNITIES TO ENGAGE WITH CSD AND NIST

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. The salary costs are generally borne by the sponsoring institution; however, in some cases, these guest research internships carry a small monthly stipend paid by NIST.

For further information, contact:

Mr. 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, salary costs are borne by the sponsoring agency; however, in some cases, agency salary costs may be reimbursed by NIST.

For further information, contact:

Mr. 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:

Mr. Matthew Scholl
(301) 975-2941
matthew.scholl@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/grants/grants.cfm

ACKNOWLEDGEMENTS

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 2014 project highlights and accomplishments for this annual report (their names are mentioned after each project write-up). The editor would also like to acknowledge Elaine Barker, Lisa Carnahan, Kevin Stine, Jim Foti (NIST); Greg Witte and Larry Feldman (G2) for reviewing and providing valuable feedback for this annual report.

The editor would also like to acknowledge Kristen Dill of Dill and Company, Inc. for designing the cover and inside layout for the 2014 annual report.

TRADEMARK INFORMATION

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK