2016 ANNUAL REPORT

NIST/ITL CYBERSECURITY PROGRAM

NIST SPECIAL PUBLICATION 800-195

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

THIS PAGE IS LEFT INTENTIONALLY BLANK.

ANNUAL REPORT 2016

NIST/ITL CYBERSECURITY PROGRAM

PATRICK O'REILLY, EDITOR
Computer Security Division
Information Technology Laboratory

KRISTINA RIGOPOULOS, EDITOR
Applied Cybersecurity Division
Information Technology Laboratory

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

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM
https://doi.org/10.6028/NIST.SP.800-195

SEPTEMBER 2017

U.S. DEPARTMENT OF COMMERCE
Wilbur L. Ross, Jr., Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Kent Rochford, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

AUTHORITY

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-195
Natl. Inst. Stand. Technol. Spec. Publ. 800-195, 156 pages (September 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-195

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

ACKNOWLEDGMENTS

The editors, Patrick O'Reilly of the Computer Security Division (CSD) and Kristina Rigopoulos of the Applied Cybersecurity Division (ACD), would like to thank their ITL colleagues who provided write-ups on their 2016 project highlights and accomplishments for this annual report (their names are mentioned after each project write-up). The editors would also like to acknowledge Elaine Barker (CSD), Lisa Carnahan (Standards Coordination Office, NIST), Greg Witte and Larry Feldman (G2) for reviewing and providing valuable feedback for this annual report.

The editors would also like to acknowledge Kristen Dill of Dill and Company, Inc. for designing the cover and inside layout for this 2016 annual report.

DISCLAIMER

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

TRADEMARK INFORMATION

All names are trademarks or registered trademarks of their respective owners.

TABLE OF CONTENTS

TABLE OF CONTENTS

THIS PAGE IS LEFT INTENTIONALLY BLANK.

WELCOME LETTER

Awareness about the importance of strong cybersecurity for maintaining trust in the economy and protecting the nation is at an all-time high. So, too, are the challenges. When it comes to cybersecurity, the National Institute of Standards and Technology (NIST) has a long history of conducting path-breaking research and development, cultivating standards and best practices, and facilitating technology transitions. We rely on open, transparent, and collaborative processes that engage private and public sector participation and attract expertise from around the world. This 2016 report captures our most noteworthy accomplishments.

In 2016, NIST continued to advance fundamental research to support security and interoperability standards and guidelines. This work was led by the Computer Security Division (CSD) in the NIST Information Technology Laboratory (ITL). Among other things, CSD is responsible for developing cybersecurity standards, guidelines, tests, and metrics for the protection of non-national security federal information systems. Recognizing the agency's need to respond to and anticipate increasing demands for its cybersecurity expertise, NIST established the Applied Cybersecurity Division (ACD) within ITL to support additional applied research and to transition effective cybersecurity technology approaches to government and business sectors nationwide. ACD helps to drive the adoption of appropriate cybersecurity solutions by government and commercial organizations – enabling solutions-oriented collaborative interactions and offering guidance on the use of research results, standards, and best practices. Other parts of NIST also are key contributors to NIST's cybersecurity portfolio.

Strong partnerships with industry, academia and government are critical to NIST's cybersecurity program. In 2016, NIST continued to collaborate with stakeholders from across the country and around the world to raise awareness and encourage use of the voluntary Cybersecurity Framework. In this spirit, NIST began to develop an update to the version first published in 2014. NIST also prepared a draft Cybersecurity Framework profile aligned with manufacturing sector goals and industry best practices. In addition, NIST developed the draft Baldrige Cybersecurity Excellence Builder self-assessment tool that complements the Cybersecurity Framework and helps organizations to better understand the effectiveness of their cybersecurity risk management efforts.

Looking ahead is vital in the realm of cybersecurity. Knowing that if large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use and compromise the confidentiality and integrity of digital communication on the Internet and elsewhere, NIST is working closely with the academic community and industry to develop protective cryptographic standards that we all rely upon. Building on its successful tradition of working openly with the worldwide cryptographic community, in 2016 NIST called for submissions for quantum-resistant public-key cryptographic algorithms for standards. These algorithms must be secure against both quantum and classical computers, and should interoperate with existing communications protocols and networks. After submissions are received late in 2017, NIST plans to spend 3-5 years working with the research community and industry to analyze the candidates before selecting algorithms for standardization.

Identity management is fundamental to security management. In 2016, NIST continued to advance solutions in identity management through projects with partners who manage innovative but practical real-world solutions. Also in the past year, NIST produced an introduction to the concepts of privacy engineering and risk management for federal information systems. The goal is to help decrease privacy risks and enable organizations to make purposeful decisions about resource allocation and effective implementation of controls in information systems. NIST also initiated an update to our Digital

WELCOME LETTER

Identity Guideline (Special Publication 800-63), which provides technical guidelines to agencies for the implementation of digital authentication. Building from these foundational resources, NIST's efforts will focus on strengthening the security, privacy, usability and interoperability of digital identity solutions that meet an organization's identity and access management needs throughout the system lifecycle.

During 2016, NIST's National Cybersecurity Center of Excellence (NCCoE) moved into a new permanent facility that expanded the Center's workspace from four to 23 separate, flexible laboratories—including two larger areas capable of safely hosting large equipment, such as automobiles. This additional space allows NCCoE to increase its collaborations and projects. In 2016, the Center published draft practice guides to support industry sectors, including healthcare, financial services, and energy; these guides are now beginning to be put to productive use. NCCoE also published draft documents to support security in key technology areas, such as cloud computing and mobile applications.

The National Initiative for Cybersecurity Education (NICE), led by NIST, is a partnership between government, academia, and the private sector that is focused on promoting a robust network and an ecosystem of cybersecurity education, training, and workforce development. In 2016, NIST released an update to the NICE Cybersecurity Workforce Framework (NCWF); it already is being used in the private and public sectors to more effectively identify, recruit, develop and maintain cybersecurity talent. The NICE framework provides a common language to categorize and describe cybersecurity work that helps organizations to build a strong staff to protect systems and data.

Our dedicated staff has accomplished a great deal in 2016, developing standards and working closely with scores of partners and drawing upon hundreds of private and public sector organizations and individuals. This is not a static endeavor. For example, NIST is fully aware of the urgent need to more aggressively address the security challenges of the Internet of Things and, more broadly, our connected world.

We welcome any and all suggestions about where and how we can better provide the nation with the kind of cybersecurity information and tools that it needs in order to advance and protect our economy and our country.

Donna F. Dodson,
Chief Cybersecurity Advisor

BACKGROUND INFORMATION OF ANNUAL REPORT

This Annual Report, formerly the *Computer Security Division Annual Report*, has been renamed to the *Information Technology Laboratory (ITL) Cybersecurity Program Annual Report*. This change reflects the opportunity to describe the many cybersecurity program highlights and accomplishments from throughout the laboratory. This Annual Report is organized into several sections, each identified by a title page.

Please note: This Annual Report covers the Federal Government's Fiscal Year (FY) 2016 from October 1, 2015 to September 30, 2016.

ITL, an operating unit under NIST, contains seven divisions. Five of these seven divisions are involved with cybersecurity efforts at NIST. Throughout this Annual Report, there are some references to particular division activities, and to work by groups within those divisions. Primarily, the authors have attributed accomplishments to ITL, since ITL staff have been involved with each cybersecurity program included in this Annual Report. At the end of each program/project write-up, one or more points of contact are provided and may be used to address questions or request for more information. Many sections also include additional references that readers may find valuable.

Below is a condensed hierarchical chart of ITL's structure:

INFORMATION TECHNOLOGY LABORATORY (ITL) HEADQUARTERS

Charles Romine, *Director*
Jim St. Pierre, *Deputy Director*
(5 of the 7 divisions (identified below) are involved with the ITL Cybersecurity Program)

Advanced Network Technologies Division (ANTD)
Abdella Battou, *Division Chief*

Applied Cybersecurity Division (ACD)
Kevin Stine, *Division Chief*

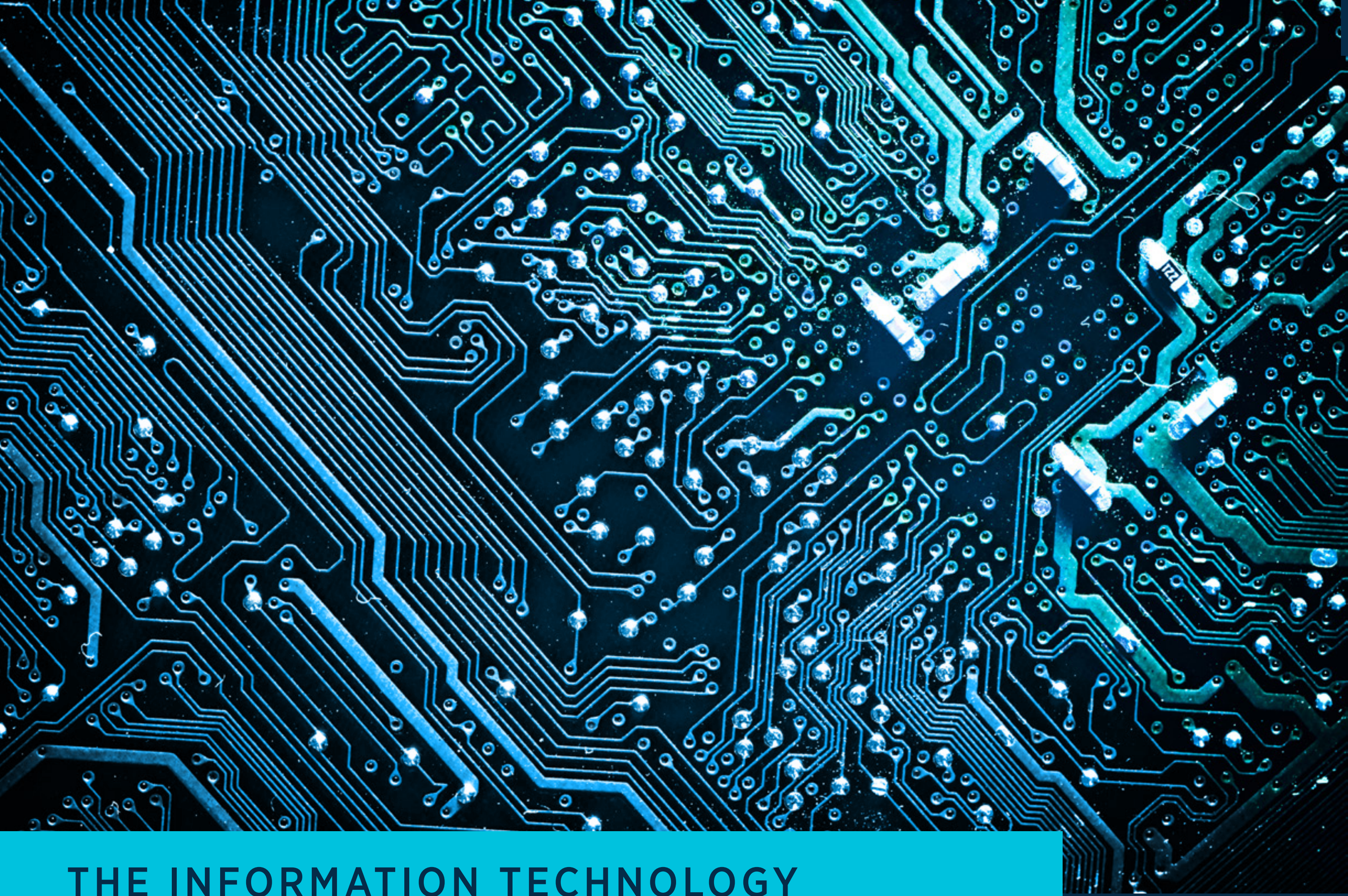
Computer Security Division (CSD)
Matthew Scholl, *Division Chief*

Information Access Division (IAD)
Shahram Orandi, *Division Chief*

Software and Systems Division (SSD)
Ram Sriram, *Division Chief*

ITL's Cybersecurity Program is very excited to share these achievements and accomplishments made during the 2016 Fiscal Year in this Annual Report.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195



THE INFORMATION TECHNOLOGY LABORATORY IMPLEMENTS THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

This section contains a list of the major activities that were accomplished during FY 2016 by the ITL Cybersecurity Program. Detailed explanations of these activities are provided in the next section.

-

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

INFORMATION TECHNOLOGY LABORATORY (ITL) CYBERSECURITY PROGRAM IMPLEMENTS 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, titled the Federal Information Security Management Act (FISMA) of 2002, included the duties and responsibilities for the National Institute of Standards and Technology, Information Technology Laboratory. There are multiple divisions within ITL that are involved with cybersecurity programs/projects. The work is being conducted collaboratively between the divisions. In December 2014, the 113th Congress updated FISMA as the Federal Information Security Modernization Act (Public Law 113-283). NIST ITL responsibilities were unchanged in the update. In 2016, the ITL Cybersecurity Program addressed its assignment through the following major activities:

- **Forty-three NIST Special Publications (SP) (20 approved as final and 23 drafts) were issued, providing management, operational, and technical security guidelines in topic areas including:**
  The 2015 annual report; cryptography (cryptographic standards used for the Federal Government, block cipher modes of operation, key management, random bit generator (RBG), Secure Hash Algorithm-3 (SHA-3) cryptography, transitioning the use of cryptographic algorithms and key lengths); mobile security (enterprise telework, remote access and bring-your-own device (BYOD), mobile device security – cloud and hybrid builds): application whitelisting; cyber threat sharing; cybersecurity event recovery; data-centric system threat modeling; de-identifying government datasets; asset management – financial services; guidelines for checklist users and developers; networks of "things"; personal identification verification (PIV); protecting Controlled Unclassified Information within nonfederal information systems and organizations; securing Apple Operating System (OS) X; security content automation protocol (SCAP); systems engineering; trustworthy email; and virtual machine (VM) protection.
- **Thirty-one NIST Interagency/Internal Reports (NISTIR) (18 approved as final and 13 drafts) were issued on a variety of topics, including:**
  Cryptography (post-quantum cryptography, lightweight cryptography, NIST cryptographic standards and guidelines development process); mobile security (mobile devices, infrastructure and platforms); attribute metadata; automation support for security control assessments; catalyzing the identity ecosystem; de-identification of personal information; Long-Term Evolution (LTE) architecture overview and security analysis; PIV; policy machine (access control framework); public safety mobile applications; SCAP; security of interactive and automated access management using Secure Shell (SSH); software identification (SWID) tags; strategic U.S. Government engagement in international standardization; trusted geolocation in the cloud; and vulnerability description ontology (VDO).
- **The National Cybersecurity Center of Excellence (NCCoE) moved into a new permanent facility:**
  This facility was made possible by the state of Maryland and Montgomery County, Maryland, and has almost 60,000 square feet of modern physical space and IT systems. The new facility expanded the Center's workspace from four to twenty-two separate, flexible laboratories—including two larger areas capable of safely housing large equipment (including a vehicle that will be used in an upcoming project on auto-related cybersecurity issues). This additional space allows NCCoE to increase its collaboration and to undertake new projects.
- **The Strategic Plan for the National Initiative for Cybersecurity Education (NICE) was issued:**
  With a mission of energizing and promoting a robust network and an ecosystem of cybersecurity education, training, and workforce development, this plan lays out important goals for the cybersecurity workforce. (See: http://csrc.nist.gov/nice/about/strategicplan.html)
- **A draft Cybersecurity Framework profile for manufacturers was developed and issued:**
  This profile can be used as a roadmap for reducing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

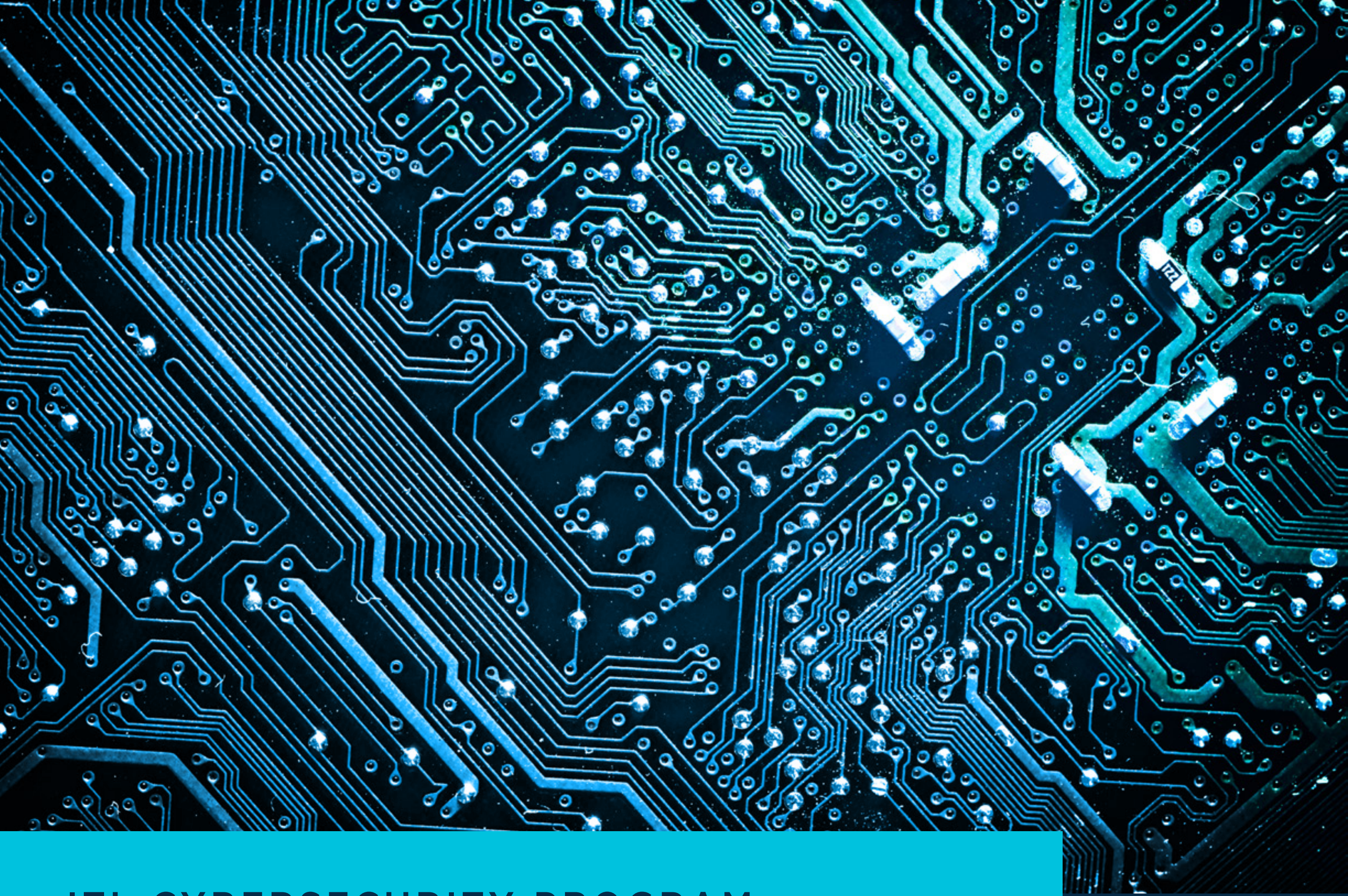
- **The Baldrige Cybersecurity Excellence Builder (BCEB) self-assessment tool was developed and issued for public comment:**
  The BCEB, aligned to the Cybersecurity Framework, is a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts. (See: https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative)
- **Continued to research, evaluate and develop standards for Post-Quantum Cryptography (PQC):**
  NIST announced a Call for Proposals to solicit, evaluate, and standardize quantum-resistant public key cryptography (a.k.a. post-quantum cryptography (PQC)) algorithms through a Federal Register Notice (FRN). The team solicited public comments regarding requirements and evaluation criteria, which were subsequently finalized. NIST plans to spend three to five years analyzing the submitted algorithms before selecting algorithms for standardization, during which time NIST will engage with the research community through conferences and workshops.
- **Initiated a lightweight cryptography project to study the performance of the current NIST-approved cryptographic standards on constrained devices:**
  To better understand the need for dedicated lightweight cryptography, ITL has created a portfolio of lightweight primitives through an open process. ITL will evaluate and recommend algorithms based on profiles, which consist of a set of design goals, physical characteristics of target devices, performance characteristics imposed by the applications, and security characteristics.
- **Continued to develop expertise in several critical research areas in cryptography:**
  ITL continues to conduct research into post-quantum cryptography (PQC), quantum algorithms, elliptic curve cryptography (ECC), privacy-enhancing cryptography, and lightweight cryptographic schemes for constrained environments.
- **A NIST/Industry joint working group was created to study the automation of cryptographic implementation testing:**
  After working with industry on the protocol necessary to exchange cryptographic test data in an automated fashion, the development of the cryptographic algorithm testing service to be hosted at NIST was begun, with the full implementation expected to take approximately one year. (See: http://csrc.nist.gov/projects/acvt)
- **Continued research and reporting results in software testing:**
  In software testing, the oracle problem refers to determining the expected output for a given set of inputs. A determination of the expected output normally requires human involvement or a mathematical model of the specification. ITL has developed an oracle-free software testing method for which NIST filed a patent application. The test settings for an input factor may represent ranges of values (called equivalence classes) for which the output is expected to remain unchanged.
- **Continued research and development of a new conformance test tool for the ANSI/NIST-ITL Machine Readable Table (MRT) Biometric Data Formats:**
  A command-line interface was developed that tests the MRTs themselves for conformance to the specification, in addition to testing American National Standards Institute (ANSI)/NIST-ITL Transactions. An initial graphical user interface was also developed to allow an easy-to-use software suite for end users. National standard bodies were encouraged to further the advancements of biometric data interchange format standards.
- **Represented the NIST/NTIA PSCR (Public Safety Communications Research Program), FirstNet (the US First Responders' Network Authority), and Public Safety stakeholders in the 3GPP (Third Generation Partnership Project):**
  The International Standards Organization, which is developing the next-generation telecommunications standard, LTE (Long Term Evolution), is ensuring that features critical to Public Safety are incorporated into the standards.
- **Continued refinement and support for the USG Federal Identity Program:**
  In continued support of Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard 201-2 (FIPS 201-2), the NIST Personal Identity Verification (PIV) Program updated and refined several supporting documents.

- **Continued involvement, research, and development of Virtualization Guidance and Standards:**
  As a natural follow-up to the publication of security guidelines for hypervisor deployment for server virtualization, ITL published SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*, after extensive public comments, followed by a conference paper titled "*Analysis of Virtual Networking Options for Securing Virtual Machines*." ITL also submitted two Special Publications and three conference papers on Virtualization Security to ISO/IEC JTC1/SC27/WG4 as a NIST/US Contribution. The submissions have now resulted in the ISO/IEC working draft 21878.
- **Ongoing involvement and outreach support among various programs:**
  ITL 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.
- **Continued support and involvement of the Information Security and Privacy Advisory Board (ISPAB):**
  NIST solicited recommendations from the Information Security and Privacy Advisory Board (ISPAB) on draft standards and guidelines regarding information security and privacy issues.
- **Provided research, collaboration, development and improving the System Security Engineering Initiative:**
  ITL published the final public draft of SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, to address the engineering-driven actions necessary to develop more defensible and survivable systems—including the components that compose and the services that depend on those systems.
- **Continued research, collaboration work with other federal agencies along with nonfederal organizations for improving Risk Management Guidelines:**
  Work began on SP 800-53 Revision 5, *Security and Privacy Controls for Systems and Organizations*, with a pre-draft call for comments, adjudication of those comments, and coordination with partners within the Joint Task Force (JTF) Transformation Initiative. SP 800-53 provides organizations with the security controls necessary to appropriately strengthen their systems and the environments in which those systems operate.
- **Published the Initial Public Draft (IPD) of SP 800-171 Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*:**
  This draft provides guidance to federal agencies for the protection of Controlled Unclassified Information when such information is resident in nonfederal systems and organizations.
- **Made significant contributions in the design, standardization, test and measurement of technologies to improve the security and robustness of the Internet's global routing protocol (Border Gateway Protocol (BGP)):**
  ITL's Internet Infrastructure Protection (IIP) program works with industry to develop the measurement science and new standards necessary to ensure the robustness, scalability, and security of the global Internet.
- **Continued research and testing with the Usability and Security project:**
  The ITL usability team's research focused primarily in four areas: passwords, understanding user behavior, cryptography, and privacy.
- **Continued research, developing and updating support tools, and providing resources for the Software Assurance and Reliability, and Computer Forensics projects:**
  ITL produced reference data and test methods for computer forensics and software quality to support the needs of the software assurance, law enforcement, and forensics communities for quality and efficiency improvements.
- **Support of FISMA, ITL conducted workshops, awareness briefings, and outreach to ITL customers:**
  These outreach activities help to ensure a clear comprehension of standards and guidelines, help share ongoing and planned activities, and help ensure that guidelines are scoped in a collaborative, open, and transparent manner. ITL public workshops addressed a diverse range of information security and technology topics, including:

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

  - NICE National K-12 Cybersecurity Education Conference,
  - NICE Annual Conference,
  - Applying Measurement Science in the Identity Ecosystem Workshop,
  - Federal Information Systems Security Educators' Association (FISSEA) Annual Conference,
  - Privacy Controls Workshop: Next Steps for SP 800-53 Appendix J,
  - NIST Trusted Identities Group (TIG) Federated Identity in Healthcare Pilot Program,
  - Cybersecurity Framework Workshop,
  - Open Meeting of The Commission on Enhancing National Cybersecurity,
  - NIST Cloud Computing Forum & Workshop IX,
  - Protecting Consumer Data: Securing Payment and Transaction Information,
  - Information Security Privacy Advisory Board (ISPAB) Meetings,
  - National Strategic Computing Initiative (NSCI): High-Performance Computing Security Workshop,
  - Exploring the Dimensions of Trustworthiness: Challenges and Opportunities,
  - Trustworthy Suppliers Framework Forum,
  - Best Practices in Cyber Supply Chain Risk Management,
  - Random Bit Generation Workshop,
  - Workshop on Software Measures and Metrics to Reduce Security Vulnerabilities,
  - Software Identification (SWID) Tag Implementation and Use Workshop,
  - Software and Supply Chain Assurance Forums,
  - Cybersecurity for Small Manufacturers webinar series,
  - Retail Cybersecurity Workshop,
  - Strengthening Cybersecurity in the Financial Sector with the new NIST Practice Guide, and
  - Cybersecurity in Retail: Trends and Challenges with Point of Sale and Payment Technologies.

- **Annual Reports:**
  The 2016 ITL Cybersecurity Program Annual Report (formerly titled *Computer Security Division Annual Report*) was produced and released as a NIST SP. Former CSD annual reports from fiscal years 2003 through 2015 are available on the Computer Security Resource Center (CSRC) at https://csrc.nist.gov/Publications/Search?requestStatusList=1,3&requestSeriesList=3,1,4,2,8,13,7,9,6,5,10,11,12&requestSortOrder=7&requestDisplayOption=brief&itemsPerPage=25&requestControlFamilyType=All&requestTopicType=All&requestControlFamilyList=&requestTopicList=15&request



ITL CYBERSECURITY PROGRAM ACCOMPLISHMENTS FOR FISCAL YEAR 2016

In FY 2016, ITL continued to research and develop guidance in a broad array of technical areas, including supply chain risk management; forensics, software, security analytics, usability and security, cloud, mobile, and privacy-enhancing technologies; hardware-enabled security; cyber-physical and embedded systems; and other projects. ITL staff and guest researchers have collaborated with global partners from government, industry, and academia, making significant contributions to help secure critical information and the infrastructure. The following sections describe ITL's Cybersecurity Program achievements, including 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.

(Editors' Note: Acronyms used throughout this Annual Report are generally defined when first used. A complete list of Acronyms used in this report is provided in Appendix A of this Annual Report.)

ITL INVOLVEMENT WITH NATIONAL AND INTERNATIONAL IT SECURITY STANDARDS

Figure 1 shows many of the national and international standards-developing organizations (SDOs) involved in cybersecurity standardization. Various ITL staff participate in many cybersecurity standards' activities either in leadership positions or as editors and contributors, including the American National Standards Institute (ANSI); the International Organization for Standardization (ISO); the International Electrotechnical Commission (IEC); the Biometric Application Programming Interface (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. (ASC X9, Inc.) (e.g., X9F – Data & Information Security Subcommittee). Many of ITL's publications have been the basis for both national and international standards projects.

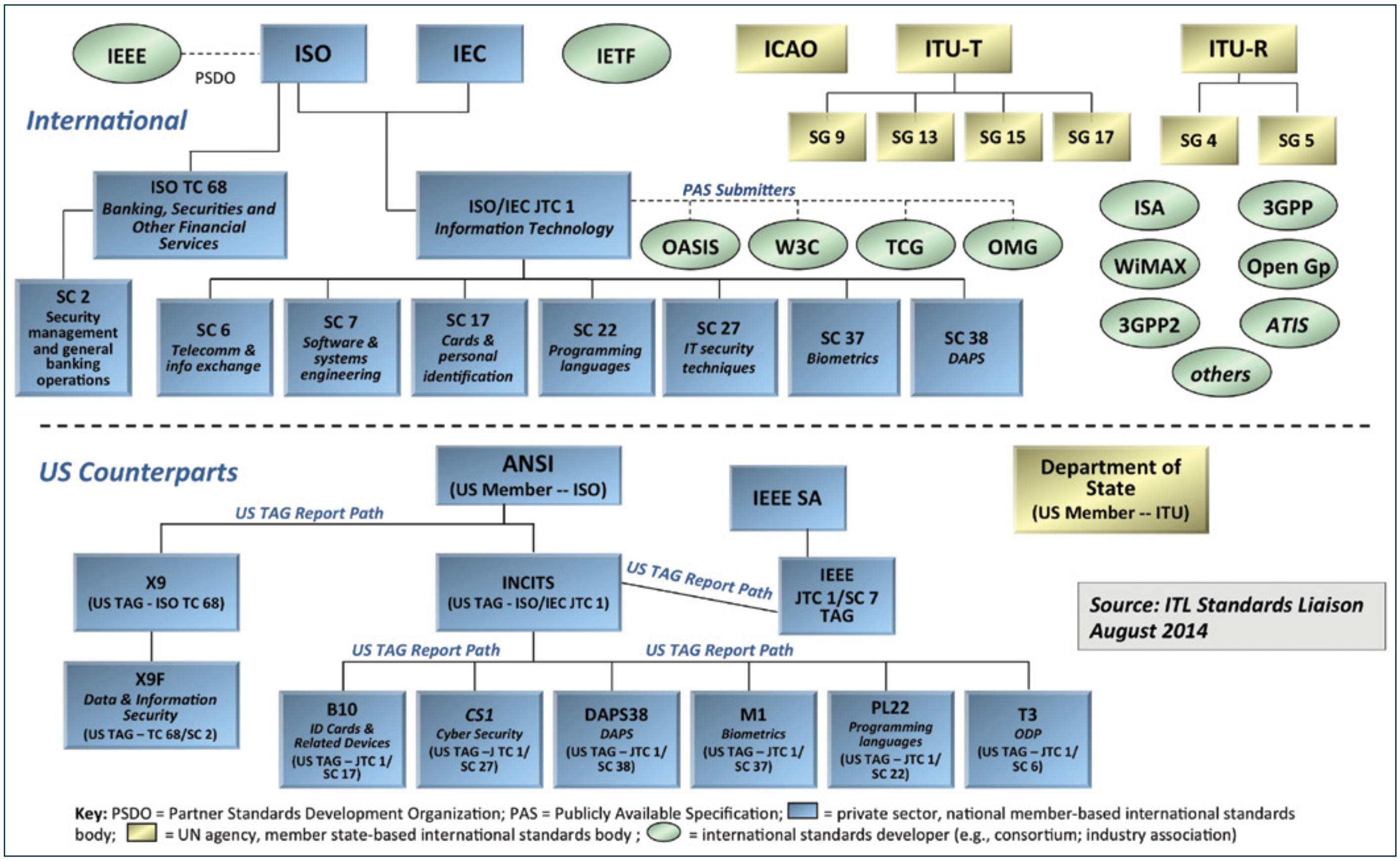
Focus on ISO and ANSI Standardization (ISO/IEC JTC1 SC27 IT Security)

The following paragraphs discuss ITL staff activities in conjunction with the InterNational Committee for Information Technology Standards (INCITS) Technical Committee Cybersecurity 1 (CS1), where ITL's Sal Francomacaro serves as the CS1 Vice Chair. CS1 is the U.S. counterpart for the ISO/IEC SC27 committee for IT Security.

IT Security Techniques Standards

ITL staff actively participate with JTC1/SC27 and its working groups to develop standards for the protection of information and Information and Communications Technology (ICT). This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Management of information and ICT security; in particular, information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to, mechanisms for



IEEE
PSDO
ISO
IEC
IETF
ICAO
ITU-T
ITU-R
International
SG 9
SG 13
SG 15
SG 17
SG 4
SG 5
ISO TC 68 Banking, Securities and Other Financial Services
ISO/IEC JTC 1 Information Technology
PAS Submitters
OASIS
W3C
TCG
OMG
ISA
3GPP
WiMAX
Open Gp
3GPP2
ATIS
others
SC 2 Security management and general banking operations
SC 6 Telecomm & info exchange
SC 7 Software & systems engineering
SC 17 Cards & personal identification
SC 22 Programming languages
SC 27 IT security techniques
SC 37 Biometrics
SC 38 DAPS
US Counterparts
ANSI (US Member -- ISO)
US TAG Report Path
IEEE SA
Department of State (US Member -- ITU)
X9 (US TAG - ISO TC 68)
INCITS (US TAG - ISO/IEC JTC 1)
US TAG Report Path
IEEE JTC 1/SC 7 TAG
Source: ITL Standards Liaison August 2014
X9F Data & Information Security (US TAG – TC 68/SC 2)
US TAG Report Path
US TAG Report Path
B10 ID Cards & Related Devices (US TAG – JTC 1/ SC 17)
CS1 Cyber Security (US TAG –J TC 1/ SC 27)
DAPS38 DAPS (US TAG – JTC 1/ SC 38)
M1 Biometrics (US TAG – JTC 1/ SC 37)
PL22 Programming languages (US TAG – JTC 1/ SC 22)
T3 ODP (US TAG – JTC 1/ SC 6)
Key: PSDO = Partner Standards Development Organization; PAS = Publicly Available Specification; ▭ = private sector, national member-based international standards body; ▭ = UN agency, member state-based international standards body ; ○ = international standards developer (e.g., consortium; industry association)

Figure 1: SDOs involved in Cybersecurity

protecting the accountability, availability, integrity and confidentiality of information;

- Security management support documentation, including terminology and guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems; and
- Security evaluation criteria and methodology.

ITL staff also engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

CONTACT:

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

Next Generation Access Control Standards

ITL has continued the development of an advanced Attribute Based Access Control (ABAC) framework called the Policy Machine, which was designed to be in alignment with an emerging ANSI/INCITS standard under the title of "Next Generation Access Control" (NGAC).

The NIST Policy Machine research and development effort 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 currently under revision.
- *Next Generation Access Control – Generic Operations & Abstract Data Structures (NGAC-GOADS).* Serban Gavrila, ITL, is the editor. The project is assigned project number 2195-D, and the document was published during FY 2016.
- *Next Generation Access Control -Implementation Requirements, Protocols and API Definitions (NGAC-IRPADS).* Project number 2193-D has been assigned. This part will be published as a technical report in FY 2018.

CONTACTS:

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

Mr. Serban Gavrila
(301) 975-4343
serban.gavrila@nist.gov

ISO Standardization of Security Requirements for Cryptographic Modules

ITL has contributed to the activities of ISO/IEC JTC 1 SC/27, which published 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. ISO/IEC 19790 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. These efforts bring consistent testing of cryptographic modules to the global community by providing ISO-equivalent standards representing FIPS 140-2, *Security Requirements for Cryptographic Modules and Derived Test Requirements [DTR]* for FIPS 140-2, *Security Requirements for Cryptographic Modules*. Mr. Randall Easter (CSD) continues as the principal editor for these standards.

ISO/IEC JTC 1/SC 27 Working Group (WG) 3 completed and published revisions, followed with updated corrections, of ISO/IEC 19790:2006 and ISO/IEC 24759:2008. 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) (see: http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2FIEC+19790%3A2012). The two ISO/IEC revisions were developed with international support and the collaboration of governments, industry and academia. Revised corrections of both standards were published on December 15, 2015.

The revision of ISO/IEC 19790:2012 addresses new security areas, such as defined software module boundaries, degraded modes of operation, trusted channels, two-factor authentication, software security, mitigation of fault induction and side-channel attacks, operational self-tests for algorithms, and lifecycle assurance from design to end-of-life.

Figure 2: Cryptographic Module Testing – ISO Standards is a chart of the ISO/IEC standards, as ex-plained above, in which CSD has played a part during the development process.

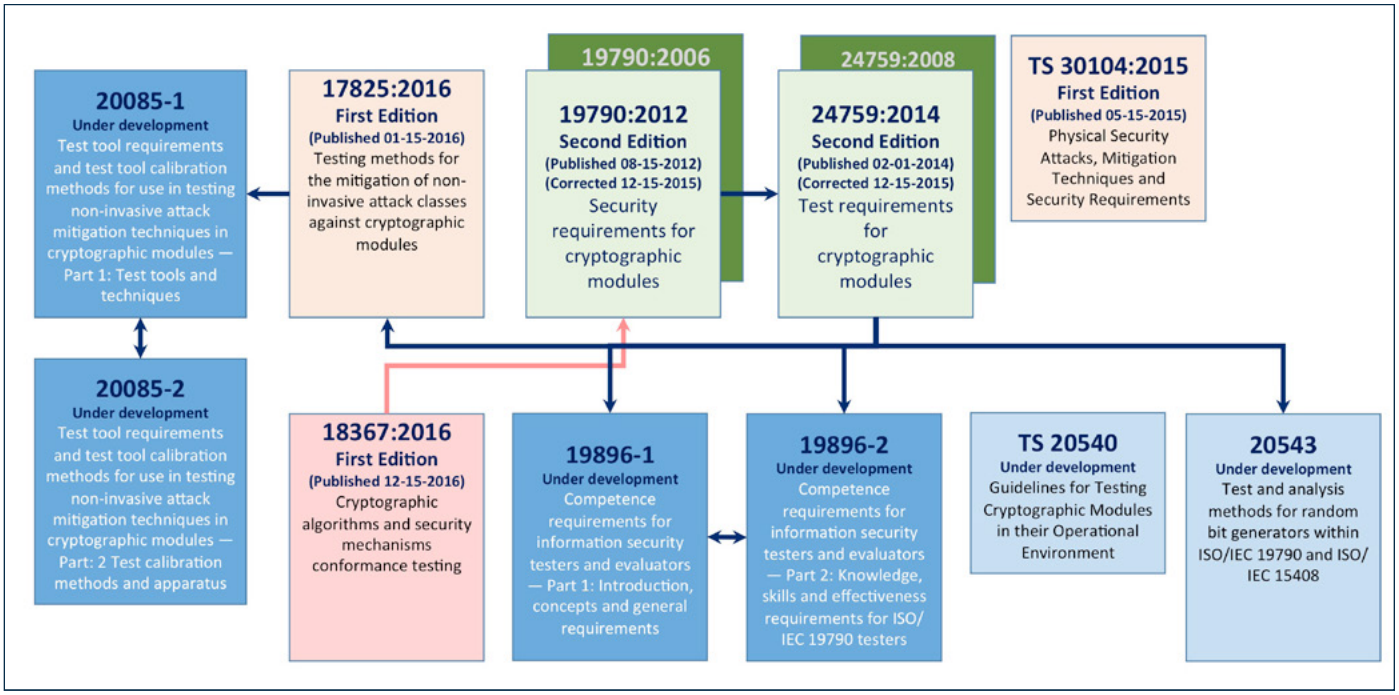

20085-1
Under development
Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques
17825:2016
First Edition
(Published 01-15-2016)
Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
19790:2006
19790:2012
Second Edition
(Published 08-15-2012)
(Corrected 12-15-2015)
Security requirements for cryptographic modules
24759:2008
24759:2014
Second Edition
(Published 02-01-2014)
(Corrected 12-15-2015)
Test requirements for cryptographic modules
TS 30104:2015
First Edition
(Published 05-15-2015)
Physical Security Attacks, Mitigation Techniques and Security Requirements
20085-2
Under development
Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part: 2 Test calibration methods and apparatus
18367:2016
First Edition
(Published 12-15-2016)
Cryptographic algorithms and security mechanisms conformance testing
19896-1
Under development
Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements
19896-2
Under development
Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers
TS 20540
Under development
Guidelines for Testing Cryptographic Modules in their Operational Environment
20543
Under development
Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

Figure 2: Cryptographic Module Testing – ISO Standards

In addition to the aforementioned standards, International Standards ISO/IEC 17825, *Testing methods for the mitigation of non-invasive attack classes against cryptographic modules,* is expected to be published in January 2017 and ISO/IEC 18367, *Cryptographic algorithms and security mechanisms conformance testing,* is on target to be published during December 2016. Mr. Easter was the editor of both standards.

International Standard ISO/IEC 17825 specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4. The test metrics are associated with the security functions specified in ISO/IEC 19790. Testing will be conducted at the defined boundary of the cryptographic module and using Input/Output (I/O) available at the defined boundary .

International Standard ISO/IEC 18367 describes conformance testing methods for cryptographic algorithms and security mechanisms. Conformance testing assures that an implementation of a cryptographic algorithm or security mechanism is correct whether implemented in hardware, software or firmware. It also confirms that it runs correctly in a specific operating environment. Testing may consist of known-answer or Monte Carlo testing, or a combination of test methods. Testing may be performed on the actual implementation or modeled in a simulation environment.

The test methods used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790 and the test metrics specified in this International Standard for each of the associated security functions specified in ISO/IEC 19790 are specified in ISO/IEC 24759. The test approach employed in this International Standard is an efficient "push-button" approach: the tests are technically sound, repeatable and have moderate costs.

ITL is also the principal editor or co-editor of other ISO/IEC documents. ITL'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 international harmonization for the implementation and testing of cryptographic algorithms and modules, while accommodating individual country preferences in the choice of approved security functions.

FOR MORE INFORMATION, SEE:

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

CONTACT:

Mr. Randall J. Easter
(240) 361-8777
randall.easter@nist.gov

Identity Management Devices and Infrastructures Standards (JTC1 SC17 Cards and Personal Identification Devices)

In the area of Identity Tokens and Secure elements, ITL has provided the technical and editorial support of Mr. Ketan Mehta (CSD) in the development and amendment of American National Standard (ANS) 504, *Generic Identity Command Set (GICS)*. GICS enables Personal Identity Verification (PIV), PIV-Interoperable (PIV-I) and Common Access Card (CAC) 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 that aligns with the last revision of the NIST SP 800-73-4, *Interfaces for Personal Identity Verification*, (PIV) specifications.

During FY 2017, ITL staff plans to:

- Contribute to the publication of several revisions of the ISO/IEC 7816 family of standards (*Identification cards - Integrated circuit cards*), which are all relevant to FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* specifications;
- Pursue the standardization and harmonization of identity standards developed in the U.S.;
- Develop requirements and identify standards gaps for Mobile Driving Licenses;
- Enhance the Machine-Readable Travel Documents (ePassport) data model to address privacy and security concerns; and
- Contribute to the development of privacy-enhanced security protocols.

ITL staff will continue to actively support relevant ID management standard initiatives, such as ISO/IEC 19286, *Integrated circuit card (ICC) Privacy-enhancing protocols and services*, and ISO/IEC 18328, *ICC managed devices*.

Web Authentication/FIDO: ITL participates in the development of online authentication specifications. These specifications are developed by the *Fast Identities Online* (FIDO) alliance, which is a consortium of private organizations. ITL also participates in the development of similar specifications (called WebAuthn) for web browsers that are being developed by the W3C consortium. Both the FIDO and WebAuthn specifications enable relying parties to create cryptographic tokens on the end-user's device and subsequently use this cryptographic token to authenticate the end user. These specifications provide multi-factor authentication directives, and they are designed to mitigate common threat vectors for Internet communications, such as phishing, man-in-the-middle, and replay attacks.

ePassport: ITL participates in the development of an ISO/IEC standard (ISO/IEC 7501) for electronic Passports. Specifically, ITL is contributing to the development of passport data structure and its access control. ITL reviews and comments on authentication protocols that are developed to ensure strong user authentication and to protect personally identifiable passport data.

Mobile Driver License: ITL is also participating in the development of an ISO standard (ISO/IEC 18013) for an International Mobile Driver License (DL). During 2016, ITL gathered and discussed functional and security requirements for Mobile DLs. ITL is now developing two models for the Mobile DLs, namely, offline and online models. Once these models are correctly defined, ITL plans to write technical specification for each model.

CONTACTS:

Mr. Salvatore Francomacaro	Mr. Ketan Mehta
(301) 975-6414	(301) 975-8405
salvatore.francomacaro@nist.gov	ketan.mehta@nist.gov

Cloud Computing Standards Within ISO/IEC JTC 1/SC 38 Cloud Computing and INCITS Cloud 38

During FY 2016, ITL has been designated by the Federal Chief Information Officer (CIO) to accelerate the Federal Government's secure adoption of cloud computing by leading efforts to identify existing standards and guidelines. Where standards are needed, ITL works closely with U.S. industry, standards developers, other government agencies, and leaders in the global standards community to develop standards that will support secure cloud computing.

This standardization effort supports federal agencies in adopting and implementing cloud computing infrastructures. This standard work includes standards development within the voluntary, consensus-based standards ecosystem and the development of NIST standards and guidelines for federal agencies, as required by government mandates. The ITL staff participates in developing standards for many aspects of cloud computing. ITL participation helps to ensure the alignment of NIST standards with those of ISO/IEC sub-committees, such as SC 27, SC 38 and their U.S. counterparts, ANSI/INCITS CS1 and Cloud 38. The large number of standards being developed in SC 27 covering areas (such as security, privacy, supply chain, personally identifiable information (PII) processing or virtualization security) interweave with many cloud computing standards being developed by these subcommittees.

Ms. Annie Sokol is a member of ITL's Cloud Computing team and the CSD representative in the standards development program. ITL provides technical and editorial representation in the development of national and international standards in both SC 27 and SC38. Ms. Sokol is currently the co-editor of ISO/IEC 19941, *Information technology–Cloud computing–Interoperability and portability*, which is intended to establish a common understanding of cloud computing interoperability and portability. This document is of interest to cloud stakeholders focusing on cloud service agreements concerning interoperability or portability among cloud services. The ISO/IEC 19941 work aligns with ITL staff involvement in the SC 38 development of ISO/IEC 19086-4 (DIS), *Information technology–Cloud computing–Service level agreement (SLA)*, which has four parts. Of particular interest, ISO/IEC 19086 – Part 1 was published in 2016 and establishes a set of common cloud SLA building blocks (e.g. concepts, terms, definitions, contexts) that can be used to create cloud Service Level Agreements (SLAs).

CONTACT:

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

Biometric Standards and Associated Conformity Assessment Testing Tools

CSD's Biometric Standards and Associated Conformity Assessment Testing Tools team contributes to the development of biometric standards. The team reviews standards documents, develops contributions and feedback and participates in technical and editorial discussions to substantiate NIST and ITL's goals in the biometric field. The team participates in the *International Committee for Information Technology Standards (INCITS) Technical Committee M1 – Biometrics* standards body and related subcommittees. The team also participates in the International Organization for Standardization/International Electrotechnical Commission *(ISO/IEC) Joint Technical Committee (JTC) 1 Subcommittee (SC) 37 – Biometrics* standards body.

CONTACT:

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

RISK MANAGEMENT

Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)

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 that was developed provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help critical infrastructure owners and operators—as well as other interested entities—to identify, assess, and manage cybersecurity-related risk, while protecting business confidentiality, individual privacy, and civil liberties.

In FY 2016, ITL continued to work with a diverse stakeholder community to support the use and understanding of the Cybersecurity Framework. This process included:

- Issuing a Request for Information (RFI) to formally gather stakeholder input about Framework use, evolution, and future governance of the Framework;
- Conducting a public workshop at NIST in Gaithersburg, MD to gather input about the current use of the Framework and the need for an update to the Framework as well as future governance of the Framework;
- Releasing the draft Baldrige Cybersecurity Excellence Builder, a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts;
- Coordinating with critical infrastructure owners and operators, regulators, and other industry organizations through a variety of meetings and industry events to ensure the understanding and use of the Framework;
- Analyzing various industry work products (such as mapping documents) for Framework correctness;
- Consulting with state and local governments, and the governments of other nations regarding their alignment with both the principles and the cybersecurity outcomes of the Framework;

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

- Consulting with international organizations and standards bodies to demonstrate and ensure continued alignment with voluntary international standards; and
- Working with both industry and regulatory organizations to apply the Framework in ways that bring efficiencies to the regulatory process.

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.

In FY 2017, ITL will continue to conduct stakeholder outreach and will work collaboratively to further understand stakeholder needs regarding tools and resources to enable more effective use of the Framework. Additionally, in early 2017, NIST will publish a minor update to the Framework and will minimize any disruption to current Framework users by focusing on clarification and refinement. NIST will also publish guidance on how Federal agencies can use the Cybersecurity Framework, particularly illustrating how the Risk Management Framework (Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*) and Cybersecurity Framework can work together to help agencies develop, implement, and continuously improve their information security programs.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/cyberframework

CONTACTS:

Team email: cyberframework@nist.gov

Mr. Matt Barrett	Mr. Jeff Marron
(301) 975-6259	(301) 975-3846
matthew.barrett@nist.gov	jeffrey.marron@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 and nonfederal organizations build effective information security 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; and
- Conducting outreach to public and private-sector organizations to facilitate the application of the suite of standards and guidelines that support the NIST Risk Management Framework (RMF) (see http://csrc.nist.gov/groups/SMA/fisma/framework.html).

During FY 2016, the ITL FISMA Implementation project continued to strengthen collaboration through the Joint Task Force (JTF) Transformation Initiative, which includes the Department of Defense (DOD), the Intelligence Community (IC), and the Committee on National Security Systems (CNSS), and various federal agencies. 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 JTF 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, ITL worked with the Department of Homeland Security (DHS) to develop guidelines for automation support for security control assessments on a security capability basis and in accordance with the NIST RMF.

In FY 2016, the ITL FISMA Team worked on the following initiatives:

- **System Security Engineering Initiative:** The final public draft of SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, was published to address the engineering-driven actions necessary to develop more defensible and survivable systems—including the components that compose and the services that depend on those systems. To ensure that the publication provides the utmost clarity and focus for our customers, several of the supporting appendices from the second public draft are being recast into their own publications. SP 800-160 will become the flagship publication for the NIST Systems Security Engineering Initiative. NIST publications specifically addressing several key systems security engineering considerations (i.e., resilience, software assurance, and hardware assurance) will be developed and published,

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
https://dx.doi.org/10.6028/NIST.SP.800-195

beginning in 2017. Additionally, the interaction of the NIST RMF with the life cycle processes in SP 800-160, will be described in future updates to existing RMF standards and guidelines.

- **Risk Management Guidelines:** Work began on SP 800-53 Revision 5, *Security and Privacy Controls for Systems and Organizations*, with a pre-draft call for comments, adjudication of those comments, and coordination with our JTF partners. SP 800-53 provides organizations with the security and privacy controls necessary to appropriately strengthen their systems and the environments in which those systems operate, and provides a process for selecting the appropriate controls, which contributes to systems that are resilient in the face of attacks and other threats and protect an individual's privacy. The implementation of SP 800-53, 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*, provides organizations with near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.
- **FISMA Outreach Activity to Public and Private-Sector Organizations:** Cybersecurity outreach briefings were conducted and support was provided to all levels of private-sector organizations and government (including federal, state and local entities) on multiple information security topics of interest. These included, for example, an effective implementation of the NIST RMF, contingency planning, interconnection security agreements, security-focused configuration management, and information security for small businesses. In addition, the ITL FISMA Team responded to hundreds of inquiries from customers, served on cybersecurity advisory panels, and conducted outreach activities with academic institutions, providing information on NIST's security standards and guidelines, and exploring new areas of cybersecurity research and development.
- **Collaboration with JTF partners and other federal organizations:** The FISMA Team worked closely with JTF partners to ensure that the five JTF publications remain current, and to designate additional special publications as JTF guidance. The five JTF publications are:

1. SP 800-30, *Guide for Conducting Risk Assessments*;
2. SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*;
3. SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;
4. SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; and
5. SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*.

The FISMA Team also collaborated with DOD, the IC, DHS, the National Archives and Records Administration (NARA), the Federal Emergency Management Agency (FEMA), the Government Accountability Office (GAO), the Office of Management and Budget (OMB), the General Services Administration (GSA), the Small Business Administration (SBA), and the Inspectors General (IGs) on multiple projects to ensure consistency with FISMA-related guidance and to protect information in a way that is commensurate with risk. In addition, the FISMA Team served as co-chairs on the Committee on National Security Systems working groups.

In FY 2016, the FISMA Team completed the following activities:

- Published the final public draft of SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*;
- Started the development of SP 800-53, Revision 5, *Security and Privacy Controls for Systems and Organizations*;
- Published the Initial Public Draft (IPD) of SP 800-171 Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, to provide guidance to federal agencies for the protection of Controlled Unclassified Information when such information is resident in nonfederal systems and organizations;
- Published the IPDs of NISTIR 8011, *Automation Support for Ongoing Assessments, Volume 1 - Overview, and Volume 2 - Hardware Asset*

Management, and adjudicated public comments in partnership with DHS;

- Started the development of a web application to automate the process for updating SP 800-53 in order to keep it as current and relevant as possible;
- Continued the development of SP 800-60, Revision 2, *Guide for Mapping Types of Information and Information Systems to Security Categories*, in partnership with the National Archives and Records Administration; and
- Continued the development of the initial public draft of SP 800-18 Revision 2, *Guide for Developing Security Plans for Federal Information Systems and Organizations*.

In FY 2017, the FISMA Team intend to:

- Finalize SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*;
- Finalize and publish the IPD of SP 800-53, Revision 5, *Security and Privacy Controls for Systems and Organizations*, and continue the development of the final publication;
- Complete the development of a web application for the automated support of SP 800-53 updates and the public comment process;
- Continue the collaboration with DHS to develop and publish additional NISTIR 8011 volumes;
- Finalize and publish the initial public draft of SP 800-60, Revision 2, *Guide for Mapping Types of Information and Information Systems to Security Categories* in partnership with NARA and OMB;
- Continue the development of SP 800-18, Revision 2, *Guide for Developing Security Plans for Federal Information Systems and Organizations*;
- Finalize and publish NIST SPs 800-12 Revision 1, *An Introduction to Information Security*, and 800-47 Revision 1, *Security Guide for Interconnecting Systems*;
- Expand cybersecurity outreach to include additional state, local, and tribal governments, as well as private-sector organizations and academic institutions;
- Continue to support federal agencies in the effective implementation of the RMF; and
- Continue the collaboration with JTF partners and other federal organizations.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

The ITL FISMA Team email is: sec-cert@nist.gov

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

Mr. Nedim Goren
(301) 975-5233
nedim.goren@nist.gov

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

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

Privacy Engineering Program

ITL research in information technology, including cybersecurity, cloud computing, big data, the Smart Grid and other cyber-physical systems; aims to improve the products and services that bring great advancements to U.S. national and economic security and the quality of life. Much of this research pertains to the trustworthiness of these information technologies and the systems in which they are incorporated. Given concerns about how information technologies may affect privacy at individual and societal levels, the ITL Privacy Engineering Program (PEP) supports the development of trustworthy information systems by applying measurement science and system engineering principles to the creation of frameworks, risk models, guidance, tools, and standards that protect privacy, and by extension, civil liberties. The PEP also seeks to promote NIST and ITL leadership in privacy research and privacy-enhancing technologies.

The PEP was formally established as a program in FY 2016 as part of ACD. In 2014, the PEP team initiated research with two workshops to explore the foundations of privacy engineering and risk management and published a draft of NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, in May 2015 to introduce a novel set of privacy engineering objectives and a privacy risk assessment framework (see http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf).

In FY 2016, the PEP focused resources in the following areas: developing a near-term strategic plan, finalizing NISTIR 8062, and coordinating with other NIST programs and research efforts to address and integrate privacy. The strategic plan is organized around the basic goals of advancing the development of privacy engineering and risk management processes and the deployment of privacy-enhancing technologies, as well as positioning NIST as a leader in privacy research.

Advancement of Privacy Engineering and Risk Management

To further the development of processes for privacy engineering and risk management (and inform its finalization of NISTIR 8062), the PEP team conducted outreach with stakeholders, researched privacy assessment and risk mitigation methods, and supported the use of its Privacy Risk Assessment Methodology (PRAM) inside and outside the Federal Government. The PEP team also worked extensively with OMB on the revision of Circular A-130, which lays out new requirements for federal agencies to address privacy risk in their information systems to ensure that the Circular and the PEP were in alignment on privacy risk management.

As a result of these efforts, the PEP team has revised NISTIR 8062 to more clearly introduce the concepts of privacy engineering and risk management, clarify the rationale for the introduction of a set of privacy engineering objectives and a risk model, and include a roadmap for the development of comprehensive privacy risk management guidance for federal agencies that parallels NIST guidance for information security.

The PEP also co-hosted a workshop in September 2016 with the Department of Transportation to gather input on changes to the privacy controls in Appendix J of NIST SP 800-53, which is undergoing its fifth revision. The workshop initiated the first stage of executing the guidance roadmap that the PEP will continue in FY 2017.

Coordination with Other NIST Programs

An important role for the PEP is a collaboration and coordination with other NIST programs and research efforts to better integrate privacy in the pursuit of more trustworthy systems.

Of particular note, the PEP put its preliminary concepts into practice with the PRAM, a set of worksheets that take an organization through a privacy risk assessment of its systems. Working with the ITL Trusted Identities Group (TIG), the PEP team supports the TIG grant awardees' use of the PRAM to evaluate privacy risks and develop mitigating controls in their pilots. The PEP team also used the PRAM for privacy evaluations of information systems in partnership with federal agencies, including DHS and GSA. The lessons learned from these PRAM evaluations have been critical to the PEP team's understanding of the practical aspects of applying privacy risk management concepts in system development.

The program also collaborated on many other projects, including a partnership PEP with TIG on a building block at the NIST National Cybersecurity Center of Excellence (NCCoE) to use the new privacy engineering objectives (see https://nccoe.nist.gov/sites/default/files/library/project-descriptions/privacy-enhanced-identity-brokers-project-description-draft.pdf). There was also collaboration with CSD and NIST's Engineering Laboratory (EL) on the big data and cyber-physical systems frameworks and related efforts, and with ITL's Information Access Division (IAD) to support a successful Build-the-Future proposal on de-identification, a process used to prevent a person's identity from being associated with information.

Figure 3: Collaboration Between PEP and Other NIST Programs in FY 2016 illustrates a number of projects from the programs described above that PEP collaborated on in FY 2016. These projects can be categorized as applied privacy projects or guidance and frameworks.

NIST Leadership in Privacy

The program worked across public and private-sector organizations to advance NIST's role in privacy. The PEP team participated in the Internet Policy Task Force's Privacy Working Group (see https://www.ntia.doc.gov/category/internet-policy-task-force) and now hold leadership positions in the Federal Privacy Council (established by Executive Order in FY 2016), and the Networking and Information Technology Research and Development (NITRD) Program's Privacy Research Interagency Working Group, whose work included drafting the National Privacy Research Strategy (see https://www.nitrd.gov/cybersecurity/nationalprivacyresearchstrategy.aspx), the Identity Ecosystem Steering Group, and the Fast Identity Online Alliance.

The PEP team presented its research at major conferences, including the RSA Conference, the International Association of Privacy Professionals Global Summit and Privacy Academy, the Institute of Electrical and Electronics Engineers International Workshop on Privacy Engineering, the Privacy + Security Forum, the TRUSTe Privacy Risk Summit, and the Computing Community Consortium's Privacy by Design Workshop, among others.

The PEP team contributed to ongoing standards and framework development efforts in various organizations, including the Identity Ecosystem Steering Group, the Fast Identity Online Alliance, and the ISO.

In FY 2017, the PEP will publish the final version of NISTIR 8062, slated to be released in January 2017 (see http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf). The PEP will also work on developing privacy risk

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

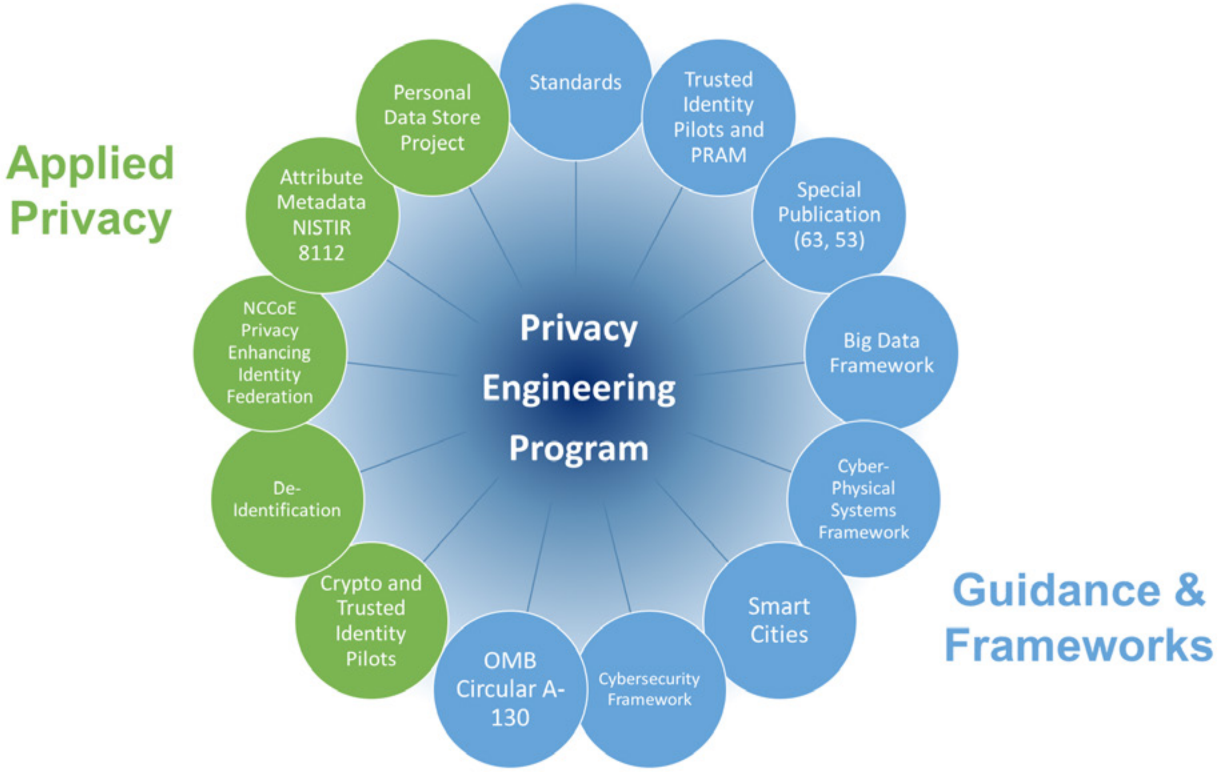

Applied Privacy
Privacy Engineering Program
Standards
Trusted Identity Pilots and PRAM
Special Publication (63, 53)
Big Data Framework
Cyber-Physical Systems Framework
Smart Cities
Cybersecurity Framework
OMB Circular A-130
Crypto and Trusted Identity Pilots
De-Identification
NCCoE Privacy Enhancing Identity Federation
Attribute Metadata NISTIR 8112
Personal Data Store Project
Guidance & Frameworks

Figure 3: Collaboration Between PEP and Other NIST Programs in FY 2016

management guidance for federal agencies, beginning with a revision of the privacy controls in NIST SP 800-53. The program will continue to collaborate with other NIST programs as they seek to address privacy challenges and will work with stakeholders to promote privacy engineering and risk management practices. The PEP team will also continue to seek leadership opportunities in public and private-sector organizations to position NIST on the leading edge of privacy research. Finally, The PEP will explore new areas for privacy research that have broad-based application and support federal agency mission-critical needs in managing privacy risk.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/itl/privacy-engineering

CONTACTS:

PEP Team email: privacyeng@nist.gov

Ms. Naomi Lefkovitz
(301) 975-2924
naomi.lefkovitz@nist.gov

Ms. Ellen Nadeau
(202) 306-4033
ellen.nadeau@nist.gov

(Editors' Note: Mr. Sean Brooks was part of this project team and has since left NIST.)

Cyber Supply Chain Risk Management (SCRM)

Information and Communications Technology (ICT) relies on a complex, globally distributed, and interconnected supply chain ecosystem to provide highly refined, cost-effective, and reusable solutions. This ecosystem is composed of various entities with multiple tiers of outsourcing, diverse distribution routes, assorted technologies, laws, policies, procedures, and practices, all of which interact to design, manufacture, distribute, deploy, use, maintain, and manage ICT products and services.

The factors that allow for low-cost, interoperability, rapid innovation, a variety of product features, and other benefits, also increase the risk of a compromise to the ICT supply chain, which may result in risks to the end user. These ICT supply chain risks may include an insertion of counterfeits, unauthorized production, tampering, theft, and the insertion of malicious software and hardware as well as poor manufacturing and development practices in the ICT supply chain.

Cyber Supply Chain Risk Management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains. It covers the entire life cycle of a system (including design, development, maintenance, and destruction), as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an ICT product or service at any stage.

In FY 2016, ITL continued to research the state of Cyber SCRM in both the public and private sectors, related standards and initiatives, effective practices, and metrics. ITL partnered with a team composed of representatives from the Federal Government (GSA and DHS), the insurance industry (Zurich and Beecher Carlson) and academia (the University of Maryland) to begin fundamental research and build the tools necessary to measure and assess the actual effectiveness of cybersecurity strategies and controls. The effort will use voluntary, secure and anonymized risk assessments based on the NIST Cybersecurity Framework to begin developing a large-scale anonymized data set that will, for the first time, demonstrate cause and effect relationships between cyber supply chain capability levels and organizational performance outcomes over time.

Also in FY 2016, ITL co-chaired, with the Department of Defense, the primary interagency working group on cyber SCRM to revise CNSS Directive (CNSSD) No. 505, *Supply Chain Risk Management*, which assigns responsibilities and establishes minimum criteria for the development and deployment of capabilities for SCRM of National Security Systems. ITL also co-chaired the Software and Supply Chain Assurance (SSCA) Forum and Working Groups, the purpose of which is to bring together a stakeholder community of government, industry, and academic experts in this field. Meetings are held quarterly and cover a variety of subjects of interest to attendees.

In April 2016, ITL held a workshop regarding an update to the NIST Cybersecurity Framework (CSF). During the workshop, information was gathered in a breakout session regarding attendees' views about improving how SCRM is covered in the CSF. Several ideas were proposed, and NIST plans to incorporate the feedback into an updated version of the CSF.

In May 2016, ITL hosted a forum event led by the Institute for Defense Analyses (IDA) about their Trustworthy Supplier Framework (TSF), a prototype toolbox that maps various existing standards and practices to the controls provided in NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. The TSF is intended to increase the utility of existing standards to buyers and program managers making supplier selections, while simultaneously allowing suppliers flexibility in meeting procurement requirements. The forum provided an opportunity for ITL to understand the needs of stakeholders in this arena. The information will be used by IDA in their further development of the Trustworthy Supplier Framework and by ITL in future updates to SP 800-161 and other related publications.

In FY 2017, ITL will continue to collaborate with stakeholders in government, industry, and academia to conduct research, produce needed standards and guidance, and seek opportunities to create greater awareness across all sectors and types and sizes of organizations. ITL will:

- Conduct research and draft guidance on how organizations identify critical systems and components that need additional protections;
- Conduct research on applicable metrics and measures useful to cyber supply chain risk management;
- Conduct an effectiveness study with the goal of demonstrating cause-and-effect relationships between cyber supply chain capability levels and organizational performance outcomes over time;
- Continue to co-chair the interagency working group on cyber supply chain risk management, and also to co-chair and sponsor the Software and Supply Chain Assurance Forum;
- Continue to engage stakeholders in identifying opportunities to create greater awareness about cyber supply chain risks and available standards, practices, guidance and related tools; and
- Continue to engage stakeholders in identifying opportunities and needs for providing additional guidance regarding identifying and implementing supply chain protections.

FOR MORE INFORMATION, SEE:

http://csrc.nist.gov/scrm/

CONTACTS:

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

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

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

BIOMETRIC STANDARDS AND ASSOCIATED CONFORMITY ASSESSMENT TESTING TOOLS

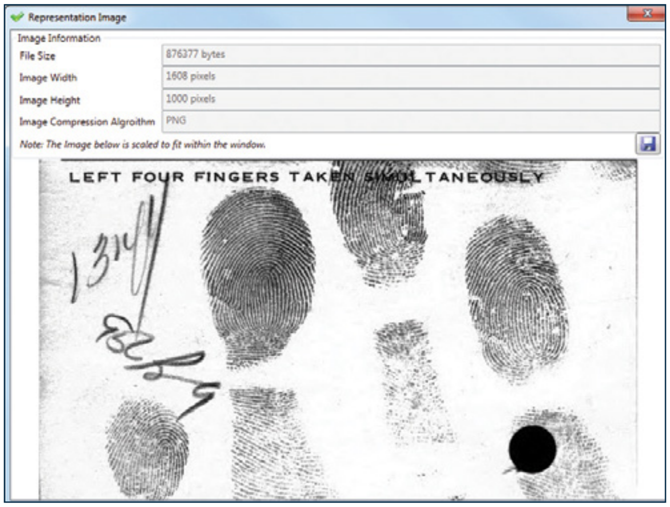
ITL supports the development of biometric conformance testing methodology standards and other conformity assessment efforts through active technical participation in the development of these standards and the development of associated conformance test software, architectures and test suites, collectively known as Biometric Conformance Test Software (BioCTS). These test tools are developed to promote the adoption of these standards and to support users, product developers, and testing labs that require conformance to selected biometric standards. ITL contributes to the development of biometric standards and participates in the *INCITS Technical Committee M1 – Biometrics* and related subcommittees and in *ISO/IEC Joint Technical Committee (JTC) 1 Subcommittee (SC) 37 – Biometrics* standards bodies. ITL plans to continue this work in FY 2017.

BioCTS

In FY 2016, the BioCTS team released refined versions of existing software and researched the use of machine-readable data to accelerate conformance test development and increase support for profiles and user-defined requirements.

There were two updates to the BioCTS for ANSI/NIST-ITL (AN) software suite in FY 2016. These updates were primarily focused on enhancing the underlying codebase, increasing performance, and adding more user-friendly features. The testing architecture has been updated to be more maintainable and more robust. The update represents a complete overhaul of the BioCTS for AN's initial release in 2012. A list of changes made to BioCTS for AN can be found in the Changelog (see https://csrc.nist.gov/Projects/Biometric-Conformance-Test-Software).

In addition to updates to BioCTS software, the team released an updated ANSI/NIST-ITL Data Extractor, illustrated in Figure 4: ANSI/NIST-ITL Extractor Software which shows the internal data records within an ANSI/NIST-ITL file. The Data Extractor allows data (images, text, etc.) to be saved from an ANSI/NIST-ITL formatted file, as well as providing a high-level overview of the file and its internal structure.



Representation Image

Image Information

File Size: 876377 bytes

Image Width: 1608 pixels

Image Height: 1000 pixels

Image Compression Algorithm: PNG

Note: The Image below is scaled to fit within the window.

Figure 4: ANSI/NIST-ITL Extractor Software

The BioCTS team researched the new Machine Readable Tables (MRTs) for the ANSI/NIST-ITL Biometric Standard (AN-MRTs) to determine their suitability for integration into conformance testing efforts. The AN-MRTs encode many of the human-readable requirements specified in the base ANSI/NIST-ITL Biometric Standard (and related profiles, such as Federal Bureau of Investigation (FBI) Electronic Biometric Transmission Specification (EBTS)) in a manner that can be parsed and understood by software. The BioCTS team developed software capable of parsing and testing these tables to ensure a valid MRT format using MRT Schema documents and MRT element definitions. The results of our tests were documented and provided to the authors of the AN-MRTs for incorporation into future versions of the tables for the benefit of all MRT users. The software used to develop these results may be released in the future as a standalone tool for validating and analyzing AN-MRT files. The new BioCTS software will use the AN-MRTs as an external resource. This will allow updates to be made to the MRTs to incorporate the latest conformance requirements, correct errors, or conduct experiments without releasing an updated version of BioCTS itself.

An initial version of this software began development in FY 2016, and this effort is expected to continue in FY 2017.

FOR MORE INFORMATION, SEE:

BioCTS - Biometric Conformance Test Tools:

https://www.nist.gov/itl/csd/biometrics/biometric-conformance-test-software-biocts

BioCTS for ANSI/NIST-ITL User Guide:

https://csrc.nist.gov/Projects/Biometric-Conformance-Test-Software/publications

CONTACT:

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

SECURITY OF CYBER-PHYSICAL AND INDUSTRIAL CONTROL SYSTEMS

Security of Cyber Physical Systems

NIST's Cyber-Physical Systems (CPS) effort will provide the next generation of "smart" co-designed and co-engineered interacting networks of physical and computational components. Specifically, ITL supports the effort by providing cybersecurity and privacy expertise to address CPS-specific cybersecurity and privacy challenges. Such challenges are related to emerging technical areas, such as personalized health care, emergency response, traffic-flow management, and electric power generation and delivery. Other phrases that are often referenced along with CPS technologies include:

- Internet of Things (IoT);
- Industrial Internet;
- Smart Cities;
- Smart Grid; and
- "Smart" Anything (e.g., Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances) (see http://www.nist.gov/cps/).

CPS aims for increased efficiency and interaction between the digital and physical worlds. Ensuring that these emerging and evolving systems are reliable, trustworthy, secure, and that they protect the privacy of information poses a unique cybersecurity challenge. Other challenges of CPS include the need for an integration with legacy components and allowance for emerging technologies as well as real-time response in support of extremely high availability, predictability, and reliability.

Cybersecurity and privacy considerations are critical to the safe and resilient design, development, and operation of CPS. Addressing both the opportunities and challenges of CPS requires a broad collaboration to develop a common foundation, including a consensus definition, vocabulary, reference architecture, and a shared understanding of the essential roles of timing, cybersecurity, and data interoperability. ITL is researching the cybersecurity and privacy needs of the broader landscape of CPS by applying their subject-matter expertise in cybersecurity and privacy to various instances of CPS. These instances may include industrial control systems, the smart grid, hardware-enabled security, and embedded systems, to name a few.

In FY 2016, ITL provided leadership for the Cybersecurity and Privacy subgroup of the CPS Public Working Group (PWG)—which focused on identifying strategies for cybersecurity and privacy in CPS as well as working collaboratively with the other subgroups to ensure the inclusion of cybersecurity as a design principle during the development processes.

After publishing a *Draft Framework for CPS* in September 2015—which compiled the work of the five PWG technical subgroups—the CPS PWG published version 1.0 of the *Framework for Cyber-Physical Systems* in May 2016. The document is the culmination of several years' work by the CPS PWG, which includes several hundred members drawn primarily from industry, academia, and government. As a follow-on to the Framework's release, in August 2016, ITL, in collaboration with NIST's Engineering Lab, hosted the Trustworthiness Launch Workshop at NIST in Gaithersburg, MD. A key goal for the workshop was to promote interaction around integrated goals for trustworthy cyber-physical systems to lay the foundation for future trustworthiness in science.

In July 2016, ITL published NIST SP 800-183, *Networks of 'Things',* which offers an underlying and foundational understanding of IoT by exploring the components that belong to most distributed systems. In FY 2017, foundational and applied research will be conducted in the areas of CPS and IoT. ITL 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.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/cps/

CONTACTS:

Mr. Jeff Marron	Ms. Suzanne Lightman
(301) 975-3846	(301) 975-6442
jeffrey.marron@nist.gov	suzanne.lightman@nist.gov

Cybersecurity for Industrial Control Systems

NISTs Industrial Control System (ICS) cybersecurity effort is focused on providing guidance and insight into the domain of securing connected physical systems. ITL, in collaboration with NIST's Engineering Laboratory, is developing and implementing guidance aimed at effectively securing ICS—initially focusing on Smart Manufacturing Environments. Utilizing a cybersecurity performance test bed for ICS, NIST will measure the performance of these systems when instrumented with cybersecurity protections, in accordance with the best practices and requirements prescribed by national and international standards and guidelines. Examples of such standards and guidelines include ISA/IEC-62443, *Industrial Automation and Control Systems (IACS) Security***,** and NIST SP 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*.

Industrial control systems are an essential component in manufacturing environments; increasing reliance on technology, communication, and the interconnectivity of ICS and IT has expanded the number of potential vulnerabilities and increased the potential risk to manufacturing operations. While these manufacturing systems become 'smarter' and increasingly connected (providing a tremendous increase of value and efficiency), they also present a new challenge regarding how cybersecurity can be effectively applied to the connected domain.

The ICS team has utilized existing standards, in conjunction with the NIST Cybersecurity Framework, to develop a target Profile for applying cybersecurity protections within manufacturing environments. The development of this profile helps establish a roadmap for reducing cybersecurity risk for manufacturers in a way that is aligned with manufacturing-sector goals and industry best practices. The profile also tailors the existing cybersecurity control language to account for unique requirements in these operational environments.

In FY 2016, leading a session during the 2016 Cybersecurity Framework Workshop, the team solicited feedback from industry partners to help advance the development of the profile. The draft Cybersecurity Framework Manufacturing Profile was published as a whitepaper that solicited comments from the public. The Profile focuses on desired cybersecurity outcomes and can be used as a roadmap to identify opportunities for improving the current cybersecurity posture of a manufacturing system.

In FY 2017, NIST will continue its research in the ICS domain to include incorporating feedback and finalizing the Manufacturing Profile, implementing the defined cybersecurity protections onto the cybersecurity performance test bed, and measuring and understanding the performance impacts of implemented cybersecurity protections.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/programs-projects/cybersecurity-smart-manufacturing-systems

http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft.pdf

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

CONTACTS:

Mr. Jeffrey Cichonski	Mr. Keith Stouffer
(301) 975-3293	(301) 975-3877
jeffrey.cichonski@nist.gov	keith.stouffer@nist.gov

FEDERAL CYBERSECURITY RESEARCH & DEVELOPMENT (R&D)

The Networking and Information Technology Research and Development (NITRD) program provides a framework in which many federal agencies come together to coordinate their networking and IT research and development (R&D) efforts. NIST remains 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 2016, the NITRD Cybersecurity and Information Assurance (CSIA) Interagency Working Group (IWG) monthly meetings provided an opportunity to learn and share information about NIST's ongoing research. Participants also learned about connections with the February 2016 Federal Cybersecurity Research and Development Strategic Plan (see https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf). With Mr. Bill Newhouse serving as the NIST co-chair of the CSIA IWG, NIST helped guide the agenda for the monthly meetings to explore the defensive elements and critical elements in the R&D Strategic Plan.

In FY 2016, members of the National Privacy Research Forum published a National Privacy Research Strategy, and a new Privacy R&D Interagency Working Group (IWG) was established, co-chaired by Naomi Lefkovitz, and Simson Garfinkel (ITL), who brought their expertise to the development process for the privacy R&D plan. (see https://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=65)

NIST is 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 publications with researchers throughout the Federal Government. The SCORE committee interacts with federal leaders and reports to the National Science & Technology Council's Committee on Homeland & National Security.

FOR MORE INFORMATION, SEE:

http://www.nitrd.gov/

CONTACT:

Mr. Bill Newhouse
(301) 975-0232
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. Voting security team members from ITL conduct research and develop guidelines and best practices for voting system security.

The primary objective of NIST's work is to support the development of the Voluntary Voting System Guidelines (VVSG), a broad set of equipment guidelines used by the EAC to certify voting systems. The current version of these guidelines is VVSG 1.1, which was approved by the EAC in March 2015. Initial efforts on the next revision of the VVSG have already begun. Beginning in 2015, NIST established public working groups to gather input and conduct the collaborative research necessary for the development of further guidelines/standards. These working groups consist of three election groups and four technology groups focused on human factors, cybersecurity, interoperability, and testing. The overall goal of the working groups is to lay the groundwork for a revision of the VVSG, as many jurisdictions are facing the need for a technology refresh since many voting systems are more than ten years old.

In the months leading up to the November 2016 election, NIST engaged with DHS, EAC, and the Department of Justice (DOJ) to help states better identify and manage their cybersecurity risks to election systems and voting systems for the upcoming election. This group ensured that election officials were aware of existing resources that are available to help them (including the guidelines and best practices that exist for voting and other IT systems, cyber hygiene scanning services by DHS, and threat and vulnerability bulletins).

In FY 2017, the voting working group will focus its efforts on the next revision of the VVSG. Based on feedback from the TGDC and election officials around the country, the new revision is expected to address new technologies and election use cases that have become commonplace in election systems. Additionally, the cybersecurity group plans to investigate security considerations and develop guidance in the areas of voter registration, electronic pollbooks, blank ballot delivery, ballot marking, auditing, and election-night reporting.

FOR MORE INFORMATION, SEE:

https://vote.nist.gov

CONTACTS:

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

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

SOFTWARE ASSURANCE & RELIABILITY

Improving computer security depends on improving software, that is, on reducing the number and severity of vulnerabilities in code. To achieve fewer vulnerabilities, it is essential to know what kinds of vulnerabilities and weaknesses there are and to know how to find them so they can be fixed. The Software Assurance Metrics and Tool Evaluation (SAMATE) program has two primary components: the Static Analysis Reference Dataset (SARD) and the Static Analysis Tool Exposition (SATE). In FY 2016, NIST produced a report on Dramatically Reducing Software Vulnerabilities and a workshop report on Software Measure and Metrics to Reduce Security Vulnerabilities.

- The purpose of SARD is to provide users, researchers, and software security assurance tool developers with a set of computer programs with known security flaws. This allows end users to evaluate tools and tool developers to test their methods. The set includes "wild" (production),

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

"synthetic" (written to test or generated for the test), and "academic" (from students) test cases. The SARD also contains real software applications with known bugs and vulnerabilities. The set is intended to encompass a wide variety of possible vulnerabilities, languages, platforms, and compilers. The SARD is a large-scale effort, gathering test cases from many contributors. ITL has more information about the SARD, including goals, structure, test suite selection, etc. at https://samate.nist.gov/index.php/SARD.html. In FY 2016, the SARD was increased by approximately 40,000 PHP (PHP is a server-side scripting language designed primarily for web development but also used as a general-purpose programming language) and over 30,000 C# test cases (C# is a new programming language designed for building a wide range of enterprise applications that run on the .NET Framework).

- SATE is designed to advance research (based on large test sets) in, and improvement of, static analysis tools that find security-relevant defects in source code. Participating toolmakers run their tools on a set of programs. Researchers, led by NIST, analyze the tool reports. The results and experiences are reported at a workshop. The tool reports and analysis are made publicly available at a later date. SATE's purpose is NOT to evaluate nor to choose the "best" tools. Rather, it is aimed at exploring the following characteristics of tools: relevance of warnings to security, their correctness, and prioritization. SATE's goals are:
    - To enable empirical research based on large test sets,
    - To encourage the improvement of tools, and
    - To speed the adoption of tools by objectively demonstrating their use on real software.

There have been five SATEs since the program began in 2008. The most recent exposition was held in 2014. In FY 2016, planning commenced for SATE VI.

FOR MORE INFORMATION, SEE:

http://samate.nist.gov

CONTACT:

Dr. Paul Black
(301) 975-4794
paul.black@nist.gov

COMPUTER FORENSICS

Digital evidence includes data on computers and mobile devices, including audio, video, and image files as well as software and hardware. Digital evidence can be a part of investigating most crimes, since material relevant to the crime may be recorded in digital form. Methods for securely acquiring, storing and analyzing digital evidence quickly and efficiently are critical. ITL promotes the efficient and effective use of computer technology to investigate crimes. The project team develops tools for testing computer forensic software, including test criteria and test sets. ITL also maintains the National Software Reference Library – a vast archive of published software applications that is an important resource for both criminal investigators and historians.

National Software Reference Library

The National Software Reference Library (NSRL) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations. The NSRL also provides a research environment to promote the development of new forensics techniques and other applications in computer science.

In FY 2016, the NSRL published four releases of the RDS, which continues to be the premier software resource. There are currently 21,000 applications and 200,000,000 files. The project team completed a project with the Stanford University Library to preserve thousands of first-generation computer packages. In FY 2017, the NSRL was expanded to include mobile apps.

Computer Forensics Tool Testing Project

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. The goal of the Computer Forensic Tool Testing (CFTT) project at NIST is to establish a methodology for testing computer forensic software tools by the development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The project is intended to provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the capabilities of the tools. A capability is required to ensure that forensic software tools consistently produce accurate and objective test results. The project team's approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing.

In FY 2016, the CFTT project was expanded to allow forensics testers to use the NIST testing methodology in their own labs and to produce standardized test reports. Currently, the project supports disk imaging testing and will be expanded to support hard-disk write blocking and mobile forensics in 2017. The CFTT project also maintains the Forensics Tool Catalog and the Computer Forensics Reference Dataset.

FOR MORE INFORMATION, SEE:

http://www.nsrl.nist.gov and

http://www.cftt.nist.gov

CONTACTS:

Mr. Doug White (301) 975-4761 doug.white@nist.gov	Dr. Jim Lyle (301) 975-3270 james.lyle@nist.gov

NATIONWIDE PUBLIC SAFETY BROADBAND NETWORK (NPSBN) CYBERSECURITY

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

In February of 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 Nationwide 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" (see 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 2016, CSD, ACD, and the NCCoE supported the joint National Telecommunications and Information Administration (NTIA) and NIST Public Safety Communications Research (PSCR) program with efforts in public-safety mobile-application security, identity management, data and application isolation technologies, and enabling cybersecurity capabilities on the PSCR 700 MHz LTE demonstration network located in Boulder, Colorado (see http://www.pscr.gov). At PSCR's Annual Public Safety Broadband Stakeholder Conference in June 2016, CSD and ACD organized and moderated a panel called "Public Safety and Network Security Enhancements," led two breakout sessions on LTE Network Security, and had a booth highlighting the cybersecurity-related efforts of PSCR.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

Figure 5: CSD and ACD researchers highlighting their work at the June 2016 Public Safety Broadband Stakeholder Meeting hosted by PSCR.

During FY 2016, CSD and ACD published NISTIR 8080: *Usability and Security Considerations for Public Safety Mobile Authentication*, and NISTIR 8135: *Identifying and Categorizing Data Types for Public Safety Mobile Applications Workshop Report*. In addition, CSD and ACD released draft NISTIR 8136; *Mobile Application Vetting Services for Public Safety - an Informal Survey*, for public comment.

CSD and ACD 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 and ACD broadened its scope within the Internet Engineering Task Force (IETF) to include efforts related to public safety.

In FY 2017, CSD and ACD 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 and ACD will continue to engage the public-safety communications community by organizing workshops and conferences and participating in events such as the Association of Public-Safety Communications Officials (APCO) Annual Meeting, PSRC's Annual Public Safety Broadband Stakeholder Conference, and the International Wireless Communications Expo (IWCE).

CONTACTS:

Ms. Sheila Frankel	Dr. Nelson Hastings
(301) 975-3297	(301) 975-5237
sheila.frankel@nist.gov	nelson.hastings@nist.gov

SMART GRID CYBERSECURITY

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 the generation systems to the distribution systems, and to exchange usage and billing information between utilities and their customers. The key to the successful deployment of the smart grid infrastructure is the development of a 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.

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 FY 2016, researchers from CSD, ACD, and the Software and Systems Division (SSD) worked on developing security tools for networks specifically designed to support the next-generation electrical power systems. The researchers concentrated on authenticating the provenance of multicast data streams from emerging power system sensors called Phasor Measurement Units. By authenticating the sensors to the utility, the utility can trust that their sensor measurements are coming from the correct sensors and have not been hijacked.

Multicast authentication of sensor data is challenging, due to the need for low-security overhead, tolerance of lossy networks, time-criticality, and high data rates. Researchers augmented an existing authentication scheme to accommodate high-data-rate sensor transmissions that are unbounded in length (meaning that there is no session expiration). Using dual-offset key chains to reduce authentication delay and the computational overhead associated with key chain commitment, they developed a new protocol called *inf*-TESLA that meets the performance requirements imposed by the physical dynamics of the power system. Significant effort was made to integrate their authentication protocol into existing network simulation software, specifically Optimized Network Engineering Tools (OPNET), thus providing potential users with the ability to evaluate the protocol on their own networks and for their own applications.

Furthermore, in an effort to address the growing interest in co-optimizing cyber and physical components to work together as a system, NIST researchers developed mathematical formalism to trade off the sensitivity of a dynamic system to attack or perturbation against the authentication overhead incurred by their protocol. This formalism was demonstrated on a power system use case showing the limiting considerations between authentication overhead and stability margins of a wide-area damping controller. The project continues to be a work-in-progress and was presented and published at ICT Systems Security and Privacy Protection Conference 2016 in Ghent, Belgium.

Timing has also become a cyber-physical security issue with the onset of utilities detecting issues in receiving and distributing time to enable distributed real-time measurement and control. In particular, the concern of the threat of spoofing and jamming has led to efforts in determining redundant sources of traceable time. The first step is developing monitoring and anomaly detection capabilities. The effort included working with the North American Synchrophasor Initiative (NASPI) Time Synchronization Task Force to begin the effort in researching requirements and documenting guidelines for industry to provide assured timing. One alternative time distribution method to the Global Positioning System (GPS) is the IEEE 1588 Precision Time Protocol (PTP)—a time synchronization protocol that is used for the electric grid and other special-purpose industrial automation and measurement networks. Discussions have begun with the NIST Time and Frequency Division about experimental designs to provide a Coordinated Universal Time (UTC) scale that would be maintained as a NIST (UTC(NIST)) PTP service over a large geographical expanse.

In FY 2017, CSD will coordinate with NIST's Engineering Laboratory (EL) and Smart Grid Program Office on the further development of a Cybersecurity Smart Grid Test Lab—part of the NIST Smart Grid Testbed Facility now under construction. CSD will also collaborate with the University of New Hampshire and ITL's Software and Systems Division on cybersecurity research. The IEEE 1588 Security Working Group is developing a new Annex to secure time distribution through (a) PTP integrated authentication and integrity verification, (b) external transport security mechanisms, (c) architecture guidance, and (d) monitoring and management guidance. The research will focus on developing a full security scheme with emphasis on PTP integrated authentication and integrity verification and monitoring/detection of the network's timing performance.

FOR MORE INFORMATION, SEE:

http://www.nist.gov/smartgrid
http://www.sgip.org

CONTACTS:

Ms. Suzanne Lightman (301) 975-6442 suzanne.lightman@nist.gov	Ms. Victoria Yan Pillitteri (301) 975-8542 victoria.pillitteri@nist.gov

CYBERSECURITY AWARENESS, TRAINING, EDUCATION, AND OUTREACH

National Initiative for Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE) is a partnership among government, academia, and the private sector that is focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure.

NICE is building on its current efforts based on its Strategic Plan—delivered to Congress in April 2016 as required by the Cybersecurity Enhancement Act of 2014—which was written with engagement and deliberation among NICE partners. The three primary goals of the plan are to: 1) accelerate learning and skills development, 2) nurture a diverse learning community, and 3) guide career development and workforce planning. NICE partners will continue to develop appropriate implementation strategies and metrics for this plan.

In FY 2016, the NICE team at NIST worked to set a solid staffing foundation for future progress. They assembled new internal team members that includes leads for academic engagement, industry engagement, government engagement, and a program manager. These, in combination with the existing NICE Director and NICE Deputy Director, completed the staffing needs for the NICE Program Office at NIST.

Many NICE communication mechanisms were also established in FY 2016. These include the NICE Public Working Group (see https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group), the NICE Quarterly eNewsletter (see https://www.nist.gov/news-events/news/search/enewsletter), and an increased presence of NICE at cybersecurity education, training, and workforce development events across the country.

Figure 6: The NICE Lead for Academic Engagement, Mrs. Davina Pruitt-Mentle, speaking with an attendee at the 20th Annual Colloquium for Information Systems Security Education Conference in Philadelphia.

In addition to NICE's continued coordination with academic and industry partners, NICE also continued its leadership in working with government partners on initiatives such as the Cybersecurity National Action Plan, the Federal Cybersecurity Workforce Strategy, and implementation of the Federal Cybersecurity Workforce Assessment Act.

In FY 2016, NICE announced grant awards for five Regional Alliances and Multi-stakeholder Partnerships to Stimulate (RAMPS) cybersecurity education and workforce development. The RAMPS grants will bring together K-12, higher education, and local employers in regions across the nation (see https://www.nist.gov/nice/regional-alliances-and-multistakeholder-partnerships-stimulate-ramps). NICE also provided grant support for the 2015 NICE Conference and Expo, the 2015 National K-12 Cybersecurity Education Conference, the Center of Academic Excellence (CAE) Community Meeting, the National Cybersecurity Summit, the NICE Challenge Project, and the Cybersecurity Jobs Heat Map.

In FY 2017, NICE plans to:

- Support the 2016 NICE Conference on October 6-7, 2016;
- Support the 2016 NICE Conference and Expo and pre-conference seminars on October 31, 2016 – November 2, 2016;
- Launch a Cybersecurity Jobs Heat Map known as "CyberSeek";
- Publish a draft of the NICE Cybersecurity Workforce Framework; and
- Provide a public webinar series (see https://www.nist.gov/nice/webinars).

FOR MORE INFORMATION, SEE:

http://www.nist.gov/nice

CONTACTS:

Mr. Rodney Petersen
(301) 975-8897
nice.nist@nist.gov

Ms. Danielle Santos
(301) 975-5048
danielle.santos@nist.gov

Computer Security Resource Center (CSRC)

The CSRC website is a vast repository of valuable information relating to cybersecurity research by NIST personnel in ITL and is one of the busiest and most expansive 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. Several divisions within ITL rely on the CSRC website to post program/project

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM: http://dx.doi.org/10.6028/NIST.SP.800-195

information, research and testing, software tools, and other information that is essential to NIST's customers worldwide. The CSRC website is home to many of the standards, guidelines, and other technical series documents that are valuable to the general public. The *Publications Released in FY 2016* section of this annual report provides additional details. During FY 2016, CSRC had more than 6.2 million page views and downloads.

The CSRC team maintains a publication announcement mailing list with more than 73,630 subscribers from government, industry, and academia—as well as individuals with a personal interest in IT security worldwide. This free email list notifies subscribers about publications that have been posted to the CSRC website, along with announcing new NIST-sponsored cybersecurity events and important news and/or announcements.

During FY 2016, the CSRC was updated daily, providing new information such as draft and final versions of technical series documents (e.g., FIPS, SPs, NISTIRs and ITL Bulletins) and updates to various program and project webpages. The CSRC team has made progress on plans for a complete redesign of the current CSRC website, including a content management system (CMS). Updating CSRC with a CMS will provide a user-friendly environment and experience. The first phase of the project, the publications section; has been completed. All technical and non-technical publications (e.g., white papers, conference papers, presentations) have been successfully integrated into the new system.

The CSRC team has spent the last portion of FY 2016 migrating the content from the current website into the CMS, and in FY 2017, a beta test site of the entire CSRC is expected to be made available. The CSRC team plans to continue testing the new website and to review feedback received, with the plan for full transition to the updated site in FY 2017.

FOR MORE INFORMATION, SEE:

http://csrc.nist.gov

CONTACTS:

Questions regarding the CSRC website can be sent to the CSRC Webmasters at:

webmaster-csrc@nist.gov

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

Ms. Nicole Keller
(301) 975-3648
nicole.keller@nist.gov

Federal Computer Security Managers' (FCSM) Forum

The Federal Computer Security Managers' (FCSM) Forum is sponsored by NIST to promote the sharing of security-related information among federal agencies. The Forum, which serves more than 1,200 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 managers in fulfillment of NIST's leadership mandate (under FISMA). It also assists NIST in establishing and maintaining relationships with other individuals or organizations that are actively addressing information security issues within the Federal Government. During FY 2016, NIST's Patricia Toth served as the Chairperson, and ACD served as the Secretariat of the Forum, with administrative and logistical support from NIST's Peggy Himes.

The Forum maintains an extensive email subscription service. Participation in the service is restricted to those Federal Government employees with a role in the management of their organization's information system security program. The Forum conducts bi-monthly meetings and an annual two-day conference for a discussion of current issues and topics of interest to those responsible for protecting sensitive (unclassified) federal systems. Events are open to federal employees and their designated support contractors.

Topics of discussion at FCSM meetings in FY 2016 included briefings on: software-aided security control selection, best practices for privileged user personal identity verification, the Cybersecurity Framework, the National Cybersecurity Center of Excellence (NCCoE) - Federally Funded Research and Development Center (FFRDC), an update on vetting the security mobile applications, and the U.S. Government Configuration Baselines (USGCB).

FY 2016's annual two-day offsite was held at NIST on August 16-17, 2016. Presentations included the current technical, operational and management information systems security topics and updates on the information system security activities of OMB, GAO, National Aeronautics and Space Administration (NASA), NARA, Federal Aviation Administration (FAA), Census Bureau, DHS, and NIST. Most presentations are available online (see http://csrc.nist.gov/groups/SMA/forum/events.html).

The following is a list of presentations that were given at the annual two-day offsite meeting (see http://csrc.nist.gov/groups/SMA/forum/events.html for links to the presentations):

- Federal CIO Council update;
- Establishing a Tier 2 Information Security risk management program: How a department-wide security gap analysis provided a basis for a new security program;
- Government Accountability Office (GAO) Information Security update;
- SP 800-150, *Guide to Cyber Threat Information Sharing*;
- NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*;
- Continuous Diagnostics and Mitigation (CDM);
- The new A-130 Policy;
- Migrating the Federal Government to Hyper Text Transfer Protocol Secure (HTTPS);
- Security beyond a "system" – fiscal service's approach to external services;
- Case study: boundary consolidation to support more efficient, effective use of resources and increased maturity in continuous monitoring;
- Lessons learned from the Federal Risk and Authorization Management Program (FedRAMP);
- CDM update, interagency communications, and agency involvement; and
- The Cybersecurity Strategy and Implementation Plan (CSIP) and FY 2016 CIO FISMA metrics.

The Forum plays a valuable role in helping NIST (and other federal agencies) develop and maintain a strong, proactive stance in the identification and resolution of new strategic and tactical IT security issues as they emerge. The email list of interested parties has steadily increased in size and provides a valuable resource for federal security program managers.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

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

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

Ms. Jody Jacobs
(301) 975-4728
jlj3@nist.gov

(Editors' Note: Pat Toth worked on this initiative until she took another position at NIST.)

Federal Information Systems Security Educators' Association (FISSEA)

The Federal Information Systems Security Educators' Association (FISSEA), founded in 1987, is a NIST organization to assist federal agency professionals with meeting information system 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, managers responsible for information system security training programs in federal agencies, contractors of these agencies, and faculty members of accredited educational institutions who are involved in information security training and education. All that is required to become a FISSEA member is a willingness to share products, information, and experiences. A working group meets monthly to administer business activities.

FISSEA communicates with its membership through a website, a mailing list, and a social networking site. The ACD staff assists FISSEA with its operations by providing staffing support for several of its activities (and by acting as FISSEA's host agency).

The 29th Annual FISSEA Conference occurred March 15-16, 2016 at NIST, and the theme was *"The Quest for the Unhackable Human: The Power of Cybersecurity Awareness and Training."* The 250+ attendees were made up of managers (specifically those responsible for information systems security awareness, training, certifications, workforce identification, compliance, etc. in federal agencies), contractors providing awareness and training support, and faculty members of accredited educational institutions who are involved in information security training and education. The attendees learned about new techniques for developing/conducting training, cost-effective practices, workforce development, and free resources and contacts.

NIST's Pat Toth, Peggy Himes, and members of the FISSEA Technical Working Group were integral to the effort to support the 2016 Annual Conference. NIST ITL Director, Charles Romine, opened the event as the welcoming speaker, and ten-year-old Reuben Abishai Paul, Founder and CEO of CyberShaolin & Prudent Games, gave the keynote address "R U #Unhackable?" Presenters at the event represented NIST, DHS, Department of State (DoS), National Security Agency (NSA), National Institute of Health (NIH), National Oceanic and Atmospheric Administration (NOAA), Federal Housing Finance Agency (FHFA), private industry, and academia. The attendees had an opportunity to visit vendors and federal agencies on the second day to discuss their specific awareness and training programs, and the Pecha Kucha fast-paced talks proved to be both entertaining and educational.

The FISSEA Educator of the Year Award is an annual recognition to honor a contemporary individual who is making special efforts to create, build, manage, or inspire an information systems security awareness, training, or education program. Susan Hansche (DHS) presented the FISSEA 2016 Educator of the Year Award to Gretchen Morris (DB Consulting Group/NASA). Gretchen's vast knowledge-base, strong work ethic, her dedication to the improvement of information security awareness and training, and her commitment to coordinating the annual FISSEA Security Contest made her the perfect recipient for the award.

Figure 7: Susan Hansche, DHS, presented the FISSEA 2015 Educator of the Year Award to Gretchen Morris, DB Consulting/NASA on March 15, 2016.

Other traditional FISSEA conference events include announcing the winners of the FISSEA Security Awareness, Training & Education Contest, which includes six categories from one of FISSEA's three key areas: awareness, training, and education. A winner is selected from each category and awarded a certificate. The categories covered the topics described below, including a new section this year related to video-based training.

In FY 2016, awarded certificates were selected by an impartial judging committee and included:

- **Poster Winner:** K. Rudolph, John Ippolito, G. Mark Hardy, Andrew Ellis, and Charles A. Filius, from Native Intelligence, Inc. and friends;
- **Website Winner:** Lisa Dorr, Sarah Moffat, Toney Rogers, and Jennifer Kimberly from U.S. Department of Health and Human Services (HHS), Office of Information Security (OIS), Governance, Risk Management, and Compliance (GRC) – Governance Division;
- **Motivational Item Winner:** K. Rudolph from Native Intelligence, Inc.;
- **Newsletter Winner:** Indian Health Service (IHS), Office of Information Technology, Division of Information Security;
- **Security Training:** The Employment and Social Development Canada (ESDC) Security Training and Awareness Program Team; and
- **Video:** Cheryl Seaman and Stephanie Erickson from NIH.

Peer's Choice Award winners were selected by peers during the conference and included:

- **Poster Winner:** Katherine Martini from DoS – Office of Cybersecurity;
- **Website Winner:** Lisa Dorr, Sarah Moffat, Toney Rogers, and Jennifer Kimberly from HHS, Office of Information Security (OIS), Governance, Risk Management, and Compliance (GRC) – Governance Division;
- **Motivational Item Winner:** K. Rudolph from Native Intelligence, Inc.;
- **Newsletter Winner**: IHS Office of Information Technology, Division of Information Security;
- **Security Training:** IHS Office of Information Technology, Division of Information Security; and
- **Video:** The ESDC Security Training and Awareness Program Team.

Another benefit of attending the 2016 FISSEA conference was the networking opportunities. The conference continues to be a valuable forum for attendees to learn about ongoing and planned training and education programs and initiatives. It also provides NIST the opportunity to help departments and agencies with fulfilling FISMA responsibilities. The 30th

Annual FISSEA Conference will be held at NIST on March 14-15, 2017.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/Federal-Info-Systems-Security-Educators-Assoc

CONTACTS:

Mr. Clarence Williams
(240) 672-8723
clarence.williams@nist.gov

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

(Editors' Note: Pat Toth worked on this initiative until she took another position at NIST.)

Information Security and Privacy Advisory Board (ISPAB)

The Information Security and Privacy Advisory Board (ISPAB) was initiated in 1987 and has 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 should 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. Title III of the E-Government Act of 2002 reaffirmed the need for this Board by giving it additional responsibilities: to thoroughly review all proposed information technology standards and guidelines developed under Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended.

The 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 duties of the Board, as dictated in the Act, are:

- To identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;
- To advise NIST and the Director of OMB on information security and privacy issues pertaining to Federal Government information systems, including a thorough review of proposed standards and guidelines developed under section 278g–3 of this title; and
- To provide an annual report of its findings to the Secretary of Commerce, the Director of OMB, the Director of the NSA, and the appropriate committees of Congress.

Congress indicated the long-term need for the Board by setting the terms of Board members to four years. The Board's charter requires that the NIST Director appoint the Chairperson and all twelve members of the Board, each of whom is selected for her/his preeminence in the IT industry or related disciplines.

Mr. Chris Boyer took over leadership from Dr. Peter Weinberger and was officially appointed by the NIST Director as the ISPAB Chair on May 1, 2016. Chris Boyer (Assistant Vice President, Global Public Policy at AT&T Services Inc.) has been a member of the Board since June 2012. In addition to his official role representing AT&T, he serves as AT&T's point of contact to the National Security Telecommunications Advisory Council (NSTAC), a federal advisory committee tasked with providing advice to the president on matters of national security and emergency preparedness (NS/EP).

The ISPAB Board currently has ten members supporting the Chair (see http://csrc.nist.gov/groups/SMA/ispab/membership.html). This year, the Board was pleased to welcome Ms. Patricia Hatter as a new member (see https://www.nist.gov/news-events/news/2016/08/nists-information-security-and-privacy-advisory-board-adds-industry-member). The following are current Board members:

- Ana (Annie) Antón, Professor and Chair, School of Interactive Computing, Georgia Institute of Technology;
- John R. Centafont, National Security Agency, Information Assurance and Cyber Defense;
- David Cullinane, CEO, TruStar, LLC;
- Gregory Garcia, Executive Vice President, McBee Strategic Consulting;
- Jeffrey Greene, Esq., Director, Government Affairs, North America & Senior Policy Counsel, Senior Policy Counsel, Cybersecurity and Identity, Symantec Corporation;
- Patricia Hatter, General Manager, Professional Services, Intel;
- Toby Levin, Retired (formerly Senior Advisor and Director of Privacy Policy, U.S. Department of Homeland Security);
- Edward Roback, Associate Chief Information Officer for Cybersecurity, U.S. Department of Treasury;
- Gale Stone, Deputy Assistant Inspector General for Audit, Social Security Administration; and

- J. Daniel Toler, Deputy Director, Federal Network Resilience, U.S. Department of Homeland Security.

During FY 2016, ISPAB held three meetings that were located at the U.S. Access Board Conference Room in Washington, D.C:

- October 21-23, 2015;
- March 23-25, 2016; and
- June 15-17, 2016.

The presenters at each Board meeting were leaders and experts representing private industry, academia, federal agency CIOs, Inspectors General, and Chief Information Security Officers.

In keeping with previous practices, at the first meeting of the fiscal year, the Board established a work plan for FY 2016. The resulting plan included the following areas of focus:

- Quantum (physics, pre-shared keys, quantum key distribution, block chains);
- Cybersecurity;
- OMB topics, including Circular A-130 revisions, cyber-marathon, CyberStats, measuring outcomes for cybersecurity, and cybersecurity protections in Federal Government acquisitions;
- DHS topics, including Fly-Away (Incident Response) Team, Einstein, Continuous Diagnostics and Mitigation (CDM), and outcome measurement methods;
- Networking and Information Technology Research and Development (NITRD) and the Build-it-in initiative and NITRD – on how competent companies acquire IT;
- National Highway Traffic Safety Administration (NHTSA) and automotive cybersecurity;
- Federal Trade Commission (FTC) – security, protecting data;
- Facial recognition, technologies, biometrics, and users;
- Privacy technologies;
- Privacy and Civil Liberties Oversight Board (PCLOB);
- Safe Harbor; and
- Acquisition.

Aligning with work-plan focus areas, the Board continues to monitor the following critical areas:

- Updates from the senior staff of federal agencies (e.g., the Deputy Under Secretary, Cybersecurity and Communications, National Protection Directorate, DHS, and Senate and Congressional staff);
- PCLOB and the establishment of the Federal Privacy Council;
- OMB Circular A-130 revisions;
- National Highway Traffic Safety Administration, autonomous vehicle technology, gaps, challenges, security and privacy;
- Privacy, transparency, and accountability for commercial unmanned aircraft systems;
- Cryptography and NIST cryptographic standards processes;
- Emerging technologies: cloud computing, big data, Internet of Things, cyber physical systems, smart cities, drones and unmanned aircraft systems, medical devices, transportation sector and vehicle-to-vehicle communication, blockchain protocol, and impacts on security and privacy;
- Commission on Enhancing National Cybersecurity;
- The NIST Cybersecurity Framework;
- Cybersecurity Information Sharing Act (CISA);
- Information sharing and analysis;
- The DHS CDM program;
- The Trusted Identities Group (TIG);
- National Cybersecurity Center of Excellence (NCCoE); and
- Realignment of IT Laboratory.

The Board submitted two recommendation letters based on the Board work from each meeting in this fiscal year. Records of the submitted letters and the received responses are accessible from http://csrc.nist.gov/groups/SMA/ispab/documentation.html.

- At the close of the October 2015 meeting, the Board submitted a recommendation letter regarding quantum computing to the NIST Director. The NIST Director responded to the Board in a letter dated January 2016.
- At the close of the March 2016 meeting, the Board submitted a recommendation letter regarding FIPS 140 and the use of ISO/IEC 19790 to the NIST Director. The Board received a response from the NIST Director in August 2016.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM: http://dx.doi.org/10.6028/NIST.SP.800-195

Copies of the current list of members and their biographies, the Board's charter, and past Board activities are located at https://csrc.nist.gov/Projects/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 information security and privacy work may email their name, affiliation, and address to Matthew Scholl at the email address below.

FOR MORE INFORMATION, SEE:

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

CONTACT:

Mr. Matthew Scholl
(301) 975-2941
matthew.scholl@nist.gov

(Editors' Note: Annie Sokol worked on this initiative until she was assigned to other projects.)

Small and Medium Size Business (SMB) Cybersecurity Outreach Workshop

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 even business closure. 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 % of all U.S. businesses – are SMBs of 500 employees or fewer (see http://www.sba.gov/sites/default/files/allprofiles12.pdf). While the threats to individual small and medium-size businesses 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 risks, 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 FBI InfraGard program 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 2016, SMB outreach workshops took place in:

- Minneapolis, Minnesota;
- McHenry, Maryland;
- Harrisonburg, Virginia;
- Arlington, Virginia;
- Ocala, Florida;
- The Villages, Florida;
- Orlando, Florida;
- Clermont, Florida;
- Charlestown, West Virginia; and
- Detroit, Michigan.

Additionally, as part of the President's Cybersecurity National Action Plan (CNAP), NIST partnered with the SBA, the FTC, and the Department of Energy (DoE) to develop and provide five cybersecurity training webinars to reach small businesses and small business stakeholders through 68 SBA District Offices, nine NIST Manufacturing Extension Partnership Centers, and other regional networks across the country.

In collaboration with the SBA and the FBI, planning is underway to identify locations and plan cybersecurity workshops in FY 2017.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/Small-Business-Community

CONTACT:

Mr. Jeffrey Marron
(301) 975-3846
Jeffrey.Marron@nist.gov

(Editors' Note: Pat Toth worked on this initiative until she took another position at NIST.)

CRYPTOGRAPHIC STANDARDS PROGRAM

Secure Hash Algorithm-3 (SHA-3) Derived Functions (NIST SP 800-185)

NIST opened a public competition in November 2007 to select a new cryptographic hash algorithm for standardization. The "SHA-3" competition ended in October 2012. NIST standardized the winning algorithm, Keccak, in FIPS 202 as the new *SHA-3 Standard*. Announced on August 5, 2015, FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, is available at: https://csrc.nist.gov/Publications/Search?requestSeriesList=3&requestStatusList=1,3&requestDisplayOption.=brief&requestSortOrder=5&itemsPerPage=All.

FIPS 202 defines four fixed-length hash functions (SHA3-224, SHA3-256, SHA3-384, and SHA3-512), and two variable-length eXtendable Output Functions (XOFs), SHAKE128 and SHAKE256. FIPS 202 also supports a flexible scheme for domain separation between different functions derived from Keccak, which ensures that different named functions will produce unrelated outputs.

NIST extended this scheme to allow users to customize their use of the function by defining a new, customizable version of the SHAKE functions, called cSHAKE, and specifying two cSHAKE variants—cSHAKE128 and cSHAKE256—for a 128- and 256-bit security strength, respectively, in DRAFT SP 800-185, *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash*.

Draft SP 800-185 defines three additional SHA-3-derived functions that provide new functionality. They are:

- KMAC128 and KMAC256, providing pseudorandom functions (PRFs) and keyed-hash functions with variable-length outputs;
- TupleHash128 and TupleHash256, providing functions that hash tuples of input strings without trivial collisions; and
- ParallelHash128 and ParallelHash256, providing efficient hash functions to hash long messages in parallel.

Published on August 4, 2016, Draft SP 800-185 is available on the CSRC website. NIST invited the public to review the draft and provide comments before September 30, 2016. NIST is in the process of addressing the received comments, and will post the final version of SP 800-185 when the comments are resolved.

FOR MORE INFORMATION, SEE:

http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html.

CONTACT:

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

(Editors' Note: Shu-jen Chang supported this program until her recent retirement)

Random Number Generation (RNG)

Random numbers are required for the secure use of most cryptographic algorithms. For example, random numbers are used to generate the keys needed for encryption and digital signature applications. The CSD Cryptographic Technology Group (CTG) began work on the specification of random bit generators in the late 1990s. SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, was published in 2007, and revised as SP 800-90A in 2012 and 2015. This document specifies several deterministic algorithms that can be used for the generation of pseudorandom bits – a sequence of bits produced by an algorithm, rather than a random physical phenomenon that produces a truly random sequence.

Two additional documents (SP 800-90B and SP 800-90C) are under development, and drafts were made available for public comment in 2012 and 2016.

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

SP 800-90B addresses the development and testing of entropy sources. Figure 8: Entropy Source Model illustrates the model that the Recommendation uses to describe an entropy source and its components: a noise source, health tests, and an optional

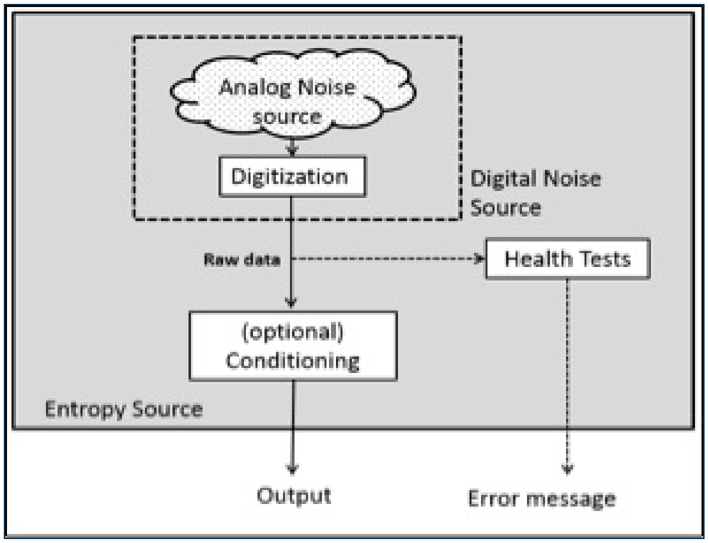


Figure 8: Entropy Source Model

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

In Figure 8: Entropy Source Model, the noise source contains the entropy-providing activity (e.g., ring oscillators); if the activity being sampled does not produce binary data, then the noise source includes a digitization process. Health tests are intended to detect whether the noise source and the entropy source (as a whole) continues to operate as expected. The optional conditioning component is responsible for reducing bias and/or increasing the entropy rate of the bits to eventually be output by the entropy source.

SP 800-90B includes descriptions of the tests for NIST's Cryptographic Algorithm Validation Program (CAVP) to validate candidate entropy sources. During FY 2016, the CTG continued the development and testing of methods for estimating the amount of entropy per noise-source output.

A draft of the document was provided for public comment in January 2016. A companion python code package was also made available to assist reviewers in evaluating the entropy estimation methods published in the draft (see https://github.com/usnistgov/SP800-90B_EntropyAssessment).

A workshop was held in May 2016 to discuss the document, and the public comment period ended shortly thereafter. The SP 800-90B development team has been reviewing the comments received during the public comment period and plans to finalize an initial version of the document in FY 2017.

The latest draft of SP 800-90B is available via the Special Publications page: http://csrc.nist.gov/publications/PubsSPs.html.

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

SP 800-90C provides basic guidance on the construction of Random Bit Generators (RBGs) from the entropy sources validated against the requirements of SP 800-90B and the Deterministic Random Bit Generators (DRBG) algorithms of SP 800-90A. SP 800-90C includes constructions for both non-deterministic random bit generators (NRBGs; also known as true random number generators) and deterministic random bit generators (also known as pseudorandom number generators). Two general models are provided in SP 800-90C, as shown in Figures 8 and 9.

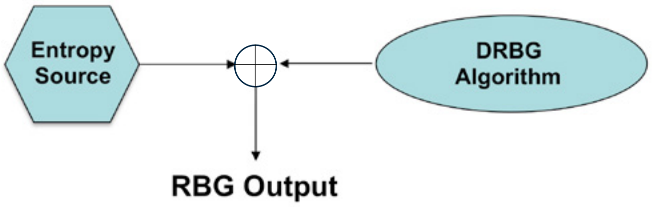


Figure 9: XOR-NRBG

Figure 9: XOR-NRBG depicts the construction of one of the NRBGs – the XOR-NRBG. In this construction, each bit output by the entropy source (as discussed in SP 800-90B) is exclusive-ORed with a bit of output from a DRBG algorithm specified in SP 800-90A.

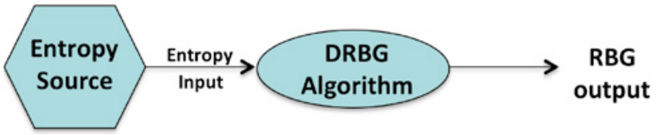


Figure 10: DRBG and Oversampling NRBG

Figure 10: DRBG and Oversampling NRBG depicts the construction used for the DRBGs and the second NRBG design – the Oversampling NRBG. The difference between the two is the availability of the entropy source and the frequency of requesting output from the entropy source. For a DRBG, an entropy source is only required for seeding the DRBG; after the initial seeding process, further requests for entropy-source output depend on the implementation and application. For the Oversampling NRBG, the entropy source must always be available and is accessed whenever bits are requested from the NRBG by a consuming application.

The latest draft of SP 800-90C is available via the Special Publications page: http://csrc.nist.gov/publications/PubsSPs.html.

PLANS FOR FY 2017:

The RBG development team has the following goals for FY 2017:

- Complete the initial version of SP 800-90B and post the comments received, along with their resolution. The testing of entropy sources by the CMVP will begin as soon as possible after the test code is ported to another language for increased performance. Members of the CMVP staff have been participating in the development of SP 800-90B to more easily prepare for such testing. Not all comments received will be addressed in this version, since the development team is anxious to begin getting feedback from the CMVP labs about the adequacy of the tests specified in SP 800-90B. Addressing some of the comments would result in a significant delay in finalizing the initial version of the document.
- Complete SP 800-90C, posting the comments received and their resolution, along with the document.
- Monitor the testing of SP 800-90B and SP 800-90C in the CMVP labs to determine problems

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

that need to be addressed in the next versions of the documents. In some cases, the problems may be addressed by additions to the FIPS 140-2 Implementation Guidance document until the documents are revised. The Implementation Guidance document is available at http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf.

- Consider the comments received during the public comment period for SP 800-90B that were not resolved before its publication. Also, address any problems that surface during CMVP testing.

FOR MORE INFORMATION, SEE:

http://csrc.nist.gov/groups/ST/toolkit/rng/

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 (e.g., for encryption and/or authentication) that is constructed from a block cipher is called a 'mode of operation.'

Several modes of operation have been specified in the SP 800-38 series of publications. The latest installment in the series, Special Publication 800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption,* was published in March 2016. It specifies two AES modes of operation, called FF1 and FF3, for inclusion in the "toolkit" of approved cryptographic algorithms. FF1 and FF3 are format-preserving encryption (FPE) modes, based on proposals that were submitted from the private sector.

Previously approved confidentiality modes are designed for binary data; ciphertext resulting from these modes may be longer than the original plaintext and may result in format problems when used by existing devices or software.

FPE modes such as FF1 and FF3 are designed for any kind of data, including non-binary formats, such as credit card numbers and social security numbers. The ciphertext resulting from an FPE mode has the same length and format as the original plaintext. Consequently, FPE modes can facilitate the retrofitting of encryption technology to existing devices or software, where a conventional encryption mode might not be feasible.

FOR MORE INFORMATION, SEE:

http://csrc.nist.gov/groups/ST/toolkit/BCM/

CONTACT:

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

Key Management

Key management is required for applying numerous cryptographic technologies and is considered one of the most critical aspects associated with the use of cryptography. The Cryptographic Technology Group (CTG) began providing guidance in managing the keys used for cryptographic applications in the late 1990s to early 2000s. NIST Special Publications have been periodically updated to address new algorithms and handling procedures. These documents are coordinated with federal agencies and with the cryptographic community, including national and international organizations, industry, and academia.

During the development and subsequent revision of these key-management documents, the development team coordinates with members of NIST's Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) to develop validation tests and address issues that arise during the validation processes.

In FY 2016, the following publications were either created or revised:

SP 800-57, Part 1, *Recommendation for Key Management, Part 1: General*:

SP 800-57, was first published in 2005, and later revised in 2007 and 2012. SP 800-57, Part 1 contains basic key-management guidance, including:

- Defining the security services that may be obtained using NIST-approved algorithms;

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

- A classification of the different types of keys to be used with cryptographic algorithms, a specification of the protection required for each key type, and identification methods for providing this protection;
- A listing of the states in which a key may exist during its lifetime;
- A discussion of a variety of key-management issues related to key management, including key usage, cryptoperiods, domain-parameter and public-key validation, backup and archiving; and
- Guidance for cryptographic algorithm and key size selection (e.g., the security strength provided by a given algorithm with a specified key size).

Another revision of the document was completed in January 2016 that includes information on and references to new and revised documents developed by the CTG (e.g., SP 800-152, as discussed below); the removal of references to the Dual_EC_DRBG, which was removed from SP 800-90A: *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*; a revision of the security-strength tables; and a revision of the key-state discussion to provide more clarification.

SP 800-57, Part 1 is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.

SP 800-131A: Transitions: R*ecommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*:

SP 800-131A was originally published in January 2011. This document provides specific guidance for transitions to the use of stronger cryptographic keys and more robust algorithms. An update of SP 800-131A was completed in November 2015. This update removes approval for the Dual_EC_DRBG that was specified in SP 800-90A; deprecates the use of non-approved key-establishment schemes; disallows the use of non-approved key-wrapping methods after 2017; and indicates that the use of the SHA-3 family of hash functions is acceptable, in addition to the use of the SHA-2 family of hash functions and some applications of SHA-1.

SP 800-131A is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf.

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

SP 800-152 provides guidance on the CKMS to be used by the Federal Government. This document contains requirements for CKMS design, implementation, procurement, installation, configuration, management, operation and use. Many of these requirements are refinements of the requirements for CKMS designers that are specified in SP 800-130: *A Framework for Designing Cryptographic Key Management Systems*. Other requirements are intended for the service providers of a CKMS used by federal agencies and their contractors. Guidance is also provided for the federal agencies in selecting CKMSs that support the security and management policies of those agencies.

This document was completed in October 2015 and is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf.

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

SP 800-56A was originally published in 2006, and revised in 2007 and 2013. This document specifies Diffie-Hellman (DH) and Menezes-Qu-Vanstone (MQV) key-establishment schemes, both elliptic curve and finite field versions. Key establishment is a procedure that results in keying material that is shared between the participants. A key-establishment scheme is defined by a cryptographic algorithm, together with an identification of other information that must be available by both parties when establishing keys. The schemes are intended for use in communication protocols (e.g., Transport Layer Security (TLS), one of the protocols used by the Internet). The key-establishment schemes in SP 800-56A use public key algorithms, and each participant in a key-agreement transaction uses a pair of keys—a public key and a private key.

Both key-agreement and key-transport schemes are specified in the document. A key-agreement scheme is a procedure in which both parties in a key-establishment transaction contribute information that is used in generating a cryptographic key. The key-agreement process includes the generation of a shared secret (which is not itself considered to be a cryptographic key), and the derivation of keying material using the shared secret. Several key-agreement schemes are specified in SP 800-56A. Figure 11: (See next page) Key-Agreement Example below provides a simplified example of a key-agreement scheme. In this example, each party:

1. Generates a key pair (either prior to or during the key-agreement transaction);
2. Obtains the public key of the other party;
3. Computes a shared secret using one's own keys and the other party's public key; and
4. Derives one or more keys from the shared secret.

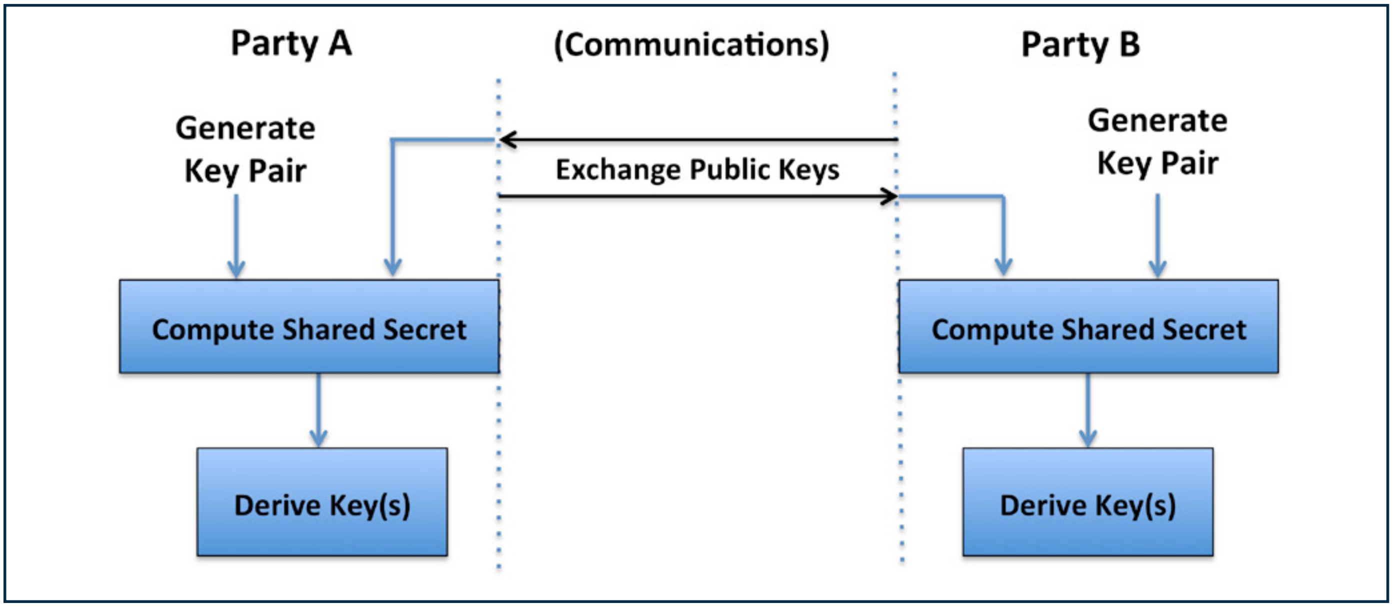


Figure 11: Key-Agreement Example

Key transport is a key-establishment method whereby one party selects a symmetric key and sends it securely to one or more other parties. In SP 800-56A, key transport can be performed following the key-agreement process depicted in Figure 11 using a key that was derived during that process. Figure 12: Key-Transport Example provides an example of a key transport scheme. In this example,

1. The sender (either party A or party B in Figure 11: Key-Agreement Example), generates a symmetric key;
2. Wraps (i.e., encrypts) that key using a key-wrapping algorithm (see SP 800-38F: *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*; SP 800-38F is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf);
3. Sends the resulting ciphertext key to the other party (i.e., the receiver); and
4. The receiver unwraps (i.e., decrypts) the received ciphertext key using a key derived during the key-agreement process to obtain the original plaintext key that was generated by the sender.

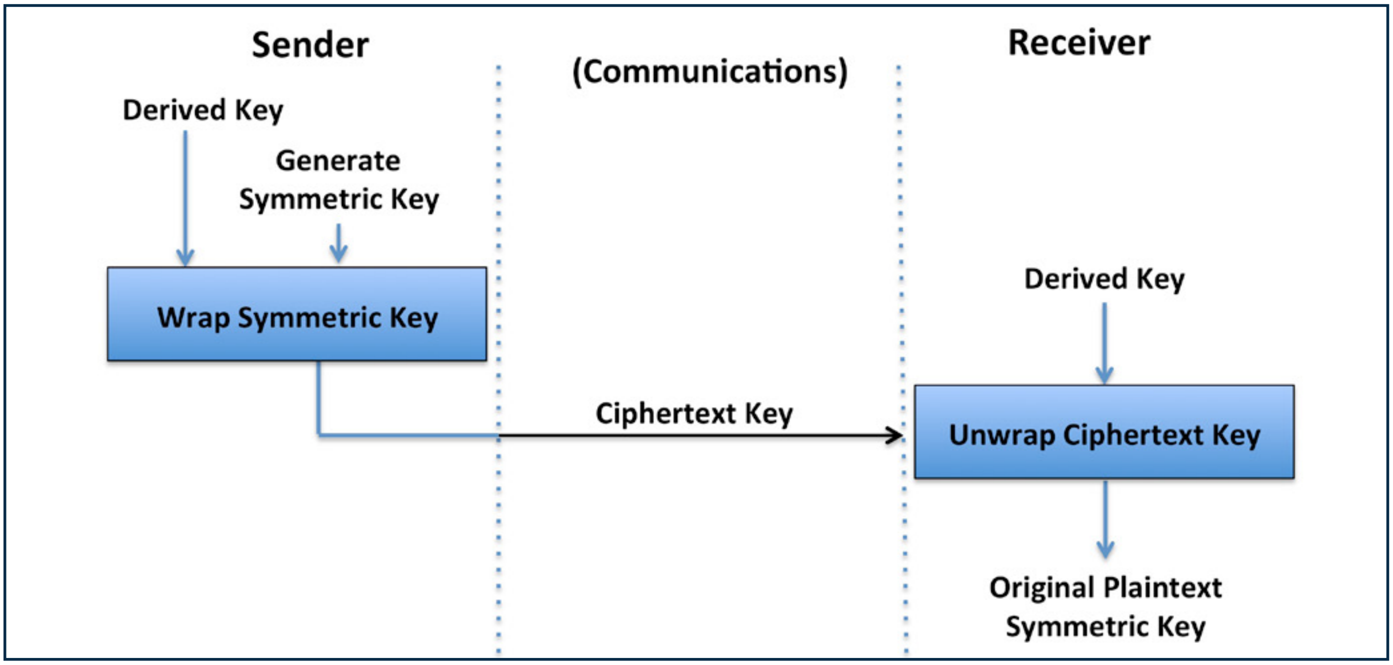


Figure 12: Key-Transport Example

The current version of SP 800-56A is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

SP 800-56A has been under revision during FY 2016. This revision will:

- Approve the use of additional parameter/key sizes for the finite field schemes; currently, only key sizes of 2048 and 3072 bits are specified. Larger key sizes will be allowed and defined in the next version.
- Allow the use of pre-defined domain parameter groups that are not currently allowed by SP 800-56A. Domain parameters are used to generate keys and compute the shared secret. Methods for generating domain parameters are specified for the finite field schemes in FIPS 186-4: *Digital Signature Standard (DSS)*. The revision of SP 800-56A will allow the use of domain-parameter groups using "safe primes" that are used in the Transport Layer Security (TLS) and Internet Key Exchange (IKE) protocols, which were not generated using the methods in FIPS 186-4. These pre-defined groups will be listed in Annex A of FIPS 140-2.
- Move all key-derivation functions to SP 800-56C: *Recommendation for Key Derivation Through Extraction-then-Expansion*. SP 800-56A currently specifies two versions of a single step key-derivation function, refers to SP 800-56C for a two-step key-derivation procedure, and refers to SP 800-135: *Recommendation for Existing Application-Specific Key Derivation Functions*, for application-specific key-derivation functions.

The revision of SP 800-56A will be available for public comment in FY 2017.

SP 800-56C: *Recommendation for Key Derivation Through Extraction-then-Expansion*:

SP 800-56C specifies techniques for the derivation of keys from a shared secret generated during a key-establishment scheme defined in SP 800-56A and SP 800-56B using a two-step extraction-then-expansion procedure. SP 800-56A is discussed above. SP 800-56B: *Recommendation for Pairwise Key-Establishment Schemes Using Integer Factorization Cryptography*, is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf.

SP 800-56C uses either HMAC or the Cipher-based Message Authentication Code (CMAC) algorithm during the two-step process. HMAC is specified in FIPS 198-1: *The Keyed-Hash Message Authentication Code (HMAC)*, and CMAC is specified for AES in SP 800-38B: *Recommendation for Block Cipher Modes of Operation: the CMAC Mode of Authentication*. FIPS 198-1 is available at http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf; SP 800-38B is available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38b.pdf.

The current version of SP 800-56C is available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-56c.pdf.

SP 800-56C is being revised to:

- Move the key derivation functions specified in SP 800-56A into SP 800-56C as well as the references to SP 800-135: *Recommendation for Existing Application-Specific Key Derivation Functions*;
- Allow the use of KMAC, as specified in Draft SP 800-185, *SHA-3 Derived Functions: cSHAKE,* KECCAK Message Authentication Code *(KMAC), TupleHash and ParallelHash*, for key derivation;
- Define additional Message Authentication Code (MAC) lengths for the new parameter-size sets that will be allowed in the revision of SP 800-56A; and
- Provide a formula for estimating the security strength for the parameter-size sets that are not explicitly listed in SP 800-56A and SP 800-56B.

The revision of SP 800-56C will be available for public comment in FY 2017.

New Documents Under Development:

A new NIST publication is under development that provides guidance on the search resistance of a bit string output from an approved cryptographic algorithm (e.g., a cryptographic key or encrypted data). Search resistance is a (rough) measure of the amount of secrecy that can be provided by a bit string, given the genealogy (i.e., how it was generated), handling (i.e., what happened to it after it was generated), the usage (i.e., what algorithm it will be used with), length, and any other secret values and processes associated with the generation and handling of that bit string. When approved algorithms are used, this document is intended to provide methods for determining the search resistance of the bit string. This document, SP 800-158: *Key Management: The Search resistance of Bit Strings Output by Cryptographic Algorithms*, has involved a considerable amount of new research, since it is an area that has not been addressed to date. This publication will be available for public comment in FY 2017.

A new document was started in FY 2016 on key storage and recovery (e.g., key backup and archiving). This document is intended to serve as a guideline for the storage and recovery of cryptographic keys that are not under the direct control of the entity using those keys (e.g., the owner). This includes the backup and archiving of copies of the keys and the metadata associated with them. The document will also discuss the recovery of those keys when required (e.g., by the key's owner or the owner's organization).

Plans for FY 2017:

During FY 2017, the CTG is expecting to accomplish the following tasks:

- Provide the drafts of SP 800-56A and SP 800-56C for public comment;
- Begin the revision of SP 800-56B;
- Provide the draft of SP 800-158 for public comment; and
- Continue the development of the key-storage document.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

Ms. Elaine Barker (301) 975-2911 elaine.barker@nist.gov	Mr. Ray Perlner (301) 975-3357 ray.perlner@nist.gov
Dr. Lily Chen (301) 975-6974 lily.chen@nist.gov	Dr. Allen Roginsky (301) 975-8136 allen.roginsky@nist.gov

Transport Layer Security

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

SP 800-52 was first published in June of 2005, and SP 800-52 Revision 1 was published in April of 2014. Since the revision, CTG has been following developments in TLS implementations, including updates and attacks. In FY 2016, a second revision began that considers these developments. This second revision will be posted for public review and comment in FY 2017.

CTG has been contributing to the development of testssl.sh (see https://github.com/drwetter/testssl.sh), an open-source program that tests TLS-enabled servers, providing information about the protocols and cipher suites supported, in addition to checking for some well-known flaws. In FY 2017, CTG will be contributing code to testssl.sh that tests a TLS server's configuration for conformance to SP 800-52 Revision 2. CTG intends to make a draft version of this code available when the draft of SP 800-52 Revision 2 is posted for public comment.

The Internet Engineering Task Force (IETF) is actively developing extensions that can be used to add functionality to TLS. CTG will continue to review updates and additions to the TLS protocol in FY 2017.

CONTACTS:

Dr. Kerry McKay (301) 975-4969 kerry.mckay@nist.gov	Dr. Lily Chen (301) 975-6974 lily.chen@nist.gov

Elliptic Curve Cryptography

Elliptic curve cryptography is critical to the adoption of strong cryptography as we migrate to higher security strengths. NIST has standardized elliptic curve cryptography for digital signature algorithms in FIPS 186: Digital Signature Standard (DSS), and for key establishment schemes in SP 800-56A: *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*.

In FIPS 186-4, NIST recommends fifteen elliptic curves of varying security strengths for use in these elliptic curve cryptographic standards. However, the provenance of the curves is not fully specified in the standard, leading to recent public concerns that there could be a hidden weakness in these curves. NIST is not aware of any vulnerability in these curves when they are implemented correctly and used as described in NIST standards and guidelines.

More than fifteen years have now passed since these curves were developed, and the community now knows more about the security of elliptic curve cryptography and practical implementation issues. Advances within the cryptographic community have led to the development of new elliptic curves and algorithms whose designers claim to offer better performance and are easier to implement in a secure manner. Some of these curves are under consideration in voluntary, consensus-based Standards Developing Organizations.

In FY 2016, NIST solicited comments on possible improvements to FIPS 186-4. In particular, comments were requested on the possibility of adding new elliptic curves to the current recommended set—as well as adding new digital signature schemes. Throughout 2016, NIST began resolving the comments and revising FIPS 186-4. It is expected that the revised draft version of FIPS 186-5 will be available for public comment in FY 2017.

CONTACTS:

Email project team: EllipticCurves@nist.gov

Dr. Dustin Moody	Dr. Lily Chen
(301) 975-8136	(301) 975-6974
dustin.moody@nist.gov	lily.chen@nist.gov

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

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.

NIST researchers have held regular seminars throughout FY 2016. The presentation topics include the latest published results and security analyses, as well as status reports on quantum computation, hash-based signatures, coding-based cryptography, lattice-based cryptography, and multivariate cryptography. Through these presentations and discussions, the project team has made significant progress in understanding the strengths and weaknesses of the existing cryptographic schemes in each category.

In April 2016, NIST published NISTIR 8105: *Report on Post-Quantum Cryptography*, which shared the team's current understanding about the status of quantum computing and post-quantum cryptography. The report also outlined NIST's initial plan to move forward in this area. At Post-Quantum Cryptography (PQCrypto) 2016, NIST announced that it would begin the *Post-Quantum Standardization Process*, a thorough multi-year effort with the objective of creating new quantum-resistant cryptographic standards for public-key encryption and digital signatures (see www.nist.gov/pqcrypto). These functionalities are much more complex than AES or SHA-3, and will require fundamentally new techniques to address several open research questions in this area (for example, how to measure security against quantum attacks when a quantum computer has not yet been built). In August 2016, NIST issued draft submission requirements and evaluation criteria for public comment. (see https://www.federalregister.gov/articles/2016/08/02/2016-18150/request-for-comments-on-post-quantum-cryptography-requirements-and-evaluation-criteria)

The NIST team also continues to be productive in post-quantum cryptography research. The results have been published at major conferences, such as Embedded Security in Cars (ESCARS), Selected Areas in Cryptography (SAC), PQCrypto, and Eurocrypt. NIST researchers have given presentations at conferences and workshops to increase awareness of the upcoming migration. NIST has also sponsored other research, education, and research events.

In FY 2017, NIST will continue to explore the security and feasibility 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 era. The *Post-Quantum Standardization Process* will begin in early FY 2017, with the issuance of the finalized submission requirements and evaluation criteria. There will be a one-year period during which quantum-resistant algorithms may be submitted for possible standardization. After the submission period, there will be a public workshop in FY 2018, followed by multiple rounds of evaluation and analysis.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/pqcrypto

CONTACTS:

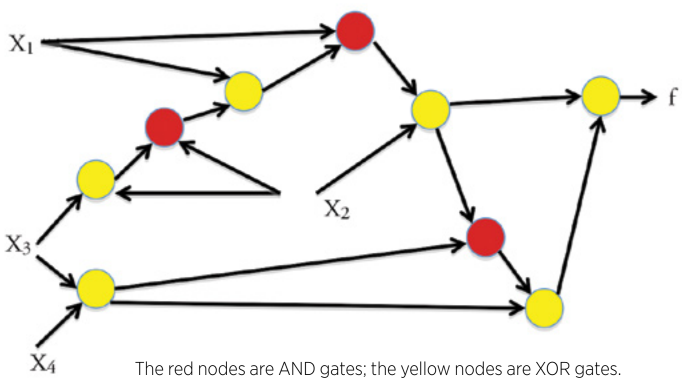
Email project team: pqc@nist.gov

Dr. Dustin Moody	Dr. Lily Chen
(301) 975-8136	(301) 975-6974
dustin.moody@nist.gov	lily.chen@nist.gov

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

Circuit Complexity

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 (X_1, X_2, X_3, and X_4) using AND and XOR gates is depicted in Figure 13.



The red nodes are AND gates; the yellow nodes are XOR gates.

Figure 13: Combinational Boolean Circuit

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 methods that design "good" circuits, as opposed to provably optimal circuits. The CTG has developed and implemented new solutions 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.

The CTG is also researching circuit-based security metrics for cryptographic functions. For a function to be secure (in particular, 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.

The CTG has published circuits that are provably optimal or close to optimal (with respect to multiplicative complexity) for important classes of functions. In the process, we 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; and iii) proving to a third party that a person's encrypted attributes satisfy some requirement, such as "over 21 and (U.S. 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, expressing functions as circuit computations with only a few multiplication (AND) gates is important. Some of the published circuits are now the standard reference for benchmarking tools in multiparty computation.

The following is a partial list of new results by our team:

- Better recursions for Karatsuba multiplication, which yielded the smallest known circuits for binary multiplication (i.e., multiplication of polynomials of degree n over the Galois Field with two elements). This yields important speed increases in elliptic curve cryptography and other applications.
- Optimal circuits were constructed - with respect to multiplicative complexity - for all predicates on four bits (see the example below). 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):

  $f = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_3x_4.$
- Computing the last term requires three multiplications. So, it is quite surprising that the full expression can be computed using only three multiplications. But, we have shown this to be true for f and all other predicates on four bits. The circuit depicted above computes f using three multiplications and six additions.
- A proof was developed 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 that the circuits can actually be built.
- A proof was developed that an explicit function requires at least 3.01n gates. This constitutes the only improvement on this problem for more than 30 years. The result is due to Magnus Find, in collaboration with mathematicians from New York University (NYU) and from the Steklov Institute, St. Petersburg, Russia.

In 2017, plans are in place to begin the implementation of combinational circuits in ASIC (application-specific integrated circuit) hardware. The team will also map the multiplicative complexity of all functions of six variables and will code a new heuristic for simultaneously reducing the size and depth of circuits.

Circuits are posted periodically at:

http://cs-www.cs.yale.edu/homes/~peralta/CircuitStuff/CMT.html

CONTACT:

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

Lightweight Cryptography

There are several emerging areas in which highly constrained devices are interconnected and working in concert to accomplish a task. Examples of these areas include automotive systems, sensor networks, healthcare, distributed control systems, the Internet of Things (IoT), cyber-physical systems, and the smart grid. Security and privacy can be very important in these areas. Because most of the modern cryptographic algorithms were designed for desktop/server environments, many of these algorithms cannot be implemented in the constrained devices used by these applications. When current NIST-approved algorithms can be engineered to fit into the limited resources of constrained environments, their performance may not be acceptable. For these reasons, NIST started a lightweight cryptography project in 2013 that was tasked with determining the need and developing a strategy for the standardization of lightweight cryptographic algorithms.

CTG staff are examining applications in constrained environments to determine whether NIST should develop lightweight cryptographic standards. This includes communicating with industry experts to understand the challenges and limitations and following the work of other standardization bodies in this area. In FY 2015, CTG organized a *Lightweight Cryptography Workshop* to discuss issues related to the security and resource requirements of applications in constrained environments and potential future standardization of lightweight primitive algorithms. Using input gathered at the workshop in FY 2016, CTG released draft NISTIR 8114, *Draft Report on Lightweight Cryptography* for public comments. This report provides an overview of the lightweight cryptography project at NIST, and describes a plan for the standardization of lightweight cryptographic algorithms. This plan involves the creation of profiles that will target specific applications and requirements where conventional cryptography may not be suitable.

CTG is organizing the second NIST workshop on *Lightweight Cryptography*, taking place at the beginning of FY 2017 to discuss the plan outlined in the draft report before it is finalized. The next steps in the plan include working with industry to create an initial set of profiles and the selection of algorithms that meet profile requirements.

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

The NIST Randomness Beacon

NIST has implemented a source of public randomness, which is available at https://beacon.nist.gov/home. It uses two independent, commercially-available sources of randomness, each with an independent hardware entropy source and SP 800-90A-approved components.

The NIST 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 of receiving the same random string.

The NIST Beacon posts bit-strings in blocks of 512 bits every 60 seconds. Each such value is time-stamped and signed to form a packet that also includes the hash of the previous value to chain the sequence of values together. This prevents all parties, even the source, from retroactively changing an output packet without being detected. The NIST Beacon keeps all output packets. At any point in time, the full history of outputs is available to users.

Tables of random numbers have probably been used for multiple purposes at least since the Industrial Revolution. In the digital age, algorithmic pseudorandom number generators (PRNGs) have largely replaced these tables. The NIST Beacon expands the use of randomness to multiple scenarios in which neither tables nor PRNGs can 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.

Although commercially available physical sources of randomness are adequate as entropy sources for currently envisioned implementations of the NIST Beacon, the NIST

Randomness Beacon project team is working on developing a source of *verifiably random* sequences. In collaboration with NIST physicists from the Physical Measurement Laboratory (PML), the project team aims to use quantum non-locality to build an entropy source whose unpredictability is guaranteed by the laws of physics. In FY 2016, a major milestone was achieved, namely, a strong loophole-free test of local realism (where individual particles are governed by elements of reality, even if these elements are hidden from us*)* (see https://www.nist.gov/news-events/news/2015/11/nist-team-proves-spooky-action-distance-really-real).

The project team has also made progress in reaching a goal of helping other institutions set up other interoperable sources. This is important because multiple sources can be combined in such a way that all sources would have to be compromised in order to degrade the common random strings.

As of the end of FY 2016, the NIST Beacon has been functioning without interruption for more than three years. During this time, the project team has received valuable input from a growing community of users. As a result, the project team will provide an enhanced version of the service during FY 2017. The enhancements are mainly intended to enable interoperability.

NIST encourages the community-at-large to research and publish novel ways in which this tool can be used.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/programs-projects/nist-randomness-beacon

CONTACT:

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

Cryptography Applications in Wireless and Mobile Security

Today, wireless networks have been integrated into modern communication systems that connect mobile devices using multiple radio technologies. Such heterogeneous networks demand integrated security solutions. The NIST team has worked closely with different working groups in the IEEE 802 LAN/MAN Standards Committee since 2006 and made solid contributions to the security solutions for wireless networks. The NIST team has been involved in the IEEE 802.11 and IEEE 802.21 working groups to develop standards for cryptographic key management schemes for the mobility environment.

NIST cryptographic standards have been extensively used in the wireless standards developed in the IEEE 802 community. In FY 2016, the NIST team actively worked with the IEEE 802.1 security group in using the Galois/Counter Mode (GCM) specified in NIST Special Publication 800-38D for Media Access Control (MAC) security (MACsec) solutions.

In FY 2016, NIST researchers continuously collaborated with the IEEE 802.21 Working Group to develop solutions for multicast group key distribution and coauthored a paper titled “Security Multicast Group Key Management and Key Distribution in IEEE 802.21.” The paper has been accepted by the Security Standardization Research Conference 2016 (SSR 2016) and will be presented on December 5-6, 2016.

In FY 2017, the NIST team will continue to contribute to IEEE 802 wireless standards and provide guidance for NIST cryptographic standard usage in wireless and mobility applications.

CONTACT:

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

Blockchains

The Cryptographic Technology Group (CTG) began studying the use of blockchains, which have been suggested as a solution for many applications. A blockchain is a distributed database that maintains a continuously growing list of records called *blocks* that are secured from revision using a hash function. Each block contains a link to the previous block. A new block is added to the chain only when multiple parties (possibly mutually untrusting parties) agree to its accuracy. In essence, a blockchain is a mutually agreed-upon record of history.

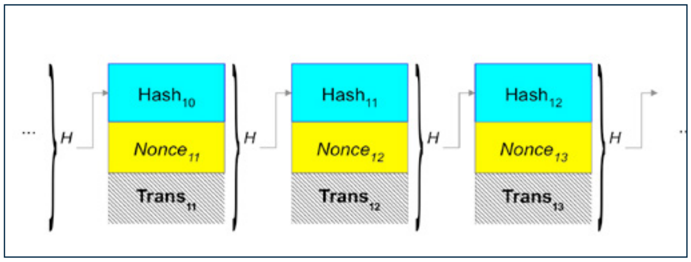


Figure 14: Example of a Blockchain

Figure 14: Example of a Blockchain illustrates three blocks in a blockchain, where each block contains at least one transaction, a nonce and the hash value of the previous block in the chain.

The most well-known example of the use of a blockchain is BitCoin and similar digital currencies. However, the use of blockchains has been proposed for other applications, such as smart contracts and various ledgering applications.

Many organizations have suggested applications for the use of blockchains, some of which may not be appropriate. The CSD is investigating the use of blockchains to determine which application types are appropriate for using blockchains and which are not. The CTG is monitoring the proposed uses of cryptography to assure that current cryptographic techniques are used properly and whether new techniques are required.

During FY 2016, the CTG participated in two blockchain workshops: the "DC Blockchain Summit" in March and the "Blockchain and Healthcare Workshop" in September. The CTG took an active role in the September workshop by reviewing papers and providing presentations on blockchains and the CTG standards that might be useful for future blockchain work. The CSD also began testing the use of several blockchain nodes.

During FY 2017, in addition to continuing familiarization with the use of blockchains and monitoring the cryptography proposed, the CTG is planning to participate in a blockchain study group sponsored by American Standards Committee X9, the financial services committee of the American National Standards Institute (ANSI).

CONTACTS:

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

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

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

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

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

Entropy as a Service (EaaS)

The security of cryptography today depends on having strong keys and keeping them secret. The ability to generate strong cryptographic keys is directly related to having access to unpredictable random data, but generating truly unpredictable random data on computing devices is hard and unreliable. As a result, weak keys are widely used in cryptographic applications, thus compromising the security of the sensitive data protected by them – potentially with disastrous consequences.

A primary goal of this project is to provide high-quality, truly unpredictable random data to devices on the Internet to enable them to generate strong cryptographic keys and attest the strength of the keys used to protect data in transit or at rest, thereby enabling cryptographic system strength attestation. Achieving this goal would provide a solid basis for achieving the goals of the Automated Cryptographic Validation Testing project (see http://csrc.nist.gov/projects/acvt/) as well as addressing the problems targeted by the Cryptographic Programs and Laboratory Accreditation (see the next section: Validated Programs, the first project in that section), where entropy estimation has persisted as one of the most difficult and labor-consuming activities, causing problems for all parties involved: the industry, the testing laboratories and the government validators.

Random data obtained from sources of true randomness that are based on unpredictable physical phenomena, such as quantum effects, is much better suited for cryptographic applications. 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 https://www.nist.gov/pml/div684/random_numbers_bell_test.cfm/

This project aims to develop a system and protocols for obtaining random data with high entropy from one or more remote sources. The high-level architecture is shown in Figure 15: (See next page) High-level Architecture of EaaS. The architecture of the Entropy-as-a-Service system consists of two main parts: the client-side and the server-side. The critical components of the system are the quantum device, the EaaS server and a secure device in the client systems that is capable of providing strong isolation and protection for the cryptographic keys stored inside the device and offering a set of basic cryptographic services.

The EaaS server is continuously fed random data from the attached quantum source. The data enters a FIFO (first in, first out)-like buffer in the server's Random Access Memory (RAM), and, when a client request arrives, the server reads the top value from the buffer, signs and encrypts it, and then sends it to the requester. The FIFO buffer shifts after every request and when new data comes from the random source. The EaaS server ensures that the FIFO buffer is erased prior to server shutdown and never paged to disk. Open implementations can help ensure that this occurs.

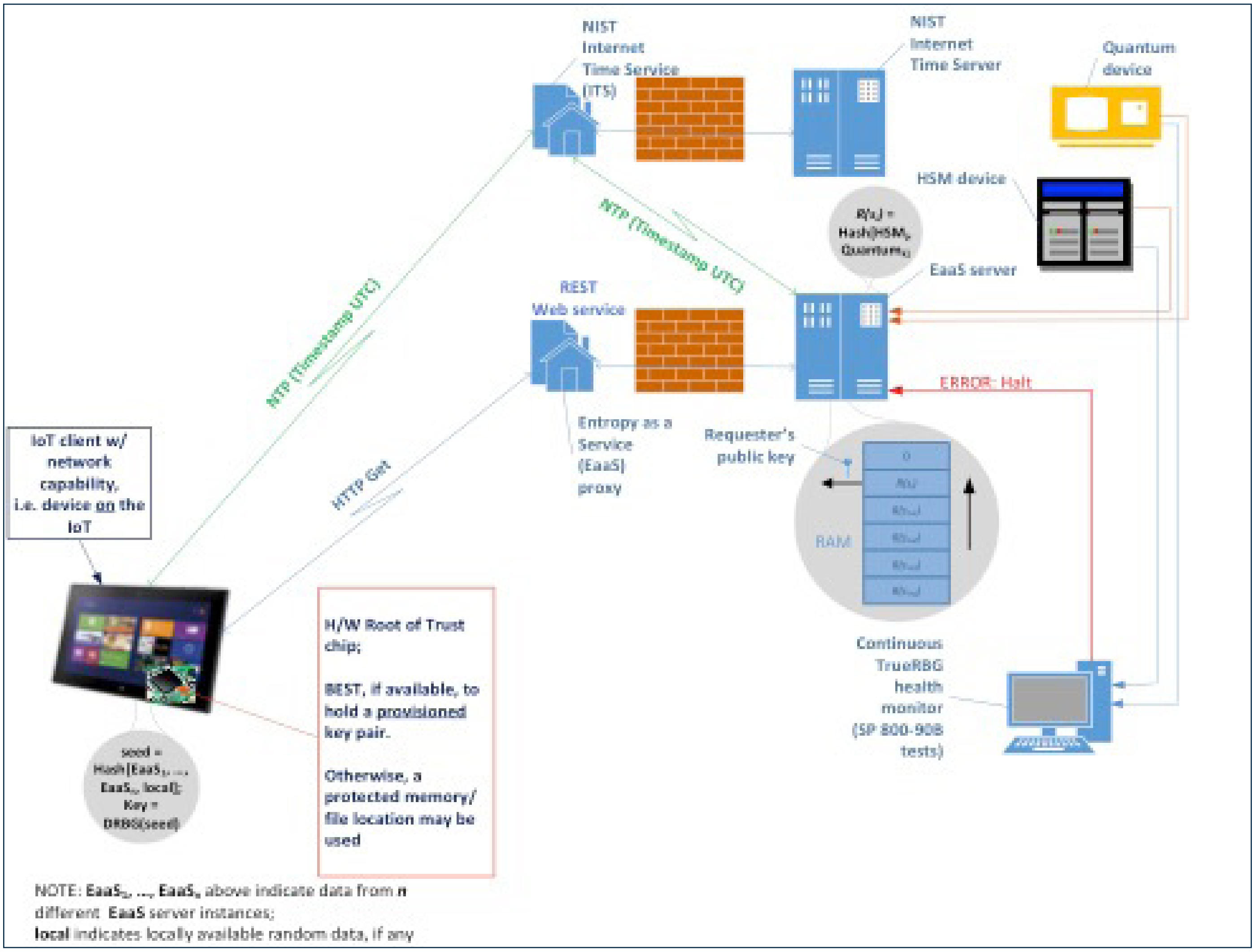
The client system consists of a classic computing device enabled with a dedicated hardware component capable of storing secret cryptographic keys and seeds. A dedicated software application bridges the communication between EaaS and the hardware component. Examples of secure hardware components are the Trusted Platform Module (TPM), TrustZone technology in Advanced Reduced Instruction Set Computing (RISC) Machine (ARM) processors, and Identity Protection Technology in Intel processors. If a client system or device doesn't have a secure hardware component, it can still use EaaS. The presence of a hardware component simply provides further guarantees to the system or device user, when present.

EaaS uses HTTP to transfer entropy payloads from the service to clients. To secure this transmission, the server encrypts the data using the client's provided public key and digitally signs the payload with the server's own private key.

Client devices mix this data with locally available random data to seed random number generators to generate strong cryptographic keys and other random values independently from the remote sources.

With the conceptual system architecture and protocols defined, the project team continues to engage with industry and academia to obtain feedback on the approach and identify possibilities for collaborative approaches to solving important cybersecurity challenges in the domains of cryptography and supply-chain management (e.g., integrated circuit counterfeiting). The team published a peer-reviewed paper on EaaS in IEEE Computer, a top professional journal, in September 2016. The team also started a collaboration with a team of researchers at the University of Florida who won a NIST research grant to explore ways to leverage EaaS in protecting against integrated circuit counterfeiting and thereby help secure the supply chain. The University of Florida researchers will start their project in FY 2017.

The team continues to develop the system to provide a publicly accessible NIST EaaS instance in FY 2017. During the summer of FY 2016, the team hosted a Summer Undergraduate Research Fellowship (SURF) student who developed a sample EaaS-client implementation with a


NIST Internet Time Service (ITS)
NIST Internet Time Server
Quantum device
HSM device
R(i,j) = Hash(HSM_i, Quantum_j)
EaaS server
NTP (Timestamp UTC)
REST Web service
ERROR: Halt
NTP (Timestamp UTC)
Entropy as a Service (EaaS) proxy
Requester's public key
0
RAM
IoT client w/ network capability, i.e. device on the IoT
HTTP Get
H/W Root of Trust chip;
BEST, if available, to hold a provisioned key pair.
Otherwise, a protected memory/ file location may be used
Continuous TrueRBG health monitor (SP 800-90B tests)
seed = Hash[EaaS_1, ..., EaaS_n, local]; Key = DRBG(seed)

NOTE: EaaS$_1$, ..., EaaS$_n$ above indicate data from *n* different EaaS server instances;
local indicates locally available random data, if any

Figure 15: High-level Architecture of EaaS

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

proper cryptographic mixing of random data obtained from multiple EaaS instances and local sources. The team plans to publish the server and client code on GitHub in FY 2017 and invite the public to voluntarily adopt it. Related to this, the project team is planning to work on developing public criteria for reputable EaaS hosts. The team succeeded in obtaining NIST funding to hire contractors to help with the implementation and hosting of the EaaS server; the contractor team has been identified, and the project will start in FY 2017.

CONTACT:

Dr. Apostol Vassilev
(301) 975-3221
apostol.vassilev@nist.gov

Automated Cryptographic Validation Testing

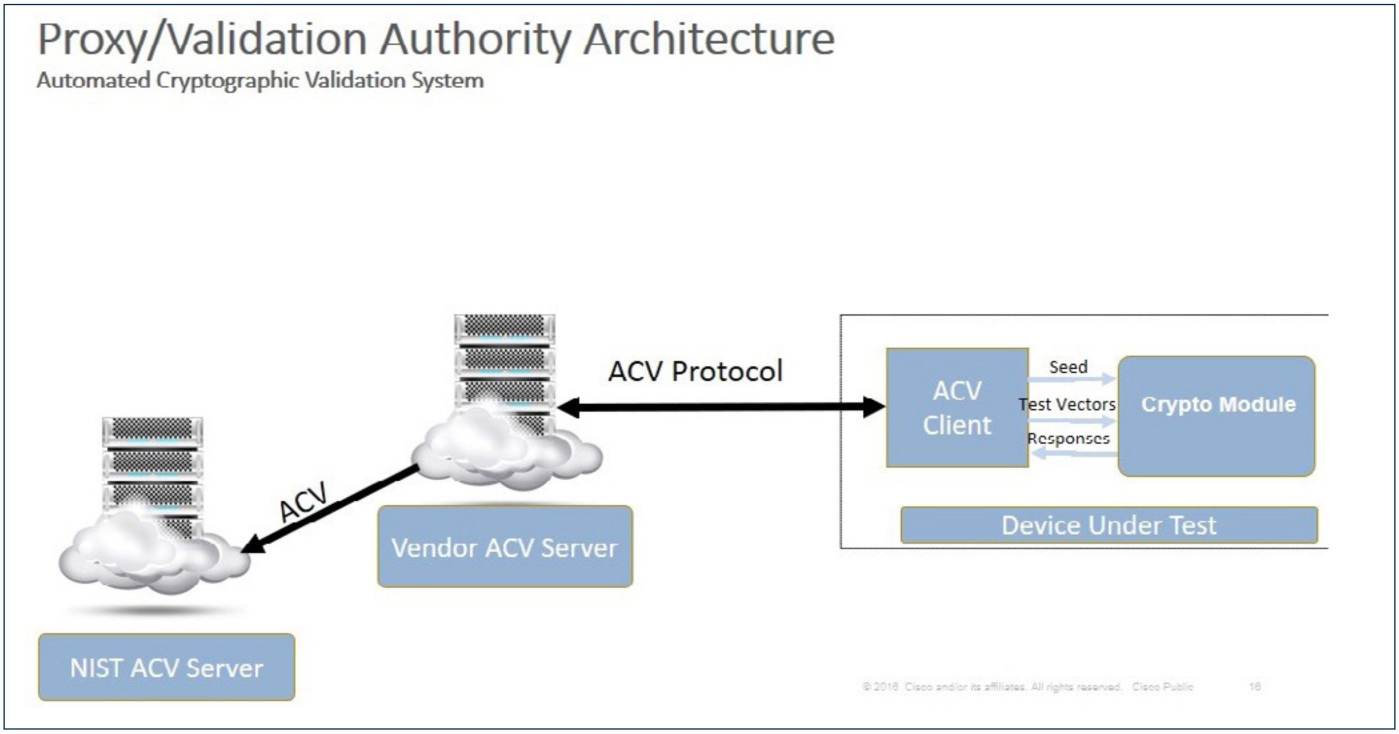
The Cryptographic Module Validation Program (CMVP) was established on July 17, 1995 by NIST to validate cryptographic modules conforming to the Federal Information Processing Standards (FIPS) 140-1, *Security Requirements for Cryptographic Modules*, and other FIPS cryptography-based standards. FIPS 140-2 was released on May 25, 2001 and supersedes FIPS 140-1.

The current implementation of the CMVP is shown in Figure 16: Current Validation Flow below. The CMVP leverages the National Voluntary Laboratory Accreditation Program (NVLAP) accredited Cryptographic and Security testing (CST) laboratories for validation testing against the derived test requirements (DTR), implementation guidance (IG), and applicable CMVP programmatic guidance. According to existing guidance, the CST laboratories must perform 100 % independent testing of the modules submitted by the vendors.

The structure and the rules under which the CMVP operates worked well for the level of the technology utilized by the Federal Government when the program was created more than two decades ago. As technology has advanced, however, the module testing process no longer satisfies the current industry and government operational needs. Testing is exceedingly long—well beyond typical product-development cycles across a wide range of technologies. The resulting validated modules often do not provide useful interfaces for integration into IT systems to enable run-time monitoring of modules for compliance with FISMA.

NIST recognizes the need to improve the efficiency and effectiveness of cryptographic module testing to reduce the time and cost required for testing, while providing a high level of assurance for Federal Government consumers.

The principal goals of this project are to collaborate with commercial or open source producers of cryptographic capabilities and government consumers of FIPS 140-validated modules to:



Proxy/Validation Authority Architecture

Automated Cryptographic Validation System

ACV Protocol

ACV

ACV Client

Seed

Test Vectors

Responses

Crypto Module

Device Under Test

Vendor ACV Server

NIST ACV Server

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public 18

Figure 16: Current Validation Flow

- Improve the efficiency and effectiveness of cryptographic module testing by adopting the best practices used by industry;
- Develop test procedures and techniques that provide assurance of module compliance to FIPS 140 in an automated manner, based on machine-readable artifacts or evidence (Examples of machine readable artifacts are Extensible Markup Language (XML) or JavaScript Object Notation (JSON) files containing logs from performed tests and the corresponding results. At this stage, we have only partially concluded the research on this and can point to examples at https://github.com/usnistgov/ACVP); and
- Identify techniques and procedures that provide continued assurance of operational compliance to FIPS 140 for cryptographic modules throughout their lifecycle.

The scope of this project is broken into multiple phases to be performed over several years.

PHASE 1

- Identify potential approaches,
- Select the best technical approach or approaches to prototype, and
- Document the technical approach.

PHASE 2

- Develop working prototypes, and
- Evaluate the prototypes against the principal goals.

PHASE 3

- Publish a draft, provide a review period, adjudicate the comments, and publish the final version.

PHASE 4

- Integrate the final version into the operational CMVP program.

Currently, the project is focused on completing the documentation of the technical approach for automating the algorithm testing and researching the approaches for automating the software module testing. The team working on this project, in collaboration with the industry, demonstrated successful automated algorithm validations at the International Cryptographic Module Conference in May 2017 for some algorithms (see https://acvts.nist.gov/acvp/home) and continues to develop the automation of the rest of algorithms currently tested by the traditional Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/index.html) with the goal of replacing it by the second quarter of 2018.

The project activities are structured by work areas in order for subject-matter experts to more narrowly focus and make progress.

1. Algorithm and Protocol Testing;
2. Cryptographic Module Testing,
   a. Hardware,
   b. Software, and
   c. Modules in cloud environments; and
3. Positioning and relationships to other Government Validation Programs.

The project has several planned deliverables, including the identification of prospective technical approaches that adopt industry best practices and produce artifacts that are machine readable and map to DTR requirements, and a selection of the best technical and feasible approaches.

CONTACT:

Dr. Apostol Vassilev
(301) 975-3221
apostol.vassilev@nist.gov

VALIDATION PROGRAMS

Federal agencies, industry, and the public rely on many of the standards and specifications supported by ITL. Poor implementations of these standards or specifications may render a product insecure, potentially placing sensitive information at risk. ITL 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 CSD 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 National Voluntary Laboratory Accreditation Program (NVLAP). Based on independent laboratory test reports and test evidence provided by the labs, the validation programs described below validate the implementation-under-test. Awarded validations are subsequently published on NIST websites.

Cryptographic Programs and Laboratory Accreditation

Cryptographic Module Validation Program (CMVP)

The Cryptographic Module Validation Program (CMVP) was developed to support the federal user communities for strong, independently tested, and commercially available cryptographic modules. Through this program, the CMVP works 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 is to provide federal agencies with a security metric to use in procuring and deploying cryptographic modules, and promote the use of validated modules by industry and the public. The testing performed by independent third-party laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP), and the validations performed by the CMVP program 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 module testing and validation are based on published NIST standards. Since federal agencies are required to use validated cryptographic modules for the protection of sensitive unclassified information, the validated modules and the validated algorithms that the modules contain represent the culmination and delivery of CSD's cryptography-based work to the end user.

The CMVP validates modules 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. While a module may be a standalone product (e.g., a virtual private network (VPN) or smart card), in many cases, a module (e.g., a cryptographic-based toolkit) is embedded into many products. Because a small number of modules may be incorporated within hundreds of products, the validation process has significant impact.

The theme for the CMVP in FY 2016 was change. The CMVP is evolving to be more efficient and consistent. The CMVP implemented an automated system, modified workflow processes to provide better transparency and strengthened collaboration with the Cryptographic Modules User Forum (CMUF).

On October 1, 2015, the CMVP began using a new automated system to manage the validation workflow. The impact to the CMVP's efficiency was dramatic. In FY 2016, the CMVP awarded 307 new certificates, 111 more than in FY 2015. Figure 17: FY 2016 CMVP Certificates by Security Level displays the number of certificates by security level for FY 2016.

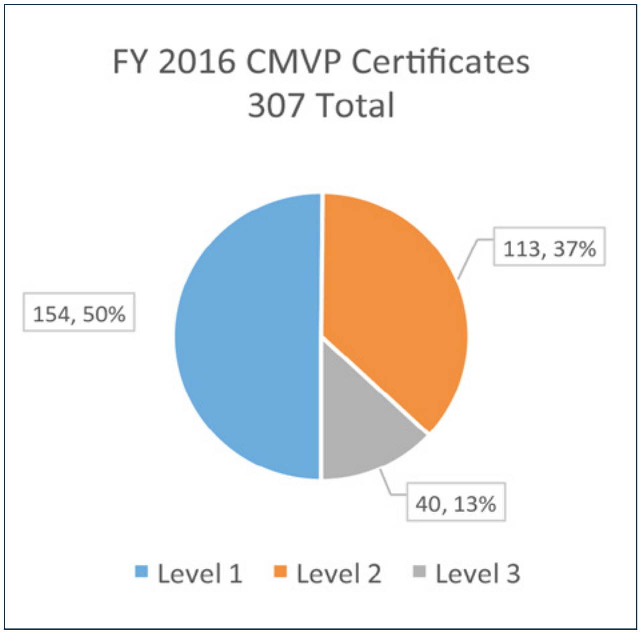


Figure 17: FY 2016 CMVP Certificates by Security Level

The automated system tracks the status of each submission and identifies the order in which the submissions should be reviewed, based on when each submission is added to the CMVP queue. Automating this housekeeping task significantly increased the efficiency of the validation process. Not only does this allow the CMVP time to focus on other tasks, it reduces the number of status messages from the laboratories that request a status for their specific submission. Status messages have dropped from 4 to 6 per week to 0 to 1 per week.

The number of submissions sitting in the CMVP queue and the average queue time have been reduced in part due to this automation. The number of modules in the queue has dropped from an average of 120 to an average of 65. The average queue length (e.g., the amount of time between the arrival of a submission and when the review begins) has dropped from an average of four months to an average of less than two months. The average amount of time to validate a module is six months, with some validations being completed within two months. In the last quarter of FY 2016, the queue was, at times, empty.

One specific area where the automated system provided dramatic improvement was the NIST billing process. Generating an invoice was reduced from an average of three weeks to one day. Similarly, receiving a notification that an invoice was paid went from an average of one week to one day. These are contributing factors to the reduction in the queue length. This achievement was due to the cooperative relationship between the CMVP and NIST Receivables, who worked through technical challenges to allow the systems to exchange information.

In May 2015, to provide greater transparency to the laboratories, the CMVP began sending a weekly report to each laboratory, providing the status of each of their submissions. Before the capability to prepare and send this report was available, the CMVP and laboratories would, at times, find that each thought the other had the next action, resulting in unnecessary delays.

In August 2015, to provide greater transparency to users, the CMVP separated the Implementation-Under-Test (IUT) list from the rest of the Modules-In-Process (MIP) list. Separating the lists allows the users to quickly and easily see that the CMVP does not have any information on the modules currently being tested (i.e., those listed in the IUT list). In fact, the IUT list is provided as a marketing service for vendors that have made a commitment to achieving validation, but whose module(s) are not yet in the MIP.

The CMVP strengthened its relationship with the CMUF by supporting the monthly CMUF general membership meetings and five CMUF working groups. The working groups are chaired by a member of industry and/or by laboratory personnel. Each working group includes a representative from the CMVP. The current working group topics include the Security Policy Template; Testing Equivalency; Revalidation in Response to Common Vulnerabilities and Exposures (CVEs); Proposed IG Integrity Testing using Random Sampling and IG Updates (IG 3.5 Documentation Requirements for Cryptographic Module Services, IG 1.20 Sub-Chip Cryptographic Subsystems, and 7.7 Key Establishment and Key Entry and Output). This CMUF collaboration allows greater progress on technical guidance and incorporates differing perspectives.

For FY 2017, the CMVP team is:

- Anticipating the approval of FIPS 140-3. When approved, the CMVP will create the necessary documents and processes to support the transition from FIPS 140-2 to FIPS 140-3;
- Continuing to invest in automation to streamline the validation process and improve review consistency. One effort that started in FY 2016 was the ability for a laboratory to request an invoice while the laboratory finalizes the submission to CMVP. If laboratories leverage this new capability, the CMVP could see a further reduction in the queue length;
- Anticipating the rollout of the new Computer Security Resource Center (CSRC) web site. This will allow the CMVP to replace the static validation pages with an interactive capability for users, along with other improvements for users. Following this, the CMVP will begin the transition to a web-based submission process to replace the current email-based process;
- Continuing to strengthen its relationship with the CMUF by collaborating on new and improved technical guidance and programmatic issues; and
- Joining the International Cryptographic Module Conference (ICMC) program committee to continue strengthening partnership within the community.

FOR MORE INFORMATION, SEE:

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

CONTACT:

Ms. Jennifer Cawthra
301-975-8514
jennifer.cawthra@nist.gov

The Cryptographic Algorithm Validation Program (CAVP)

The Cryptographic Algorithm Validation Program (CAVP) provides federal agencies in the United States and Canada with assurance that a cryptographic algorithm has been implemented completely and correctly, as specified in its approved Federal Information Processing Standard (FIPS-Approved) or NIST-recommended cryptographic algorithm standard. The CAVP was established in 2013 as a joint program in collaboration between NIST and the Communications Security Establishment (CSE) of Canada. Prior to this date, the CAVP's functions were included in the Cryptographic Module Validation Program (CMVP). With the increase in the number and complexity of FIPS-Approved and NIST-recommended cryptographic algorithms, it was deemed necessary to establish the CAVP as an independent program.

The CAVP's goal is to provide federal agencies with a security metric to use in validating cryptographic algorithm implementations, and promote the use of validated algorithms by industry and the public. The testing is carried out by independent third-party laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP), and the validations performed by the CAVP program provide this metric. Federal agencies, industry, and the public can choose validated implementations of cryptographic algorithms from the CAVP Validated Algorithms List and have confidence in the claimed level of security and assurance of correct implementation.

The validation of cryptographic algorithms by the CAVP is a prerequisite to the validation of a cryptographic module by the CMVP and is also used by other programs outside of NIST as well. Since federal agencies are required to use validated cryptographic modules for the protection of sensitive unclassified information, the validated modules and the validated algorithms that the modules contain represent the culmination and delivery of CSD's cryptography-based work to the end user.

The CAVP validation program provides documented methodologies for conformance testing through defined sets of security requirements. For the CAVP, a validation system document is designed for each FIPS-approved or NIST-recommended cryptographic algorithm. See the website for a listing (see http://csrc.nist.gov/groups/STM/cavp/). The four Annexes to FIPS 140-2 reference the underlying cryptographic algorithm standards or methods.

By the end of 2016, the CAVP had issued approximately 23,559 validations, representing the algorithm validations of approximately 18 approved algorithms, including 5 modes of operation.

The CAVP issued approximately 4,000 algorithm validations in FY 2016, an increase of approximately 600 validations from the previous year. The increase in validations is attributed to an increase in cryptographic modules being validated and other outside programs now requiring CAVP validated implementations, e.g., the National Information Assurance Partnership (NIAP).

The number of algorithms submitted for validation continues to grow, representing significant growth in the number of validations expected to be available in the future.

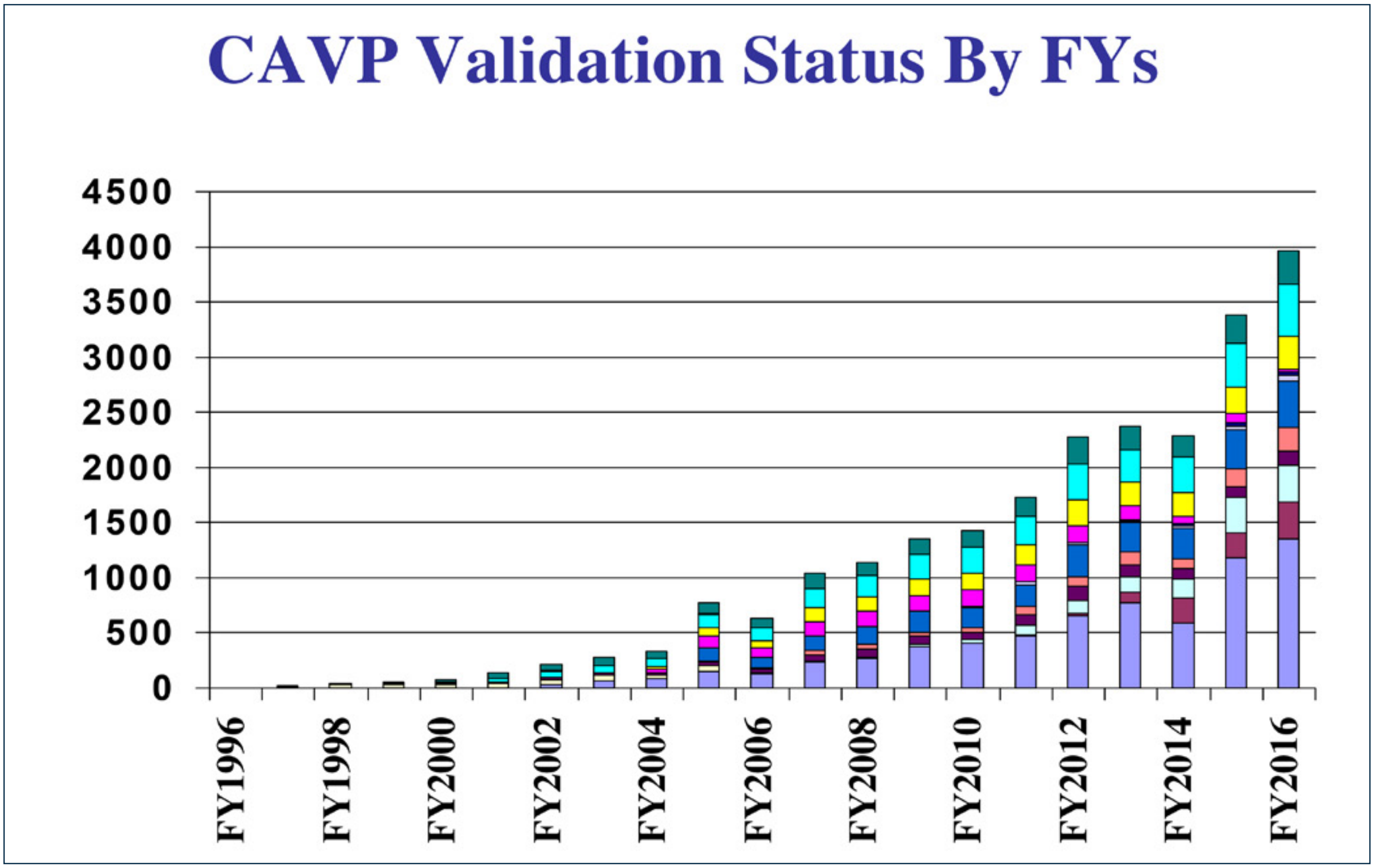


Figure 18: CAVP Validation Status by Fiscal Year

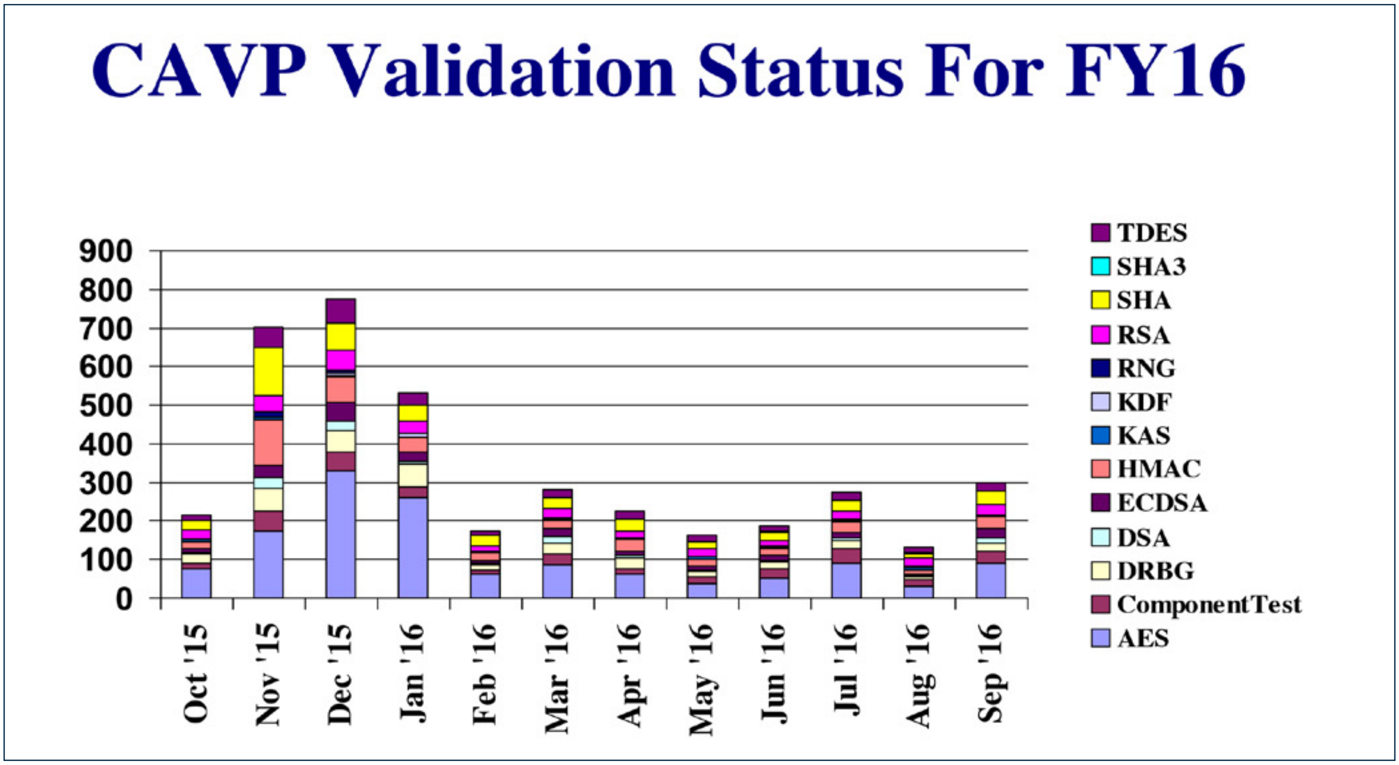
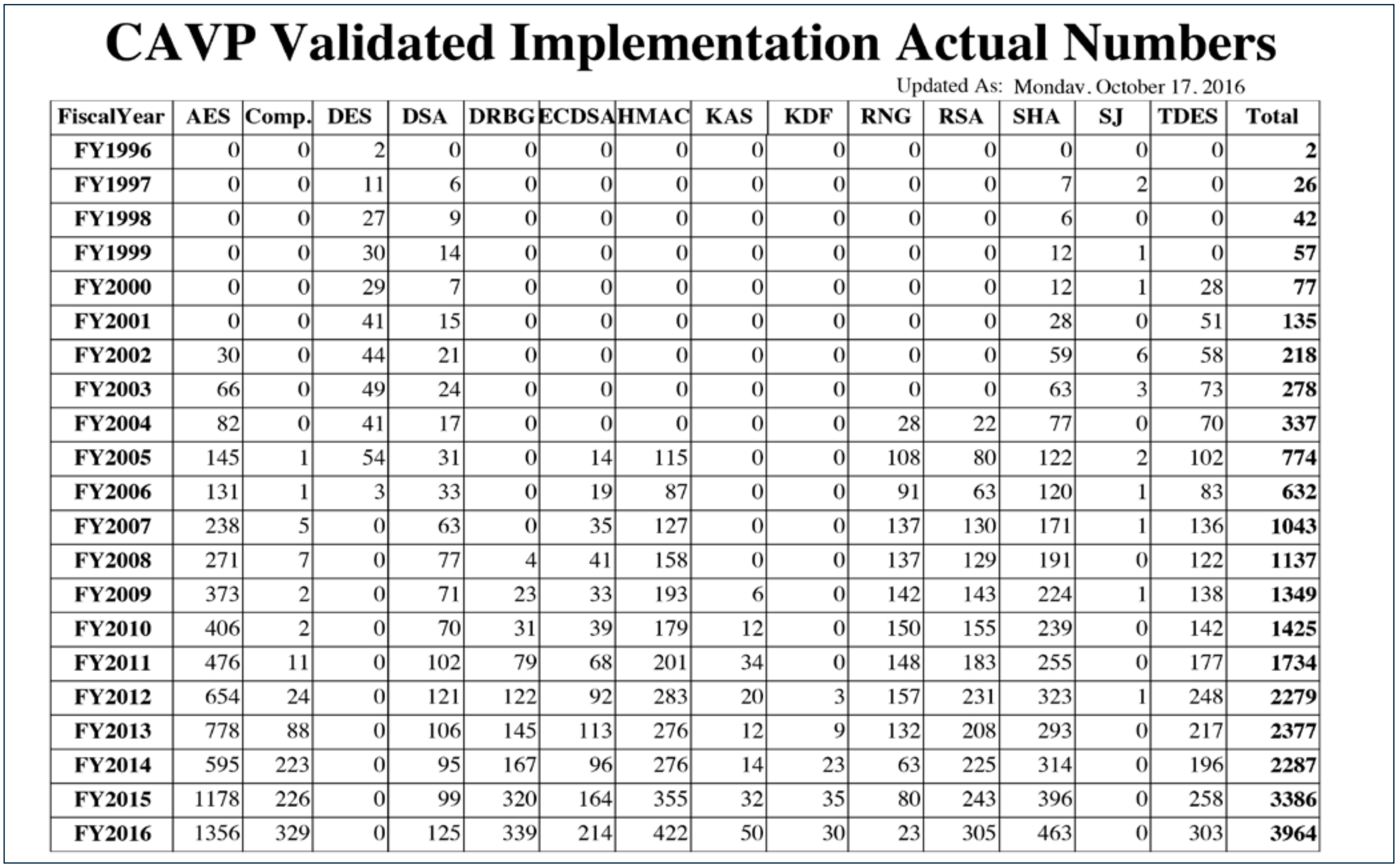


Figure 19: CAVP Validation Status for FY 2016



CAVP Validated Implementation Actual Numbers

Updated As: Monday, October 17, 2016

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	406	2	0	70	31	39	179	12	0	150	155	239	0	142	**1425**
FY2011	476	11	0	102	79	68	201	34	0	148	183	255	0	177	**1734**
FY2012	654	24	0	121	122	92	283	20	3	157	231	323	1	248	**2279**
FY2013	778	88	0	106	145	113	276	12	9	132	208	293	0	217	**2377**
FY2014	595	223	0	95	167	96	276	14	23	63	225	314	0	196	**2287**
FY2015	1178	226	0	99	320	164	355	32	35	80	243	396	0	258	**3386**
FY2016	1356	329	0	125	339	214	422	50	30	23	305	463	0	303	**3964**

Figure 20: CAVP Validated Implementation Actual Numbers

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program

CONTACT:

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

(Editors' Note: Sharon Keller worked on this program until her recent retirement.)

Automated Security Testing and Test Suite Development

The CAVP utilizes the requirements and specifications of the NIST standards (i.e., FIPS and Special Publications) to develop algorithm validation test suites and an automated security testing tool. 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 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 used by independent third-party laboratories accredited by 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 of 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 requires the chaining of information from one block to the next.

During the last few years, the CSD Cryptographic Technology Group (CTG) has expanded its publications to contain not only the algorithm's specifications, but also requirements for 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 CMVP if the requirements are considered applicable to the cryptographic module. However, some of these usage requirements may 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:

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

- SP800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*;
- 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.

TABLE 1: CRYPTOGRAPHIC ALGORITHMS & NIST TECHNICAL DOCUMENTS (FIPS & SPS)

CRYPTOGRAPHIC ALGORITHM/COMPONENT	FEDERAL INFORMATION PROCESSING STANDARD (FIPS) OR SPECIAL PUBLICATION (SP) OR OTHER REFERENCE DOCUMENT
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 Algorithm (DSA)	FIPS 186-2, *Digital Signature Standard (DSS), with change notice 1* and
	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 and
	FIPS 186-4, *Digital Signature Standard (DSS)*, and ANS X9.62
RSA algorithm	FIPS 186-4, *Digital Signature Standard (DSS)* and
	ANS 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)
Hashing algorithms SHA3-224, SHA3-256, SHA3-384, SHA3-512	FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015*
SHA-3 Extendable-Output Functions (XOFs) SHAKE128, SHAKE256	FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015*
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*
Keyed-Hash Message Authentication Code (HMAC) using SHA-1, SHA-2 and SHA-3	FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*
Cipher-based Message Authentication Code (CMAC) Mode for Authentication	SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*
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*
GCM, Galois Message Authentication Code (GMAC), and eXtended Packet Number (XPN) Modes	SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*
XTS-AES Mode	SP 800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*

Table 1: Cryptographic Algorithms & NIST Technical Documents (FIPS & SPs)

TABLE 1 (CONT.): CRYPTOGRAPHIC ALGORITHMS & NIST TECHNICAL DOCUMENTS (FIPS & SPS)

CRYPTOGRAPHIC ALGORITHM/COMPONENT	FEDERAL INFORMATION PROCESSING STANDARD (FIPS) OR SPECIAL PUBLICATION (SP) OR OTHER REFERENCE DOCUMENT
Key Wrapping	SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*
DH and MQV 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 schemes without the Key Derivation Functions (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 the 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 a 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

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program

CONTACTS:

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

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

(Editors' Note: Sharon Keller worked on this program until her recent retirement.)

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 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, *Security Content Automation Protocol (SCAP) Version*

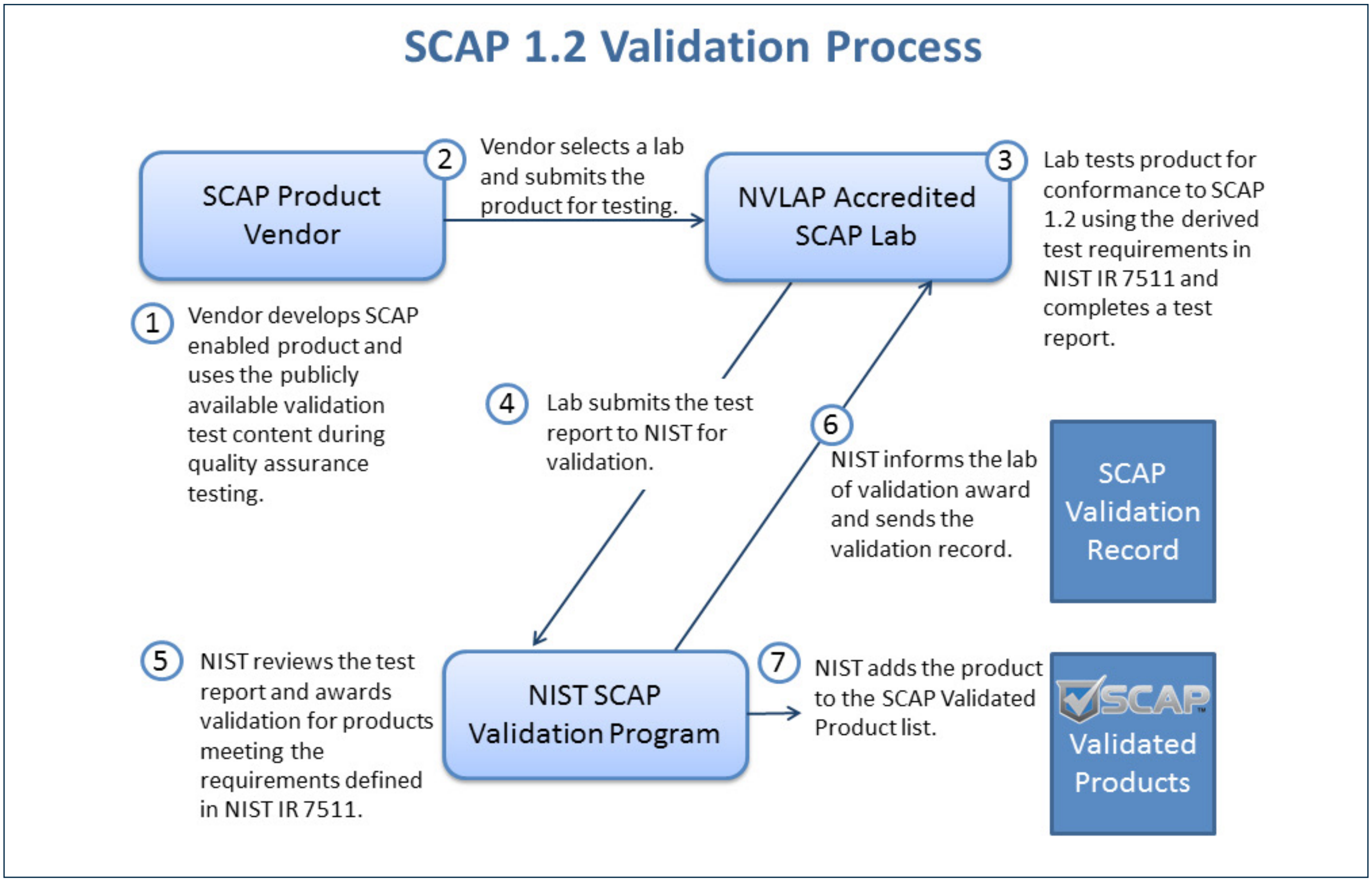

SCAP 1.2 Validation Process
SCAP Product Vendor
2 Vendor selects a lab and submits the product for testing.
NVLAP Accredited SCAP Lab
3 Lab tests product for conformance to SCAP 1.2 using the derived test requirements in NIST IR 7511 and completes a test report.
1 Vendor develops SCAP enabled product and uses the publicly available validation test content during quality assurance testing.
4 Lab submits the test report to NIST for validation.
6 NIST informs the lab of validation award and sends the validation record.
SCAP Validation Record
5 NIST reviews the test report and awards validation for products meeting the requirements defined in NIST IR 7511.
NIST SCAP Validation Program
7 NIST adds the product to the SCAP Validated Product list.
SCAP Validated Products

Figure 21: SCAP 1.2 Validation Process

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 an NVLAP-accredited laboratory. Once the lab completes product testing, the lab submits a test report to the SCAP Validation Program at NIST for review. NIST reviews the test report and awards a validation if all requirements have been met. Once a validation is awarded, the SCAP Validation Record is sent to the lab, and the information about the newly validated product is posted on the SCAP Validated Products web page. Figure 21: SCAP 1.2 Validation Process illustrates the SCAP 1.2 Validation Process.

All resources and information necessary for preparing products for SCAP 1.2 validation are published on the SCAP Validation Program web pages (see the url below). The most current NISTIR 7511 revision, as well as SCAP capabilities and supported platforms, are available on the home page (see http://scap.nist.gov/validation). The resources page includes 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 the 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 identify the product versions that were tested in the laboratory, along with details about each validation, such as the tested platforms, SCAP capabilities, the validation test suite version, and the lab that performed the product test.

In FY 2016, several products successfully completed testing and were awarded validations, bringing the total number of SCAP 1.2-validated products to fifteen. Most vendors of configuration scanning products are SCAP validated, and vendors continually pursue validation for new platforms, capabilities, and versions of SCAP. 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 2017, NISTIR 7511 will be updated, adding requirements to test products for conformance to SCAP 1.3. New capabilities include testing the ability of products to process the most recent Open Vulnerability and Assessment Language (OVAL) versions and to read Software Identification (SWID) tags. The modular structure of the SCAP Validation Program supports the addition of these new test requirements, as well as new platforms and capabilities, without needing to re-design the entire program. Vendors benefit from the modular structure by choosing the capabilities and platforms that satisfy the needs of their customers.

FOR MORE INFORMATION, SEE:

http://scap.nist.gov/validation

CONTACT:

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

IDENTITY AND ACCESS MANAGEMENT

NIST Personal Identity Verification Program (NPIVP)

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 (detailed below). 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 conformance tests for these two components are Cryptographic and Security Testing (CST) Laboratories accredited by the NVLAP. As of September 2016, there were seven such facilities (see http://csrc.nist.gov/groups/SNS/piv/npivp/testing_facilities.html).

The interface specifications for the PIV Smart Card Application and PIV Middleware are found in a FIPS 201 companion document, namely, SP 800-73-4, *Interfaces for Personal Identity Verification*. The conformance tests for these specifications are detailed in SP 800-85A-4, *PIV Card Application and Middleware Interface Test Guidelines.* To implement these tests and to generate conformance test reports, CSD also developed and maintains an integrated toolkit called the "PIV Interface Test Runner," which conducts tests on both PIV Smart Card Applications and PIV Middleware products. This toolkit is provided to accredited NPIVP test facilities for product testing and to the general public as open source software.

The NPIVP team is also closely involved in activities related to the revision of specifications of the PIV companion documents, such as SP 800-73, SP 800-76, *Biometric Specifications for Personal Identity Verification*, and SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification. This ensures that specification revisions in the PIV documents* are fully reflected in the conformance test documents, SP 800-85A-4 and SP 800-85B (*PIV Data Model Conformance Test Guidelines)* as well as in the "PIV Interface Test Runner" toolkit. The changes to PIV specifications in PIV companion documents necessitated that NPIVP make a major update to the conformance test documents and consequently to the "PIV Interface Test Runner" toolkit in 2016. The updated Test Runner is available at http://csrc.nist.gov/groups/SNS/piv/npivp/sw-downloads.html.

The NPIVP team also maintains the Validation List for PIV Smart Card Application and the PIV Middleware products that are PIV-conformant implementations. Updates to the PIV Smart Card Application validation list were necessary in 2016 to comply with the sunset date for some Random Number Generators (RNGs), as outlined in SP 800-131A, *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.* More information about the sunset can be found at http://csrc.nist.gov/groups/SNS/piv/npivp/announcements.html.

In FY 2017, the NPIVP team will continue to fine-tune its toolkit and perform acceptance testing for PIV Smart Card Applications and PIV Middleware.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/NIST-Personal-Identity-Verification-Program

CONTACTS:

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

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

Personal Identity Verification (PIV) and FIPS 201 Revision Efforts

Figure 22: 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 CSD and the Information Access Division (IAD). CSD activities in FY 2016 directly supported the latest revision of FIPS 201 (i.e., FIPS 201-2) by updating the relevant publications associated with FIPS 201-2 and by developing several new publications. CSD performed the following activities during FY 2016 in support of HSPD-12:

- Published Draft SP 800-116 Revision 1, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS).* This document provides best practice guidelines for integrating the PIV Card with the PACS that authenticate the PIV cardholders in federal facilities. The document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal Government facilities and assets.
- Published SP 800-156, *Representation of PIV Chain-of-Trust for Import and Export.* This document provides the data representation of a chain-of-trust record for the exchange of records between issuers. The exchanged record can be used by an agency to personalize a PIV Card for a transferred employee, or by a service provider to personalize a PIV Card on behalf of client federal agencies. The data representation is based on a common XML schema to facilitate interoperable information sharing and data exchange. The document also provides support for data integrity through digital signatures and confidentiality through encryption of chain-of-trust data in transit and at rest.
- Published a white paper, Best Practices for Privileged User PIV Authentication, in response to OMB's *30-day Cybersecurity Sprint* effort and subsequent OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, which requires federal agencies to use PIV credentials for authenticating privileged users. The white paper outlines the risks of password-based single-factor authentication, and describes best practices for the use of multi-factor PIV-based user authentication for privileged users.
- Published SP 800-166, *Derived PIV Application and Data Model Test Guidelines*. SP 800-166 contains the derived test requirements and test assertions for testing the Derived PIV Application and associated Derived PIV data objects residing on a mobile device. The tests verify the conformance of these artifacts to the technical specifications of SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*. SP 800-157 specifies standards-based, secure, reliable, interoperable public-key infrastructure (PKI)-based identity credentials. SP 800-166 is targeted at vendors of Derived PIV Applications, issuers of Derived PIV Credentials, and entities that will conduct conformance tests on these applications and credentials.
- Published SP 800-85A-4, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance),* to align the testing requirements with FIPS 2012, SP 800-73-4, and SP 800-78-4.

In FY 2017, CSD will continue to focus on updating relevant publications associated with FIPS 201-2, including

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

finalizing SP 800-116 Revision 1. CSD will also continue to provide technical and strategic inputs to the PIV-related initiatives.

FOR MORE INFORMATION, SEE:

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

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

Authentication

To support Office of Management and Budget (OMB) requirements, CSD developed SP 800-63, *Electronic Authentication Guideline*. OMB defines four levels of assurance that a federal agency must select, based on a risk assessment to determine the impact of an authentication failure. This guideline covers remote authentication of users (such as private individuals) interacting with government IT systems over the Internet. It defines technical requirements for each of the four levels of assurance in the areas of identity proofing, authenticators, credential binding, management processes, authentication protocols and federation. The newest revision underway in 2016 establishes three individual assurance categories that can map into the original OMB levels of assurance. The categories are:

- **Identity Assurance Level** - the robustness of the identity proofing process and the binding between an authenticator and the records pertaining to a specific individual;
- **Authentication Assurance Level** - the robustness of the authentication process itself; and,
- **Federation Assurance Level** - the robustness of the assertion protocol utilized by a federation to communicate authentication and attribute information (if applicable) to a relying party.

Since the initial release of SP 800-63, CSD has released two revisions to address changes in modern technology and lessons learned from practical implementations by federal departments and agencies.

In addition, market forces have resulted in an inflexion point in how departments and agencies authenticate users. NIST and the private-sector partners have observed that some public and private-sector identity assurance standards have become outdated or have simply not been adopted. Specifically, SP 800-63 was originally written to address an online world that is much different than today. Innovation has offered new perspectives in how trusted identities can be established. Practical implementations of SP 800-63 have informed us of areas of strengths, weaknesses, and techniques not utilized by federal agencies or the private sector. Note that our online adversaries are targeting user names and passwords as the simplest point of entry to gain unauthorized access to sensitive systems and data.

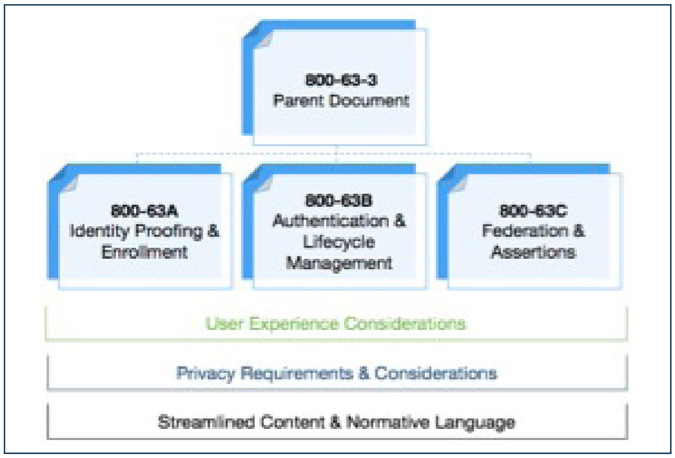

800-63-3
Parent Document
800-63A
Identity Proofing & Enrollment
800-63B
Authentication & Lifecycle Management
800-63C
Federation & Assertions
User Experience Considerations
Privacy Requirements & Considerations
Streamlined Content & Normative Language

Figure 23: New SP 800-63-3 Structure

CSD, in collaboration with the ACD Trusted Identities Group, hosted the two-day workshop "Applying Measurement Science in the Identity Ecosystem" in January 2016. NIST gathered critical feedback from over 200 industry, academic, and public-sector stakeholders regarding new directions that NIST should take in authentication guidance and in methods for measuring the strength of relevant technologies and processes. The workshop culminated in the release of NISTIR 8103, *Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps*.

In May 2016, ITL released a public preview draft of NIST SP 800-63-3, with an updated name, *Digital Authentication Guideline*. This body of work represents a significant departure from prior versions of the special publication. The guideline has been divided into a family of standalone documents that focus on outcomes and innovation where possible, rather than prescriptive processes and technologies (see Figure 23). A significant number of requirements were updated or removed, with many new requirements introduced, including increased allowances for the use of biometrics in authentication systems. SP 800-63-3, while required for federal agencies, suggests requirements for solutions often provided by the private sector; hence, many updates were garnered from innovation in the market, workshop feedback, and a dialog with all sectors while the guideline was open for comment. CSD and ACD also piloted a new approach to managing stakeholder feedback and document updates. During the development of the SP 800-63 revision, drafts of the documents were made available on GitHub, an online version management and collaboration tool that allowed us to openly discuss comments in real time and accept edits directly into the document from ITL stakeholders. This was the first time that an 800 series draft Special Publication was published on GitHub; the use of GitHub proved successful and will continue to be used to manage SP 800-63-3 as the document transitions from public preview to final version.

In FY 2017, CSD will publish the final SP 800-63-3 revision, giving agencies an increased set of secure, privacy-enhancing, and user-friendly options to deliver safe digital services to their constituents. The final version may also serve as a foundation for future authentication shared services that the government will offer, such as those directed by the Cybersecurity National Action Plan (CNAP).

Work on 800-63-3 will continue after the document becomes final. ITL will work on identifying ways to measure authentication systems in a more systematic and scientific way, allowing NIST to specify additional metrics that would be required in future authentication systems, based on risk. Work on biometric authentication will capitalize on the opportunity to enhance the authentication performance and security of a range of modalities (e.g., fingerprint, voice, or iris recognition). NIST will explore the inclusion of additional industry best practices into future revisions of SP 800-63-3. NIST will also research methods to ensure that practices align with the security and privacy demands of digital services offered by government. In addition to the topics described above, the team will research approaches that harmonize U.S. Government requirements on an international scale, promoting easy-to-implement cross-border trusted identity solutions. This helps avoid challenges that result from disparate, nationally unique authentication guidelines that may disrupt international interoperability.

FOR MORE INFORMATION, SEE:

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

https://pages.nist.gov/800-63-3

CONTACT:

Mr. Paul Grassi
(703) 786-8275
paul.grassi@nist.gov

Access Control and Privilege Management

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

In FY 2016, the following activities were accomplished for this project:

- Researched the requirement and capabilities for Access Control (AC) policy composing and verification technology;
- Studied attribute considerations for access mechanism implementation; the results are presented in the internal draft of a NIST SP, *Attribute Consideration for Access Control Systems* (no publication number has been assigned to this internal draft SP), which is scheduled to be released during FY 2017);
- Researched the AC requirements and functions for distributed systems, including Big Data, Cloud, IoT, and the Smart Grid; and
- Published NIST SP 800-178, *A Comparison of Attribute Based Access Control (ABAC) Standards for Data Services*, and worked on two internal draft NIST SPs: 1) Draft SP 800-192: *Verification and Test Methods for Access Control Polices/Models*, and 2) Draft SP (no number yet assigned), *Attribute Consideration for Access Control Systems*; both SPs are related to access control and privilege management.

In FY 2017, CSD will continue the above research. 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 network systems;

- Increase the security and safety of static (connected) distributed systems by applying the testing and verification tool for the AC 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 AC rules and policies.

Figure 24 (below) illustrates the application of access control and privilege management within and among organizations.

CONTACTS:

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

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

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

Conformance Verification for Access Control Policies

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

To formally and precisely capture the security properties that 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 the 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.

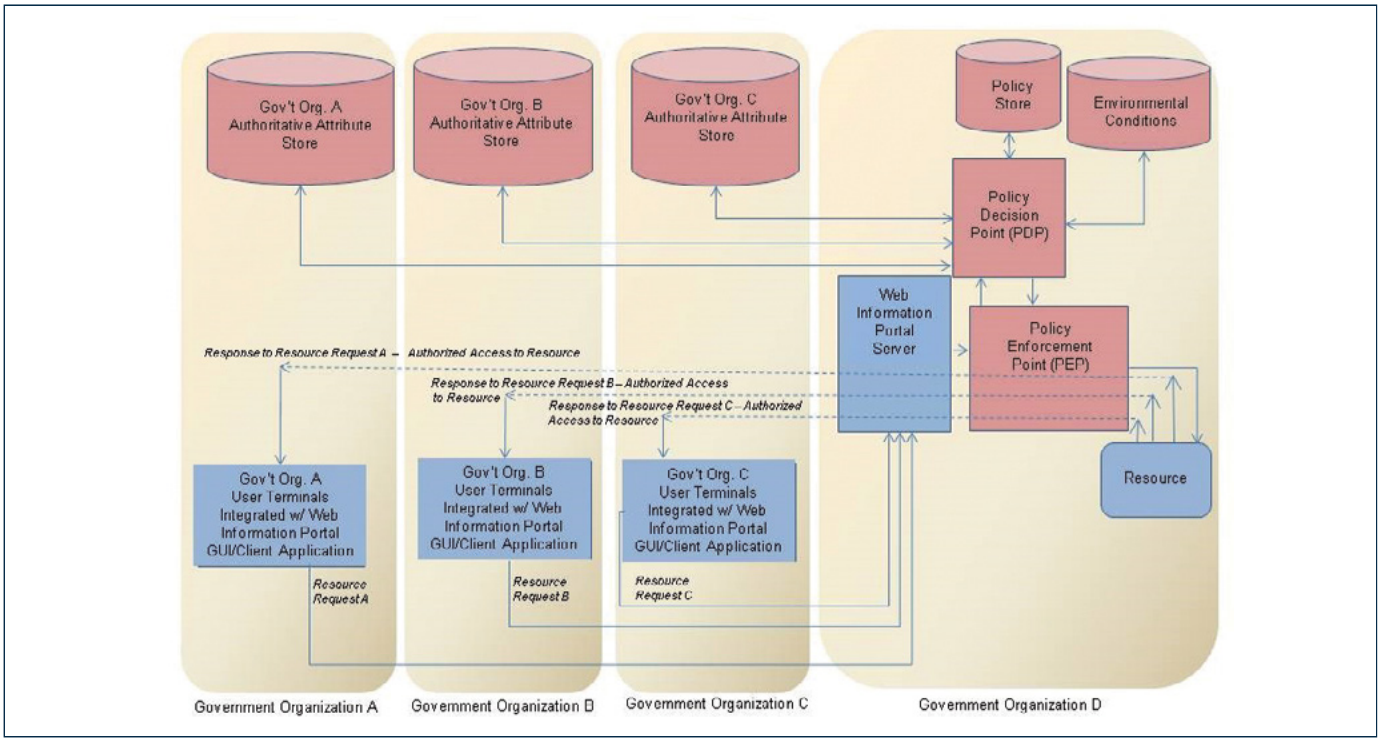

Gov't Org. A Authoritative Attribute Store
Gov't Org. B Authoritative Attribute Store
Gov't Org. C Authoritative Attribute Store
Policy Store
Environmental Conditions
Policy Decision Point (PDP)
Web Information Portal Server
Policy Enforcement Point (PEP)
Resource
Response to Resource Request A – Authorized Access to Resource
Response to Resource Request B – Authorized Access to Resource
Response to Resource Request C – Authorized Access to Resource
Gov't Org. A User Terminals Integrated w/ Web Information Portal GUI/Client Application
Gov't Org. B User Terminals Integrated w/ Web Information Portal GUI/Client Application
Gov't Org. C User Terminals Integrated w/ Web Information Portal GUI/Client Application
Resource Request A
Resource Request B
Resource Request C
Government Organization A
Government Organization B
Government Organization C
Government Organization D

Figure 24: Access Control and Privilege Management

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
https://dx.doi.org/10.6028/NIST.SP.800-195

Most research on AC model or policy verification techniques is 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 the verification or test processes to generate fault reports. Even though correct verification is achieved, and counter-examples may be generated when faults are found, those methods provide no information about the source of faults that might allow conflicts in privilege assignment, the leakage of privileges, or a conflict-of-interest in 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 because a fault might not be caused by one particular access rule. Thus, it requires manually analyzing each rule in the policy to find the correct solution for correcting the fault.

To address the issue, CSD developed the Access Control Property Tool (ACPT), shown in Figure 25, which allows a user to compose, verify, test, and generate access control policies. CSD also 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.

In FY 2016, CSD accomplished the following:

- Funded and supported two Small Business Innovation Research (SBIR) Phase II projects for access control tool developments;
- Enhanced the usability and fixed bugs of the ACRLCS (the Access Control Rule Logic Circuit Simulation System) to provide more capability for policy fault detection;
- Published a conference paper: *General Methods for Access Control Policy Verification*, and an article: *Access Control Policy Verification* for policy test case generation;
- Worked with industrial and academic organizations in exploring new capabilities that helped to improve the usability of the AC tools (ACPT and ACRLCS), resulting in additional usage; ACPT was downloaded by 405 users and organizations; and
- Enhanced the capability of ACPT by adding an *object inheritance* capability for basic access control models.

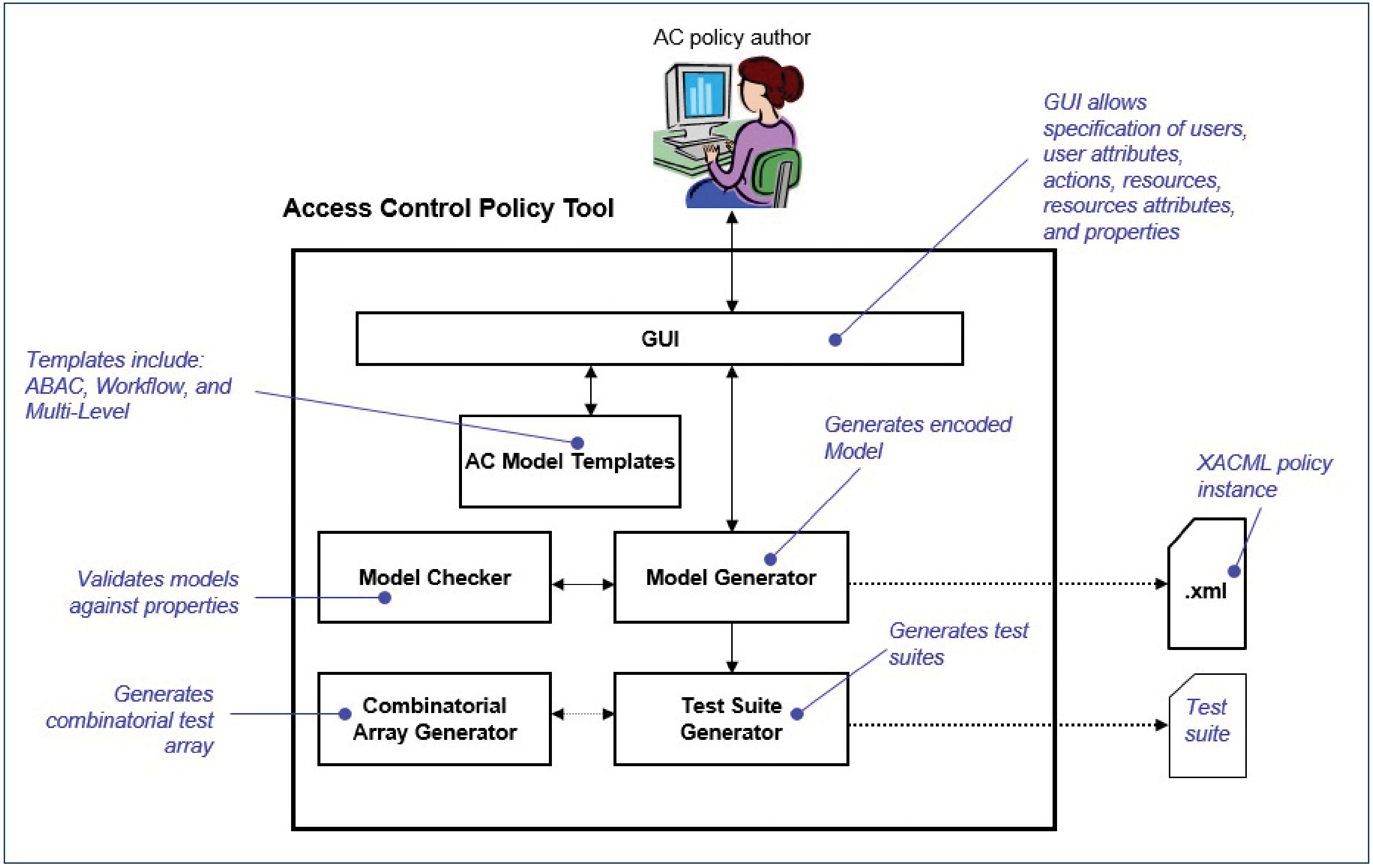

AC policy author
Access Control Policy Tool
GUI allows specification of users, user attributes, actions, resources, resources attributes, and properties
GUI
Templates include: ABAC, Workflow, and Multi-Level
AC Model Templates
Generates encoded Model
XACML policy instance
Validates models against properties
Model Checker
Model Generator
.xml
Generates test suites
Generates combinatorial test array
Combinatorial Array Generator
Test Suite Generator
Test suite

Figure 25: Access Control Property Tool (ACPT)

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM: http://dx.doi.org/10.6028/NIST.SP.800-195

In FY 2017, CSD is planning to conduct further research on efficient testing technology, new capabilities, and enhance the performance of the ACPT and ACRLCS.

Figure 25 (See previous page) shows the system architecture of the NIST Access Control Policy Tool (ACPT), which allows access control policy authors to compose, verify, and test access control policy implementation.

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 for 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 Attribute-Based Access Control (ABAC) and Multi-Level Security (MLS) as well as some fundamental security properties.

FOR MORE INFORMATION, SEE:

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, environmental conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. For example, access to a database could be restricted to users with particular attributes, such as membership in a group (e.g., employees) and other conditions (e.g., part of the Human Resource Department). 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.

CSD is conducting research that provides information for using ABAC to improve information sharing within and among organizations based on the planning, design, implementation, and operational considerations. The research also includes technologies such as attribute assurance, attribute engineering/management, identity system integration, attribute federation, situational awareness (real-time or contextual) mechanisms, policy management, and natural-language policy translation to digital policy. Figure 26 (See next page) illustrates the interaction of many of these components. The goal of this research is to improve information sharing, while maintaining control of that information for federal agencies.

In FY 2016, the project team:

- Worked on the book *Attribute-Based Access Control – Models & Deployments;* publishing is planned for March 2017 by Artech House;
- Published NIST Special Publication 800-178, *A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications document*; and
- Continued research, in partnership with the Trusted Identities Group (TIG) and the National Cybersecurity Center of Excellence (NCCoE), on the attribute assurance of ABAC.

In FY 2017, CSD will continue the research of ABAC formal models, as well as details and extended topics of ABAC capabilities, such as attribute considerations, ABAC implementation examples, ABAC mechanisms, and ABAC standards. The ABAC project will pursue the following objectives:

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

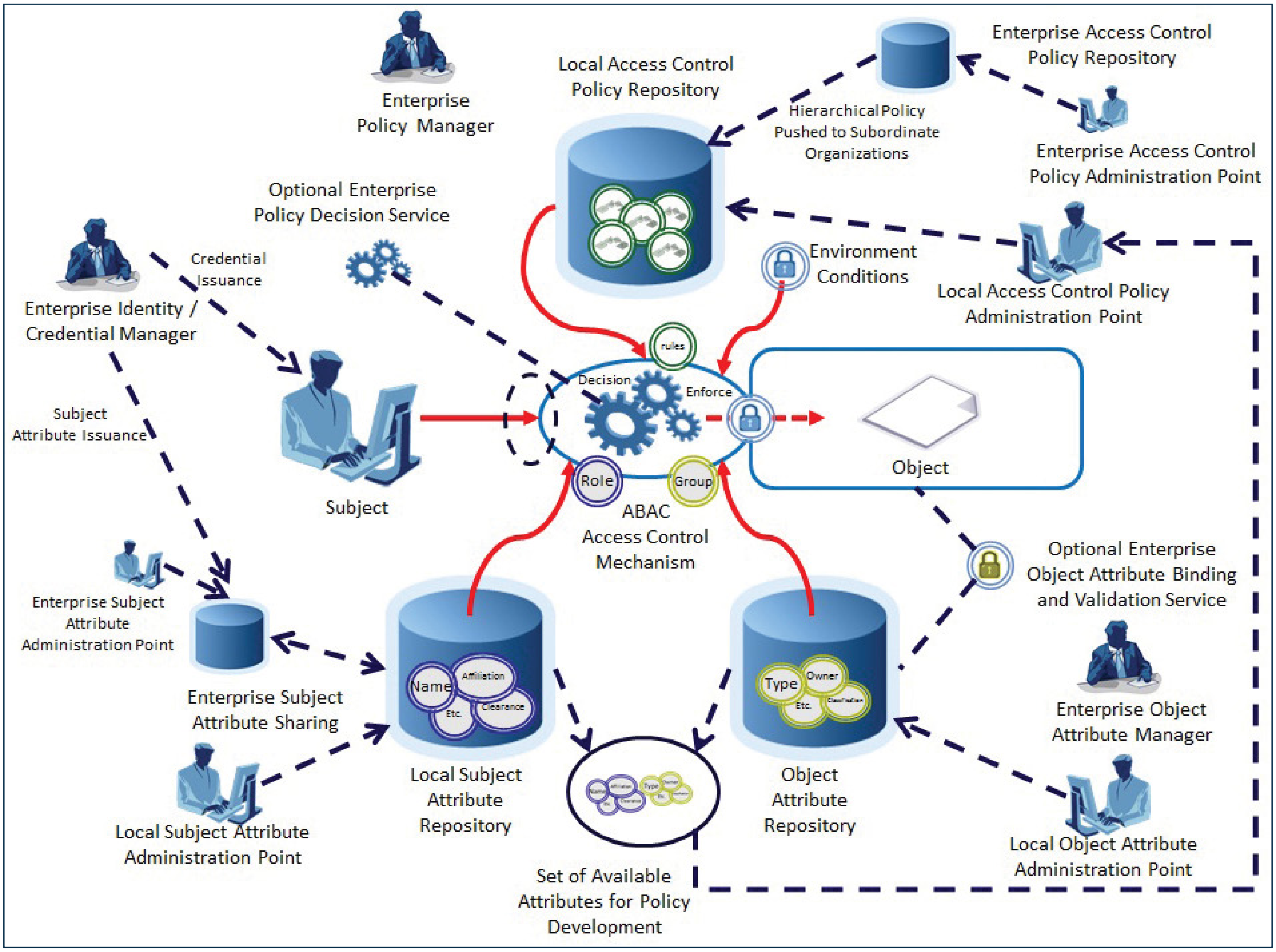

Enterprise Policy Manager
Local Access Control Policy Repository
Enterprise Access Control Policy Repository
Hierarchical Policy Pushed to Subordinate Organizations
Enterprise Access Control Policy Administration Point
Optional Enterprise Policy Decision Service
Credential Issuance
Enterprise Identity / Credential Manager
Environment Conditions
Local Access Control Policy Administration Point
rules
Decision
Enforce
Subject Attribute Issuance
Subject
Object
Role
Group
ABAC Access Control Mechanism
Optional Enterprise Object Attribute Binding and Validation Service
Enterprise Subject Attribute Administration Point
Enterprise Subject Attribute Sharing
Name
Affiliation
Etc.
Clearance
Type
Owner
Etc.
Classification
Enterprise Object Attribute Manager
Local Subject Attribute Repository
Object Attribute Repository
Local Subject Attribute Administration Point
Local Object Attribute Administration Point
Set of Available Attributes for Policy Development

Figure 26: ABAC Access Control Mechanism Chart

- 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;
- Promote the adoption of ABAC for a more secure and flexible method for information sharing in a standalone or enterprise environment; and
- Provide testing methods for ABAC policy and implementations.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

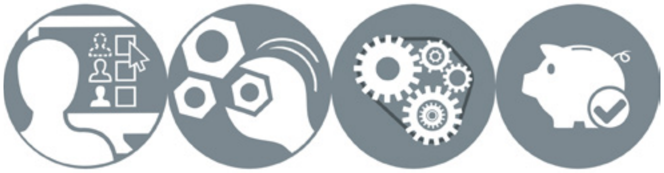
Dr. Vincent Hu (301) 975-4975 vhu@nist.gov	Mr. David Ferraiolo (301) 975-3046 david.ferraiolo@nist.gov
Mr. Rick Kuhn (301) 975-3337 kuhn@nist.gov	

Trusted Identities Group (TIG)

ACD's Trusted Identities Group (TIG) is tasked with improving online identity for individuals and organizations so they can employ solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation (see http://www.nist.gov/itl/tig). The TIG focuses

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

on outcomes that meet the four guiding principles that identity solutions be privacy-enhancing and voluntary, secure and resilient, interoperable, cost-effective and easy to use.



Through the promotion of government and commercial adoption of privacy-enhancing, secure, interoperable, and easy-to-use identity solutions, the TIG drives trust, convenience, and innovation in digital identity.

The TIG is a partnership model that supports the private sector, advances risk management practices, develops and revises guidance and standards to be co-developed with private and public stakeholders, assists agencies in the implementation of identity solutions in their systems, promotes international interoperability of identity standards and solutions, and funds innovative projects through pilots and other funding mechanisms.

To achieve these ends, the TIG is working to advance measurement science, technology, and standards adoption in digital identity by focusing on four primary tactics: partnerships, publications, market intelligence, and communications.

Partnerships

External Projects. The TIG funds external projects, including a pilot program that impacted more than 6.7 million individuals in its first four years. These projects aim to catalyze the marketplace to begin developing solutions aligned with the guiding principles. The marketplace is currently transitioning from broad market issues to targeting specific gaps and market impediments as the identity ecosystem matures. The pilots develop and deploy technology, models, and frameworks that wouldn't otherwise exist in the marketplace. In FY 2016, the pilot programs made remarkable progress; the 24 projects include more than 170 partner organizations across 12 sectors—including the development or deployment of 14 multi-factor authentication solutions. Over the course of the fiscal year, six new pilots were launched (including five supporting state services and one driving federated identity in healthcare) (See https://www.nist.gov/itl/tig/pilot-projects).

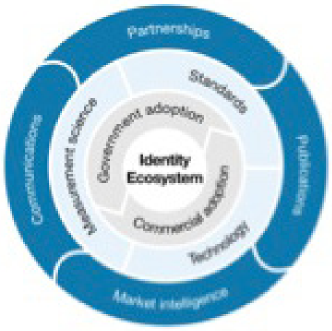


Figure 27: NIST employs four primary tactics: partnerships, publications, market intelligence, and communications

Identity Ecosystem Framework. The privately-led Identity Ecosystem Steering Group (IDESG) laid the groundwork for better digital identity transactions with the release of the Identity Ecosystem Framework (IDEF) in early FY 2016. The IDEF lays a foundation for the Identity Ecosystem by providing a baseline set of requirements that define how to execute transactions involving digital identity that puts users at the center by aligning with the four guiding principles, continually improving online commerce, the efficiency of digital services, and online interactions (see http://www.idesg.org/News-Events/Press-Releases/ID/74/Identity-Ecosystem-Framework-Released-Creating-Unprecedented-Rules-of-the-Road-for-Online-Identity).

Strategic partners. The TIG works alongside many professional organizations, agencies, and entities in the identity community on a daily basis. Their partnerships allow them to gain stronger insights, evolve their thinking and ideas, create more robust publications, orchestrate successful events, participate in speaking engagements across the country, bring in outside experts to review TIG federal funding opportunities, and allow for a broader reach of messaging and announcements. Under this model, the TIG works to co-develop NIST publications, creating an increasingly inclusive approach to producing the best possible documents. The TIG also works directly with agencies on their solutions to provide expert advice in the risk management of identity solutions and the implementation of those solutions.

Several publications were released in 2016 (many through the use of GitHub, to best ensure that the broad community can stay involved in their efforts and that they are transparent and informative every step of the way). Details are provided below; the list is current as of the end of FY 2016. The updated publications list can be found on the TIG resources page (see https://www.nist.gov/itl/tig/resources).

- Draft SP 800-63-3: *Digital Authentication Guideline* (see https://pages.nist.gov/800-63-3/)
- Draft NISTIR 8149: *Developing Trust Frameworks to Support Identit*y Federation (see https://pages.nist.gov/NISTIR-8149/)
- Publications that apply measurement science in the Identity Ecosystem:
  - NISTIR 8103: Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps (see http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8103.pdf)
  - Strength of authentication:
    - Discussion Draft: Strength of Function for Authenticators – Biometrics (see https://pages.nist.gov/SOFA/)
    - Discussion Draft: Measuring Strength of Authentication (see https://www.nist.gov/sites/default/files/nstic-strength-authentication-discussion-draft.pdf)
  - Attribute metadata and confidence scoring:
    - Draft NISTIR 8112: Attribute Metadata (see https://pages.nist.gov/NISTIR-8112/)
    - Discussion Draft: Attribute Metadata and Confidence Scoring (see https://www.nist.gov/sites/default/files/nstic-attribute-confidence-metadata-discussion-draft.pdf)
  - Strength of identity proofing:
    - Discussion Draft: Measuring Strength of Identity Proofing (see https://www.nist.gov/sites/default/files/nstic-strength-identity-proofing-discussion-draft.pdf)

Market Intelligence

The TIG is continuously identifying, collecting, and analyzing metrics to gain greater insight into the development and adoption of TIG-aligned solutions. This work aids NIST in measuring the market shift toward these solutions and honing efforts moving forward so NIST most effectively uses program resources. This increases the likelihood that, with each new initiative, the TIG meets the market—rather than expecting the market to meet them.

Communications

The TIG also leverages external communications to inform the public about its work and engage a variety of audiences to collaborate on projects as well as to align efforts and maximize the impact of NIST's investment in cybersecurity initiatives. The TIG works with government and industry groups to raise public awareness of cybersecurity tools and concepts, such as by collaborating with the National Cybersecurity Alliance on campaigns, including Lock Down Your Login, National Cybersecurity Awareness Month, and Data Privacy Day. The TIG also regularly shares achievements and announcements via published documents, speaking engagements all over the country, webinars, their website and blog, social media engagement and outreach, and customized events for stakeholders. For instance, in FY 2016, the TIG coordinated the Advanced Identity Workshop, which brought together over 200 technology vendors, cybersecurity researchers, policy makers, and other experts from the public and commercial sectors.

In FY 2017, the TIG will continue to work to advance measurement science, technology, and standards adoption in identity management and focus on their four primary tactics of partnerships, publications, market intelligence, and communications. The TIG plans to also move on to new endeavors, such as:

- The identification of opportunities and mechanisms to complement the work of their pilot programs;
- Increased work alongside federal agencies to address specific identity challenges through the NCCoE;
- New research projects;
- Additional standards work;
- Increased communication efforts to educate audiences of all types;
- Continued engagement with various NIST programs to further integrate the Identity Ecosystem into NIST cybersecurity efforts; and,
- Continued focus on industry engagement.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/itl/tig

CONTACTS:

Dr. Mike Garcia	Ms. Kristina Rigopoulos
(202) 494-4122	(202) 309-4791
michael.garcia@nist.gov	kristina.rigopoulos@nist.gov

RESEARCH IN EMERGING TECHNOLOGIES

Secure Development Toolchain Competitions

Many security weaknesses in federal information systems stem from software security vulnerabilities induced by software flaws present in current-generation software products. CSD tracks software security vulnerabilities (in the National Vulnerability Database), and seeks techniques for the measurement of security vulnerabilities and techniques that reduce the impact and prevalence of security vulnerabilities in newly developed products or in new versions of existing products.

One approach to reducing the number of security vulnerabilities in software is to improve the development tools that are available. By identifying languages and software development tools that support a reduction of vulnerabilities, and by stimulating the creation of better tools and tool usage techniques, the approach should help developers produce applications with fewer vulnerabilities. While it is impossible to assure the total absence of security vulnerabilities in this way, it might well be possible to rule out specific, significant classes of vulnerabilities that currently provide the basis for many serious exploits.

CSD is developing an empirical, competitive approach to finding the most effective and usable combinations of tools to produce software systems that are relatively free of exploitable vulnerabilities. Multiple competitions are planned that will be based on an idea developed during the *Designing a Secure Systems Engineering Competition Workshop* that was conducted by the National Science Foundation in 2010. The workshop proposed a competition for the development of a set of tools to help non-security-expert developers to rapidly build a significant application with zero vulnerabilities, as detected by an extensive public test suite.

The participants in the planned competitions would implement software systems to solve challenge problems using software development tool chains ("toolchains") of their own choosing, within specified time periods. The toolchains may include existing technologies (e.g., existing software libraries and frameworks, code generators, reusable source code, or bug-finding tools), novel technologies, or any combination thereof. Each competition would apply a time pressure by simulating a deadline in the software development process, increasing the likelihood of an introduction of security flaws. The objective of the toolchains would be to detect or prevent security flaws while still supporting the quick-paced software development of applications with rich feature sets. Through the demonstration of security-flaw avoidance in a time-constrained setting, CSD would seek to show that wide-scale improvements in the overall security of software products could be realized without sacrificing a time-to-market goal. The competitions, which would be open to all interested parties, would aim to provide consistent application and measurement of commercial and research software development, composition, and reuse techniques.

In FY 2016, CSD partially reformulated the existing toolchain testing infrastructure to mitigate test infrastructure reliability problems uncovered by a dry run of the competition and by subsequent inspections. A key part of this reformulation was the consolidation of multiple operating systems into a single operating system for all components. Additionally, CSD developed an installation guide to assist with the building, installing, and operating of the toolchain testing infrastructure. The current infrastructure uses several third-party components and concurrently-running virtual machines. The installation guide describes the required system configurations, account provisioning on local hosts, installation and integration of third-party components and packages, and the network configuration. An updated version of these elements as well as a document describing the manual steps for performing simplified, script-oriented testing in the absence of a continuous integration system was also developed.

In FY 2017, CSD plans to substantially simplify portions of the testing infrastructure to improve reliability and reproducibility, to perform a second round of testing, and to publicly announce the first toolchain competition.

CONTACTS:

Mr. Lee Badger	Mr. Christopher Johnson
(301) 975-3176	(301) 975-3247
lee.badger@nist.gov	christopher.johnson@nist.gov

Networks of "Things"

The Internet of Things (IoT) increasingly appears to be the next great technology revolution. It is expected to impact everything from healthcare delivery, to how food is produced, to how we work, to all forms of transportation and communication, and to virtually all forms of automation. IoT will impact everyone, and in multiple ways.

With a technology revolution of such large impact on society, it is imperative that IoT-based systems can be trusted. This means that they should exhibit secure, reliable,

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

and private behaviors as well as many other attributes associated with quality (see references 2 and 4 below). Privacy is particularly important because IoT-based systems will likely produce huge amounts of data as a result of sensing and surveillance (see references 1, 3, and 4 below). This is the "big data" challenge associated with IoT. Therefore, techniques, tools, and methods to mitigate the numerous "trust" challenges are needed before these automated IoT-based networks manage much of daily life.

Historically, there has been little in the way of formal, analytic, or even descriptive information about the building blocks that govern the operation, trustworthiness, and life cycle of the Internet of Things. A composability model and vocabulary that defines principles common to most, if not all networks of things, was needed to address the question: "What is the science, if any, underlying IoT?" NIST SP 800-183, *Networks of 'Things'* does exactly that – it offers an underlying and foundational science to IoT that is based on a belief that IoT involves sensing, computing, communication, and actuation. The document describes five core building blocks (called *primitives*): (1) sensor, (2) aggregator, (3) communication channel, (4) eUtility, and (5) decision trigger.

SP 800-183 is unique in that it uses two acronyms, IoT and NoT (Network of Things), extensively and interchangeably. IoT is the outward facing acronym that most people are familiar with; a NoT is an unfamiliar term, but has the advantage of referencing a more specific set of interconnected objects to which one can apply the building blocks described above.

The relationship between IoT and NoT is subtle—IoT is an instantiation of a NoT, whereby IoT has its "things" tethered to the Internet. A different type of NoT could be a Local Area Network (LAN), with none of its "things" connected to the Internet. Social media networks, sensor networks, and the Industrial Internet are all variants of NoTs. This differentiation in terminology helps to separate use cases of varying vertical and quality domains (transportation, medical, financial, agricultural, safety-critical, security-critical, performance-critical, and high assurance, to name a few). The distinctions are useful since there is no singular IoT, and it is meaningless to speak of comparing one IoT to another. But one NoT can be compared to another NoT – that makes this viewpoint and the associated definition actionable.

Future work in this area will refine the definitions of the five core NoT building blocks. For example, instead of just considering an all-purpose sensor, categories of sensors will be explored. This will involve a decomposition of the building blocks. The research team will also demonstrate how to apply these definitions to vertical markets. In addition, the team will present these results in Revision 1 of NIST SP 800-183, which should be produced in late 2017 or early 2018.

FOR MORE INFORMATION, SEE:

1. NIST SP 800-183, *Networks of 'Things'*, July 2016, https://doi.org/10.6028/NIST.SP.800-183.

2. J. Voas and G. Hurlburt, "Third Party Software's Trust Quagmire", IEEE *Computer*, December 2015.

3. J. Voas, "Demystifying IoT", IEEE *Computer*, June 2016.

4. C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet of Things Security Hands-On", IEEE *Security and Privacy*, January 2016.

CONTACT:

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

Cloud Computing Security and Forensics

The term cloud computing was initially coined in 1997 by Professor Ramnath Chellappa of Emory University. During his talk, titled "Intermediaries in Cloud-Computing", which was presented at the Institute for Operations Research and the Management Sciences (INFORMS) meeting in Dallas, Texas, he referred to a cloud as an important new "computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone." The international IT literature and media later provided many definitions, models, and architectures, but it was not until 2011, when NIST published SP 800-145, *The NIST Definition of Cloud Computing,* that the world coalesced on the cloud deployment and service models, definitions and descriptions provided in SP 800-145.

Following the December 2010 Federal Government's "Cloud First" policy issued as part of the 25-point plan for the U.S. Federal Government's (USG) IT modernization and reform, NIST assumed a technical leadership role for the federal agencies' efforts related to the adoption and development of cloud computing standards. The goal was to accelerate the Federal Government's adoption of secure and effective cloud computing solutions to reduce costs and improve services.

In addition to the initial definition of cloud computing, NIST built a USG cloud computing technology roadmap that focused on security, interoperability, and portability

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

requirements, and lead efforts to develop standards and guidelines in close collaboration with standards bodies, the private sector, and other stakeholders. NIST also developed a cloud computing reference architecture, a security reference architecture and, during 2016, focused on developing the guidance for applying a risk-based approach to cloud adoption and the guidance for applying the SP 800-53 Revision 4 security and privacy controls to cloud-based federal information systems.

During FY 2016, NIST also started researching the security challenges encountered when leveraging application containers and microservices for the implementation of cloud-based federal information systems and the security challenges encountered when implementing cloud-based federated identity solutions, along with the impact on the system's security posture. Some of the current work is focusing on the development of an open security controls assessment language (OSCAL) that aims to revolutionize every step in the life cycle of a cloud-based information system and on the development of a cloud forensics reference architecture that is derived from the cloud security reference architecture mentioned above. Details regarding the latest projects are provided below.

CSD Role in the NIST Cloud Computing Program

During FY 2016, NIST continued to promote the development of publications, national and international standards, and specifications in support of the USG's effective and secure use of cloud computing, as well as providing technical guidance to federal agencies for secure and effective cloud-computing adoption. During FY 2016, NIST's cloud computing security and forensic science activities included the development of the following guidance and/or recommendations:

- **NIST Draft SP 800-173,** *Guide for Applying the Risk Management Framework to Cloud-based Federal Information Systems*. This publication provides guidance in using 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*, to issue an authorization to operate for cloud-based information systems. The draft document will be posted for public comment by December 31, 2016.
- **NIST Draft SP 800-174,** *Security and Privacy Controls for Cloud-based Federal Information Systems.* This document, which is anticipated to be available for public comments by the end of the first quarter of 2017, provides a cloud overlay of the SP 80053 Revision 4 security controls for cloud-based ecosystems.

NIST is also leading the research and development of the projects listed below:

- Members of the NIST Cloud Security Working Group, in collaboration with the Cloud Security Alliance's members are researching the security challenges encountered when leveraging application containers and microservices for the implementation of cloud-based information systems. Based on this research, NIST will issue an interagency report documenting the findings and will provide recommendations based on best practices for mitigating the identified challenges.
- Members of the NIST Cloud Security Working Group are researching the security challenges encountered when implementing cloud-based federated identity solutions and the impact on the overall system's security posture. Based on this research, NIST will issue an interagency report documenting the findings and will provide recommendations based on the best practices for mitigating the identified challenges.
- Members of the NIST Cloud Forensic Science Working Group are working on defining a cloud forensics reference architecture that leverages NIST SP 500-299: *Cloud Security Reference Architecture* and NISTIR 8006, *NIST Cloud Computing Forensic Science Challenges*.
- Members of a NIST-led Tiger Team is developing an OSCAL, a hierarchical, formal language that aims to support the transfer of security information in formats that are compliant with the security controls catalog of choice.

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

CSD staff co-chaired several significant cloud computing efforts in 2016:

- Co-Chaired the NIST Cloud Computing Security Working Group and led the working group on the development of the NIST SP 800-173, *Guide for Applying the Risk Management Framework to Cloud-based Federal Information Systems;* NIST SP 800-174, *Security and Privacy Controls for Cloud-based Federal Information Systems* (both described above); and on researching the topics listed above.

- Co-Chaired the NIST Cloud Computing Forensic Science Working Group and led the development of *the cloud forensics reference architecture.*
- Co-Chaired the NIST Cloud Computing Interoperability and Portability Working Group and addressed issues facing cloud computing with respect to interoperability and portability, standards, and common and functional terminologies.

CSD staff members participated in various standards development organizations, all listed in the section of this report dedicated to international standards.

In FY 2017, NIST will continue collaboration with the private sector, academia and other public-sector entities on developing guidance and specifications that support the broad adoption of innovative cloud solutions. Some of the very effective frameworks for such collaborations that NIST is hosting are the public working groups with international participation.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

CONTACT:

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

Policy Machine – Next Generation Access Control

CSD has continued the development of an advanced Attribute Based Access Control (ABAC) framework called the Policy Machine, which is designed to be in alignment with an emerging ANSI/INCITS standard under the title of “Next Generation Access Control” (NGAC).

The Policy Machine (PM) is a fundamental reworking of traditional access control into a form suited to the needs of a modern, distributed, interconnected enterprise. The PM is based on a flexible infrastructure that can provide access control services for several different types of resources that are accessed by different types of applications and users. The PM infrastructure is scalable and can support policies of various types simultaneously while remaining manageable in the face of changing technology, organizational restructuring, and increasing amounts of data. The PM provides a framework capable of supporting combinations of both current access control approaches and newly conceived types of policy without extension.

NIST and other members of an Ad Hoc INCITS working group are continuing to develop a three-part NGAC standard. This work is being conducted 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 and Abstract Data Structures.

An initial standard from this work was published in 2013 and is now available from ANSI as *INCITS 499: NGAC Functional Architecture (NGAC–FA)*. However, based on experience with similar efforts (e.g., Project 2193-D, Project 2195-D, and the revised NISTIR 7987, *Policy Machine: Features, Architecture, and Specification*), work is underway to update this standard.

In 2016, the standard for Project 2195-D was approved and is now available from the ANSI e-standards store as INCITS 526: NGAC Generic Operations and Abstract Data Structures (NGAC-GOADS).

The eXtensible Access Control Markup Language (XACML) and NGAC are very different ABAC standards with similar goals and objectives. What are the similarities and differences between these two standards? What are their comparative advantages and disadvantages? To answer these questions, in October 2016 NIST published SP 800-178, *A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)*, to describe and compare these standards with respect to the criteria derived from ABAC issues or considerations identified by NIST SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*: operational efficiency, attribute and policy management, scope and type of policy support, and support for administrative review and resource discovery.

In FY 2017, CSD plans to issue a new version of the PM through GitHub as an open source distribution to allow widespread experimentation and transfer. Example data services (e.g., email, file management, records management, workflow) are planned to be provided with the distribution. The new version will reflect new features and enhanced performance, and will complete (for purposes of balloting) the revised INCITS 499, and the Project 2193–D standard.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

Mr. David Ferraiolo	Mr. Serban Gavrila
(301) 975-3046	(301) 975-4242
david.ferraiolo@nist.gov	serban.gavrila@nist.gov

Security for a Virtualized Infrastructure

Virtualization technology has now found ubiquitous adoption in data centers used for hosting enterprise applications as well as for providing cloud services. This technology has been used not only for configuring and deploying virtualized hosts (Server Virtualization) but also for virtual networks (Network Virtualization) and virtualized storage (Storage Virtualization). Together, these three components constitute the virtualized infrastructure in a data center.

The core component of a virtualized infrastructure is the virtualized host (i.e., a physical host running a server virtualization product) that can support multiple computing stacks (called Virtual Machines or VMs), each with a different platform configuration (e.g., operating system (OS)) and each with unique security needs. Application programs loaded into a VM are often valuable server programs (e.g., webserver, database management system) that support important business processes and generally need more security protection than do other virtual hosts such as workstations. Protection for application programs in a VM (in fact for the entire VM) can be provided through a combination of the following: the secure configuration of the virtualized host, the secure configuration of the virtual network and the secure configuration of the virtualized storage associated with the VM.

Just like their physical counterparts (i.e., physical servers), VMs can be protected through host-level and network-level security measures. Hence, the focus of research in FY 2014 and prior years was on the secure configuration of the virtualized hosts (specifically Hypervisor configuration and deployment). Recognizing the fact that VMs are the end-nodes of a virtual network, research on the secure virtual network configuration for VM protection was started in FY 2015 and continued in FY 2016. The outcome of the research was the identification of four virtual network configuration areas impacting VM security: network segmentation, network path redundancy, traffic control using firewalls, and VM traffic monitoring. Each area was analyzed, and the corresponding security recommendations have been provided.

In FY 2016, the project team produced the following two publications: *Analysis of Virtual Networking Options for Securing Virtual Machines* which was submitted to the *Seventh International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2016)* (Note: The abstract to this paper can be found in the Publications Released FY 2016 – Conference Papers section later in this Annual Report), and SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*.

In FY 2017, research on the secure configuration of the third component of a virtualized infrastructure (i.e., virtualized storage) will continue. The resulting findings and security recommendations will either be included as additions to SP 800-125A, *Security Recommendations for Hypervisor Deployment,* or as a separate document.

CONTACT:

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

Cyber Threat Information Sharing

As cyber attacks increase in both sophistication and frequency, it is important to collect and analyze cyber threat information from a variety of internal and external sources, and use it to develop, enhance, and deploy proactive, threat-informed, cyber defense capabilities. Cyber threat information includes indicators (i.e., artifacts or observable events that suggest that an attack is imminent, that an attack is underway, or that a compromise may have already occurred); information about the tactics, techniques, and procedures (TTPs) of actors; recommended courses of action; and other information that is used to characterize threats. Because threat actors often use the same TTPs against multiple targets, exchanging cyber threat information allows organizations to leverage the collective knowledge, experience, and analysis capabilities of their peers, thereby increasing the overall awareness and security of an entire sharing community. Through the exchange of cyber threat information, organizations can gain a more complete understanding of their threat environment by correlating their observations with those of others.

CSD has established a cyber threat information sharing initiative, which is focused on providing guidance on how an organization can establish information sharing and coordination capabilities that enhance or augment their existing cybersecurity practices. The guidance covers threat-informed detection, protection and response capabilities; data privacy and sensitivity; data collection and retention practices; the use of open standards for information exchange; de-identification and anonymization; and guidance on how an organization can establish, participate in, and maintain coordination and information sharing relationships. The guidance will help incident responders, network defenders, and operations personnel consider what information is sharable, the circumstances under which sharing is permitted, with whom the information may be shared, and how the information should be protected.

As an example of this guidance, in FY 2016, CSD released a second draft of SP 800-150, *Guide to Cyber Threat Information Sharing*. The draft publication was released for public comment on April 21, 2016. This publication is intended to help organizations prepare for an exchange of cyber threat information, both consuming cyber threat information from external sources and producing information for other organizations to use. Organizations may have substantially different capabilities for detecting threats, responding to attacks, diagnosing causes, and handling sensitive incident-related information, but this guidance is intended to help organizations collaborate and exchange cyber threat information despite these organizational differences. CSD will release the final version of SP 800-150, in October 2016.

In FY 2017, CSD plans to continue to conduct research, prepare guidance, and participate in standards development activities that are focused on increased interoperability and operational tempo through near real-time cyber threat information sharing, including:

- Expressing cyber threat information using machine-readable formats,
- Developing automated mechanisms for exchanging cyber threat information,
- Describing automated courses of action,
- Publishing cyber threat information metadata, and
- Safeguarding cyber threat information.

NIST will also help foster cyber threat information sharing by supporting information sharing initiatives by public and private sector organizations, including:

- Information Sharing and Analysis Centers (ISACs),
- Information Sharing and Analysis Organizations (ISAOs),
- Federal/State/Local agencies,
- Law Enforcement,
- Fusion Centers, and
- Sector Coordinating Councils.

CONTACTS:

Mr. Christopher Johnson
(301) 975-3247
christopher.johnson@nist.gov

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

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

The Ontology of Authentication

Over the past 30 years, NIST has been at the forefront of recommending best practices for authentication. Recommendations have included the usage of passwords, biometrics, authentication hardware devices, and Public Key Infrastructure (PKI) solutions in enterprise settings. In FY 2015, CSD began researching the classification of general authentication features. This investigation was prompted by the general call to move away from passwords toward the growing number of alternative authentication methods (e.g., biometrics, smart cards, etc.). A notional ontology of authentication was developed that included a detailed taxonomy, a metrology, and a framework for assessing alternatives.

Research over the past year led to updates to the authentication taxonomy (see Figure 28) to encapsulate current and emerging mechanisms and was the basis for *Expanding Continuous Authentication with Mobile Devices*, which was published in the IEEE Computer magazine. The taxonomy now covers a wide assortment of commonly used human-machine, machine-machine, human-human, and attribute attestation methods. Human-human authentication was included due to the number of systems that use human interaction as a backup system when a user has trouble with a man-machine interface. In addition, the research uncovered an emerging branch of authentication –continuous authentication – that supports user monitoring as a part of the authentication.

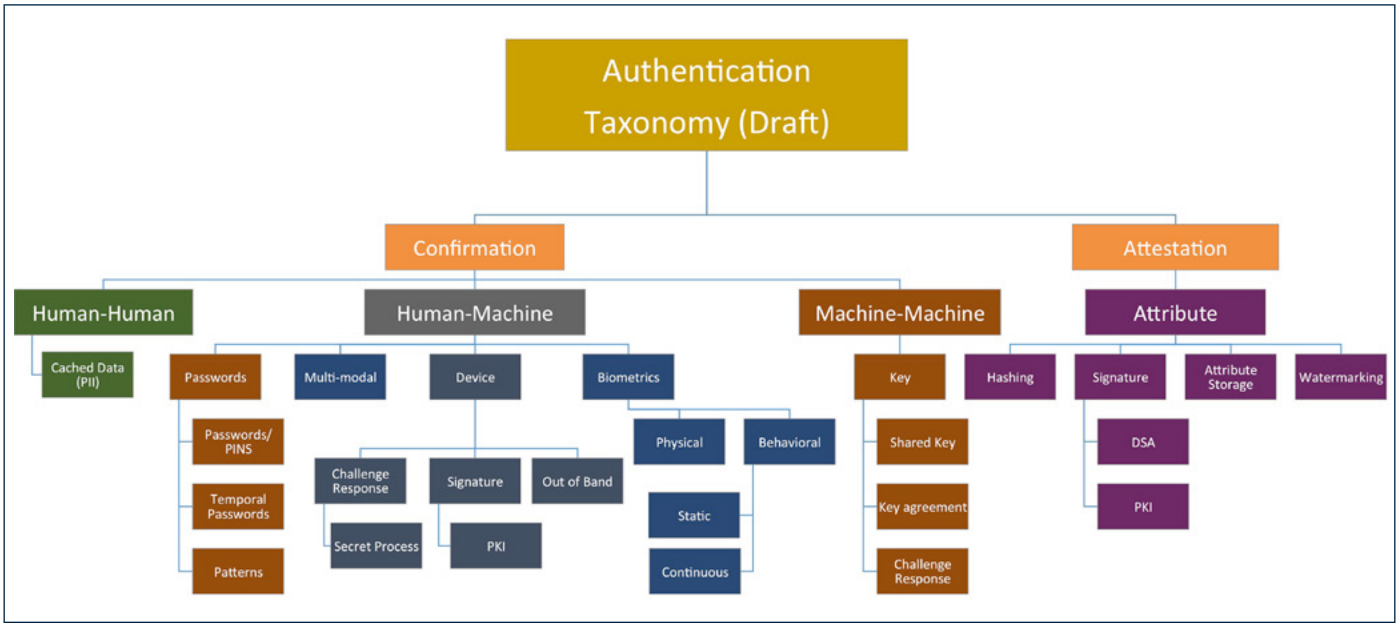


Figure 28: Draft Authentication Taxonomy

The notional authentication ontology attempts to define a metrology framework that is useful for better understanding, comparing, and measuring the appropriateness of authentication technologies to a specific use-case. The measurement framework separates metrics into security, usability, deployability, and manageability categories (see Figure 29). It is important to note that each category may overlap or impact the others. Security and usability are of special interest; while usability is often thought of as a tradeoff to security, both must be satisfied for the user to support the security of the system.

Security
Deployability
Usability
Manageability

Figure 29: Suitability Framework for Authentication

The security category is broken down into the following foundational areas:

- Uniqueness of the relationship to the entity,
- Protection and resilience of a token against compromise,
- Protection of a token during delivery,
- Protection of metadata in storage, and
- Protection / resilience of storage backup.

The usability category follows the ISO 9241-11 (1988) areas of:

- Effectiveness,
- Efficiency, and
- Satisfaction.

Specific methods of calculating measurements in these categories are not currently included and may be unique to each authentication mechanism and environment. The framework supports integration with the programmatic categories of deployability and manageability, but measurement areas in these categories are not currently defined, as they are often well specified within organizations.

Future programmatic efforts will be focused toward a NISTIR to describe the research results, encourage further discussion with the community, and provide recommendations for future standards development efforts, with the goal of moving toward specifying independently measurable strength requirements rather than specific implementation requirements.

The program status was presented and well received at the 2016 World eID and Cybersecurity Conference. As this program is to eventually define the future development of standards, concerns as to the immediate adoptability were received and will inform future research. Additional work to identify interdependencies, such as with identity management and authorization controls and requirements, should help allay these concerns.

In addition, NIST CSD will work with the community in FY 2017 to identify and address common areas of authentication requirements to create a framework for researching and developing authentication mechanisms using this ontology. If a clear metrology can be established, future access control process implementations should be less susceptible to vulnerabilities specific to individual implementations.

CONTACT:

Dr. Kim Schaffer
(301) 975-8375
kim.schaffer@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address the private sector's most pressing cybersecurity issues. As a public-private partnership, industry experts and technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—choose to work with the NCCoE to develop practical, example cybersecurity solutions using standards, best practices, and commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps technical capabilities to the NIST Cybersecurity Framework and details the steps needed to recreate the example solution in the real world. The NCCoE aims to provide practical cybersecurity solutions that are cost-effective, repeatable, and scalable to increase the rate of adoption and accelerate effective innovation across business sectors.

Below is a list of NCCoE's highlights and accomplishments for FY 2016:

Publications

- **Draft Special Publication (SP) 1800-4, *Mobile Device Security: Cloud & Hybrid Builds Practice Guide*:** demonstrated how commercially available technologies can meet an organization's needs to secure sensitive enterprise data accessed by and/or stored on employees' mobile devices. The guide describes approaches for securing mobile devices in both a cloud-based architecture and also an architecture using a hybrid of cloud and enterprise architecture (see https://nccoe.nist.gov/projects/building_blocks/mobile_device_security).
- **Draft SP 1800-5, *Financial Services IT Asset Management Practice Guide*:** demonstrated how an organization can, in an automated fashion, gain customized insight into 1) what is on its network, 2) the status of each hardware and software component in its environment, and 3) how to prioritize resources to address vulnerabilities. This kind of understanding and insight can help increase a financial organization's cybersecurity resilience by enhancing the visibility of assets, revealing which applications are actually being used, identifying vulnerable assets, enabling faster response to security alerts, and reducing help-desk response times (see https://nccoe.nist.gov/projects/use_cases/financial_services_sector/it_asset_management
- ***Wireless Medical Infusion Pumps* Final Project Description:** examined the security of wireless medical devices on an enterprise network using infusion pumps as a use case (see https://nccoe.nist.gov/projects/use_cases/medical_devices).
- ***Domain Name System-Based Security for Electronic Mail* Final Project Description:** explored a security platform that provides trustworthy email exchanges across organizational boundaries to help businesses improve the privacy and security protections of their employees' operations (see https://nccoe.nist.gov/projects/building_blocks/secured_email).
- ***Data Integrity: Recovering from a Destructive Malware Attack* Final Project Description:** explored methods to effectively recover operating systems, databases, user files, applications, and software/system configurations. It will also explore

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

issues of auditing and reporting (user activity monitoring, file system monitoring, database monitoring, scanning backups/snapshots for malware, and rapid recovery solutions) to support recovery and investigations (see https://nccoe.nist.gov/projects/building_blocks/data_integrity).

- ***Privacy-Enhanced Identity Federation* Project Description Draft:** examined how privacy-enhancing technologies that leverage market-dominant standards can be integrated into identity broker solutions to meet the privacy objectives of users and organizations (see https://nccoe.nist.gov/projects/building_blocks/privacy-enhanced-identity-brokers).
- ***Multi-factor Authentication for e-Commerce* Draft Project Description:** examined how multi-factor authentication for e-commerce transactions that are tied to existing web analytics and contextual risk calculation can increase assurance in purchaser or user identity and thus help reduce the risk of online identification and authentication fraud (see https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce).
- ***Securing Non-Credit Card, Sensitive Data* Draft Project Description:** explored the implementation of data masking and tokenization, coupled with fine-grained access control such as Attribute Based Access Control, which may significantly improve the security of personally identifiable information (PII) transmitted and stored during commercial payment transactions, as well as PII shared internally within a retail organization and externally with business partners (see https://nccoe.nist.gov/projects/use_cases/securing-sensitive-consumer-data).
- ***Mobile Application Single Sign-On* Draft Project Description:** explored the use of multi-factor authentication and mobile single sign-on for native and web applications to improve interoperability between mobile platforms, applications, and identity providers, irrespective of the application development platform used in their construction (see https://nccoe.nist.gov/projects/use_cases/mobile-sso).
- ***Authentication for Law Enforcement Vehicle Systems* Draft Project Description:** explored implementing an integrated set of authentication mechanisms, improving system security, usability, and safety (see https://nccoe.nist.gov/projects/use_cases/authentication-law-enforcement-vehicle-systems).
- ***Identity and Access Management for Smart Home Devices* Concept Paper:** outlined potential project topics for exploration, including identification, authentication, and authorization for Internet of Things devices, specifically within the smart home (see https://nccoe.nist.gov/projects/project-concepts/idam-smart-home-devices).

Events

NCCoE hosted several events to support project development and receive feedback on proposed example solutions. Highlights include:

- **NCCoE Building Dedication,** February 8, 2016, Rockville, MD: NCCoE hosted a ribbon cutting and building dedication ceremony for its new facility in Rockville. (see https://nccoe.nist.gov/news/nist-and-nccoe-celebrate-move-expanded-cybersecurity-facility).
- **Protecting Consumer Data: Securing Payment and Transaction Information Workshop,** March 22, 2016, University of Alabama Birmingham: The NCCoE hosted a full-day workshop with retail industry members and technology vendors to explore consumer-facing retail cybersecurity issues in depth. The participants recognized that cybersecurity incidents affecting consumer-facing businesses threaten the financial security of companies and the public, weakening consumer confidence, eroding individual privacy protections, and damaging the brand value and reputation of businesses. Topics included methods to combat online fraud (e.g., through multi-factor authentication for e-commerce transactions) and to safeguard customer profiles (e.g., through secure handling of sensitive, non-credit card consumer data). (See https://nccoe.nist.gov/events/consumer-facing-retail-sector-workshop.)
- **Pre-Workshop: Maritime and Oil & Natural Gas,** April 5, 2016, Rockville, MD: In coordination with the NIST Cybersecurity Framework Workshop, the NCCoE facilitated an open session with members of the maritime and oil and natural gas industries to identify and prioritize hard cybersecurity challenges that can be addressed jointly (see https://nccoe.nist.gov/events/pre-workshop-maritime-and-oil-and-natural-gas-open-session).

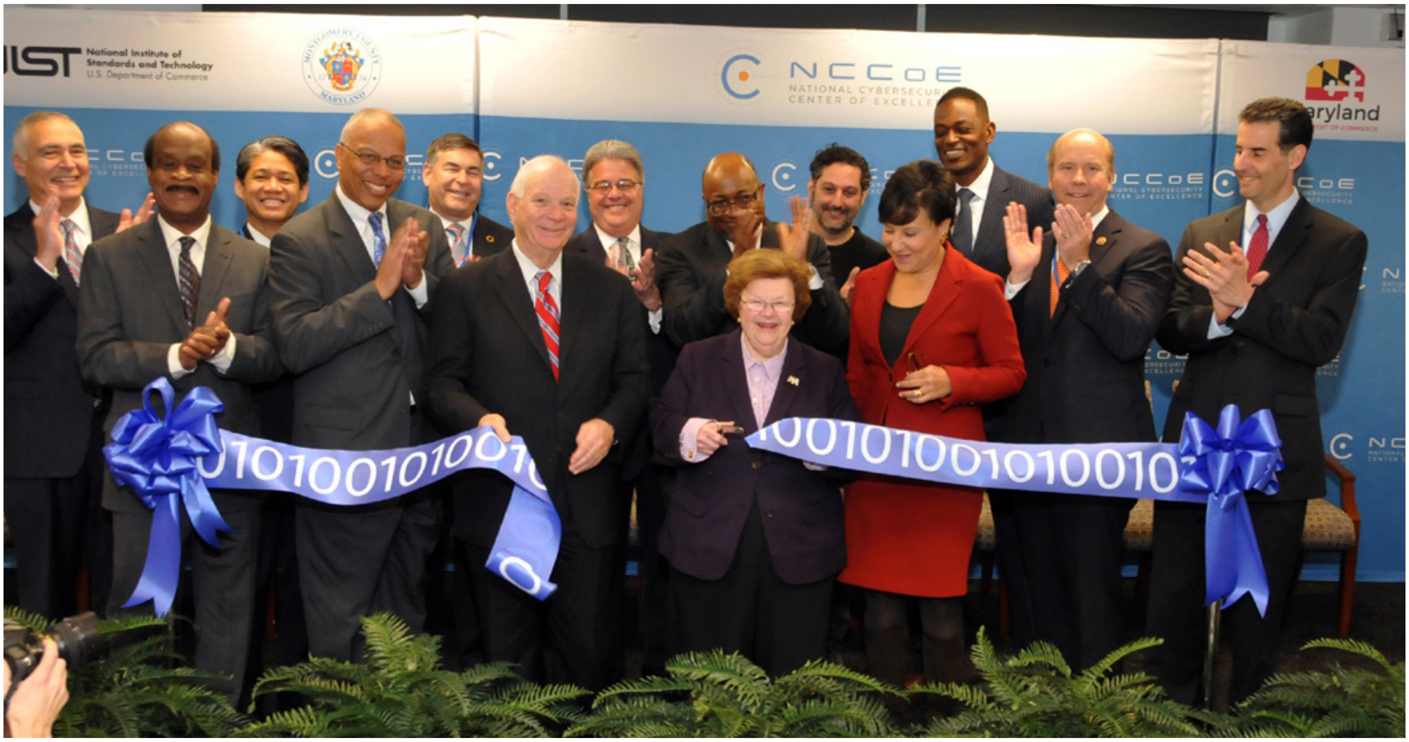


Figure 30: NCCoE Building Dedication

FRONT ROW (from left to right): Ike Leggett, Montgomery County Executive; Maryland Lt Governor Boyd Rutherford; Senator Ben Cardin; Senator Barbara Mikulski; Commerce Secretary Penny Pritzker; Rep. John Delaney; and Rep. John Sarbanes.

BACK ROW (from left to right): Al Grasso, President and Chief Executive Officer, MITRE; Gil Quiniones, President and Chief Executive Officer, New York Power Authority; Michael Brown, President and Chief Executive Officer, Symantec; Robert Caret, University System of Maryland Chancellor; Willie E. May, Director, NIST and Under Secretary of Commerce for Standards and Technology; Amit Yoran, RSA President; and Dean Garfield, President and Chief Executive Officer, Information Technology Industry Council. Photo credit: Joseph Andrucyk/State of Maryland Office of the Governor.

NCCoE staff were invited to speak at more than 30 industry events and conferences. Highlights include:

- **RSA Conference,** February 29-March 4, 2016, San Francisco: Nate Lesser, NCCoE Deputy Director, delivered a keynote address at the State of Maryland-hosted luncheon and presented a session on the NCCoE Wireless Infusion Pumps project (see https://nccoe.nist.gov/events/rsa-conference-2016).
- **Healthcare Information and Management Systems Society (HIMSS) Conference,** February 29-March 4, 2016, Las Vegas: NCCoE engineers demonstrated the Wireless Infusion Pumps and Securing Electronic Health Records on Mobile Devices projects (see https://nccoe.nist.gov/events/himms-conference-and-exhibition).
- **Christian Science Monitor's Passcode Conversation,** October 8, 2015, Washington, D.C.: Government leaders discussed ongoing cybersecurity challenges, such as how to adopt a proactive approach to effectively defend tomorrow's networks and how to disrupt attacks upon organizational systems. Nate Lesser, NCCoE Deputy Director, participated in the Keynote Panel Discussion and described the center's work in collaborating and coordinating between public and private sector.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

Figure 31: Gavin O'Brien (NCCoE, NIST) provided a demonstration on securing electronic health records on mobile devices.

In FY 2017, the NCCoE plans to release six SP-1800 practice guides:

- Domain Name System-Based Secured Email,
- Situational Awareness: Secured Networking Infrastructure for the Energy Sector,
- Wireless Medical Infusion Pumps,
- Derived Personal Identity Verification Credentials,
- Data Integrity: Recovering from a Destructive Malware Attack, and
- Mobile Application Single Sign-On.

In addition to the release of these practice guides, NCCoE plans to attend both national and international cybersecurity conferences to present NCCoE projects and participate in panels to help increase the rate of adoption and accelerate innovation. The NCCoE has already been selected to speak at the 2017 HIMSS conference.

FOR MORE INFORMATION, SEE:

https://nccoe.nist.gov/

CONTACT:

Mr. Timothy McBride
(301) 975-0214
timothy.mcbride@nist.gov

INTERNET INFRASTRUCTURE PROTECTION

ITL's Internet Infrastructure Protection (IIP) program, led by the Advanced Network Technologies Division (ANTD), works with industry to develop the measurement science and new standards necessary to ensure the robustness, scalability, and security of the global Internet. The research focuses on the measurement and modeling techniques necessary to understand, predict, and control the behavior of Internet-scale networked information systems. The ITL staff use these insights to guide the design, analysis, and standardization of new technologies aimed at improving the robustness of the Internet's core infrastructure. Recent efforts have focused on enhancing the security of the Internet's Domain Name System (DNS), the Border Gateway Protocol (BGP), and Electronic mail (Email) and messaging infrastructures. In addition, the IIP program addresses other systemic vulnerabilities in core Internet technologies, such as those that enable massive-scale Distributed Denial of Service (DDoS) attacks.

In FY 2016, ITL staff made significant contributions to the design, standardization, test and measurement of technologies to improve the security and robustness of the Internet's global routing protocol BGP. NIST staff were key contributors to Internet Engineering Task Force (IETF) standards to add cryptographic validation to BGP (see, https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol/), and to address the robustness issues associated with large-scale routing policy violations (see, https://www.rfc-editor.org/rfc/rfc7908.txt). In addition, NIST developed and released open-source reference implementations of these emerging IETF specifications, online test tools to foster their adoption and measurement systems to track their operational deployment. Figure 32 below is a visualization generated by one such monitoring tool of the emerging global structure of the Resource Public Key Infrastructure (RPKI). The RPKI has been designed to provide the trust infrastructure upon which Internet routing security technologies can be based.

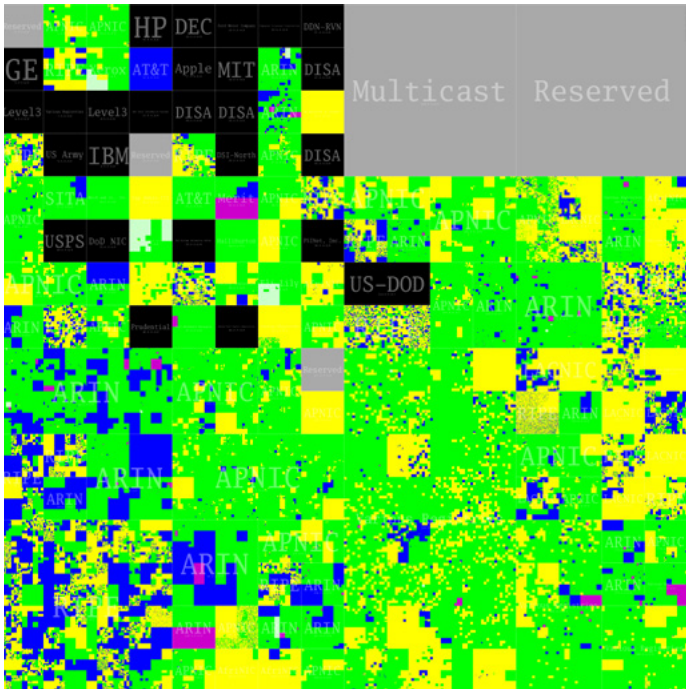
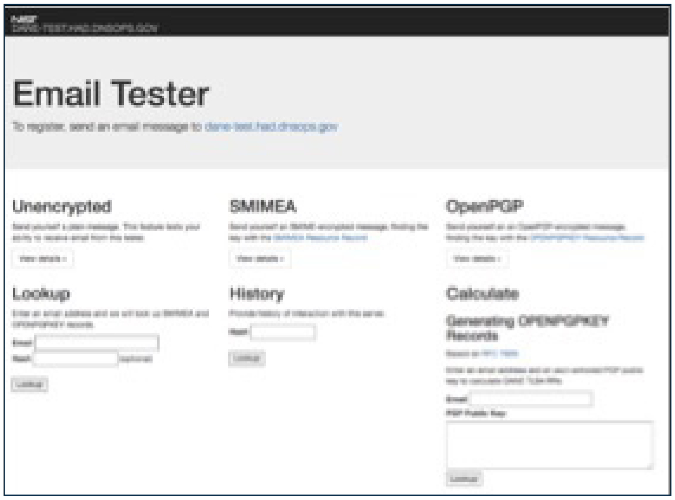


Figure 32: NIST Visualization of the Evolving Coverage and Depth of the Internet's Global Resource Public Key Infrastructure for BGP security.

In FY 2016, as technology specifications and implementations matured, the ITL staff began a series of outreach efforts with the networking industry to increase the understanding and foster the adoption of BGP security mechanisms. The ITL staff organized and led a workshop at the June North American Network Operators Group (NANOG) meeting aimed at addressing the practical issues, state of vendor support and existing operational experience with emerging BGP security technologies (see, https://www.nanog.org/meetings/abstract?id=2846). The ITL staff also initiated a nationwide BGP security pilot deployment project with the Internet2 research and education community.

ITL's High Assurance Domains (HAD) project aims to leverage NIST's previous successes in the development and deployment of Domain Name System Security Extentions (DNSSEC) technologies to enable scalable solutions of long standing Internet security issues. In FY 2016, the project focused on addressing the issues of Email phishing attacks and developing scalable techniques to enable the cryptographic protection of Email message exchanges. NIST published NIST SP 800-177, *Trustworthy Email*, a comprehensive guidance on the deployment and use of emerging DNS-based authentication mechanisms to combat email phishing and spam. In addition, ITL developed and deployed online test tools to assist network operators in the configuration and verification of their deployment of emerging anti-phishing technologies.

The second focus area for the HAD project in FY 2016 was the advancement of specifications, implementations and deployment of IETF DNS-based Authentication of Named Entities (DANE) technology that leverages a secured DNS as a ubiquitous key discovery and management infrastructure. In FY 2016, the ITL staff contributed to the development of IETF DANE specifications and developed distributed test and measurement tools to assist in their adoption and use in the global Internet. Figure 33 (See next page) shows the user interface to the recently released NIST DANE test system that enables product developers and network operators to test their use of the DANE technologies to store, retrieve and validate various types of cryptographic keying material for end-to-end email security, and for general transport-layer security (TLS) for web and other applications.



NIST
DANE-TEST.HAD.DNSOPS.GOV

Email Tester

To register, send an email message to dane-test.had.dnsops.gov

Unencrypted

Send yourself a plain message. This feature tests your ability to receive email from the tester.

View details »

SMIMEA

Send yourself an SMIME encrypted message, finding the key with the SMIMEA Resource Record

View details »

OpenPGP

Send yourself an an OpenPGP encrypted message, finding the key with the OPENPGPKEY Resource Record

View details »

Lookup

Enter an email address and we will look up SMIMEA and OPENPGPKEY records.

Email:

Nasl: (optional)

Lookup

History

Provide history of interaction with the server.

Nasl:

Lookup

Calculate

Generating OPENPGPKEY Records

Based on RFC 7929

Enter an email address and an ascii-armored PGP public key to calculate DANE TLSA RRs

Email:

PGP Public Key:

Lookup

Figure 33: NIST DANE Test system for Secure Email

The HAD project staff also collaborated with the NCCoE DNS-Based Secured Email project that tested and produced detailed deployment guidance for commercial implementations of DANE-based server-to-server security for email transport (see https://nccoe.nist.gov/projects/building_blocks/secured_email).

The ITL staff in the Advanced Distributed Denial of Service (DDoS) Mitigation Techniques project are working with the community to document and quantitatively characterize the applicability, effectiveness and impact of various approaches to filtering spoofed Internet Protocol (IP) traffic streams and develop consensus recommendations and deployment guidance that can drive their adoption in Federal network environments and throughout the Internet industry. In FY 2016, the NIST staff developed benchmarking methodologies to characterize the performance implications of various techniques to block spoofed IP packets in commercial routers and developed draft deployment guidance for these mechanisms in a variety of network interconnection scenarios.

Advanced DDoS Mitigation Techniques
Distributed Denial of Service (DDoS)

In addition to understanding the barriers to deployment and adoption of existing DDoS mitigation techniques, the ITL staff began the research and evaluation of new, scalable means of DDoS detection and mitigation, based upon Software Defined Networking (SDN) technologies.

In FY 2017, the major milestones for Internet Infrastructure Program will include:

- Completing the publication of IETF standards for BGP security and increasing outreach and pilot deployment activities to foster commercial deployment of these technologies;
- Continuing to develop and mature DANE specifications and technologies for scalable key management in the Internet and conducting research on their applicability to emerging problem domains, such as authentication in consumer networks; and
- Publishing NIST guidance on current DDoS mitigation techniques and continuing to research and develop new approaches based upon emerging SDN technologies.

FOR MORE INFORMATION, SEE:

Robust Inter-Domain Routing Project:
https://www.nist.gov/programs-projects/robust-inter-domain-routing

NIST RPKI Deployment Monitor and Test System:
https://www.nist.gov/services-resources/software/nist-rpki-deployment-monitor-and-test-system

BGP Secure Routing Extension (BGP–SRx) Prototype:
https://www.nist.gov/services-resources/software/bgp-secure-routing-extension-bgp-srx-prototype

BRITE - BGPSEC / RPKI Interoperability Test & Evaluation System:
https://www.nist.gov/services-resources/software/brite-bgpsec-rpki-interoperability-test-evaluation-system

High Assurance Domains Project:
https://www.nist.gov/programs-projects/high-assurance-domains

NIST SP 800-177 Trustworthy Email:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177.pdf

NIST DANE Test System:
https://dane-test.had.dnsops.gov/

Advanced DDoS Mitigation Techniques Project:
https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques

Software Defined Virtual Networks Project:
https://www.nist.gov/programs-projects/software-defined-virtual-networks

CONTACT:

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

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 under constant threat of attack and are frequently undergoing change, with new and updated software being deployed along with updated configurations. The wide variety of computing products, the dynamic nature of software, 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 informed 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, including hardware, software, and data;
- 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 the 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 for product developers and implementers. Through close work with partners in government, industry, and academia, CSD continues to facilitate the definition and development of security automation approaches that enable organizations to understand and manage IT security risks.

During FY 2016, CSD has continued to work to build on previous security automation work, as follows:

- Identified and addressed gaps in the current specifications;
- Evolved existing approaches to achieve greater scalability and impact;
- Participated in working groups in standards development organizations to promote international consensus around standardized approaches;
- Provided additional guidance on architectural, design, and analysis concerns; and
- Developed and maintained tools and reference implementations.

CSD is currently working with its partners in various standards-development organizations, including ISO, IETF, Organization for the Advancement of Structured Information Standards (OASIS), 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

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

operational and security data sources and the collective action of security components.

Additionally, CSD is working with the vulnerability community to enable the automated analysis of metrics such as the Common Vulnerability Scoring System (CVSS), establishing a baseline of the minimum information needed to properly inform the vulnerability management process, and facilitating the sharing of vulnerability information across language barriers. To assist in this work, a public draft of NISTIR 8138, *Vulnerability Description Ontology (VDO): A Framework for Characterizing Vulnerabilities,* was created to foster a conversation and collect feedback on the best mechanisms to improve the degree of automation within vulnerability management processes. CSD is planning to develop this document iteratively with the vulnerability community to ensure participation from as many stakeholders as possible.

Security automation standardization work has been focused in three areas: the evolution and international adoption of the Security Content Automation Protocol (SCAP), the development of software asset management standards to support operational and cybersecurity use cases, and the development of security automation consensus standards. 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 the 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 2 (below): SCAP 1.2 Specifications for details.

Since the release of SCAP 1.2, CSD has worked to improve guidance around the use of SCAP specifications. In FY 2015, CSD released draft NISTIR 8058, *Security Content Automation Protocol (SCAP) Version 1.2 Content Style Guide: Best Practices for Creating and Maintaining SCAP 1.2 Content,* which provides guidance for SCAP 1.2 content creators to ensure that stylistic variations in SCAP 1.2 content are addressed in a way that improves the accuracy and consistency of results, avoids performance problems, reduces user effort, lowers content maintenance burdens, and enables content reuse. To achieve this, the report documents best practices for content creation and encourages their use by SCAP content authors and maintainers. Feedback on this report is welcomed and will help CSD to work toward producing a final version of this document.

CSD is actively working on an SCAP 1.3 revision. In July 2016, CSD posted drafts for public comment of SP 800-126 Revision 3 and SP 800-126A. SP 800-126 Revision 3, is *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3*. SP 800-126A is *SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3*. These publications collectively document the draft requirements for SCAP 1.3. SP 800-126A is a new publication that allows SCAP 1.3 to take advantage of selected minor version updates of SCAP component specifications, as well as designated Open Vulnerability and Assessment Language (OVAL) platform schema revisions. The SCAP 1.3 revision includes the following changes:

- Adoption of the Open Vulnerability and Assessment Language (OVAL) 5.11.1, which was released in April 2015;
- Adoption of the Common Vulnerability Scoring System (CVSS) v3, which was released in June 2015;
- Removal of support for CVSSv2; and
- Deprecation of support for older specification revisions and SCAP 1.0.

TABLE 2: SCAP 1.2 SPECIFICATIONS

SPECIFICATIONS	DESCRIPTION
Languages	
Extensible Configuration Checklist Description Format (XCCDF) 1.2	Used for authoring security checklists/benchmarks and for reporting the results of evaluating them
Open Vulnerability and Assessment Language (OVAL) 5.11.1	Used for representing system-configuration information, assessing machine state, and reporting assessment results
Open Checklist Interactive Language (OCIL) 2.0	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) 1.1	Used to express information about assets and to define the relationships between assets and reports
Asset Identification 1.1	Used to uniquely identify assets based on known identifiers and other asset information
Identification Schemes	
Common Platform Enumeration (CPE) 2.3	A nomenclature and dictionary of hardware, operating systems, and applications; a method to identify the applicability to platforms
Software Identification (SWID) Tags 2015	A structured metadata format for describing a released software product
Common Configuration Enumeration (CCE) 5	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

CSD is currently considering the public feedback received on the drafts while preparing the final versions of these publications for release in early FY 2017. CSD is also working on an updated version of SCAPVal, the SCAP content validation tool. Once the specification revision is complete, CSD will also work to update the SCAP Validation Program to support SCAP 1.3. More information on SCAP 1.3 can be found at: https://scap.nist.gov/revision/1.3/.

CSD is also starting to plan a SCAP 2.0 release. This release will further define the interfaces and use of transport protocols for SCAP tools to provide component-level interoperability between products supporting various SCAP functions. By providing more interoperability, SCAP v2 will provide the basic software and configuration posture information needed to make and automate management decisions for networked devices as part of the license, vulnerability and

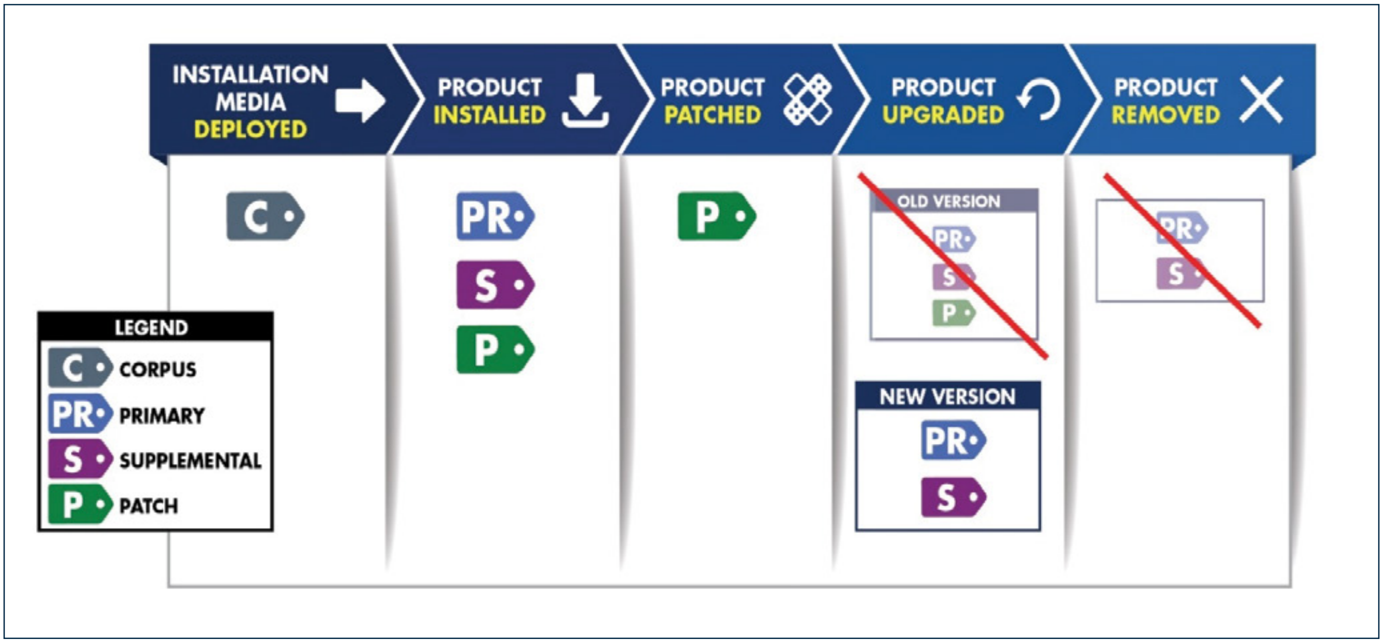


Figure 34: SWID Tags Support the Software Product Lifecycle

configuration management practices, supporting improved networked device hygiene. Furthermore, the posture information provided by SCAP v2 products will provide much of the context needed to prevent, detect, and respond to network attacks. This additional context will enable SCAP v2 information to be applied for application whitelisting, the detection of anomalous behavior, the gathering and use of indicators, the use of machine-readable threat information, and orchestrating courses of action. CSD is preparing a draft whitepaper for release in early FY 2017 that will outline an approach, a development plan identifying the new and revised specifications that will be needed, and a transition plan for moving from SCAP 1.x to SCAP 2.0.

Software Asset Management Standards

CSD has been collaborating with industry partners in support of ISO/IEC's revision of standard ISO/IEC 19770-2:2009, *Information technology—Software asset management—Part 2: Software identification tag*, which establishes a specification for tagging software to support identification and management. An updated revision of this standard, ISO/IEC 19770-2:2015, was published on October 1, 2015. The software identification (SWID) data model defined by this standard describes an XML format for software publishers to provide authoritative identification, categorization, software relationships (e.g., dependency, bundling, and patch), executable and library footprint details, and other metadata for software. This information can be used to support operational and cybersecurity use cases around managing software deployments, managing software licenses, managing software vulnerabilities and related software patches, and assessing secure software configurations.

To supplement the requirements in ISO/IEC 19770-2:2015, CSD collaborated with DHS, NSA, and MITRE on the development of NISTIR 8060, *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*. NISTIR 8060, published in April 2016, provides an overview of the capabilities and usage of SWID tags as part of a comprehensive software lifecycle. This report introduces SWID tags in an operational context, provides guidelines for the creation of interoperable SWID tags, and highlights key usage scenarios for which SWID tags are applicable. Figure 34 illustrates several types of SWID tags and how these support multiple elements of the software product life cycle, including deployment, installation, patching, upgrading and removal.

Additionally, NIST has worked with the TCG to integrate SWID tags into the Trusted Network Communications (TNC) protocol, through the *SCAP Messages for IF-M* specification.

The information provided within SWID tags enhances the SCAP use cases by providing authoritative information that can be used to create Common Platform Enumeration (CPE) names, to support the targeting of checklists, and to associate software flaws to products, based on a defect in a software library or executable. CSD is currently working on a SWID tag validation tool, called SWIDVal, that will validate a SWID tag document against the ISO/IEC 19770-2:2015 and NISTIR 8060 requirements. This tool is planned for an early access release in FY 2017. CSD is also planning to work on a revision of NISTIR 8060 with additional tag signature requirements for release in late FY 2017.

Development of Security Automation Consensus Standards

CSD has been promoting the broad international adoption of SCAP by encouraging the integration of SCAP into other standards, and by adapting SCAP to address specific gaps and challenges. CSD has continued its collaboration with its 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. The SACM working group has been working on identifying use cases, requirements, and architectural models to provide information to facilitate 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. CSD is working with DHS, the Center for Internet Security (CIS), and the TCG to bring existing work into the IETF SACM working group, including OVAL and specifications related to the TNC protocol.

The working group has been developing the following Internet Drafts:

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

Also, within the IETF, CSD has been collaborating with the Managed Incident Lightweight Exchange (MILE) working group in order to develop the Resource-Oriented Lightweight Information Exchange (ROLIE) specification. This specification seeks to address the security automation information discovery and dissemination use cases by defining how tools are expected to communicate with security automation information repositories. ROLIE allows for the transport, retrieval, and storage of any security automation-relevant information types. The ROLIE draft has undergone two major revisions, with the final draft nearing completion. In addition, CSD has begun the process of collaborating with MILE and other stakeholders to create extension drafts for ROLIE that address a number of information types, including vulnerability, configuration checklist, and software metadata information types.

The main ROLIE draft can be found at https://datatracker.ietf.org/doc/draft-ietf-mile-rolie/. Additional information on ROLIE and on the extension drafts can be found in the working repository on GitHub: https://github.com/CISecurity/ROLIE/.

CSD also worked with its government and industry partners in the TCG to define a number of specifications related to the TNC protocol. The first such publication is the TNC SCAP Messages for IF-M specification that supports carrying the 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.

INTERNET DRAFT	PURPOSE
https://datatracker.ietf.org/doc/draft-ietf-sacm-terminology/	Definition of the common terminology used within several working-group documents.
https://datatracker.ietf.org/doc/draft-ietf-sacm-requirements/	Listing architectural and specification requirements for SACM specifications.
https://datatracker.ietf.org/doc/draft-ietf-sacm-architecture/	Definition of the SACM architecture to provide information for the development of methods to exchange security automation information (i.e., transports).
https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/	Definition of the SACM information model to provide information for the development of data models.

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.

Updated versions of the ECP and SWID related specifications, along with a usage scenario around vulnerability assessment are currently being worked on in the SACM working group, which available through the following locations:

https://datatracker.ietf.org/doc/draft-haynes-sacm-ecp/

https://datatracker.ietf.org/doc/draft-coffin-sacm-nea-swid-patnc/

https://datatracker.ietf.org/doc/draft-ietf-sacm-vuln-scenario/

Additionally, CSD has several members who are actively engaged on the CVE Board, which is working to improve the assignment of CVE identifiers for vulnerabilities, with the overall goal of improving the automated processing of vulnerabilities and the timeliness of CVE identifier issuance.

Finally, CSD has worked with the FIRST by participating in two Special Interest Groups (SIGs). The CVSS SIG (CVSS-SIG) is focused on maintaining and improving the CVSS scoring model, based on community feedback. The CVSS-SIG published CVSS Revision 3 (CVSS v3) in June 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 standards-developing organizations (SDOs), SCAP and its 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.

FOR MORE INFORMATION, SEE:

http://scap.nist.gov/

CONTACT:

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

Security Automation Reference Data

Through the NVD and the NCP (see below), 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 toward being able to standardize communications and toward the collection and storage of relevant data in standardized formats, as well as providing 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 a comprehensive cybersecurity vulnerability database that allows the tracking of vulnerability trends over time. This trending service allows users to assess changes in vulnerability discovery rates within specific products or within specific types of vulnerabilities. NVD data is represented using the SCAP specifications. 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.

As of the end of September 2016, the NVD contained the following resources:

- Over 79,000 vulnerability advisories, with an average of 30 new vulnerabilities added daily;
- 83 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;
- 293 non-SCAP security checklists (e.g., English prose guidance and configuration scripts);

- 249 U.S. Computer Emergency Readiness Team (US-CERT) alerts; 4,458 US-CERT vulnerability summaries; and 10,286 SCAP machine-readable software flaw checks; and
- A product dictionary with over 115,000 operating system, application, and hardware name entries; and over 63,900 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. The PCI mandates the use of NVD vulnerability severity scores in measuring the risk to payment card servers worldwide and for prioritizing vulnerability patching. The PCI's use of NVD severity scores helps enhance credit card transaction security and protects consumers' personal information.

In the past year, the NVD began providing Common Vulnerability Scoring System (CVSS) base scores following the CVSS v3 specification and will soon include this information in the data feeds (see https://www.first.org/cvss/specification-document). An update of the web site is planned to enhance the user's experience.

FOR MORE INFORMATION, SEE:

https://nvd.nist.gov

CONTACTS:

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

Mr. Robert Byers
(301) 975-3279
robert.byers@nist.gov

National Checklist Program (NCP)

There are many threats to 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, 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 mandates that NIST "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, a revision of 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, OMB mandated the use of SCAP-validated products for the 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.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

At the end of FY 2016, there are a total of 367 checklists posted on the NCP website (see http://checklists.nist.gov). Of that total, 154 of the checklists, addressing 96 platforms, are SCAP-expressed and can be used with SCAP-validated products.

Organizations can use checklists obtained from the NCP website for automated security configuration patch assessment. The NCP currently provides metadata and links to the latest operating systems and applications checklists, including MacOS 10.10, Windows 10, Internet Explorer 11.0, Internet Explorer 10.0, Office 2016, Red Hat Enterprise Linux, 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 fully vetted SCAP content that has successfully demonstrated conformance to the requirements outlined in SP 800-126. Tier III & IV checklists are considered production-ready and are intended for use with SCAP-validated products.

Tier II checklists document the recommended security settings in a machine-readable format such as the XCCDF-only (i.e., no OVAL content), proprietary format, or 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 the 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 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 https://scap.nist.gov/validation/resources.html).

The NCP is defined in SP 800-70 Revision 3, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, which can be found at http://csrc.nist.gov/publications/PubsSPs.html.

FOR MORE INFORMATION, SEE:

https://checklists.nist.gov

CONTACT:

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

Apple OS X Security Configuration

CSD's OS X security configuration team is working to develop secure system configuration baselines supporting different operational environments for Apple OS X Version 10.10, "Yosemite." 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 are based on a collection of resources, including the existing NIST OS X configuration guidance, the DOD OS X Recommended Settings, the Defense Information Systems Agency (DISA) OS X Security Technical Implementation Guide (STIG), and the Center for Internet Security (CIS) OS X Security Benchmark.

The project team researched and tested 250 settings for OS X 10.10. Among other collected data, each setting has a designated Common Configuration Enumeration (CCE) number, which aids in long-term tracking of the setting. Figure 35 illustrates the various categories that comprise the baselines. Note that a higher quantity of settings in a category does not imply greater importance over other categories.

The team finished developing shell scripts that apply the settings to an OS X 10.10 system. The settings are organized into three key baselines, which are appropriate for different environments:

- The Standalone baseline describes small, informal computer installations that are used for home or business purposes,
- The Managed baseline is appropriate for centrally managed, networked systems, and
- The Specialized Security-Limited Functionality (SSLF) baseline is appropriate for systems where security requirements are more stringent and where the implementation of security safeguards is likely to reduce functionality.

In FY 2016, the security configuration was updated to have 250 settings after the internal testing on select CSD systems was completed. In June 2016, the draft SP 800-179, *Guide to Securing Apple OS X 10.10 Systems for IT Professionals*, was published for public comment

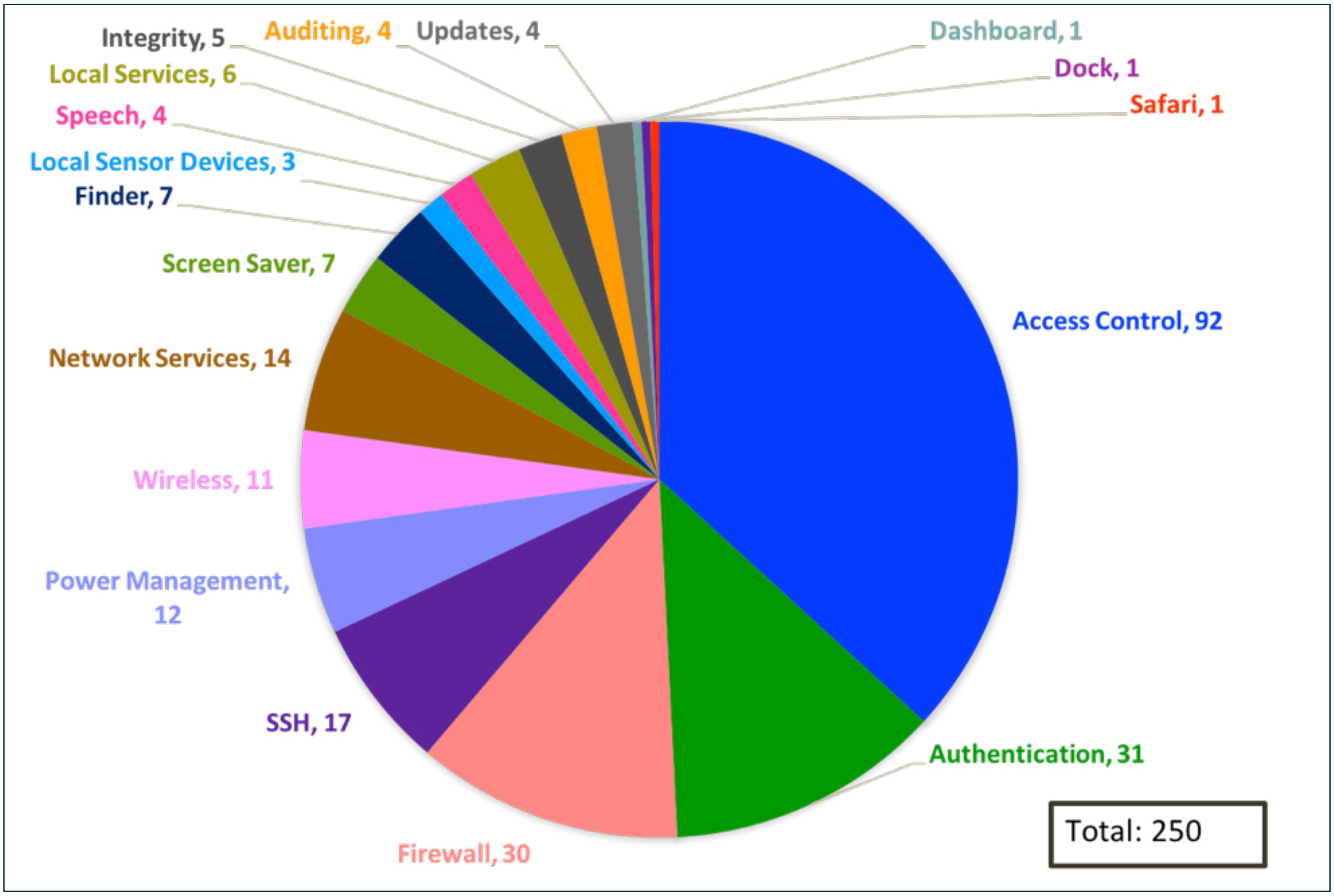


Figure 35: Configuration Categories

(see https://csrc.nist.gov/publications/ Search?request SeriesList==1,&requestStatusList=1,3,&requestDisplay Option=brief&requestSortORder=5&itemsPerPage= All).

The purpose of this document is to explain the settings, their security significance, and how to configure them for the three baselines described above. All feedback received during the comment period was addressed and incorporated into the draft document.

In FY 2017, the team plans on accomplishing the following:

- Complete the final version of SP 800-179, *Guide to Securing Apple OS X 10.10 Systems for IT Professionals*;
- Continue to refine the script and add more settings to the configuration;
- Update the security configuration guide for MacOS 10.12; and
- Investigate translating security guidance into the SCAP format, which is defined and discussed in other sections of this report. SCAP will be used to express configuration settings and check system configuration compliance.

FOR MORE INFORMATION, SEE:

http://csrc.nist.gov/projects/apple-os/

https://github.com/usnistgov/applesec

CONTACTS:

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

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

Mr. Murugiah Souppaya
(301) 975-8443
murugiah.souppaya@nist.gov

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

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 the security risk analysis of computer networks. A standard model will enable an organization 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. The methodology used 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, trade-offs between security costs and security benefits are analyzed.

Computer systems are vulnerable to both known and zero-day attacks. Enterprises have begun to move parts of their networks from a traditional infrastructure into cloud computing environments. Cloud providers offer virtual servers that can be rented on demand by users. This paradigm enables cloud customers to acquire computing resources with high efficiency, low cost and great flexibility. However, it also introduces many security problems that need to be solved. Diversity has long been regarded as a security mechanism for improving the resilience of software and networks against various attacks. More recently, diversity has found new applications in cloud computing security, moving target defense, and improving the robustness of network routing. However, most existing efforts rely on intuitive and imprecise notions of diversity, and the few existing models of diversity are designed for a single system running diverse software replicas or variants. In FY 2016, CSD has attempted to formally model network diversity as a security metric by designing and evaluating a series of diversity metrics. In particular, CSD has devised a biodiversity-inspired metric based on the effective number of distinct resources. CSD has also proposed two complementary diversity metrics, based on the least and the average attacking efforts, respectively. CSD published two papers in this area:

1. *Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero Day Attacks*, IEEE Transactions on Information Forensics and Security, 11(5) May *2016 (see* http://ieeexplore.ieee.org/document/7378495/*).*
2. *Diversifying Networks Services under Cost Constraints for Better Resilience against Unknown Attacks*, 30th International Federation for Information Processing (IFIP) Conference on Data and Application Security and Privacy, Trento, Italy, July 18th to 21st 2016 (see http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=920658).

In FY 2017, CSD plans to develop new techniques and metrics for Cloud Computing threat modeling and network forensics analysis using Bayesian networks. CSD also plans to publish the results as a NIST report and as white papers in conferences and journals.

FOR MORE INFORMATION, SEE:

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 designing and implementing algorithms to both detect attackers and limit their ability to intrude into a system. Most of the work leverages graph theory (the math of dots and lines) and algorithmic complexity analysis (the math around fast computation). 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), the University of Maryland, and the Center for Applied Internet Data Analysis. ARL's participation helps focus the work on solving immediate critical problems facing U.S. Government networks. However, research solutions are made publicly available and are designed to be generally applicable to as many environments as possible.

In FY 2016, the AIM project completed research in several areas: algorithms for measuring the ease at which networks can be broken apart, efficient representations for attack graphs, and an analysis of how to increase the robustness of the African Internet. More specifically, the project team accomplished the following:

- The team discovered a linear-time algorithm to implement a heuristic for vertex partitioning that enables effective partitioning on massive graphs (tested on graphs up to 34 million nodes). This enables one to measure the ease at which terrorist activity or global conflicts can break apart large networks, for example, the entire Internet (the research was published in the *International Journal of Computer Science: Theory and Application*).
- The team discovered an efficient representation for attack graphs that grows linearly in the number of nodes, while most attack graph research uses an inefficient graph representation that grows quadratically in the number of nodes and that creates unnecessary edge connections (this research was published in the proceedings of the *Tenth International Conference on Software Engineering Advances*).
- The team studied how to increase the robustness of the African Internet, creating the first country-level topology maps of Africa, and measured the growth of Internet connectivity (this research was a precursor to more global connectivity studies; it was published in the proceedings of the *7th European Alliance for Innovation International Conference on e-Infrastructure and e-Services for Developing Countries*).

In FY 2017, the AIM project will work on new methods for assuring private communication on the Internet, network anomaly detection, efficient graph algorithms for access control computations (to restrict external leakage of insider information), and methods for using attack graphs to perform defense-in-depth measurements.

FOR MORE INFORMATION, SEE:

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

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 investigation of actual failures has shown that most failures are triggered by one or two parameters, and progressively fewer by three, four, or more parameters (see Figure 36 - next page); this relationship is called the Interaction Rule. These results have important implications for testing software and systems. 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 with a doable number of tests can provide 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 the impact on real-world problems.

Project highlights for FY 2016 include the development of an efficient method for testing rule-based systems using covering arrays and the development of a prototype tool; invited lectures at conferences and universities; leading the Fifth International Workshop on Combinatorial Testing, held in conjunction with the eighth IEEE International Conference on Software Testing; development of a real-time combinatorial coverage measurement tool; and analyzing the factors involved in different types of software faults. Collaborators include researchers from the University of Texas at Arlington, the University of Texas at Dallas, East Carolina University, and Duke University.

NIST also submitted a patent on an oracle-free testing method based on two-layer covering arrays (see below). In software testing, the oracle problem refers to determining the expected output for a given set of inputs. A determination of the expected output requires expert knowledge and normally cannot be automated without a mathematical model of the specification. The test settings for an input factor may represent ranges of values (called equivalence classes) for which the output is expected to remain unchanged. For example, a shipping program may charge the same rate for any package under one pound, a second rate for packages one pound to 10 pounds, and a third rate for packages over 10 pounds. Values within each of these ranges are equivalent with respect to the cost calculation. Thus, any value within an equivalent range may be substituted for any other, and the program output should be unchanged. Similarly, equivalent values for any combination of input variables will also produce the same output.

The test method works by generating two test arrays: a primary array and a secondary array. The entries of a primary array represent the names of equivalence classes of input factors. For each test row of the primary array, a second array is computed. The settings in the second array are the

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

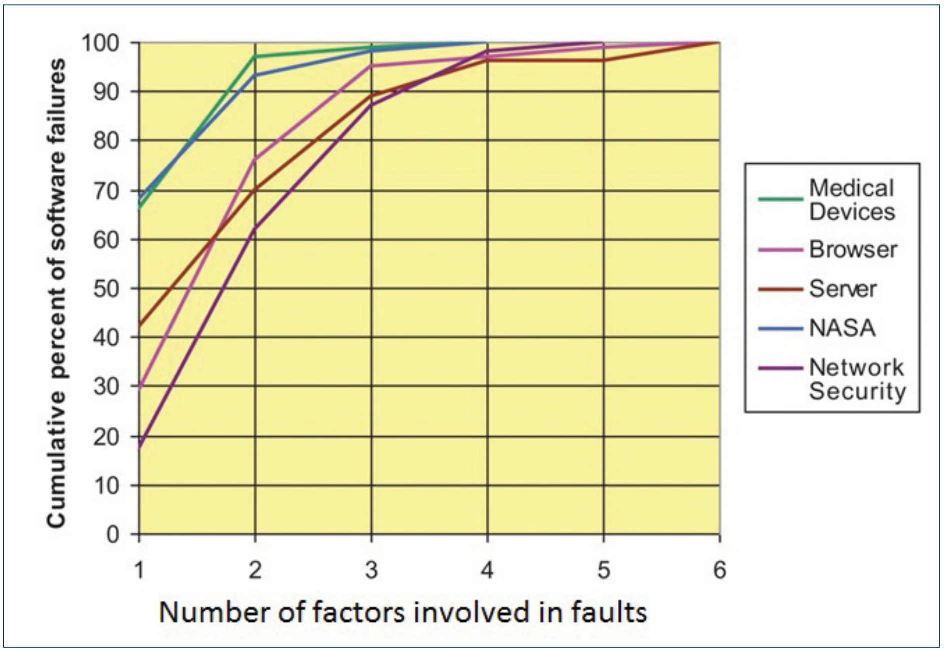


Figure 36: Interaction Rule Graph

values from equivalence classes corresponding to the names of equivalence classes in the primary array. If the outputs corresponding to one row of the primary array differ, then either the equivalence classes were defined incorrectly or the code is faulty in some way. This method can detect a large class of software faults automatically after equivalence classes have been defined, without a conventional test oracle.

Technology transfer activities included the publication of a number of technical papers and software distributions; publication of the results of a Cooperative R&D (CRADA) project with Lockheed Martin; release of enhanced combinatorial measurement tools; input modeling and fault location tools; a provisional patent application on the oracle-free testing method; and seminars at a number of conferences, universities, and federal agencies.

Plans for FY 2017 include the development of a mathematical model for the evolution of t-way faults in software; combinatorial testing for big data software; measurement of input model combination coverage of network protocol software; trial use of prototype methods and tools for oracle-free testing methods; analysis of empirical data on failures; further development of methods and tools for fault localization; and seminars, workshops, and tutorials at professional meetings and research labs.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

Mr. Rick Kuhn	Dr. Raghu Kacker
(301) 975-3337	(301) 975-2109
kuhn@nist.gov	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.

This project 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 firmware. Previous work in this project described methods to protect boot firmware

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

as part of the NIST SP 800-147 series, now standardized by ISO/IEC JTC 1/SC 27, *IT Security Techniques*, as ISO/IEC 19678:2015, *Information Technology – BIOS Protection Guidelines*. Building on this work in FY 2016, the project team researched techniques and requirements for securing firmware throughout the platform. The goal of this effort is to protect platform firmware from unauthorized changes, detect accidental or malicious corruption, and recover from destructive attacks.

The results of this research will be documented in a new set of draft guidelines that are expected to be released in FY 2017. The upcoming draft guidelines will facilitate discussions with industry, standards organizations, and consortiums over technologies, standards, and specifications that can support firmware protection, detection and recovery.

FOR MORE INFORMATION, SEE:

http://csrc.nist.gov/projects/root-trust/

CONTACT:

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

USABILITY AND SECURITY

Usability is an often overlooked but critical component of cybersecurity. There is a belief that there is an inherent tradeoff between cybersecurity and usability. Computers can be theoretically secure but so unusable that they do not improve security because users are forced to perform in less secure ways. The opposite is true as well; systems that are easy to use and not secure are eventually unusable due to worms, viruses, and botnets. The usability principles of efficiency, effectiveness and user satisfaction must be incorporated to ensure that it is easy for users to do the right thing and hard for them to do the wrong thing. NIST has been working to develop usability and security metrics, facilitate the integration of usability principles into product design processes, and lead research projects to investigate methods for aligning user goals with organizational security goals.

During FY 2016, the usability team's research focused primarily in four areas: passwords, understanding user behavior, cryptography, and privacy.

1. Password Research:

The **password** research included examining password policies from two perspectives. The Password Policy Taxonomy project is exploring the relationship between usability and security by focusing on the password policy itself and how users of a policy understand it. To tackle the ambiguity inherent in many password policies, a formal language for representing a password policy was previously developed. Having clear, unambiguous policy statements enables us to explore password policies in much greater detail, discuss the relative merits of different statements, compare and contrast policies, explore plain language policy representations and user interpretations, and examine the interplay between usability and security in password policies. A Password Policy Question-Answer System (PPQAS) was designed, developed and tested. The system is a flexible application and is designed to collect users' interpretations of various password policies and map each interpretation of a policy's regulating statements to elements of the formal language via a dynamic set of questions and answers and to store those mappings for analysis.

The second effort examines how users interpret and apply password rules. Ambiguous terminology in password rules affects user comprehension. This research investigated user comprehension of ambiguous terminology in password rules, using a combination of quantitative and qualitative methods in a usable security study with 60 participants.

Results showed:

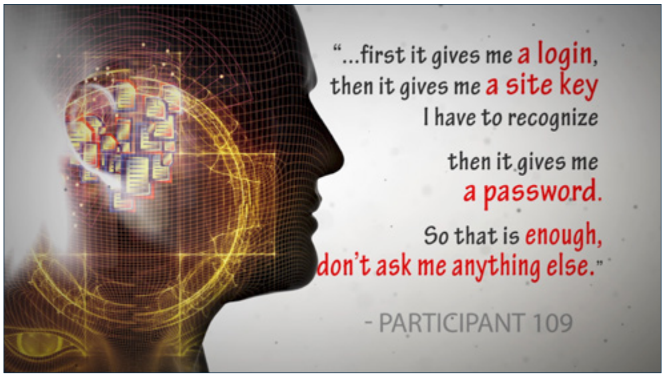
- That manipulating password rule terminology causes users' interpretation of the allowed character space to shrink or expand.
- Users are confused by the terms "non-alphanumeric," "symbols," "special characters," and "punctuation marks" in password rules.
- Additionally, users are confused by partial lists of allowed characters using "e.g." or "etc."

This research provides data-driven usability guidance on constructing clearer language for password policies.

2. Understanding User Behavior:

Understanding user behavior is critical to achieving security objectives. One example of this achieving security objectives is preventing successful phishing attacks. Phishing is the attempt to obtain sensitive information by posing as a trustworthy entity in an electronic communication, often in the form of emails appearing to be from legitimate parties that contains links or attachments. It is a major cyber threat facing government organizations. To help combat this threat, many organizations utilize some type of phishing awareness training to make their staff more aware of phishing threats and consequences. To ultimately improve awareness training, it is important to understand *why* the staff do or do not fall victim to phishing attacks. For example, an employee opening an email attachment could be a means of conducting the attack. This project partnered with the NIST Office of Information Systems Management (OISM) and Office of Safety, Health and Environment (OSHE) to better understand operational phishing awareness training. Results showed that user context is the key to understanding user behavior regarding phishing attacks. For example, staff who are responsible for paying bills and invoices are more likely to be victimized by fake unpaid invoice emails.

Another noteworthy program in user behavior is the research into Security Fatigue. People are repeatedly bombarded with messages about the dangers lurking on the Internet, about the security breaches of major corporations and the U.S. government, and about the need to be constantly attentive while online. To combat these dangers and stay safe while online, users are forced to update passwords, run antivirus software programs, and accept unwieldy terms of agreements, often without a clear understanding of why and to what end. The research team interviewed 40 participants to understand their relationships with cybersecurity.


"...first it gives me a login,
then it gives me a site key
I have to recognize
then it gives me
a password.
So that is enough,
don't ask me anything else."
- PARTICIPANT 109

The team discovered that:

- People reach a saturation point and become inured to the issue of cybersecurity.
- People are told they need to be constantly on alert, constantly doing "something," but they are not even sure what that something is or what might happen if they do or do not do it.

The team calls this "security fatigue." This security fatigue and the resignation and loss of control associated with it certainly presents a challenge to efforts aimed at promoting online security and the protection of online privacy.

This research on security fatigue was a popular topic with users and many media outlets interested in it. According to the NIST Public Affairs Office, there were:

- 17,550 page views of the news story on NIST.gov (the fourth most visited page in 2016 on the NIST website);
- 7.9K total views for Facebook posts on the story;
- 2,327 views of the story on Eurekalert (an online news release repository operated by The American Association for the Advancement of Science (AAAS));
- 2,172 plays of the video on Kaltura (the platform hosting the video on the NIST news story page), 81 shares, 51 downloads; and
- 918 video views on YouTube.

The news outlets included: BBC News, MSN.com, Politico, Federal News Radio, Bloomberg BNA, the Register, and McClatchy DC, and many others included quotes by the authors, such as: " 'Users are tired of being overwhelmed by the need to be constantly on alert...' said the study by the National Institute of Standards and Technology, a unit of the Department of Commerce."

3. Cryptography

The team's cryptographic research is concerned with creating a baseline understanding of the current practices and challenges of organizations that are developing products that use cryptography. The research team considered the entire process, from the identification of a market opportunity and the conceptualization of the product; the assembling of the product team; the design, implementation and testing of the product; and finally, the marketing, sale and end-user support. Based on the research, ITL will use this new understanding to help improve the assurance of cryptographic tools and the usability of cryptographic software and resources.

The following contributions were made:

- The research team identified opportunities to better characterize the cryptographic practices and types of resources and standards used by cryptographic developers.
- Research offers new insights into the challenges that cryptographic implementations introduce into organizational practices, such as recruitment, product lifecycle and transitions, the management of employees, the evaluation of cryptographic work, and product explanation to customers.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

- The research team studied methods to quantify and rank factors that developers consider when evaluating the quality of a cryptographic implementation.

4. Privacy

A new area was initiated to examine privacy and de-identification. A Federal Government stakeholder's meeting was organized to discuss the topic, after which NIST provided additional guidance through multiple training sessions to other federal agencies, a NIST Interagency Report, and a NIST Special Publication.

De-identification regarding private data set release, or the release of other information about a private data set (such as summarizing statistics), is a class of procedures intended to restrict or limit the ability of a recipient of such a release to re-identify a particular individual in the data set and infer potentially sensitive information about the individual (whether in an absolute, or in a probabilistic sense). De-identification is a collection of methods with the goal of protecting the privacy of the individual, while simultaneously preserving the utility of the released data (or other summarizing statistics).

ITL researchers are evaluating *differentially private algorithms,* a subset of de-identification techniques. The team is considering the possible tradeoffs between protecting the privacy of individuals and the usefulness of information, such as might occur when a research database with de-identified personal information is released.

The following are the publications that were released for the Usability and Security project during FY 2016:

- NISTIR 8080, *Usability and Security Considerations for Public Safety Mobile Authentication*. (July 2016) (see http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8080.pdf)
- NISTIR 8150, *Government Data De-Identification Stakeholder's Meeting, Meeting Report*. (September 2016) (see http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8150.pdf)
- Choong, Y. Y., & Greene, K. K. (2016, September). *What's a Special Character Anyway? Effects of Ambiguous Terminology in Password Rules*. Published in the Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 60, No. 1, pp. 760-764). Sage CA: Los Angeles, CA: SAGE Publications.
- Theofanos, M., Garfinkel, S. and Choong, Y.Y., (2016). *Secure and Usable Enterprise Authentication: Lessons from the Field. IEEE Security & Privacy*, *14*(5), pp.14-21.
- Greene, K.K., and Choong, Y.Y. "*Must I, Can I? I Don't Understand Your Ambiguous Password Rules.*" This article was accepted on 09/12/2016 and will appear in Issue 1 of the 2017 Volume of Journal of Information and Computer Security.
- Stanton, B., Theofanos, M., Spickard Prettyman, S., Furman, S., "*Security Fatigue*", *IT Professional*, Vol. 18, Issue 5, pp. 26-32, Sept.-Oct. 2016, doi:10.1109/MITP.2016.84
- Stanton, B., Theofanos, M., Spickard Prettyman, S., Furman, S. (2016). *The Power of Qualitative Methods: Aha Moments in Exploring Cybersecurity and Trust*. User Experience Magazine, 16(5). Retrieved from http://uxpamagazine.org/the-power-of-qualitative-methods/
- Steves, M., Theofanos, M., (2016) "*What's in your policy? Do your users know?"* National Institute of Standards and Technology Interagency Report (NISTIR) that was submitted to IEEE Security and Privacy.
- Garfinkle, S., Theofanos, M. and Choong,Y.Y., "*Secure and Usable Enterprise Authentication: Lessons from the Field*," to appear in *IEEE Security & Privacy,* September/October 2016, a special issue on usable security.

The proposed plans for FY 2017 for this project consist of the following activities:

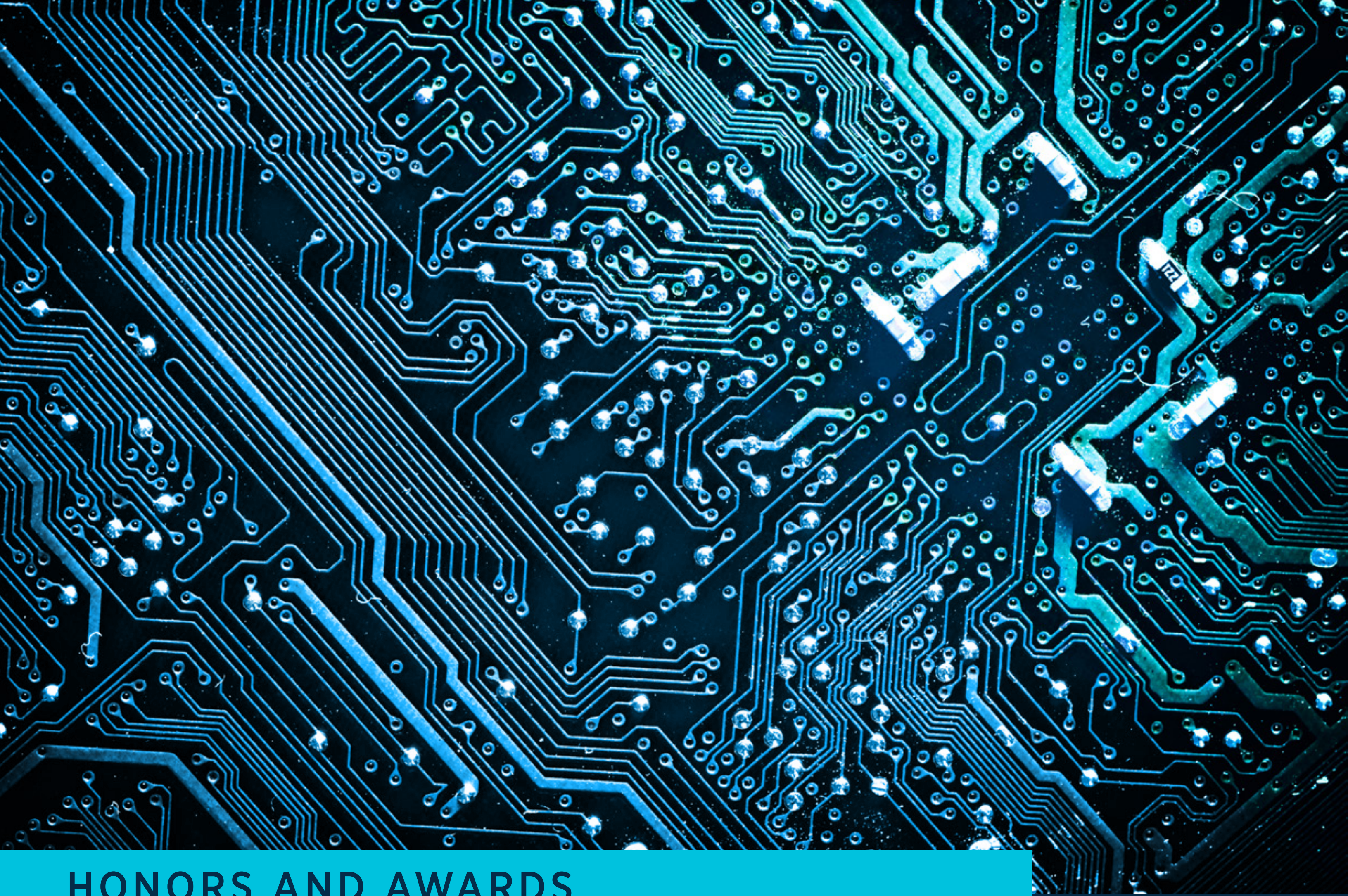
- Examine users in healthcare and their behaviors and perceptions of security;
- Complete interviews with companies that develop cryptographic products;
- Perform usability testing on a password policy tool;
- Finalize usability chapters for the revision of 800-63, Digital Identity Guidelines;
- Extend the password rules comprehension research; and
- Develop test methods for de-identification algorithms.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/Usability-Of-Security

CONTACTS:

Ms. Mary Theofanos (301) 975-5889 maryt@nist.gov	Mr. Brian Stanton (301) 975-2103 brian.stanton@nist.gov



HONORS AND AWARDS

This section recognizes ITL staff who have received honors and/or awards for their cybersecurity accomplishments.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

Department of Commerce Gold Medal Award

Leah Kauffman, Nathan Lesser, Timothy McBride, Gavin O'Brien, Lucy Salah, and Karen Waltermire (Applied Cybersecurity Division, National Cybersecurity Center of Excellence (NCCoE)); *Murugiah Souppaya* (Computer Security Division); *Kevin Kimball* (NIST Director's Office); Keith Bubar (Acquisition Management Division); and *Lauren Didiuk* (Department of Commerce, Office of General Counsel).

Front Row (Left/Right): Waltermire, Salah, Kauffman
Back Row Left/Right: Lesser, Kimball, O'Brien, McBride
Absent: Bubar, Souppaya, and Didiuk

The group is recognized for establishing the National Cybersecurity Center of Excellence (NCCoE) to accelerate the adoption of cybersecurity standards and best practices. With industry partnerships, the NCCoE builds practical security reference designs that can be rapidly applied to the real challenges that businesses face today. This achievement includes the Department's first Federally Funded Research and Development Center (FFRDC) and the Nation's first FFRDC devoted wholly to cybersecurity.

Department of Commerce Silver Medal Award

Elaine Barker, Lawrence Bassham, Shu-jen Chang, Lily Chen, Quynh Dang, Morris Dworkin, John Kelsey, Rene Peralta, Ray Perlner and Andrew Regenscheid (All work for the Computer Security Division, Information Technology Laboratory)

(Left/Right): Regenscheid; Dang; Barker; Kelsey; Chang; Bassham; Dworkin; Chen; Perlner; Peralta

The group is recognized for exceptional technical innovation in leading a global effort to develop Federal Information Processing Standard (FIPS) 202, the "SHA-3" hash function standard. Cryptographic hash functions are critical components of the technologies (e.g., digital signatures and message authentication) that secure global communications, international electronic commerce and more. Advances in cryptanalysis in 2004-2007 weakened the security of many widely used hash functions, broadly threatening cybersecurity. SHA-3 is intended to provide security for decades.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

Department of Commerce Bronze Medal Award

Bill Fisher and Jerome "Jay" Thomson (Applied Cybersecurity Division, National Cybersecurity Center of Excellence (NCCoE)); *Beth Bly and Deana Ramsburg* (Customer Access and Support Division); *Alex Folk* (Information Technology Laboratory Office); *Robert Densock* (Information Technology Security & Networking Division); *Lynn Flanagan* (Department of Commerce, Office of General Counsel); *Jatin Patel* (Gaithersburg Design and Construction Division, Facilities Improvement Group); *Kevin Conrad and Cheri Smith* (Emergency Services Office, Security Systems and Access Control Group).

Group Photo: (Left/Right) (front) Bly; Smith; Ramsburg;
(back) Folk; Thomson; Conrad; Densock; Fisher;
Individual Photo Top/Bottom: Flanagan; Patel

The team is recognized for outstanding leadership and teamwork in coordinating the design and construction of the facility housing the National Cybersecurity Center of Excellence. In 12 months, this team transformed a 65,000-square-foot biotech facility into a state-of-the-art cybersecurity research center that is home to 28 laboratories and other workspaces for collaboration among government, academia and industry. During this time, this high-performing team brought together the necessary leadership skills, team-building techniques, contracting and procurement expertise, project management discipline, physical security methods, construction knowledge, and attention to detail required to complete this high-priority effort.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

Ms. Donna Dodson Nominated 1 of the 11 Most Influential Women in Government IT for 2016

The United Nations adopted February 11th as an International Day of Women and Girls in Science. This day celebrates the impact and importance of women in science, technology, engineering and management, also known as STEM, and focuses on the significance of encouraging women of all ages to enter STEM fields. Within the Federal Government, there have been many women over the years that have made significant, influential, and positive impacts on Information Technology.

One of the eleven Women in the Federal Government chosen to receive this great honor is Ms. Donna Dodson of the National Institute of Standards and Technology (NIST). Donna works in the Information Technology Laboratory (ITL) as the Associate Director Chief Cybersecurity Advisor, and she is also the Director of the National Cybersecurity Center of Excellence (NCCoE), a program at NIST. Donna manages the lab's research and development; she also has a key role in developing relationships with academia, industry, and government agencies to analyze and improve cybersecurity best practices.

Dr. Ron Ross is the recipient of 5 awards during 2016

National Cybersecurity Hall of Fame: Class of 2015

Dr. Ron Ross was inducted into the National Cybersecurity Hall of Fame. The Hall of Fame is a national program that describes its mission as honoring "the innovative individuals and organizations which had the vision and leadership to create the foundational building blocks for the Cybersecurity industry." Dr. Ross was honored as a key pioneer of the Federal Information Security Management Act (FISMA) security standards and his role as one of the world's leading experts on cybersecurity. His induction recognized his leadership as the principal architect of the NIST Risk Management Framework and lead developer of the first set of unified cybersecurity standards for the Federal Government.

(See Source: http://www.cybersecurityhalloffame.com)

Service to America Medal for Homeland Security and Law Enforcement

Dr. Ross was awarded a Service to America Medal for his work having "instituted a state-of-the-art risk assessment system that has protected federal computer networks from cyber attacks and helped secure information critical to our national and economic security." The Samuel J. Heyman Service to America Medals honor members of the Federal workforce, highlighting the work of employees who significantly contribute to the governance of the United States.
(See Source: https://servicetoamericamedals.org/honorees/view_profile.php?profile=409)

Government Executive of the Year Award

Dr. Ross was also recognized, as part of the Government Computer News (GCN) Annual Awards, as the Government Executive of the Year. The award honored Dr. Ross' contributions to securing federal information systems. GCN's editor in chief, Troy Schneider, stated that "there is virtually no corner of federal IT in 2015 that doesn't need to take cybersecurity into account, and there is probably no government executive more central to those security efforts than Ron Ross."
(See Source: https://gcn.com/articles/2015/10/07/ron-ross-nist.aspx?m=1)

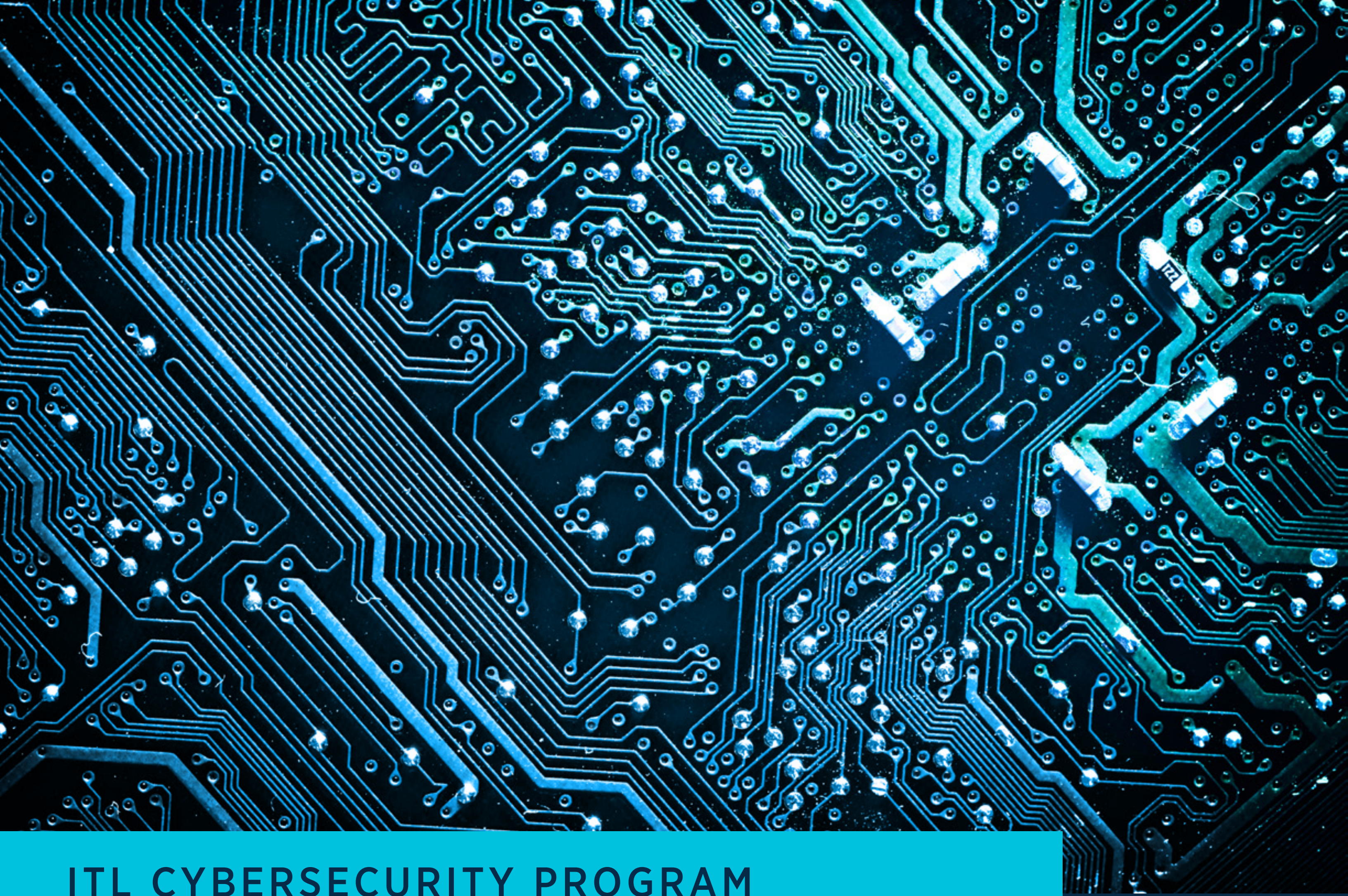
Federal 100 Award

For the third time, Dr. Ross was recognized as one of Federal Computer Week's Federal 100 awardees. The Federal 100 Awards recognize government and industry leaders who have played pivotal roles in the Federal Government IT community.

Ross personally has been a critical driver for getting agencies – and many other key stakeholders – to move beyond checklist-based security. He spent much of 2015 evangelizing in the federal community, making sure that both NIST Special Publication 800-160 on systems security engineering and the Risk Management Framework that he developed were put to good use.
(See Source: https://fcw.com/articles/2016/03/28/fed100_ross-ron.aspx?m=1)

2015 Presidential Rank Award

Dr. Ron Ross was awarded the 2015 Presidential Rank Award. The Civil Service Reform Act of 1978 established the Presidential Rank Awards Program to recognize a select group of career members of the Senior Executive Service (SES) for exceptional performance over an extended period. Later, the Rank Award statute was amended to extend eligibility to senior career employees with a sustained record of exceptional professional, technical, and/or scientific achievement at a national or international level.
(See Source: https://www.opm.gov/policy-data-oversight/senior-executive-service/presidential-rank-awards/presidential-rank-awards-2015-full-list.pdf)



ITL CYBERSECURITY PROGRAM PUBLICATIONS RELEASED IN FY 2016

This section provides a compiled list of ITL cybersecurity publications that were released during FY 2016 (from October 1, 2015 to September 30, 2016). The first portion provides a list of the technical documents. The second portion provides abstracts that represent a brief summary of each document (technical and non-technical).

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

DRAFT PUBLICATIONS

TABLE 3: NO DRAFT FIPS RELEASED DURING FY 2016

TABLE 4: SPECIAL PUBLICATIONS (SPs)

PUBLICATION NUMBER	PUBLICATION TITLE	DRAFT RELEASED
SP 800-188	*De-Identifying Government Datasets*	August 2016
SP 800-185	*SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash*	August 2016
SP 800-184	*Guide for Cybersecurity Event Recovery*	June 2016
SP 800-180	*NIST Definition of Microservices, Application Containers and System Virtual Machines*	February 2016
SP 800-179	*Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist*	June 2016
SP 800-177 (2nd Draft)	*Trustworthy Email*	March 2016
SP 800-175A	*Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*	April 2016
SP 800-175B	*Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*	March 2016
SP 800-171 Rev. 1	*Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*	August 2016
SP 800-166	*Derived PIV Application and Data Model Test Guidelines*	February 2016
SP 800-160 (Final Public Draft) (2nd Draft)	*Systems Security Engineering Guideline: An Integrated Approach to Building Trustworthy Resilient Systems*	September 2016 May 2016
SP 800-156	*Representation of PIV Chain-of-Trust for Import and Export*	December 2015
SP 800-154	*Guide to Data-Centric System Threat Modeling*	March 2016
SP 800-150 (2nd Draft)	*Guide to Cyber Threat Information Sharing*	April 2016
SP 800-126 Rev. 3	*The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3*	July 2016
SP 800-126A	*SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3*	July 2016
SP 800-116 Rev. 1	*A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*	December 2015
SP 800-114 Rev. 1	*User's Guide to Telework and Bring Your Own Device (BYOD) Security*	March 2016
SP 800-90C (2nd Draft)	*Recommendation for Random Bit Generator (RBG) Constructions*	April 2016
SP 800-90B (2nd Draft)	*Recommendation for the Entropy Sources Used for Random Bit Generation*	January 2016
SP 800-46 Rev. 2	*Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*	March 2016
SP 1800-5	*IT Asset Management: Financial Services*	October 2015
SP 1800-4	*Mobile Device Security: Cloud and Hybrid Builds*	November 2015

TABLE 5: NIST INTERAGENCY OR INTERNAL REPORTS (NISTIRs)

PUBLICATION NUMBER	PUBLICATION TITLE	DRAFT RELEASED
NISTIR 8144	*Assessing Threats to Mobile Devices and Infrastructure: The Mobile Threat Catalogue*	September 2016
NISTIR 8138	*Vulnerability Description Ontology (VDO): A Framework for Characterizing Vulnerabilities*	September 2016
NISTIR 8136	*Mobile Application Vetting Services for Public Safety*	June 2016
NISTIR 8114	*Report on Lightweight Cryptography*	August 2016
NISTIR 8112	*Attribute Metadata*	August 2016
NISTIR 8105	*Report on Post-Quantum Cryptography for Public Comment*	February 2016
NISTIR 8103	*Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps*	February 2016
NISTIR 8085	*Forming Common Platform Enumeration (CPE) Names from Software Identification (SWID) Tags*	December 2015
NISTIR 8080	*Usability and Security Considerations for Public Safety Mobile Authentication*	November 2015
NISTIR 8071	*LTE Architecture Overview and Security Analysis*	April 2016
NISTIR 8063 [final version published as SP 800-183]	*Primitives and Elements of Internet of Things (IoT) Trustworthiness*	February 2016
NISTIR 8060 (Final Public Draft)	*Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*	December 2015
NISTIR 8011 Volumes 1 & 2	*Automation Support for Security Control Assessments* *Volume 1: Overview* *Volume 2: Hardware Asset Management*	February 2016

FINAL APPROVED PUBLICATIONS

TABLE 6: NO FIPS PUBLISHED IN FY 2016

TABLE 7: FINAL - SPs		
PUBLICATION NUMBER	**PUBLICATION TITLE**	**RELEASE DATE**
SP 800-183	*Networks of 'Things'*	July 2016
SP 800-182	*Computer Security Division 2015 Annual Report*	July 2016
SP 800-177	*Trustworthy Email*	September 2016
SP 800-175A	*Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*	August 2016
SP 800-175B	*Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*	August 2016
SP 800-171 (update)	*Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*	January 2016
SP 800-167	*Guide to Application Whitelisting*	October 2015
SP 800-166	*Derived PIV Application and Data Model Test Guidelines*	June 2016
SP 800-156	*Representation of PIV Chain-of-Trust for Import and Export*	May 2016
SP 800-152	*A Profile for U.S. Federal Cryptographic Key Management Systems*	October 2015
SP 800-131A Rev. 1	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*	November 2015
SP 800-125B	*Secure Virtual Network Configuration for Virtual Machine (VM) Protection*	March 2016
SP 800-114 Rev. 1	*User's Guide to Telework and Bring Your Own Device (BYOD) Security*	July 2016
SP 800-85A-4	*PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)*	April 2016
SP 800-73-4 (update)	*Interfaces for Personal Identity Verification*	February 2016
SP 800-70 Rev. 3	*National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*	December 2015
SP 800-57 Part 1 Rev. 4	*Recommendation for Key Management, Part 1: General*	January 2016
SP 800-46 Rev. 2	*Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*	July 2016
SP 800-38G	*Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*	March 2016 (and updated August 2016)
SP 500-316	*Framework for Cloud Usability*	December 2015

TABLE 8: FINAL - NISTIRs

PUBLICATION NUMBER	PUBLICATION TITLE	RELEASE DATE
NISTIR 8150	*Government Data De-Identification Stakeholder's Meeting, Meeting Report*	September 2016
NISTIR 8135	*Identifying and Categorizing Data Types for Public Safety Mobile Applications: Workshop Report*	May 2016
NISTIR 8113	*SATE V Ockham Sound Analysis Criteria*	March 2016
NISTIR 8105	*Report on Post-Quantum Cryptography for Public Comment*	March 2016
NISTIR 8103	*Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps*	September 2016
NISTIR 8101	*A Rational Foundation for Software Metrology*	January 2016
NISTIR 8080	*Usability and Security Considerations for Public Safety Mobile Authentication*	July 2016
NISTIR 8074 Volumes 1 & 2	*Volume 1: Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* *Volume 2: Supplemental Information*	December 2015
NISTIR 8060	*Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*	April 2016
NISTIR 8055	*Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research*	January 2016
NISTIR 8054 (update)	*NSTIC Pilots: Catalyzing the Identity Ecosystem*	March 2016
NISTIR 8053	*De-Identification of Personal Information*	October 2015
NISTIR 8040	*Measuring the Usability and Security of Permuted Passwords on Mobile Platforms*	April 2016
NISTIR 7987 Rev. 1	*Policy Machine: Features, Architecture, and Specification*	October 2015
NISTIR 7977	*NIST Cryptographic Standards and Guidelines Development Process*	March 2016
NISTIR 7966	*Security of Interactive and Automated Access Management Using Secure Shell (SSH)*	October 2015
NISTIR 7904	*Trusted Geolocation in the Cloud: Proof of Concept Implementation*	December 2015
NISTIR 7511 Rev. 4	*Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*	January 2016

TABLE 9: ITL BULLETINS	
PUBLICATION DATE	**BULLETIN TITLE**
September 2016	*Demystifying the Internet of Things*
August 2016	*NIST Updates Personal Identity Verification (PIV) Guidelines*
July 2016	*Improving Security and Software Management Through the Use of SWID Tags*
June 2016	*Extending Network Security into Virtualized Infrastructure*
May 2016	*Combinatorial Testing for Cybersecurity and Reliability*
April 2016	*New NIST Security Standard Can Protect Credit Cards, Health Information*
March 2016	*Updates to the NIST SCAP Validation Program and Associated Test Requirements*
February 2016	*Implementing Trusted Geolocation Services in the Cloud*
January 2016	*Securing Interactive and Automated Access Management Using Secure Shell (SSH)*
December 2015	*Stopping Malware and Unauthorized Software through Application Whitelisting*
November 2015	*Tailoring Security Controls for Industrial Control Systems*
October 2015	*Protection of Controlled Unclassified Information*

Other NIST Publications

NIST released other publications in FY 2016, as "White Papers," and as Concept Papers and Project Descriptions from NCCoE.

TABLE 10: OTHER NIST PUBLICATIONS (CONCEPT PAPERS, PROJECT DESCRIPTIONS, AND WHITE PAPERS) POSTED FOR PUBLIC COMMENT		
PUBLICATION TYPE	**PUBLICATION TITLE**	**RELEASE DATE**
Concept Paper (Draft)	*Identity and Access Management for Smart Home Devices*	June 2016
Project Description (Draft)	*Authentication for Law Enforcement Vehicle Systems*	*September 2016*
Project Description (Final) (Draft)	*Data Integrity: Recovering from a Destructive Malware Attack*	May 2016 December 2015
Project Description (Final)	*Domain Name System-Based Security for Electronic Mail*	March 2016
Project Description (Draft)	*Mobile Application Single Sign-on: for Public Safety and First Responders*	July 2016
Project Description (Draft)	*Multifactor Authentication for e-Commerce: Online Authentication for the Retail Sector*	May 2016
Project Description (Draft)	*Securing Non-Credit Card, Sensitive Consumer Data: Consumer Data Security for the Retail Sector*	May 2016
White Paper (Draft)	*Baldrige Cybersecurity Excellence Builder (BCEB): Key questions for improving your organization's cybersecurity performance*	September 2016
White Paper (Final) (Draft)	*Best Practices for Privileged User PIV Authentication*	April 2016 February 2016
White Paper (Draft)	*Cybersecurity Framework Manufacturing Profile*	September 2016

ITL CYBERSECURITY PROGRAM RELATED PUBLICATIONS

During FY 2016, the ITL staff authored a significant number of standards, guidelines, recommendations and other research papers. These were published as NIST technical series documents (e.g., Federal Information Processing Standards (FIPS), Special Publications (SP), NIST Internal or Interagency Reports (NISTIRs), and Information Technology Laboratory (ITL) Bulletins), other NIST publications, or as externally-published documents (e.g., journal articles, conference papers, books, and other papers).

Additionally, the NCCoE began posting public drafts of documents in two new series: Concept Papers and Project Descriptions. Concept Papers identify potential project topics for NCCoE to explore with stakeholders and technology collaborators. After reviewing public comments on a draft Concept Paper, NCCoE can better understand specific challenges and needs, and may possibly draft a Project Description. Formerly issued as "Building Blocks" and "Use Cases," Project Descriptions describe a particular problem that is relevant across a sector. Through collaboration with community members and vendors of cybersecurity solutions, NCCoE will develop a reference design that can be used by sector organizations to address that challenge.

In FY 2016, ITL published 20 NIST Special Publications, 18 NISTIRs and 12 ITL Bulletins in the areas of cybersecurity and privacy. Additionally, ITL continued to engage stakeholders by posting numerous draft documents for public comment, including 23 Special Publications, 13 NISTIRs, 6 NCCoE Project Descriptions, 1 NCCoE Concept Paper, and 3 NIST "white papers." ITL research was also published externally, as 18 journal articles and 18 conference papers. They are listed below, with abstracts and full text links, under (External Publications).

In the October 19, 2015 *Federal Register*, NIST announced the withdrawal of six FIPS that had become obsolete: FIPS 181, 185, 188, 190, 191, and 196. NIST had received only one comment in response to a January 16, 2015 *Federal Register Notice* requesting public feedback on their proposed withdrawal. (The titles of the withdrawn FIPS are: 181 - *Automated Password Generator (APG)*, 185 - *Escrowed Encryption Standard*, 188 - *Standard Security Label for Information Transfer*, 190 - Guideline for the Use *of Advanced Authentication Technology Alternatives*, 191 - *Guideline for The Analysis of Local Area Network Security*, and 196 - *Entity Authentication Using Public Key Cryptography*.)

Two significant efforts to revise major publications were begun. ACD solicited public input to develop preliminary drafts of SP 800-63-3, *Digital Authentication Guideline*, during a "Public Preview" phase that enabled stakeholders to provide dynamic, interactive feedback. A subseries of documents that will revise the current SP 800-63-2, *Electronic Authentication Guideline*, will be posted for public comment as official public drafts in early FY 2017 (see https://pages.nist.gov/800-63-3/). Meanwhile, CSD posted a call for comments on SP 800-53 Revision 4, S*ecurity and Privacy Controls for Federal Information Systems and Organizations*, to begin preparing for the release of a draft of Revision 5 for public comment in FY 2017.

The ITL Cybersecurity Framework team worked closely with the Baldrige Performance Excellence Program to develop the *Baldrige Cybersecurity Excellence Builder (BCEB): Key questions for improving your organization's cybersecurity performance*, which was posted for public comment on the Baldridge Cybersecurity Initiative website (see https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative). The BCEB is a voluntary self-assessment tool that enables organizations to better understand the effectiveness of their cybersecurity risk management efforts.

Top Downloads

Publications are available for download from CSRC (see http://csrc.nist.gov/publications/), the NCCoE website (see https://nccoe.nist.gov/library) and the main NIST Publications site (see https://www.nist.gov/publications/). The following lists summarize the most-downloaded ITL publications for FY 2016, using weblog data (and excluding traffic from spiders and web crawlers):

Top 10 Most-Downloaded Publications (with estimated number of downloads):

1. SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (303,162);
2. SP 800-145, *The NIST Definition of Cloud Computing* (235,191);
3. *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0 (180,163);
4. SP 800-61 Revision 2, *Computer Security Incident Handling Guide* (153,723);
5. SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* (116,991);

6. SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (112,104);
7. FIPS 197, *Advanced Encryption Standard (AES)* (108,162);
8. SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (81,887);
9. SP 800-12, *An Introduction to Computer Security: the NIST Handbook* (81,768); and
10. SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (80,960).

Top 3 FIPS:

1. FIPS 197, *Advanced Encryption Standard (AES)* (108,162);
2. FIPS 140-2, *Security Requirements for Cryptographic Modules* (79,565); and
3. FIPS 199, *Standards for Security Categorization of Federal Information and information Systems* (70,846).

Top 3 NISTIRs:

1. NISTIR 7298 Rev. 2, *Glossary of Key Information Security Terms* (36,110);
2. NISTIR 7316, *Assessment of Access Control Systems* (19,902); and
3. NISTIR 8053, *De-Identification of Personal Information* (17,970).

Top 3 ITL Bulletins:

1. *The System Development Life Cycle (SDLC)*, April 2009 (46,298);
2. *Cloud Computing: A Review of Features, Benefits, and Risk, and Recommendations for Secure, Efficient Implementations*, June 2012 (7,309); and
3. *New NIST Security Standard Can Protect Credit Cards, Health Information*, April 2016 (6,150).

FY 2017 Plans

ITL will continue to publish its research in the publication series mentioned here. Additionally, ITL is developing a new version of CSRC—planned for release in FY 2017—that will significantly improve information about its cybersecurity and privacy publications, including features such as advanced searching and filtering; abstracts, keywords, and authors; links to superseding/superseded versions of publications; and a significantly more robust taxonomy of topical headings to help users easily find related content (including publications) on the CSRC website. More publication-related features will be added incrementally after the website's initial rollout.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

Mr. Jim Foti	Mr. Patrick O'Reilly
(301) 975-8018	(301) 975-4751
james.foti@nist.gov	patrick.oreilly@nist.gov

NIST Technical Series Publications and Other NIST Publications

The following tables list NIST Technical Series publications and other NIST publications released by ITL on CSRC—either as draft or final publications—during FY 2016 (from October 1, 2015 to September 30, 2016). Abstracts and links to the full text of these publications are provided in the sections that follow.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

ABSTRACTS OF PUBLICATIONS RELEASED IN FY 2016

The following sections provide abstracts of NIST SPs, security-related NISTIRs, and other NIST publications listed in the previous section. If a publication was released as a draft *and* final publication during FY 2016, only the final publications are listed below. Any updated publications with minor technical or editorial changes, identified in the tables above as "updates," are not listed below. Technical reports are listed in reverse numerical order by report number; other documents are listed alphabetically by title.

NIST SPs

SP 800-188 (DRAFT)

De-Identifying Government Datasets

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-188

De-identification removes identifying information from a dataset so that the remaining data cannot be linked with specific individuals. Government agencies can use de-identification to reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing government data. Previously, NIST published NISTIR 8053, "De-Identifying Personal Data," which provided a survey of de-identification and re-identification techniques. This document provides specific guidance to government agencies that wish to use de-identification. Before using de-identification, agencies should evaluate their goals in using de-identification and the potential risks that de-identification might create. Agencies should decide upon a de-identification release model, such as publishing de-identified data, publishing synthetic data based on identified data, and providing a query interface to the identified data that incorporates de-identification. Agencies can use a Disclosure Review Board to oversee the process of de-identification; they can also adopt a de-identification standard with measurable performance levels. Several specific techniques for de-identification are available, including de-identification by removing identifiers and transforming quasi-identifiers and the use of formal de-identification models that rely upon Differential Privacy. De-identification is typically performed with software tools that may have multiple features; however, not all tools that mask personal information provide sufficient functionality for performing de-identification. This document also includes an extensive list of references, a glossary, and a list of specific de-identification tools, although the mention of these tools is only to be used to convey the range of tools currently available, and is not intended to imply recommendation or endorsement by NIST.

SP 800-185 (DRAFT)

SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-185

This Recommendation specifies four SHA-3-derived functions: cSHAKE, KMAC, TupleHash, and ParallelHash. cSHAKE is a customizable variant of the SHAKE functions defined in FIPS 202. KMAC (for KECCAK Message Authentication Code) is a variable-length message authentication code algorithm based on KECCAK; it can also be used as a pseudorandom function. TupleHash is a variable-length hash function that is designed to hash tuples of input strings unambiguously. ParallelHash is a variable-length hash function that can hash non-overlapping subsets of very long messages in parallel.

SP 800-184 (DRAFT)

Guide for Cybersecurity Event Recovery

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-184

In light of an increasing number of cybersecurity events, organizations can improve resilience by ensuring that their risk management processes include comprehensive recovery planning. Identifying and prioritizing organization resources helps to guide effective plans and realistic test scenarios. This preparation enables rapid recovery from incidents when they occur and helps to minimize the impact on the organization and its constituents. Additionally, continually improving recovery planning by learning lessons from past events, including those of other organizations, helps to ensure the continuity of important mission functions. This publication provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning. It also provides an example scenario that demonstrates guidance and informative metrics that may be helpful for improving resilience of the information systems.

SP 800-183

Networks of 'Things'

https://doi.org/10.6028/NIST.SP.800-183

[This was originally released for public comment as draft NISTIR 8063, *Internet of Things (IoT) Trustworthiness*, in February 2016.]

System primitives allow formalisms, reasoning, simulations, and reliability and security risk-tradeoffs to be formulated and argued. In this work, five core primitives belonging to most distributed systems are presented. These primitives apply well to systems with large amounts of data, scalability concerns, heterogeneity concerns, temporal concerns, and elements of unknown pedigree with possible nefarious intent. These primitives are the basic building blocks for a Network of 'Things' (NoT), including the Internet of Things (IoT). This document offers an underlying and foundational understanding of IoT based on the realization that IoT involves sensing, computing, communication, and actuation. The material presented here is generic to all distributed systems that employ IoT technologies (i.e., 'things' and networks). The expected audience is computer scientists, IT managers, networking specialists, and networking and cloud computing software engineers.

SP 800-182

Computer Security Division 2015 Annual Report

https://doi.org/10.6028/NIST.SP.800-182

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 those 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 2015, 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 2015.

SP 800-180 (DRAFT)

NIST Definition of Microservices, Application Containers and System Virtual Machines

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-180

Many variations and definitions of application containers exist in industry, causing considerable confusion among those who attempt to explain what a container is. This document provides a NIST-standard definition to application containers, microservices that reside in application containers and operating system virtual machines. Furthermore, this document explains the similarities and differences between a Services Oriented Architecture (SOA) and Microservices, as well as the similarities and differences between Operating System Virtual Machines and Application Containers.

SP 800-179 (DRAFT)

Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-179

This publication assists IT professionals in securing Apple OS X 10.10 (i.e., Yosemite) desktop and laptop systems within various environments. It provides detailed information about the security features of OS X 10.10 and security configuration guidelines. The publication recommends and explains tested, secure settings with the objective of simplifying the administrative burden of improving the security of OS X 10.10 systems in three types of environments: Standalone, Managed, and Specialized Security-Limited Functionality.

SP 800-177

Trustworthy Email

https://doi.org/10.6028/NIST.SP.800-177

This document gives recommendations and guidelines for enhancing trust in email. The primary audience includes enterprise email administrators, information security specialists and network managers. This guideline applies to federal IT systems and will also be useful for small or medium-sized organizations. Technologies recommended in support of core Simple Mail Transfer Protocol (SMTP) and the Domain Name System (DNS) include mechanisms for authenticating a sending domain: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC). Recommendations for email transmission security include the Transport Layer Security (TLS) protocols and the associated certificate authentication protocols. Recommendations for email content security include the encryption and authentication of message content using S/MIME (Secure/Multipurpose Internet Mail Extensions) and the associated certificate and key distribution protocols.

SP 800-175A

Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies

https://doi.org/10.6028/NIST.SP.800-175A

This document is part of a series intended to provide guidance to the Federal Government for using cryptography and NIST's cryptographic standards to protect sensitive, but unclassified digitized information during transmission and while in storage. SP 800-175A provides guidance on the determination of requirements for using cryptography. It includes a summary of laws and regulations concerning the protection of the Federal Government's sensitive information, guidance regarding the conduct of risk assessments to determine what needs to be protected and how best to protect that information, and a discussion of the relevant security-related documents (e.g., various policy and practice documents).

SP 800-175B

Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

https://doi.org/10.6028/NIST.SP.800-175B

This document is intended to provide guidance to the Federal Government for using cryptography and NIST's cryptographic standards to protect sensitive, but unclassified digitized information during transmission and while in storage. The cryptographic methods and services to be used are discussed.

SP 800-171 Revision 1 (DRAFT)

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-171-Rev-1

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully carry out its designated missions and business operations. This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI: (i) when the CUI is resident in nonfederal information systems and organizations; (ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and (iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry. The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

SP 800-167

Guide to Application Whitelisting

https://doi.org/10.6028/NIST.SP.800-167

An application whitelist is a list of applications and application components that are authorized for use in an organization. Application whitelisting technologies use whitelists to control which applications are permitted to be executed 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.

SP 800-166

Derived PIV Application and Data Model Test Guidelines

https://doi.org/10.6028/NIST.SP.800-166

SP 800-157 contains technical guidelines for the implementation of standards-based, secure, reliable, interoperable PKI-based identity credentials that are issued for mobile devices by federal departments and agencies to individuals who possess and prove control over a valid PIV Card. This document, SP 800-166, contains the requirements and test assertions for testing the Derived PIV Application and associated Derived PIV data objects implemented on removable hardware tokens and within mobile devices. The tests reflect the design goals of interoperability and interface functions.

SP 800-160 (2 Drafts)

Systems Security Engineering Guideline: An Integrated Approach to Building Trustworthy Resilient Systems

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-160

This publication addresses the engineering-driven actions necessary to develop more defensible and survivable systems—including the components that compose and the services that depend on those systems. It starts with and builds upon a set of well-established International Standards for systems and software engineering published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE), and infuses systems security engineering techniques, methods, and practices into those systems and software engineering processes. The ultimate objective is to address security issues from the perspective of stakeholder requirements and protection needs and to use established engineering processes to ensure that such requirements and needs are addressed with appropriate fidelity and rigor early and in a sustainable manner throughout the life cycle of the system.

SP 800-156

Representation of PIV Chain-of-Trust for Import and Export

https://doi.org/10.6028/NIST.SP.800-156

This document provides a common XML-based data representation of a chain-of-trust record to facilitate the exchange of PIV Card enrollment data. The exchanged record is the basis for personalizing a PIV Card for a transferred employee and, also for service providers to personalize a PIV Card on behalf of client federal agencies.

SP 800-154 (DRAFT)

Guide to Data-Centric System Threat Modeling

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-154

Threat modeling is a form of risk assessment that models aspects of the attack and defense sides of a particular logical entity, such as a piece of data, an application, a host, a system, or an environment. This publication examines data-centric system threat modeling, which is threat modeling that is focused on protecting particular types of data within systems. The publication provides information on the basics of data-centric system threat modeling so that organizations can successfully use it as part of their risk management processes. The general methodology provided by the publication is not intended to replace existing methodologies, but rather to define fundamental principles that should be part of any sound data-centric system threat modeling methodology.

SP 800-152

A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)

https://doi.org/10.6028/NIST.SP.800-152

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)*.

SP 800-150 (2nd Draft)

Guide to Cyber Threat Information Sharing

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-150

Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Cyber threat information includes indicators of compromises; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents. Organizations that share cyber threat information can improve their own security postures as well as those of other organizations. This publication provides guidelines for establishing and participating in cyber threat information-sharing relationships. This guidance helps organizations establish information sharing goals, identify cyber threat information sources, scope information sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of their overall cybersecurity practices.

SP 800-131A Revision 1

Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

https://doi.org/10.6028/NIST.SP.800-131Ar1

At the start of the 21st century, NIST began the task of providing cryptographic key management guidance, which includes defining and implementing appropriate key management procedures, using algorithms that adequately protect sensitive information, and planning ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. SP 800-57, Part 1 was the first document produced in this effort, and includes a general approach for transitioning from one algorithm or key length to another. This Recommendation (SP 800-131A) provides more specific guidance for transitions to the use of stronger cryptographic keys and more robust algorithms.

SP 800-126 Revision 3 (DRAFT)

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-126-Rev-3

The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. This publication defines the technical composition of SCAP version 1.3 in terms of its component specifications, their interrelationships and interoperation, and the requirements for SCAP content.

SP 800-126A (DRAFT)

SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-126A

The Security Content Automation Protocol (SCAP) is a multi-purpose framework of component specifications that support automated configuration, vulnerability, and patch checking, security measurement, and technical control compliance activities. The SCAP version 1.3 specification is defined by the combination of SP 800-126 Revision 3 and this document. This document allows the use of particular minor version updates to SCAP 1.3 component specifications and the use of particular Open Vulnerability and Assessment Language (OVAL) core schema and platform schema versions. Allowing the use of these updates and schemas provides additional functionality for SCAP 1.3 without causing any loss of existing functionality.

SP 800-125B

Secure Virtual Network Configuration for Virtual Machine (VM) Protection

https://doi.org/10.6028/NIST.SP.800-125B

Virtual machines (VMs) are key resources to be protected, since they are the compute engines hosting mission-critical applications. Since VMs are the end nodes of a virtual network, the configuration of the virtual network is an important element in the security of the VMs and their hosted applications. The virtual network configuration areas discussed in this document are network segmentation, network path redundancy, traffic control using firewalls, and VM traffic monitoring. This document analyzes the configuration options under these areas and presents a corresponding set of recommendations for secure virtual network configuration for VM protection.

SP 800-116 Revision 1 (DRAFT)

A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-116-Rev.%201

This recommendation provides a technical guideline to use Personal Identity Verification (PIV) Cards in physical access control systems (PACS), enabling federal agencies to operate as government-wide interoperable enterprises. This recommendation covers the risk-based strategy to select appropriate PIV authentication mechanisms as expressed within Federal Information Processing Standard (FIPS) 201-2.

SP 800-114 Revision 1

User's Guide to Telework and Bring Your Own Device (BYOD) Security

https://doi.org/10.6028/NIST.SP.800-114r1

Many people telework, and they use a variety of devices, such as desktop and laptop computers, smartphones, and tablets, to read and send email, access websites, review and edit documents, and perform many other tasks. Each telework device is controlled by the organization, a third party (such as the organization's contractors, business partners, and vendors), or the teleworker; the latter is known as bring your own device (BYOD). This publication provides recommendations for securing BYOD devices used for telework and remote access, as well as those directly attached to the enterprise's own networks.

SP 800-90B (2nd Draft)

Recommendation for the Entropy Sources Used for Random Bit Generation

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-90-B

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

SP 800-90C (2nd Draft)

Recommendation for Random Bit Generator (RBG) Constructions

http://csrc.nist.gov/publications/PubsSPs.html#SP-800-90-C

This Recommendation specifies constructions for the implementation of random bit generators (RBGs). An RBG may be a deterministic random bit generator (DRBG) or a non-deterministic random bit generator (NRBG). The constructed RBGs consist of DRBG mechanisms, as specified in SP 800-90A, and entropy sources, as specified in SP 800-90B.

SP 800-85A-4

PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)

https://doi.org/10.6028/NIST.SP.800-85A-4

SP 800-73 contains the technical specifications to interface with the smart card to retrieve and use the PIV identity credentials. This document, SP 800-85A, contains the test assertions and test procedures for testing smart card middleware as well as the card application. The tests reflect the design goals of interoperability and PIV Card functions.

SP 800-70 Revision 3

National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

https://doi.org/10.6028/NIST.SP.800-70r3

A security configuration checklist is a document that contains instructions or procedures for configuring an IT product for an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected. To facilitate the development of checklists and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). This publication explains how to use the NCP to find and retrieve checklists, and it also describes the policies, procedures, and general requirements for participation in the NCP.

SP 800-57 Part 1 Revision 4

Recommendation for Key Management, Part 1: General

https://doi.org/10.6028/NIST.SP.800-57pt1r4

This publication provides general cryptographic key management guidance and is the first of three parts. Part 1 defines cryptographic security services that may be provided, provides background information regarding the NIST-approved cryptographic algorithms, classifies keys and other cryptographic information according to their functions, specifies the protections required for each key type, identifies the functions involved in key management and discusses a variety of key management issues related to the use of keys. Part 2 provides guidance on policy and security planning requirements for U.S. government agencies, and Part 3 provides guidance when using the cryptographic features of current systems.

SP 800-46 Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

https://doi.org/10.6028/NIST.SP.800-46r2

For many organizations, their employees, contractors, business partners, vendors, and/or others use enterprise telework or remote access technologies to perform work from external locations. All components of these technologies, including organization-issued BYOD client devices, should be secured against expected threats as identified through threat models. This publication provides information on security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework, remote access, and BYOD technologies. It also gives advice on creating related security policies.

SP 800-38G

Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption

https://doi.org/10.6028/NIST.SP.800-38G

This Recommendation specifies two methods, called FF1 and FF3, for format-preserving encryption (FPE). Both of these methods are modes of operation for an underlying, approved symmetric-key block cipher algorithm. FPE transforms data that is formatted as a sequence of symbols (e.g., a sequence of decimal numbers) so that the encrypted form of the data has the same format and length as the original plaintext data. Thus, an FPE-encrypted Social Security Number would be a sequence of nine decimal digits, rather than a sequence of symbols that may not be decimal numbers and would very likely be longer than the original plaintext, as is the case for other encryption modes.

SP 500-316

Framework for Cloud Usability

https://doi.org/10.6028/NIST.SP.500-316

Organizations are increasingly adopting cloud-based services to meet their business needs. However, due to the complexity and diversity of cloud systems it is important to evaluate the user experience using within a framework that encompasses the characteristics that define the user experience. In this paper, we propose a cloud usability framework to provide a structure to evaluate the key attributes of the cloud user experience. The framework includes five attributes and 19 elements that characterize this user experience. Generally these describe the consumer's expectations of the cloud. The framework can be the foundation for developing usability metrics for organizations interested in measuring the user experience when adopting the cloud.

SP 1800-5 (DRAFT)

IT Asset Management: Financial Services

http://csrc.nist.gov/publications/PubsSPs.html#SP-1800-5

While a physical asset management system can tell you the location of a computer, it cannot answer questions like, "What operating systems are our laptops running?" and "Which devices are vulnerable to the latest threat?" An effective IT asset management (ITAM) solution can tie together physical and virtual assets and provide management with a complete picture of what, where, and how assets are being used. ITAM enhances visibility for security analysts, which leads to better asset utilization and security. This NIST Cybersecurity Practice Guide provides a reference build of an ITAM solution. The build contains descriptions of the architecture, all products used in the build and their individual configurations. Additionally, this guide provides a mapping of each product to multiple relevant security standards. While the reference solution was demonstrated with a certain suite of products, the guide does not endorse these specific products. Instead, it presents the characteristics and capabilities of the products that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with a financial service company's existing tools and infrastructure.

SP 1800-4 (DRAFT)

Mobile Device Security: Cloud and Hybrid Builds

http://csrc.nist.gov/publications/PubsSPs.html#SP-1800-4

This document proposes a reference design on how to architect enterprise-class protection for mobile devices accessing an organization's resources. The example solutions presented here can be used by any organization implementing an enterprise mobility management solution. This project contains two distinct builds: cloud and hybrid. The cloud build uses cloud-based services and solutions, while the hybrid build achieves the same functionality, but hosts at least some of the data and services within an enterprise's own infrastructure. The example solutions and architectures presented here are based on open standards and commercially available products.

NISTIRs

NISTIR 8150

Government Data De-Identification Stakeholder's Meeting, Meeting Report

https://doi.org/10.6028/NIST.IR.8150

The first Government Data De-Identification Stakeholder's Meeting was held at the National Institute of Standards and Technology on June 29, 2016. This meeting featured 80 participants from 67 different government agencies. Following the keynote, five panels discussed agency case studies, agency needs, available solutions, governance, and evaluation of de-identification techniques. Eighteen presenters from eleven agencies spoke for 10-minutes each. After each speaker's presentation, audience members asked questions and elaborated on points that the speakers made. Overall, it was the sense of the attendees that there is a need for collaboration and the sharing of techniques for the de-identification of government data.

NISTIR 8144 (DRAFT)

Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue

http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8144

Mobile devices pose a unique set of threats, yet typical enterprise protections fail to address the larger picture. To fully address the threats presented by mobile devices, a wider view of the mobile security ecosystem is necessary. This document discusses the Mobile Threat Catalogue, which describes, identifies, and structures the threats posed to mobile information systems.

NISTIR 8138 (DRAFT)

Vulnerability Description Ontology (VDO): a Framework for Characterizing Vulnerabilities

http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8138

This document aims to describe a more effective and efficient methodology for characterizing the vulnerabilities found in various forms of software and hardware implementations, including, but not limited to, information technology systems, industrial control systems or medical devices to assist in the vulnerability management process. The primary goal of the described methodology is to enable automated analysis using metrics such as the Common Vulnerability Scoring System (CVSS). Additional goals include establishing a baseline of the minimum information needed to properly inform the vulnerability management process, and facilitating the sharing of vulnerability information across language barriers.

NISTIR 8136 (DRAFT)

Mobile Application Vetting Services for Public Safety: an Informal Survey

http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8136

The Middle Class Tax Relief Act of 2012 mandated the creation of the Nation's first nationwide, high-speed communications network dedicated for public safety. The law instantiated a new federal entity, the Federal Responder Network Authority (FirstNet), to build, maintain, and operate a new Long Term Evolution (LTE) network. This network has the potential to equip first responders with a modern array of network devices. Mobile applications stand to be an important resource that will be utilized by this network. However, current mobile application developers may not be equipped with the unique needs and requirements that must be met for operation on FirstNet's network. It would benefit the public safety community to leverage the mobile application vetting services and infrastructures that already exist. These services currently target the general public and enterprise markets. The purpose of this document is to be an overview of existing mobile application vetting services, the features these services provide and how they relate to public safety's needs. This document is intended to aid public safety organizations when selecting mobile application vetting services for use in analyzing mobile applications.

NISTIR 8135

Identifying and Categorizing Data Types for Public Safety Mobile Applications: Workshop Report

https://doi.org/10.6028/NIST.IR.8135

The Association of Public-Safety Communications Officials (APCO), in cooperation with FirstNet and the Department of Commerce held a half-day workshop on June 2, 2015, "Identifying and Categorizing Data Types for Public Safety Mobile Applications." The goal of this workshop was to begin identifying different types of data that will flow through applications that operate on the National Public Safety Broadband Network (NPSBN). A diverse group of first responders, industry leaders, and government representatives attended the workshop. This document describes the workshop and captures the input received from the workshop attendees.

NISTIR 8114 (DRAFT)

Report on Lightweight Cryptography

http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8114

NIST-approved cryptographic standards are designed to perform well using general-purpose computers. In recent years, there has been an increased deployment of small computing devices that have limited resources with which to implement cryptography. When current NIST-approved algorithms can be engineered to fit into the limited resources of constrained environments, their performance may not be acceptable. For these reasons, NIST started a lightweight cryptography project that was tasked with learning more about the issues and developing a strategy for the standardization of lightweight

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

cryptographic algorithms. This report provides an overview of the lightweight cryptography project at NIST, and describes plans for the standardization of lightweight cryptographic algorithms.

NISTIR 8113

SATE V Ockham Sound Analysis Criteria

https://doi.org/10.6028/NIST.IR.8113

Static analyzers examine the source or executable code of programs to find problems. Many static analyzers use some heuristics or approximations to handle programs up to millions of lines of codes. We established the Ockham Sound Analysis Criteria to recognize static analyzers whose findings are always correct. In brief the criteria are (1) the analyzer's findings are claimed to always be correct, (2) it produces findings for most of a program, and (3) even one incorrect finding disqualifies an analyzer. This document begins by explaining the background and requirements of the Ockham Criteria in more detail. In Static Analysis Tool Exposition (SATE) V, one tool, Frama-C, examined pertinent parts of the Juliet 1.2 test suite to participate. We reviewed eight classes of warnings, including improper buffer access, NULL pointer dereference, integer overflow, and others. This document details the many technical and theoretical challenges we addressed to classify and review the warnings against the Criteria. It also reports anomalies, our observations, and interpretations. Frama-C reports led to the discovery of three unintentional, systematic flaws in the Juliet test suite involving 416 test cases. Our conclusion is that Frama-C satisfied the SATE V Ockham Sound Analysis Criteria.

NISTIR 8112 (DRAFT)

Attribute Metadata

http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8112

This NIST Internal Report contains a metadata schema for attributes that may be asserted about an individual during an online transaction. The schema can be used by relying parties to enrich access control policies, as well as during runtime evaluation of an individual's ability to access protected resources. Attribute metadata could also create the possibility for data sharing permissions and limitations on individual data elements. There are other possible applications of attribute metadata, such as the evaluation and execution of business logic in decision support systems; however, the metadata contained in this document is focused on supporting an organization's risk-informed authorization policies and evaluation.

NISTIR 8105

Report on Post-Quantum Cryptography

https://doi.org/10.6028/NIST.IR.8105

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. This Internal Report shares NIST's current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST's initial plan to move forward in this space. The report also recognizes the challenge of moving to new cryptographic infrastructures and, therefore, emphasizes the need for agencies to focus on crypto agility.

NISTIR 8103

Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps

https://doi.org/10.6028/NIST.IR.8103

On January 12-13, 2016, ACD hosted a workshop on "Applying Measurement Science in the Identity Ecosystem" to discuss the application of measurement science to digital identity management. This document summarizes the concepts and ideas presented at the workshop and serves as a platform to receive feedback on the major themes discussed at that event.

NISTIR 8101

A Rational Foundation for Software Metrology

https://doi.org/10.6028/NIST.IR.8101

Much software research and practice involves ostensible measurements of software, yet little progress has been made on an SI-like metrological foundation for those measurements since the work of Gray, Hogan, et al. in 1996-2001. Given a physical object, one can determine physical properties using measurement principles and express measured values using standard quantities that have concrete realizations. In contrast, most software metrics are simple counts that are used as indicators of complex, abstract qualities. In this report we revisit software metrology from two directions: first, top down, to establish a theory of software measurement; second, bottom up, to identify specific purposes for which software measurements are needed, quantifiable properties of software, relevant units, and objects of measurement. Although there are structural obstacles to realizing the vision of software metrology that works like physical metrology for all desired measurands, progress is possible if we start with a rational foundation.

NISTIR 8085 (DRAFT)

Forming Common Platform Enumeration (CPE) Names from Software Identification (SWID) Tags

http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8085

This report describes the association between the use of SWID Tags and the Common Platform Enumeration (CPE) specifications. The publication is intended as a supplement to NIST Internal Report 8060, *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*. Both SWID and CPE support automated and accurate software asset management. Such automation, in turn, helps organizations to minimize exposure to publicly disclosed software vulnerabilities, enforce organizational policies regarding authorized software, and control network resource access from potentially vulnerable endpoints. NISTIR 8085 provides guidance to support CPE naming using information from a SWID tag based on the International Organization for Standardization/International Electrotechnical Commission 19770-2:2015 standard.

NISTIR 8080

Usability and Security Considerations for Public Safety Mobile Authentication

https://doi.org/10.6028/NIST.IR.8080

There is a need for cybersecurity capabilities and features to protect the National Public Safety Broadband Network (NPSBN). However, cybersecurity requirements should not compromise the ability of first responders to complete their missions. In addition, the diversity of public safety disciplines means that one solution may not meet the usability and security needs of different disciplines. Understanding how public safety users operate in their different environments will allow for usable cybersecurity capabilities and features to be deployed and used. Although first responders work in a variety of disciplines, this report is focused on the Fire Service, Emergency Medical Services (EMS), and Law Enforcement. This report describes the constraints presented by their personal protective equipment (PPE), specialized gear, and unique operating environments and how such constraints may interact with mobile authentication requirements. The overarching goal of this work is analyzing which authentication solutions are the most appropriate and usable for first responders using mobile devices in operational scenarios in the field.

NISTIR 8074 (2 volumes)

Volume 1: *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*

https://doi.org/10.6028/NIST.IR.8074v1

This interagency report sets out proposed U.S. Government strategic objectives for pursuing the development and use of international standards for cybersecurity and makes recommendations to achieve those objectives. The recommendations cover interagency coordination, collaboration with the U.S. private sector and international partners, agency participation in international standards development, standards training and education, the use of international standards to achieve mission and policy objectives, and other issues.

Volume 2: *Supplemental Information*

https://doi.org/10.6028/NIST.IR.8074v2

This report provides background information and analysis in support of NISTIR 8074 Volume 1, “Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity.” It provides a current summary of ongoing activities in critical international cybersecurity standardization and an inventory of U.S. Government and U.S. private sector engagement. It also provides information for federal agencies and other stakeholders to help plan more effective participation in international cybersecurity standards development and related conformity assessment activities.

NISTIR 8071 (DRAFT)

LTE Architecture Overview and Security Analysis

http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8071

Cellular technology plays an increasingly large role in society, as it has become the primary portal to the Internet for a large segment of the population. One of the main drivers making this change possible is the deployment of 4th generation (4G) LTE cellular technologies. This document serves as a guide to the fundamentals of how LTE networks operate and explores the LTE security architecture. This is followed by an analysis of the threats posed to LTE networks and supporting mitigations.

NISTIR 8063 (DRAFT)

Primitives and Elements of Internet of Things (IoT) Trustworthiness

http://csrc.nist.gov/publications/drafts/nistir-8063/nistir_8063_draft.pdf

System primitives allow formalisms, reasoning, simulations, and reliability and security risk tradeoffs to be formulated and argued. In this document, five core primitives belonging to most distributed systems are presented. These primitives apply well to systems with large amounts of data, scalability concerns, heterogeneity concerns, temporal concerns, and elements of unknown pedigree with possible nefarious intent. These primitives form the basic building blocks for a Network of 'Things' (NoT), including the Internet of Things (IoT). This report offers an underlying and foundational science to IoT.

NISTIR 8060

Guidelines for the Creation of Interoperable Software Identification (SWID) Tags

https://doi.org/10.6028/NIST.IR.8060

This report provides an overview of the capabilities and usage of SWID tags as part of a comprehensive software lifecycle. As instantiated in the International Organization for Standardization/International Electrotechnical Commission 19770-2 standard, SWID tags support numerous applications for software asset management and information security management. This report introduces SWID tags in an operational context, provides guidelines for the creation of interoperable SWID tags, and highlights key usage scenarios for which SWID tags are applicable.

NISTIR 8055

Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research

https://doi.org/10.6028/NIST.IR.8055

This report documents proof-of-concept research for DPC. Smart card-based PIV Cards cannot be readily used with most mobile devices, such as smartphones and tablets, but DPC can be used instead to PIV-enable these devices and provide multi-factor authentication for mobile device users. This report captures existing requirements related to DPC, proposes an architecture that supports these requirements, and then demonstrates how such an architecture could be implemented and operated.

NISTIR 8053

De-Identification of Personal Information

https://doi.org/10.6028/NIST.IR.8053

De-identification removes identifying information from a dataset so that individual data cannot be linked with specific individuals. De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing information. De-identification attempts to balance the contradictory goals of using and sharing personal information while protecting privacy. Several U.S. laws, regulations and policies specify that data should be de-identified prior to sharing. In recent years, researchers have shown that some de-identified data can sometimes be re-identified. Many kinds of information can be de-identified, including structured information, free-format text, multimedia, and medical imagery. This document summarizes roughly two decades of de-identification research, discusses current practices, and presents opportunities for future research.

NISTIR 8040

Measuring the Usability and Security of Permuted Passwords on Mobile Platforms

https://doi.org/10.6028/NIST.IR.8040

Password entry on mobile devices significantly impacts both usability and security, but there is a lack of usable security research in this area, specifically for complex password entry. To address this research gap, we set out to assign strength metrics to passwords for which we already had usability data to have a more meaningful comparison between usability and security. This document reports a method of optimizing the input of randomly generated passwords on mobile devices via password permutation to allow for a comparison of password usability data. We found that the number of keystrokes saved—the efficiency gained—via permutation depends on the number of onscreen keyboard changes required in the original password rather than on password length. Additionally, we created and are releasing Python scripts (publicly available from https://github.com/usnistgov/PasswordMetrics) for the experiments on entropy loss we conducted across passwords ranging in length from 5 to 20 characters.

NISTIR 8011 (DRAFT; 2 volumes)

Automation Support for Security Control Assessments

NIST is pleased to announce the initial public draft release of NIST Internal Report (NISTIR) 8011, *Automation Support for Security Control Assessments*, Volumes 1 and 2. This NISTIR represents a joint effort between NIST and the Department of Homeland Security to provide an operational approach for automating security control assessments in order to facilitate information security continuous monitoring (ISCM), ongoing assessment, and ongoing security authorizations in a way that is consistent with the NIST Risk Management Framework overall and the guidance in NIST SPs 800-53 and 800-53A in particular.

NISTIR 8011 will ultimately consist of 13 volumes. Volume 1 introduces the general approach to automating security control assessments, 12 ISCM security capabilities, and terms and concepts common to all 12 capabilities. Volume 2 provides details specific to the hardware asset management security capability. The remaining 11 ISCM security capability volumes will provide details specific to each capability but will be organized in a very similar way to Volume 2.

Volume 1: *Overview*

http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf

Volume 1 of NISTIR 8011 introduces concepts to support an automated assessment of most of the security controls in SP 800-53. Referencing SP 800-53A, the controls are divided into more granular parts (determination statements) to be assessed. The parts of the control assessed by each determination statement are called control items. These control items are then grouped into the appropriate security capabilities. As suggested by SP 800-53 Revision 4, security capabilities are groups of controls that support a common purpose. For effective automated assessment, testable defect checks are defined that bridge the determination statements to the broader security capabilities to be achieved and to the SP 800-53 security control items themselves. The defect checks correspond to security sub-capabilities—called sub-capabilities because each is part of a larger capability. Capabilities and sub-capabilities are both designed with the purpose of addressing a series of attack steps. Automated assessments (in the form of defect checks) are performed using the test assessment method defined in SP 800-53A by comparing a desired and actual state (or behavior).

Volume 2: *Hardware Asset Management Assets*

http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-2.pdf

This document, Volume 2 of NISTIR 8011, addresses the Hardware Asset Management (HWAM) information security capability. The focus of the HWAM capability is to manage risk created by unmanaged devices on a network. Unmanaged devices are targets that attackers can use to gain and more easily maintain a persistent platform from which to attack the rest of the network.

NISTIR 7987 Revision 1

Policy Machine: Features, Architecture, and Specification

https://doi.org/10.6028/NIST.IR.7987r1

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.

NISTIR 7977

NIST Cryptographic Standards and Guidelines Development Process

https://doi.org/10.6028/NIST.IR.7977

This document describes the principles, processes and procedures that drive cryptographic standards and guidelines development efforts at NIST. This document reflects public comments received on two earlier versions, and will serve as the basis to guide NIST's future cryptographic standards and guidelines development efforts. It will be reviewed and updated every five years, or more frequently if a need arises, to help ensure that NIST fulfills its role and responsibilities for producing robust, effective cryptographic standards and guidelines.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

NISTIR 7966

Security of Interactive and Automated Access Management Using Secure Shell (SSH)

https://doi.org/10.6028/NIST.IR.7966

Users and hosts must be able to access other hosts in an interactive or 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 SSH protocol. The SSH protocol supports several mechanisms for interactive and automated authentication. The management of this access requires proper provisioning, termination, and monitoring processes. However, the security of SSH key-based access has been largely ignored to date. This publication assists organizations in understanding the basics of SSH interactive and automated access management in an enterprise, focusing on the management of SSH user keys.

NISTIR 7904

Trusted Geolocation in the Cloud: Proof of Concept Implementation

https://doi.org/10.6028/NIST.IR.7904

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

NISTIR 7511 Revision 4

Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements

https://doi.org/10.6028/NIST.IR.7511r4

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

ITL Bulletins

***Combinatorial Testing for Cybersecurity and Reliability* (May 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_05.pdf

This bulletin focuses on NIST's combinatorial testing work. Combinatorial testing is a proven method for more effective software testing at lower cost. The key insight underlying combinatorial testing's effectiveness resulted from a series of studies by NIST from 1999 to 2004. NIST research showed that most software bugs and failures are caused by one or two parameters, with progressively fewer by three or more.

***Demystifying the Internet of Things* (September 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_09.pdf

This bulletin summarizes the information presented in SP 800-183, *Networks of 'Things'*. This publication offers an underlying and foundational science to the IoT based on the realization that IoT involves sensing, computing, communication, and actuation.

***Extending Network Security into Virtualized Infrastructure* (June 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_06.pdf

This bulletin summarizes the information presented in SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*. That publication provides an analysis of various virtual network configuration options for the protection of VMs and presents recommendations based on the analysis.

***Implementing Trusted Geolocation Services in the Cloud* (February 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_02.pdf

The bulletin summarizes the information presented in NISTIR 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation*. The publication explains security challenges involving Infrastructure as a Service (IaaS) cloud computing technologies and geolocation.

Improving Security and Software Management Through the Use of SWID Tags **(July 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_07.pdf

This bulletin summarizes the information presented in NISTIR 8060, *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*. The publication provides an overview of the capabilities and usage of SWID tags as part of a comprehensive software lifecycle.

New NIST Security Standard Can Protect Credit Cards, Health Information **(April 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_04.pdf

This bulletin summarizes the information presented in SP 800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*, which specifies two methods for format-preserving encryption, FF1 and FF3.

NIST Updates Personal Identity Verification (PIV) Guidelines **(August 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_08.pdf

This bulletin summarizes the information presented in SP 800-156, *Derived PIV Application and Data Model Test Guidelines*, and SP 800-166, *Representation of PIV Chain-of-Trust for Import and Export*. These publications support FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which specifies the model for identity credentials that are hosted on a smart card (i.e., the PIV card) and/or on mobile devices (i.e., Derived PIV Credentials).

Protection of Controlled Unclassified Information **(October 2015)**

http://csrc.nist.gov/publications/nistbul/itlbul2015_10.pdf

This bulletin summarizes the information presented in SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. This publication explains why the protection of CUI while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully carry out its designated missions and business operations.

Securing Interactive and Automated Access Management Using Secure Shell (SSH) **(January 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_01.pdf

This bulletin summarizes the information presented in NISTIR 7966, *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*. The publication assists organizations in understanding the basics of SSH interactive and automated access management in an enterprise, focusing on the management of SSH user keys.

Stopping Malware and Unauthorized Software through Application Whitelisting **(December 2015)**

http://csrc.nist.gov/publications/nistbul/itlbul2015_12.pdf

This bulletin summarizes the information presented in SP 800-167, *Guide to Application Whitelisting*. The publication is intended to assist organizations in understanding the basics of application whitelisting. An application whitelist is a list of applications and application components that are authorized for use in an organization.

Tailoring Security Controls for Industrial Control Systems **(November 2015)**

http://csrc.nist.gov/publications/nistbul/itlbul2015_11.pdf

This bulletin summarizes the information presented in SP 800-82 Rev. 2, *Guide to Industrial Control Systems (ICS) Security*. The publication provides guidance on how to secure 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.

Updates to the NIST SCAP Validation Program and Associated Test Requirements **(March 2016)**

http://csrc.nist.gov/publications/nistbul/itlbul2016_03.pdf

This bulletin summarizes the information presented in NISTIR 7511 Rev. 4, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*. This is the fourth revision of the NISTIR that defines the requirements and associated test procedures necessary for products or modules to achieve one or more SCAP validations.

Concept Papers (NCCoE)

Identity and Access Management for Smart Home Devices (DRAFT)

https://nccoe.nist.gov/projects/project-concepts/idam-smart-home-devices

This concept paper identifies potential project topics for the National Cybersecurity Center of Excellence (NCCoE) to explore with stakeholders and technology collaborators. Through research and discussion, the NCCoE has identified several areas of interest within a broader cybersecurity subject, in this case, improved security for connected devices, or the "Internet of Things." Public comments on this concept paper will help the NCCoE understand specific challenges and needs, and may be used to help define a challenge statement, use cases, and/or a project description. Comments will be reviewed on an ongoing basis. Our hope is that stakeholders will help identify models, methodologies, protocols, best practices, or standards from other industries that may be relevant to securing smart home technology.

Project Descriptions (NCCoE)

Authentication for Law Enforcement Vehicle Systems (DRAFT)

https://nccoe.nist.gov/projects/use_cases/authentication-law-enforcement-vehicle-systems

Law enforcement vehicles often serve as mobile offices. In-vehicle laptops or other computer systems are used to access a wide range of software applications and databases hosted and operated by federal, state, and local agencies, with each typically requiring a different username and password. This operational environment presents unique security challenges. Officers must frequently leave the vehicle unattended, perhaps on short notice, and must be able to gain access to systems quickly once they return or possibly while the vehicle is in motion. These needs discourage the use of screen locks and traditional single sign-on solutions. This project demonstrated an integrated set of authentication mechanisms, improving system security, usability, and safety. This project also explored additional capabilities, such as proximity authentication, Distributed Control System (DPC) integration with First Responder Network Authority (FirstNet), and integration with vehicle drive-away protection and Computer Assisted Dispatch systems to indicate whether the officer is in the vehicle. This project will result in a freely available NIST Cybersecurity Practice Guide that will enable members of the community to more easily and effectively incorporate proximity access and reduced-sign-on technologies.

Data Integrity: Recovering from a Destructive Malware Attack

https://nccoe.nist.gov/projects/building_blocks/data_integrity

Threats of destructive malware, malicious insider activity, and even honest mistakes create the imperative for organizations to be able to quickly recover from an event that alters or destroys any form of data (database records, system files, configurations, user files, application code, etc.). Organizations must be confident that recovered data is accurate and safe. The National Cybersecurity Center of Excellence (NCCoE)—in collaboration with members of the business community and vendors of cybersecurity solutions—built an example solution to address these complex data integrity challenges. Multiple systems need to work together to prevent, detect, notify, and recover when data integrity is jeopardized. This project explored methods to effectively monitor and detect data corruption in commodity components (server, operating system, applications, and software configurations) as well as custom applications and data. The project also explored issues of auditing and reporting (user activity monitoring, file system monitoring, database monitoring, scanning backups/snapshots for malware and rapid recovery solutions) to support recovery and investigations. To address real-world business challenges around data integrity, the resulting example solution was composed of open-source and commercially available components. Ultimately, this project resulted in a publicly available NIST Cybersecurity Practice Guide—a description of the solution and practical steps needed to implement an example solution that addresses these existing challenges.

Domain Name System-Based Security for Electronic Mail

https://nccoe.nist.gov/projects/building_blocks/secured_email

The Domain Name System-Based Security for Electronic Mail project produced a proof-of-concept security platform that demonstrated trustworthy email exchanges across organizational boundaries. The product of the project was a security platform that included the authentication of mail servers, the signing and encryption of email, and binding cryptographic key certificates to the servers; it also included a practice guide that explained how to configure and use the demonstrated platform to satisfy both operational and security requirements. Domain Name System Security Extension (DNSSEC) protocols were used to authenticate server addresses and certificates by binding the X.509 certificates used for TLS to DNS names verified by DNSSEC. The business value of the security platform resulted from this project not only improves privacy and security protection for users' operations, but also expands the set of available DNS security applications and encourages wider implementation of the protocols that provide Internet users with confidence that entities to which they believe they are connecting are the entities to which they are actually connecting. This project resulted in one or more demonstration prototype DNS-based secure email platforms, a publicly available NIST Cybersecurity Practice Guide that explains how to employ the platform(s) to meet federal and industry security and privacy requirements, platform documentation necessary to compose a DNS-based email security platform from off-the-shelf components, and any recommendations for improvements to applicable standards documentation. The secure email project involved the composition of a variety of components that were provided by a number of different vendors. Client systems, DNS/DNSSEC services, mail transfer agents, and certificate providers (Certificate Authorities or CAs) were included. The NCCoE entered into cooperative research and development agreements with technology providers for components and expertise that included DNS resolvers (stub and recursive) for DNSSEC, authoritative DNS servers for DNSSEC signed zones, mail servers and mail security components, and extended validation and domain validation TLS certificates.

Mobile Application Single Sign-on: for Public Safety and First Responders **(DRAFT)**

https://nccoe.nist.gov/projects/use_cases/mobile-sso

Mobile platforms offer a significant operational advantage to public safety stakeholders by giving them access to mission critical information and services while deployed in the field, during training and exercises, or participating in the day-to-day business and preparations during non-emergency periods. However, these advantages can be limited if unnecessary or complex authentication requirements stand in the way of an official providing emergency services, especially when any delay – even seconds – is a matter of containing or exacerbating an emergency situation. The vast diversity of public safety personnel, missions, and operational environments magnifies the need for a nimble authentication solution for public safety. This project is exploring various multi-factor authenticators currently in use, or expected to be offered in the future, by the public safety community as their next generation networks are brought online. The effort is not only building an interoperable solution that can accept various authenticators to speed access to online systems while maintaining an appropriate amount of security, but the project also focuses on delivering single sign-on (SSO) capabilities to both native and web/browser-based applications. It is not enough to have an authenticator that is easy to use. This project is working to identify technical options for the public safety community to consider for deployment to ensure individuals in the field are not kept from meeting their mission goals by unnecessary authentication prompts. This project will result in a freely available NIST Cybersecurity Practice Guide that details the technical decisions, tradeoffs, lessons-learned, and build instructions, based on market-dominant standards, such that public safety organizations can accelerate the deployment of a range of mobile authentication and SSO services to their population of users.

Multifactor Authentication for e-Commerce: Online Authentication for the Retail Sector **(DRAFT)**

https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce

As greater security control mechanisms are implemented at the point of sale, retailers in the United States may see a drastic increase in e-commerce fraud, similar to what has been widely observed in the UK and Europe following the rollout of Europay, MasterCard and Visa (EMV) chip-and-PIN technology approximately ten years ago. Consumers, retailers, payment processors, banks, and card issuers are all impacted by the security risks of e-commerce transactions. Retailers bear the cost for fraudulent, card-not-present transactions, motivating them to reduce fraud to avoid damage to reputation and eliminate potential revenue losses, which have been estimated to be over $3 billion. Part of e-commerce fraud reduction includes an increased level of assurance in purchaser or user identity. In collaboration with stakeholders in the retail and e-commerce ecosystem, the NCCoE has determined that implementing multifactor authentication for e-commerce transactions can help reduce the risk of false online identification and authentication fraud. Consumers and retailers will adopt multi-factor authentication mechanisms if they do not unnecessarily encumber the purchasing process, or if they are applied evenly across the entire sector. Building on this collaboration with the business community and vendors of cybersecurity solutions, the NCCoE explored methods to effectively identify and authenticate purchasers during e-commerce transactions and develop an example solution composed of open-source and commercially available components. This project produced a NIST Cybersecurity Practice Guide—a publicly available description of the solution and practical steps needed to implement practices that effectively identify and authenticate purchasers during e-commerce transactions.

Securing Non-Credit Card, Sensitive Consumer Data: Consumer Data Security for the Retail Sector (DRAFT)

https://nccoe.nist.gov/projects/use_cases/securing-sensitive-consumer-data

As a result of payment card industry standards and a strong understanding of the value of valid credit card information in the black market, the retail industry has already invested in security mechanisms to protect credit card data, also referred to as cardholder data. However, this cardholder data is not the only valuable consumer information that is transmitted and stored by retailers. Other data that can be personally identifiable and is transmitted and stored in this ecosystem includes, but is not limited to, consumer purchasing habits (including geographical locations, preferences, search history), the dates of birth, home or business addresses, phone numbers, email addresses, user ids, passwords, IP addresses, and Social Security Numbers. As seen following high-profile data breaches in the healthcare sector, PII is valued at up to 20 times more than credit card data, with a single credit card number sold at $1 and the average individual's PII sold at $20. In collaboration with stakeholders in the retail and commercial payment ecosystem, the NCCoE has determined that implementing data masking and tokenization, coupled with fine-grained access control such as Attribute Based Access Control2, may significantly improve the security of PII transmitted and stored during commercial payment transactions, as well as PII shared internally within a retail organization and externally with business partners. Building on this collaboration with the business community and vendors of cybersecurity solutions, the NCCoE is exploring methods of effectively masking and tokenizing PII during commercial payment transactions and developing an example solution composed of open-source and commercially available components to address these real-world business challenges. This project will produce a NIST Cybersecurity Practice Guide—a publicly available description of the solution and practical steps needed to implement practices that more effectively secure the handling of non-credit card, sensitive consumer data.

Other NIST Publications

Baldrige Cybersecurity Excellence Builder (BCEB): Key questions for improving your organization's cybersecurity performance **(DRAFT)**

https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf

The *Baldrige Cybersecurity Excellence Builder* is a voluntary self-assessment tool that enables organizations to better understand the effectiveness of their cybersecurity risk management efforts. It helps organizational leaders identify opportunities for improvement, based on their cybersecurity needs and objectives, as well as their larger organizational needs, objectives, and outcomes. This self-assessment, can be used to:

- Determine cybersecurity-related activities that are important to business strategy and critical service delivery;
- Prioritize investments in managing cybersecurity risk;
- Determine how best to enable the workforce, customers, suppliers, partners, and collaborators to be risk conscious and security aware, and to fulfill their cybersecurity roles and responsibilities;
- Assess the effectiveness and efficiency of the use of cybersecurity standards, guidelines, and practices;
- Assess the cybersecurity results achieved; and

Like the “Framework for Improving Critical Infrastructure Cybersecurity” (Cybersecurity Framework) and the “Baldrige Excellence Framework”, the *Baldrige Cybersecurity Excellence Builder* is not a one-size-fits-all approach. It is adaptable and scalable to an organization’s needs, goals, capabilities, and environment. It does not prescribe how an organization’s cybersecurity policies and operations should be structured. Through interrelated sets of open-ended questions, it encourages the use of approaches that best fit the organization.

Best Practices for Privileged User PIV Authentication

http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf

The Cybersecurity Strategy and Implementation Plan (CSIP), published by the OMB on October 30, 2015, requires that federal agencies use PIV credentials for authenticating privileged users. This will greatly reduce unauthorized access to privileged accounts by attackers impersonating system, network, security, and database administrators, as well as other IT personnel with administrative privileges. This white paper further explains the need for multi-factor PIV-based user authentication to take the place of password-based single-factor authentication for privileged users. It also provides best practices for agencies implementing PIV authentication for privileged users.

Cybersecurity Framework Manufacturing Profile **(DRAFT)**

http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft.pdf

This document provides the Cybersecurity Framework implementation details developed for the manufacturing environment. The “Manufacturing Profile” of the Cybersecurity Framework can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices.

External Publications

The following journal articles and conference papers were published during FY 2016. For conference papers, the contributions listed below were either i) accepted for a conference held during FY 2016, or ii) accepted for a conference held prior to FY 2016 with final proceedings published in FY 2016 (and not listed in an earlier CSD Annual Report). All NIST authors are identified using *italics*; publications are listed alphabetically by author.

Links to document preprints are available at http://csrc.nist.gov/publications/articles/ and https://www.nist.gov/publications/.

Journal Articles

J. Aspnes, Z. Diamadi, A. Yampolskiy, K. Gjøsteen and *R. Peralta*, **Spreading Alerts Quietly and the Subgroup Escape Problem**, *Journal of Cryptology* 28(4), pp. 796-819 (October 2015).

https://doi.org/10.1007/s00145-014-9181-1

We introduce a new cryptographic primitive called a blind coupon mechanism (BCM). In effect, a BCM is an authenticated bit commitment scheme, which is AND-homomorphic. We show that a BCM has natural and important applications. In particular, we use a BCM to construct a mechanism for transmitting alerts undetectably in a message-passing system of *n* nodes. Our algorithms allow an alert to quickly propagate to all nodes without its source or existence being detected by an adversary, who controls all message traffic. Our proofs of security are based on a new subgroup escape problem, which seems hard on certain groups with bilinear pairings and on elliptic curves over the ring $\mathbf{Z}_n$.

J. Boyar, *M. Find* and *R. Peralta*, **On Various Nonlinearity Measures for Boolean Functions**, *Cryptography and Communicatio*n 8(3), pp. 313-330 (July 2016).

https://doi.org/10.1007/s12095-015-0150-9

A necessary condition for the security of cryptographic functions is to be “sufficiently distant” from linear, and cryptographers have proposed several measures for this distance. In this paper, we show that six common measures, *nonlinearity, algebraic degree, annihilator immunity, algebraic thickness, normality,* and *multiplicative complexity,* are incomparable in the sense that, for each pair of measures, μ_1, μ_2, there exist functions f_1,f_2 with f_1 being more nonlinear than f_2 according to μ_1, but less nonlinear according to μ_2. We also present new connections between two of these measures. Additionally, we give a lower bound on the multiplicative complexity of collision-free functions.

T. Chen, F.-C. Kuo, W. Ma, W. Susilo, D. Towey, *J. Voas* and Z. Zhou, **Metamorphic Testing for Cybersecurity, Computer** (*IEEE Computer*) 49(6), pp. 48-55 (June 2016).

https://doi.org/10.1109/MC.2016.176

Metamorphic testing (MT) can enhance security testing by providing an alternative to using a test oracle, which is often unavailable or impractical. The authors report how MT detected previously unknown bugs in real-world critical applications such as code obfuscators, giving evidence that software testing requires diverse perspectives to achieve greater cybersecurity.

M. Find, M. Göös, M. Järvisalo, P. Kaski, M. Koivisto, and J. Korhonen, **Separating OR, SUM, and XOR Circuits**, *Journal of Computer and System Sciences* 82(5), pp. 793-801 (August 2016).

https://doi.org/10.1016/j.jcss.2016.01.001

Given a boolean $n \times n$ matrix A, we consider arithmetic circuits for computing the transformation $x \mapsto Ax$ over different semirings. Namely, we study three circuit models: monotone OR-circuits, monotone SUM-circuits (addition of non-negative integers), and non-monotone XOR-circuits (addition modulo 2). Our focus is on *separating* OR-circuits from the two other models in terms of circuit complexity:

1. We show how to obtain matrices that admit OR-circuits of size O(n)O(n), but require SUM-circuits of size $\Omega(n^{3/2}/\log^2 n)$.
2. We consider the task of *rewriting* a given OR-circuit as an XOR-circuit and prove that any subquadratic-time algorithm for this task violates the strong exponential time hypothesis.

M. Iorga and A. Karmel, **Managing Risk in a Cloud Ecosystem**, *IEEE Cloud Computing Magazine* 2(6), pp. 51-57 (November-December 2015).

https://doi.org/10.1109/MCC.2015.122

Economies of scale, cutting-edge technology advancements, and a higher concentration of expertise enable cloud providers to offer state-of-the-art cloud ecosystems that are resilient, self-regenerating, and secure—far more secure than the environments of consumers who manage their own systems. This has the potential to greatly benefit many organizations. The key to the successful implementation of a cloud-based information system is a level of transparency into the cloud provider's service. This article focuses on security risks related to the operation and use of cloud-based information systems.

M. Iorga and K. Scarfone, **Using a Capability Oriented Methodology to Build Your Cloud Ecosystem**, *IEEE Cloud Computing Magazine* 3(2), pp. 58-63 (March-April 2016).

https://doi.org/10.1109/MCC.2016.38

Organizations often struggle to capture the necessary functional capabilities for each cloud-based solution adopted for their information systems. Identifying, defining, selecting, and prioritizing these functional capabilities and the security components that implement and enforce them is surprisingly challenging. This article explains recent developments by NIST in addressing these challenges. The article focuses on the capability-oriented methodology for orchestrating a secure cloud ecosystem proposed as part of the NIST Cloud Computing Security Reference Architecture. The methodology recognizes that risk can vary for cloud actors within a single ecosystem, so it takes a risk-based approach to functional capabilities. The result is an assessment of which cloud actor is responsible for implementing each security component and how implementation should be prioritized. Cloud actors, especially cloud consumers, that follow the methodology can more easily make well-informed decisions regarding their cloud ecosystems.

C. Kolias, A. Stavrou, *J. Voas, I. Bojanova* and *D. R. Kuhn*, **Learning Internet of Things Security 'Hands-On'**, *IEEE Security & Privacy* 14(1), pp. 37-46 (January-February 2016).

https://doi.org/10.1109/MSP.2016.4

What can you glean from using inexpensive, off-the-shelf parts to create IoT use cases? As it turns out, a lot. The fast productization of IoT technologies is leaving users vulnerable to security and privacy risks.

B. Stanton, M. Theofanos, S. Spickard Prettyman, S. Furman, **Security Fatigue**, *IT Professional*, Vol. 18, Issue 5, pp. 26-32, Sept.-Oct. 2016,

https://doi.org/10.1109/MITP.2016.84

Security fatigue has been used to describe experiences with online security. This study identifies the affective manifestations resulting from decision fatigue and the role it plays in users' security decisions. A semi structured interview protocol was used to collect data (N = 40). Interview questions addressed online activities; computer security perceptions; and the knowledge and use of security icons, tools, and terminology. Qualitative data techniques were used to code and analyze the data identifying security fatigue and contributing factors, symptoms, and outcomes of fatigue. Although fatigue was not directly part of the interview protocol, more than half of the participants alluded to fatigue in their interviews. Participants expressed a sense of resignation, loss of control, fatalism, risk minimization, and decision avoidance, all characteristics of security fatigue. The authors found that the security fatigue users experience contributes to their cost-benefit analyses in how to incorporate security practices and reinforces their ideas of lack of benefit for following security advice.

M. Theofanos, S. Garfinkel, and *Y. Choong*, **Secure and Usable Enterprise Authentication: Lessons from the Field**. *IEEE Security & Privacy*, 14(5), pp.14-21 (February 2016).

There are now more than 5.4 million Personal Identity Verification (PIV) and Common Access Card (CAC) identity cards deployed to US government employees and contractors. These cards are widely used to gain physical access to federal facilities, but their use to authenticate logical access to government information systems has been uneven. We report the reasons for the uneven deployment and then compare the results of a 26,691-person survey within the Department of Defense (DoD) and a 4,573-person survey within the Department of Commerce (DOC) to show that the use of smart-cards for 2-factor authentication results in improved usability and security when compared with 1-factor, password-only systems. We show that these benefits extend beyond the smart cards to other systems within the organizations that solely employ password authentication. We argue that PKI token-based authentication systems, such as smartcards, are likely to provide authentication that is simultaneously more secure and more usable than other 2-factor approaches, such as combining strong passwords with cell phones or with time-based hardware identity tokens.

D.R. Kuhn, R. Kacker and Y. Lei, **Measuring and Specifying Combinatorial Coverage of Test Input Configurations**, *Innovations in Systems and Software Engineering*, pp. 1-13 (November 14, 2015).

https://doi.org/10.1007/s11334-015-0266-2

A key issue in testing is *how many tests are needed for a required level of coverage or fault detection*. Estimates are often based on error rates in initial testing, or on code coverage. For example, tests may be run until a desired level of statement or branch coverage is achieved. Combinatorial methods present an opportunity for a different approach to estimating the required test set size, using characteristics of the test set. This paper describes methods for estimating the coverage of, and ability to detect, the *t*-way interaction faults of a test set based on a covering array. We also develop a connection between (static) combinatorial coverage and (dynamic) code coverage, such that if a specific condition is satisfied, 100 % branch coverage is assured. Using these results, we propose practical recommendations for using combinatorial coverage in specifying test requirements, and for improving estimates of the fault detection capacity of a test set.

P. Mell, R. Harang and A. Gueye, **Linear Time Vertex Partitioning on Massive Graphs**, *International Journal of Computer Science: Theory and Application*, 5(1), pp. 1-11 (2016).

http://www.orb-academic.org/index.php/journal-of-computer-science/article/view/232

The problem of optimally removing a set of vertices from a graph to minimize the size of the largest resultant component is known to be NP-complete. Prior work has provided near optimal heuristics with a high time complexity that function on up to hundreds of nodes and less optimal but faster techniques that function on up to thousands of nodes. In this work, we analyze how to perform vertex partitioning on massive graphs of tens of millions of nodes. We use a previously known and very simple heuristic technique: iteratively removing the node of the largest degree and all its edges. This approach has an apparent quadratic complexity since, upon removal of a node and adjoining set of edges, the node degree calculations must be updated prior to choosing the next node. However, we describe a linear time complexity solution using an array whose indices map to node degree and whose values are hash tables indicating the presence or absence of a node at that degree value. We empirically demonstrate linear scalability on random graphs of up to 15,000 nodes and evaluate our memory usage vs. runtime tradeoffs. We then demonstrate tractability on massive graphs through the execution on a graph with 34 million nodes representing Internet-wide router connectivity.

K. Schaffer, **Expanding Continuous Authentication with Mobile Devices**, *Computer (IEEE Computer)* 48(11), pp. 92-95 (November 2015).

https://doi.org/10.1109/MC.2015.333

More sophisticated methods of detecting user interaction with computers and smartphones are needed for better security and usability. Multimodal continuous authentication is one of the more promising authentication methods on the horizon.

K. Schaffer and *J. Voas*, **Whatever Happened to Formal Methods for Security?** *Computer (IEEE Computer)* 49(8), pp. 70-79 (August 2016).

https://doi.org/10.1109/MC.2016.228

A panel of seven experts discusses the state of the practice of formal methods (FM) in software development, with a focus on FM's relevance to security.

A. Vassilev and *R. Staples*, **Entropy as a Service: Unlocking Cryptography's Full Potential**, Computer (IEEE Computer), 49(9), pp. 98-102 (September 2016).

https://doi.org/10.1109/MC.2016.275

Securing the Internet requires strong cryptography, which depends on good entropy for generating unpredictable keys. Entropy as a service provides entropy from a decentralized root of trust, scaling across diverse geopolitical locales and remaining trustworthy unless much of the collective is compromised.

J. Voas, **Demystifying the Internet of Things**, *Computer (IEEE Computer)* 49(6), pp. 80-83, (June 2016).

https://doi.org/10.1109/MC.2016.162

IoT is a distributed network of smart sensors that enables the precise control and monitoring of complex processes over arbitrary distances; every object in the Internet infrastructure is interconnected into a global dynamic expanding network. In what's called the Internet of Things, sensors and actuators embedded in physical objects – from roadways to pacemakers – are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet.

J. Voas, and G. Hurlburt, **Third-Party Software's Trust Quagmire**, *Computer (IEEE Computer)*, 48(12), pp. 80-87 (December 2015).

https://doi.org/10.1109/MC.2015.372

Integrating software developed by third-party organizations into a larger system raises concerns about the software's quality, origin, functionality, security, and interoperability. Addressing these concerns requires rethinking the roles of the software's principal supply-chain actors—vendor, assessor, and evaluator.

J. Voas, and *K. Schaffer*, **Insights on Formal Methods of Cybersecurity**, *Computer (IEEE Computer)*, 49(5), pp. 102-105, (May 2016).

https://doi.org/10.1109/MC.2016.131

Seven experts weigh in on the current use and practice of formal methods in cybersecurity.

M. Zhang, L. Wang, S. Jajodia, *A. Singhal* and M. Albanese, **Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero-Day Attacks**, *IEEE Transactions on Information Forensics and Security* 11(5), pp. 1071-1086, (May 2016).

https://doi.org/10.1109/TIFS.2016.2516916

Network diversity has long been regarded as a security mechanism for improving the resilience of software and networks against various attacks. More recently, this diversity has found new applications in cloud computing security, moving-target defense, and improving the robustness of network routing. However, most existing efforts rely on intuitive and imprecise notions of diversity, and the few existing diversity models are mostly designed for a single system running diverse software replicas or variants. At a higher abstraction level, as a global property of the entire network, network diversity and its effect on security have received limited attention. In this paper, we take the first step toward formally modeling network diversity as a security metric by designing and evaluating a series of diversity metrics. In particular, 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. We provide guidelines for instantiating the proposed metrics and present a case study on estimating software diversity. Finally, we evaluate the proposed metrics through simulation.

Conference Papers

D. Bobor, S. Jajodia, L. Wang and *A. Singhal*, **Diversifying Network Services under Cost Constraints for Better Resilience against Unknown Attacks, 30th IFIP Conference on Data and Application Security and Privacy** (DBSec 2016), Trento, Italy, July 18-21, 2016. In *Lecture Notes in Computer Science* 9766, *Data and Applications Security and Privacy* XXX, S. Ranise and V. Swarup, eds., Switzerland: Springer International, 2016, pp. 295-312.

https://doi.org/10.1007/978-3-319-41483-6_21

Network diversity as a security mechanism has received revived interest recently due to its potential for improving the resilience of software and networks against unknown attacks. Recent work show that this diversity can be modeled and quantified as a security metric at the network level. However, such an effort does not directly provide a solution for improving the network diversity, and existing network hardening approaches are largely limited to handling previously known vulnerabilities by disabling existing services. In this paper, we take the first step toward an automated approach to diversifying network services under various cost constraints in order to improve the network's resilience against unknown attacks. Specifically, we provide a model of network services and formulate the diversification requirements as an optimization problem. We devise optimization and heuristic algorithms for efficiently diversifying relatively large networks under different cost constraints. We also evaluate our approach through simulations.

S. Câmara, *D. Anand, V. Pillitteri* and L. Carmo, **inf-TESLA: Multicast Delayed Authentication for Streaming Sensor Data in Electric Power Systems**, *31st IFIP TC 11 International Conference (SEC 2016)*, Ghent, Belgium, May 30, 2016 – June 1, 2016. In *IFIP Advances in Information and Communication Technology* 471, *ICT Systems Security and Privacy Protection*, J.-H. Hoepman and S. Katzenbeisser, eds., Switzerland: Springer International, 2016, pp. 32-46.

https://doi.org/10.1007/978-3-319-33630-5_3

Multicast authentication of synchrophasor data is challenging due to the design requirements of Smart Grid monitoring systems, such as low security overhead, tolerance of lossy networks, time-criticality and high data rates. In this work, we propose *inf*-TESLA, Infinite Timed Efficient Stream Loss-tolerant Authentication, a multicast, delayed authentication protocol for communication links that are used to stream synchrophasor data for wide area control of electric power networks. Our approach is based on the authentication protocol TESLA, but is augmented to accommodate high frequency transmissions of unbounded length. The *inf*-TESLA protocol utilizes the Dual Offset Key Chains mechanism to reduce authentication delay and the computational cost associated with key chain commitment. We provide a description of the mechanism using two different modes for disclosing keys and demonstrate its security against a man-in-the-middle attack attempt. We compare our approach against the TESLA protocol in a 2-day simulation scenario, showing a reduction of 15.82 % and 47.29 % in computational cost by the sender and receiver, respectively, and a cumulative reduction in the communication overhead.

Y. Choong, K. Greene, **What's a Special Character Anyway? Effects of Ambiguous Terminology in Password Rules**. Published in the *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 60, No. 1, pp. 760-764). Sage CA: Los Angeles, CA: SAGE Publications. (September 2016).

Although many aspects of passwords have been studied, no research to date has systematically examined how ambiguous terminology affects the user experience during password rule comprehension, a necessary precursor to password generation. Our research begins to address this gap by focusing on users comprehension of password generation rules. Varying terms special characters, symbols, non-alphanumeric characters, and punctuation are used in different password rules, but mostly without explicit definition. In this laboratory study, we used character-selection and compliance-checking tasks with 60 participants to investigate effects of varying terms on users' password rule comprehension. Results show that manipulating terminology caused participants conception of the allowed character space to shrink or expand. Our quantitative and qualitative data show that participants were extremely confused by the variety of terms for special character. Seemingly small changes in language have large, observable impacts on users understanding of password rules. Language in password requirements must be carefully constructed to ensure that people fully comprehend the allowable character space. This research is an important first step to providing data-driven guidance on constructing clearer language for password rules.

I. V. Bojanova, P. E. Black, Y. Yesha, Y. Wu, **A Structured Framework to Express Software Bugs**. *IEEE International Conference on Software Quality, Reliability & Security* (QRS 2016), Vienna, Austria, 08/01/2016 to 08/03/2016, (Aug 2016).

https://doi.org/10.1109/QRS.2016.29

To achieve higher levels of assurance for digital systems, we need to answer questions such as, does this software have bugs of these critical classes? Do these two tools generally find the same set of bugs, or different, complimentary sets? Can we guarantee that a new technique discovers all problems of this type? To answer such questions, we need a vastly improved way to describe classes of vulnerabilities and chains of failures. This paper presents a descriptive framework that will lift the current realm of best efforts and useful heuristics. Our framework includes rigorous definitions and (static) characteristics of bug classes, along with their related dynamic properties, such as proximate, secondary, and tertiary causes and consequences (CCC), and sites. The paper discusses the buffer overflow class, the injection class, and the interaction frequency control class, and provides examples of applying our taxonomy to describe particular vulnerabilities.

A. M. Delaitre, C. D. De Oliveira, A. Hoole, I. Traore, **Improving Vulnerability Detection Measurement**, *20th International Conference on Evaluation and Assessment in Software Engineering*, Limerick, Ireland, June 2016.

The Software Assurance Metrics and Tool Evaluation (SAMATE) project at the National Institute of Standards and Technology (NIST) has created the Software Assurance Reference Dataset (SARD) to provide researchers and software security assurance tool developers with a set of known security. Following an empirical evaluation of a runtime monitoring framework, deficiencies were discovered in two existing test suites which led to a collaboration with NIST to provide replacements. Test Suites 45 and 46 are analyzed, discussed, and updated to improve accuracy, consistency, reciseness, and automation. Empirical results show metrics such as recall, precision, and F-Measure are all impacted by invalid base assumptions regarding the test suites.

B. Stivalet and *E. N. Fong*, **Large Scale Generation of Complex and Faulty PHP Test Cases**, *2016 IEEE International Conference on Software Testing, Verification and Validation (ICST)*, Chicago, IL, April 2016,

https://doi.org/10.1109/ICST.2016.43

Developing good test cases is an intellectually demanding and critical task, and it has a strong impact on the effectiveness and efficiency of the whole testing process. This paper presents an automated generator of test cases, which are designed to evaluate source code security analyzers. The generator produces PHP: Hypertext Preprocessor (PHP) programs with most common vulnerabilities embedded in various code complexities. It also produces programs without vulnerabilities to test for false positives. The generator is modular and extensible. We describe its internal design and how it works. The generated PHP test cases were added to the Software Assurance Reference Dataset (SARD) and will be used to assess the effectiveness of static analyzers. We conclude with the current state of the tool, its benefits and future work.

F. E. Boland and *C. D. De Oliveira*, **A Real World Software Assurance Test Suite**, *The 27th Annual IEEE Software Technology Conference*, Long Beach, CA, October 2015.

The design of a test suite to test and measure software assurance using automated tools must have the following characteristics: relevance, statistical significance, and inclusion ground truth. The IARPA (Intelligence Advanced Research Projects Activity) STONESOUP (Securely Taking on Software of Uncertain Provenance) Program [1] has produced such a test suite. Our presentation will characterize this test suite called the STONESOUP Phase 3 Test Suite. This test suite consists of 7769 individual test cases, of which 4581 are in C and 3188 are in Java. All of these test cases may be accessed independently. Each test case is derived from real-world open source applications. This test suite is significant in that it is the first test suite of its kind (to our knowledge) to be based on large real-world code sets. Our presentation will describe the test suite format and contents, as well as the structure of the test cases in the test suite. Additional relevant information pertaining to the test suite including the test case naming convention and how to specify the metadata xml file will also be provided, containing all the instructions needed to build, execute and score a given test case.

R. Chandramouli, A**nalysis of Virtual Networking Options for Securing Virtual Machines**, *Seventh International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2016)*, Rome, Italy, March 20-24, 2016, pp. 95-102.

http://www.thinkmind.org/download.php?articleid=cloud_computing_2016_5_20_20037

Cloud Data centers are predominantly made up of Virtualized hosts. The networking infrastructure in a cloud (virtualized) data center, therefore, consists of the combination of physical IP network (data center fabric) and the virtual network residing in virtualized hosts. Network Segmentation (Isolation), Traffic flow control using firewalls and Intrusion Detection System/Intrusion Prevention Systems (IDS/IPS) form the primary network-based security techniques, with the first one as the foundation for the other two. In this paper, we describe and analyze three generations of network segmentation techniques: Virtual Switches & Physical NIC-based, Virtual Local Area Network (VLAN)-based & Overlay-based. We take a detailed look at the overlay-based virtual network segmentation and its characteristics, such as scalability and ease of configuration.

D. Ferraiolo, R. Chandramouli, D. R. Kuhn and *V. Hu*, **Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)**, *2016 ACM International Workshop on Attribute Based Access Control (ABAC '16)*, New Orleans, Louisiana, United States, March 11, 2016, pp. 13-24.

https://doi.org/10.1145/2875491.2875496

XACML and NGAC are very different attribute-based access control standards with similar goals and objectives. An objective of both is to provide a standardized way for expressing and enforcing vastly diverse access control policies in support of various types of data services. The two standards differ with respect to the way that access control policies and attributes are specified and managed, and decisions are computed and enforced. This paper is presented as a consolidation and refinement of public draft SP 800-178, describing, and comparing these two standards.

D. R. Kuhn, V. Hu, D. Ferraiolo, R. N. Kacker and Y. Lei, **Pseudo-Exhaustive Testing of Attribute Based Access Control Rules**, Fifth International Workshop on Combinatorial Testing (IWCT 2016) in *Proceedings of the 2016 IEEE Ninth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, Chicago, Illinois, United States, April 11-15, 2016, pp. 51-58.

https://doi.org/10.1109/ICSTW.2016.35

Access control typically requires translating policies or rules given in natural language into a form such as a programming language or decision table, which can be processed by an access control system. Once rules have been described in machine-processable form, testing is necessary to ensure that the rules are implemented correctly. This paper describes an approach based on combinatorial test methods for efficiently testing access control rules, using the structure of ABAC to detect a large class of faults without a conventional test oracle.

D. R. Kuhn, R. N. Kacker and Y. Lei, **Estimating t-Way Fault Profile Evolution During Testing**, *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, Atlanta, Georgia, United States, June 10-14, 2016, pp. 596-597.

https://doi.org/10.1109/COMPSAC.2016.110

Empirical studies have shown that most software interaction faults involve one or two variables interacting, with progressively fewer triggered by three or more, and no failure has been reported involving more than six variables interacting. This paper introduces a model for the origin of this distribution, evaluates model predictions against empirical data, and discusses implications for the removal of interaction faults and reliability growth.

C. Liu, *A. Singhal* and D. Wijesekera, **A Probabilistic Network Forensics Model for Evidence Analysis**, *IFIP WG 11.3 International Conference on Digital Forensics*, New Dehli, India, January 4-6, 2016. In *IFIP Advances in Information and Communication Technology* 484, pp. 189-210.

https://doi.org/10.1007/978-3-319-46279-0_10

Modern-day attackers use sophisticated multi-stage and/or multi-host attack techniques and anti-forensic tools to cover their attack traces. Due to the limitations of current intrusion detection systems and forensic analysis tools, evidence often has false positive errors or is incomplete. Additionally, because of the large number of security events, discovering an attack pattern is much like finding a needle in a haystack. Consequently, reconstructing attack scenarios and holding attackers accountable for their activities are major challenges.

This chapter describes a probabilistic model that applies Bayesian networks to construct evidence graphs. The model helps address the problems posed by false positive errors, analyze the reasons for missing evidence and compute the posterior probabilities and false positive rates of attack scenarios constructed using the available evidence. A companion software tool for network forensic analysis was used in conjunction with the probabilistic model. The tool, which is written in Prolog, leverages vulnerability databases and an anti-forensic database similar to the NIST National

Vulnerability Database (NVD). The experimental results demonstrate that the model is useful for constructing the most-likely attack scenarios and for managing errors encountered in network forensic analysis.

P. Mell and R. Harang, **Minimizing Attack Graph Data Structures**, *Tenth International Conference on Software Engineering Advances (ICSEA 2015)*, Barcelona, Spain, November 15-20, 2015, pp. 376-385.

http://www.thinkmind.org/index.php?view=article&articleid=icsea_2015_14_30_10293

An attack graph is a data structure representing how an attacker can chain together multiple attacks to expand their influence within a network (often in an attempt to reach some set of goal states). Restricting attack graph size is vital for the execution of high degree polynomial analysis algorithms. However, we find that the most widely cited and recently used "condition/exploit" attack graph representation has a worst-case quadratic node growth with respect to the number of hosts in the network when a linear representation will suffice. In 2002, a node linear representation in the form of a "condition" approach was published but was not significantly used in subsequent research. In analyzing the condition approach, we find that (while node linear) it suffers from edge explosions: the creation of unnecessary complete bipartite sub-graphs. To address the weaknesses in both approaches, we provide a new hybrid "condition/vulnerability" representation that regains linearity in the number of nodes and that removes unnecessary complete bipartite sub-graphs, mitigating the edge explosion problem. In our empirical study modeling an operational 5968-node network, our new representation had 94 % fewer nodes and 64 % fewer edges than the currently used condition/exploit approach.

D. Moody and *R. Perlner*, Vulnerabilities of **'McEliece in the World of Escher'**, *7th International Workshop on Post-Quantum Cryptography (PQCrypto 2016)*, Fukuoka, Japan, February 24-26, 2016. In *Lecture Notes in Computer Science* 9606, *Post-Quantum Cryptography*, T. Takagi, ed., Berlin: Springer International, 2016, pp. 104-117.

https://doi.org/10.1007/978-3-319-29360-8_8

Recently, Gligoroski et al. proposed code-based encryption and signature schemes using list decoding, block-wise triangular private keys, and a non-uniform error pattern based on "generalized error sets." The general approach was referred to as McEliece in the World of Escher. This paper demonstrates attacks that are significantly cheaper than the claimed security level of the parameters given by Gligoroski et al. We implemented an attack on the proposed 80-bit parameters that recovered private keys for both encryption and signatures in approximately two hours on a single laptop. We further find that increasing the parameters to avoid our attack will require parameters to grow by (at least) two orders of magnitude for encryption, and may not be achievable at all for signatures.

D. Simos, K. Kleine, *D. R. Kuhn* and *R. N. Kacker*, **Combinatorial Coverage Analysis of Subsets of the TLS Cipher Suite Registry**, *High Confidence Software and Systems Conference*, Annapolis, Maryland, United States, May 10-12, 2016.

http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=920193

We present a combinatorial coverage measurement analysis for (subsets) of the TLS cipher suite registries by analyzing the specified ciphers of IANA, ENISA, BSI, Mozilla and NSA Suite B. The method introduced here may contribute toward the design of quality measures of cipher suites, and may also be applied more broadly to the analysis of configurable systems.

A. Singhal, C. Liu and D. Wijesekera, **A Logic Based Network Forensics Model for Evidence Analysis** [poster], *22nd ACM Conference on Computer and Communications Security (CCS '15)*, Denver, Colorado, United States, October 12-15, 2015, p. 1677.

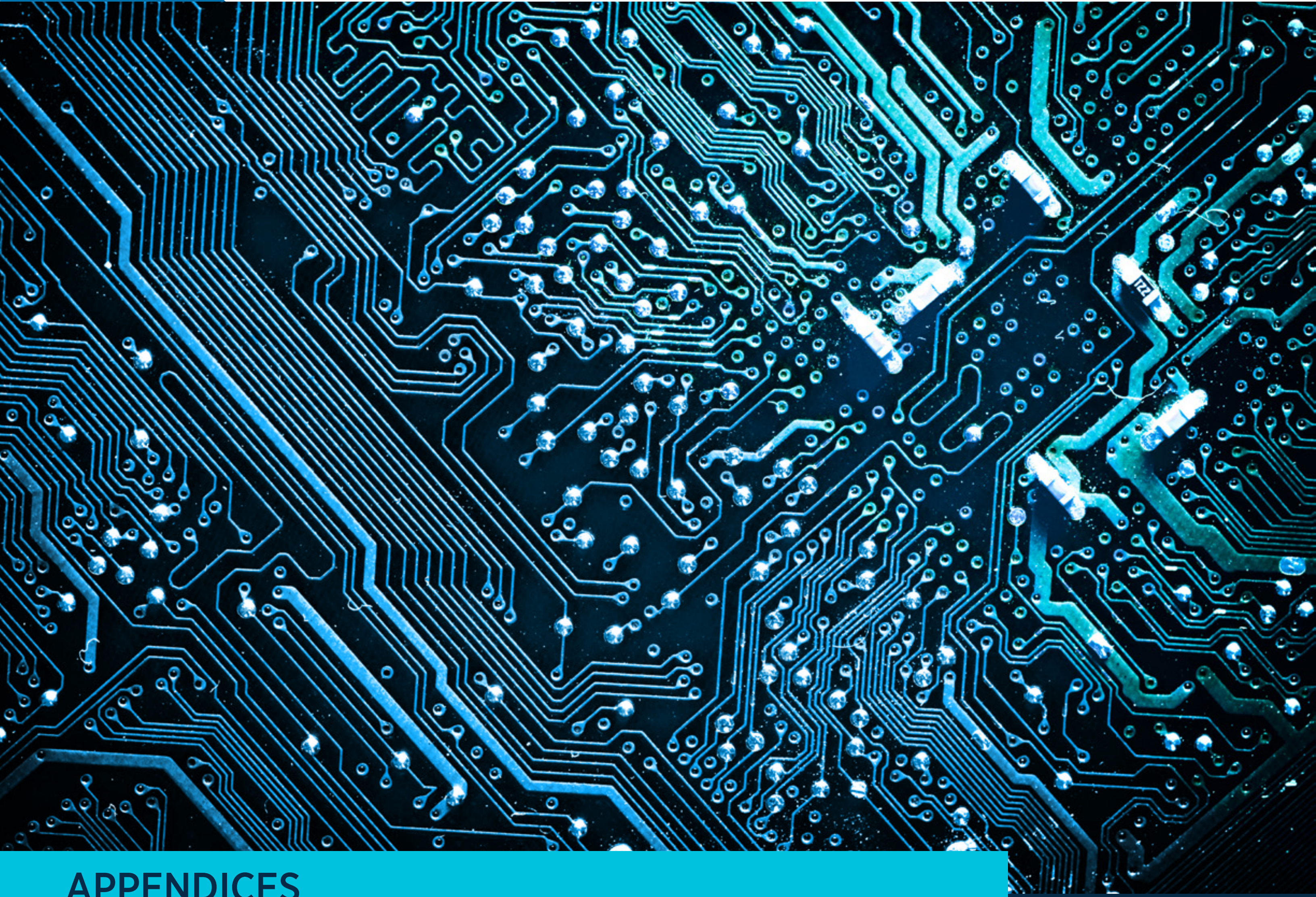
https://doi.org/10.1145/2810103.2810106

Modern-day attackers tend to use sophisticated multi-stage/multi-host attack techniques and anti-forensics tools to cover their attack traces. Due to the current limitations of intrusion detection and forensic analysis tools, reconstructing attack scenarios from evidence left behind by the attackers of an enterprise system is challenging. In particular, reconstructing attack scenarios by using the information from IDS alerts and system logs that have a large number of false positives is a big challenge. In this poster, we present a model and an accompanying software tool that systematically addresses how to resolve the above problems to reconstruct the attack scenario. These problems include a large amount of data, including non-relevant data and evidence destroyed by anti-forensic techniques. Our system is based on a Prolog system using known vulnerability databases and an anti-forensics database that we plan to extend to a standardized database like the NIST National Vulnerability Database (NVD). In this model, we use different methods, including mapping the evidence to system vulnerabilities, inductive reasoning and abductive reasoning to reconstruct attack scenarios. The goal of this work is to reduce the investigators' time and effort in reaching a definite conclusion about how an attack occurred. Our results indicate that such a reasoning system can be useful for network forensics analysis.

X. Sun, *A. Singhal* and P. Liu, **Who Touched My Mission: Towards Probabilistic Mission Impact Assessment**, *2015 Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '15)*, Denver, Colorado, United States, October 12, 2015, pp 21-26.

https://doi.org/10.1145/2809826.2809834

Cyber attacks inevitably have negative impacts on relevant missions. However, concrete methods to accurately evaluate such impacts are rare. In this paper, we propose a probabilistic approach based on Bayesian networks for quantitative mission impact assessment. A System Object Dependency Graph (SODG) is first built to capture the intrusion propagation process at the low operating system level. On top of the SODG, a mission-task-asset (MTA) map can be established to associate the system objects with corresponding tasks and missions. Based on the MTA map, a Bayesian network can be constructed to leverage the collected intrusion evidence and infer the probabilities of tasks and missions being tainted. This approach is promising for effective quantitative mission impact assessment.



APPENDICES

This section contains 3 Appendices (List of Acronyms, NIST/ITL Cybersecurity Events, and Ways to Engage with ITL Cybersecurity Program and with NIST.

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

Appendix A: Acronyms

3GPP	3rd Generation Partnership Project
AAAS	American Association for the Advancement of Science
ABAC	Attribute Based Access Control
AC	Access Control
ACD	Applied Cybersecurity Division
ACM	Association for Computing Machinery
ACPT	Access Control Policy Tool
ACRLCS	Access Control Rule Logic Circuit Simulation
AES	Advanced Encryption Standard
AIM	Algorithms for Intrusion Measurement
AKA or a.k.a	also known as
AN	ANSI/NIST-ITL
ANS	American National Standards
ANSI	American National Standards Institute
ANTD	Advanced Network Technologies Division
APCO	Association of Public-Safety Communications Officials
API	Application Programming Interface
ARF	Asset Reporting Format
ARL	Army Research Laboratory
ARM	Advanced Reduced Instruction Set Computing (RISC) Machine
ASC X9	Accredited Standards Committee X9
ASKDF	Application-Specific Key Derivation Functions
BCEB	Baldrige Cybersecurity Excellence Builder
BGP	Border Gateway Protocol
BGP-SRx	BGP Secure Routing Extension
BioAPI	Biometric Application Programming Interface
BioCTS	Biometric Conformance Test Software
BIOS	Basic Input/Output System
BT-SEG	Bluetooth Security Expert Group
BYOD	Bring-Your-Own Device
CAC	Common Access Card
CAE	Centers of Academic Excellence
CAVP	Cryptographic Algorithm Validation Program
CCC	Causes and Consequences
CCE	Common Configuration Enumeration
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CCSS	Common Configuration Scoring System
CDH	Confactor Diffie-Hellman
CDM	Continuous Diagnostics and Mitigation
CFTT	Computer Forensic Tool Testing
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity Information Sharing Act
CKMS	Cryptographic Key Management System
CMAC	Cipher-based Message Authentication Code
CMS	Content Management System
CMUF	Cryptographic Modules User Forum
CMVP	Cryptographic Module Validation Program
CNAP	Cybersecurity National Action Plan
CNSS	Committee on National Security Systems
CNSSD	CNSS Directive
COMPSAC	Computer Software and Applications Conference
CPE	Common Platform Enumeration
CPS	Cyber-Physical Systems
CRADA	Cooperative Research and Development Agreement
CS1	Cybersecurity 1

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
https://dx.doi.org/10.6028/NIST.SP.800-195

CSD	Computer Security Division
CSE	Communications Security Establishment
CSF	Cybersecurity Framework
CSIA	Cybersecurity and Information Assurance
CSIP	Cybersecurity Strategy and Implementation Plan
CSRC	Computer Security Resource Center
CST	Cryptographic and Security Testing
CSWG	Cybersecurity Working Group
CTG	Cryptographic Technology Group
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DANE	DNS-based Authentication of Named Entities
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DHS	Department of Homeland Security
DIS	Draft International Standard
DISA	Defense Information Systems Agency
DKIM	Domain Keys Identified Mail
DL	Driver License
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOC	Department of Commerce
DOD	Department of Defense
DoE	Department of Energy
DOJ	Department of Justice
DoS	Department of State
DPC	Derived PIV Credentials
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTR	Derived Test Requirements
EAC	Election Assistance Commission
EaaS	Entropy as a Service
EBTS	Electronic Biometric Transmission Specification
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECP	Enterprise Compliance Profile
EL	Engineering Laboratory
EM	Encoded Message
EMS	Emergency Medical Services
EO	Executive Order
EMV	Europay, MasterCard, and Visa Chip-and-PIN Technology
ESCARS	Embedded Security in Cars
ESDC	Employment and Social Development Canada
FAA	Federal Aviation Administration
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCKMSs	Federal Cryptographic Key Management Systems
FCSM	Federal Computer Security Managers
FDA	Federal Drug Administration
FDCC	Federal Desktop Core Configuration
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
FHFA	Federal Housing Finance Agency

FIDO	Fast Identities Online
FIFO	First In, First Out
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
FM	Formal Methods
FPE	Format-Preserving Encryption
FRN	Federal Register Notice
FTC	Federal Trade Commission
FY	Fiscal Year
GAO	Government Accountability Office
GCM	Galois/Counter Mode
GCN	Government Computer News
GCSE	Group Communication System Enablers
GICS	Generic Identity Command Set
GPS	Global Positioning System
GRC	Governance, Risk Management, and Compliance
GSA	General Services Administration
HAD	High Assurance Domains
HAVA	Help America Vote Act
HHS	Health and Human Services
HIMSS	Healthcare Information and Management Systems Society
HMAC	Hash-based Message Authentication Code
HSPD-12	Homeland Security Presidential Directive-12
HTTPS	Hyper Text Transfer Protocol Secure
HWAM	Hardware Asset Management
IaaS	Infrastructure as a Service
IACS	Industrial Automation and Control Systems
IAD	Information Access Division
IARPA	Intelligence Advanced Research Projects Activity
IC	Intelligence Community
ICC	Integrated Circuit Card
ICMC	International Cryptographic Module Conference
ICS	Industrial Control SystemsICSEA International Conference on Software Engineering Advances
ICST	International Conference on Software Testing, Verification and Validation
ICSTW	International Conference on Software Testing, Verification and Validation Workshops
ICT	Information and Communications Technology
IDA	Institute for Defense Analyses
IDEF	Identity Ecosystem Framework
IDESG	Identity Ecosystem Steering Group
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFIP	International Federation for Information Processing
IG	Implementation Guidance
IGs	Inspector Generals
IHS	Indian Health Service
IIP	Internet Infrastructure Protection
IKE	Internet Key Exchange
INCITS	InterNational Committee for Information Technology Standards
INFORMS	Institute for Operations Research and the Management Sciences
I/O	Input/Output

IoT	Internet of Things
IP	Internet Protocol
IPD	Initial Public Draft
IPS	Intrusion Prevention Systems
ISA	International Society of Automation
ISACs	Information Sharing and Analysis Centers
ISAOs	Information Sharing and Analysis Organizations
ISCM	Information Security Continuous Monitoring
ISO	International Organization for Standardization
ISPAB	Information Security and Privacy Advisory Board
IT	Information Technology
ITAM	IT asset management
ITL	Information Technology Laboratory
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
IUT	Implementation Under Test
IWCE	International Wireless Communications Expo
IWCT	International Workshop on Combinatorial Testing
IWG	Interagency Working Group
JSON	JavaScript Object Notation
JTF	Joint Task Force
JTC 1	Joint Technical Committee 1
KBKDF	Key-Based Key Derivation functions
KDF	Key Derivation Functions
KMAC	Keccak Message Authentication Code
LTE	Long-Term Evolution
MAC	Media Access Control
MAC	Message Authentication Code
MACsec	Media Access Control Security
MCPTT	Mission Critical Push-To-Talk
MILE	Managed Incident Lightweight Exchange
MIP	Modules-In-Process
MLS	Multi-Level Security
MMT	Multi-Block Message Test
MQV	Menezes-Qu-Vanstone
MRT	Machine Readable Table
MT	Metamorphic testing
MTA	Mission-task-asset
NANOG	North American Network Operators Group
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NASPI	North American Synchrophasor Initiative
NASPO	North American Security Products Organization
NCCoE	National Cybersecurity Center of Excellence
NCP	National Checklist Program
NCWF	National Cybersecurity Workforce Framework
NGAC	Next Generation Access Control
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
NHTSA	National Highway Traffic Safety Administration
NIAP	National Information Assurance Partnership
NICE	National Initiative for Cybersecurity Education

NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NITRD	Networking and Information Technology Research and Development
NOAA	National Oceanic and Atmospheric Administration
NoT	Network of Things
NPIVP	NIST Personal Identity Verification Program
NPSBN	National Public Safety Broadband Network
NRBG	Non-deterministic Random Bit Generator
NSA	National Security Agency
NSCI	National Strategic Computing Initiative
NS/EP	National Security and Emergency Preparedness
NSRL	National Software Reference Library
NSTAC	National Security Telecommunications Advisory Council
NSTIC	National Strategy for Trusted Identities in Cyberspace
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
NVLAP	National Voluntary Laboratory Accreditation Program
NYU	New York University
OASIS	Organization for the Advancement of Structured Information Standards
OCIL	Open Checklist Interactive Language
OIS	Office of Information Security
OISM	Office of Information Systems Management
OMB	Office of Management and Budget
OPNET	Optimized Network Engineering Tools
OS	Operating System
OSCAL	Open Security Controls Assessment Language
OSHE	Office of Safety, Health and Environment
OVAL	Open Vulnerability and Assessment Language
PACS	Physical Access Control Systems
PCI	Payment Card Industry
PCLOB	Privacy and Civil Liberties Oversight Board
PEP	Privacy Engineering Program
PHP	PHP: Hypertext Preprocessor
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	PIV-Interoperable
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
P.L.	Public Law
PLC	Programmable Logic Controller
PM	Policy Machine
PML	Physical Measurement Laboratory
PPE	Personal Protective Equipment
PPQAS	Password Policy Question-Answer System
PQC	Post-Quantum Cryptography
PQCrypto	Post-Quantum Cryptography
PRAM	Privacy Risk Assessment Methodology
PRFs	Pseudorandom Functions
PRNGs	Pseudorandom Number Generators
ProSe	Proximity Services
PSCR	Public Safety Communications Research
PSS	Probabilistic Signature Scheme
PTP	Precision Time Protocol
PWG	Public Working Group

RAM	Random Access Memory
RAMPS	Regional Alliances and Multi-stakeholder Partnerships to Stimulate
RBAC	Role-Based Access Control
RBG	Random Bit Generator
R&D	Research and Development
RDS	Reference Data Set
RFI	Request for Information
RISC	Reduced Instruction Set Computing
RMF	Risk Management Framework
RNG	Random Number Generation
ROLIE	Resource-Oriented Lightweight Information Exchange
RPKI	Resource Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
SAC	Selected Areas in Cryptography
SACM	Security Automation and Continuous Monitoring
SAMATE	Software Assurance Metrics and Tool Evaluation
SARD	Static Analysis Reference Dataset
SATE	Static Analysis Tool Exposition
SBA	Small Business Administration
SBIR	Small Business Innovation Research
SC	Subcommittee
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCAPVal	SCAP Content Validation Tool
SCORE	Special Cyber Operations Research and Engineering
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SDN	Software Defined Networking
SDO	Standards Developing Organizations
SES	Senior Executive Service
SGCC	Smart Grid Cybersecurity Committee
SGIP	Smart Grid Interoperability Panel
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIG	Special Interest Group
SLA	Service Level Agreement
SMB	Small and Medium-size Business
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Services Oriented Architecture
SODG	System Object Dependency Graph
SP	Special Publications
SPF	Sender Policy Framework
SRTP	Secure Real-time Transport Protocol
SSCA	Software and Supply Chain Assurance
SSD	Software and Systems Division
SSH	Secure Shell
SSLF	Specialized Security-Limited Functionality
SSO	Single Sign-on
SSR	Security Standardization Research
STEM	Science, Technology, Engineering, and Mathematics
STIG	Security Technical Implementation Guide
STONESOUP	Securely Taking on Software of Uncertain Provenance
STVMG	Security Testing, Validation, and Measurement Group
SURF	Summer Undergraduate Research Fellowship
SWID	Software Identification
TCG	Trusted Computing Group
TDEA	Triple Data Encryption Algorithm
TDES	Triple Data Encryption Standard
TESLA	Timed Efficient Stream Loss-tolerant Authentication
TGDC	Technical Guidelines Development Committee

TIG	Trusted Identities Group
TLS	Transport Layer Security
TMSAD	Trust Model for Security Automation Data
TNC	Trusted Network Communications
TPM	Trusted Platform Module
TSF	Trustworthy Supplier Framework
TTPs	Tactics, Techniques, and Procedures
U.S.C.	U.S. Code
US-CERT	U.S. Computer Emergency Readiness Team
USG	U.S. Government
USGCB	United States Government Configuration Baseline
UTC	Coordinated Universal Time
VDO	Vulnerability Description Ontology
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VRDX-SIG	Vulnerability Reporting and Data eXchange SIG
VVSG	Voluntary Voting System Guidelines
WG	Working Group
XACML	eXtensible Access Control Markup Language
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language
XOFs	Extendable-Output Functions
XPN	eXtended Packet Number
XTS	XEX Tweakable Block Cipher with Ciphertext Stealing

APPENDIX B: NIST CYBERSECURITY EVENTS HELD DURING FY 2016

Below is a compiled list of all the NIST cybersecurity events that were hosted and/or sponsored by NIST's ITL cybersecurity program. The list has been arranged in chronological order from most recent (September 30, 2016, the end of the fiscal year for Federal Government) to the beginning of FY 2016 (October 1, 2015).

SEPTEMBER 2016:

NSCI: High-Performance Computing Security Workshop
September 29-30
NIST Gaithersburg, MD.

Open Meeting of The Commission on Enhancing National Cybersecurity
September 19
America University of Washington College of Law
Washington D.C.

NIST Cloud Computing Forum & Workshop IX
September 13-15
NIST Gaithersburg, MD.

Privacy Controls Workshop: Next Steps for NIST Special Publication 800-53, Appendix J
September 8
Department of Transportation Washington, D.C.

AUGUST 2016:

Exploring the Dimensions of Trustworthiness: Challenges and Opportunities
August 30-31
NIST Gaithersburg, MD.

Open Meeting of the Commission on Enhancing National Cybersecurity
August 23
University of Minnesota

JULY 2016:

Open Meeting of the Commission on Enhancing National Cybersecurity
July 14
Hilton University of Houston

The Software and Supply Chain Assurance (SSCA) Summer 2016 Working Group Sessions
Co-sponsor
July 13-15
McLean, VA

Workshop on Software Measures and Metrics to Reduce Security Vulnerabilities
July 12
NIST, Gaithersburg, MD

JUNE 2016:

Open Meeting of the Commission on Enhancing National Cybersecurity
June 21
University of California, Berkeley in the Chevron Auditorium at the International House

Information Security Privacy Advisory Board (ISPAB) Meeting
June 15-17
Washington D.C.

National Cyber Summit
NIST National Initiative for Cybersecurity Education (NICE) was a co-sponsor
June 7-9
Huntsville, Alabama

MAY 2016:

Trustworthy Suppliers Framework Forum
May 25
NIST, Gaithersburg, MD

Open Meeting of the Commission on Enhancing National Cybersecurity
May 16
Vanderbilt Hall, New York University (NYU) School of Law, Center on Law and Security

Random Bit Generation Workshop 2016
May 2-3
NIST, Gaithersburg, MD

APRIL 2016:

Software Identification (SWID) Tag Implementation and Use Workshop
April 26-27
National Cybersecurity Center of Excellence (NCCoE)

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

Webinar: 2016-NIST-NSTIC-02 National Strategy for Trusted Identities in Cyberspace (NSTIC) Federated Identity in Healthcare Pilot Program
April 18
Webinar hosted by NIST's TIG

1st Commission on Enhancing National Cybersecurity Meeting
April 14
Department of Commerce

Cybersecurity Framework Workshop 2016
April 6-7
NIST Gaithersburg, MD.

Pre-Workshop: Maritime and Oil & Natural Gas Open Session
April 5
Hosted by the National Cybersecurity Center of Excellence (NCCoE) with the Cybersecurity Framework Workshop
NIST Gaithersburg, MD.

MARCH 2016:

Software and Supply Chain Assurance Forums
Co-sponsor
March 8-10
McLean, Virginia

Information Security Privacy Advisory Board (ISPAB) Meeting
March 23-25
Washington D.C.

Workshop - Protecting Consumer Data: Securing Payment and Transaction Information
NIST's National Cybersecurity Center of Excellence (NCCoE)
March 22
University of Alabama, Birmingham

29th Annual FISSEA Conference: "The Quest for the Un-hackable Human: The Power of Cybersecurity Awareness and Training"
M arch 15-16
NIST Gaithersburg, MD.

FEBRUARY 2016:

Trustworthy Suppliers Framework Forum
(***Postponed due to inclement weather – rescheduled in May 2016***)
February 16

National Cybersecurity Center of Excellence Building Dedication Event
February 8
at the NIST National Cybersecurity Center of Excellence (NCCoE)

JANUARY 2016:

Strengthening Cybersecurity in the Financial Sector with the new NIST Practice Guide
January 14
Webinar – NIST's National Cybersecurity Center of Excellence (NCCoE)

NIST Advanced Identity Workshop: Applying Measurement Science in the Identity Ecosystem
January 12-13
NIST

DECEMBER 2015:

Software and Supply Chain Assurance Forums
Co-sponsor
December 2-4
McLean, Virginia

NOVEMBER 2015:

Cybersecurity in Retail: Trends and Challenges with Point of Sale and Payment Technologies
November 19
The Universities at Shady Grove (USG)
Rockville, MD

NICE Conference and Expo 2015
November 3-4
San Diego, CA

OCTOBER 2015:

National K-12 Cybersecurity Conference
October 1-2, 2015
Linthicum, MD

Information Security and Privacy Advisory Board (ISPAB)
October 21-23
Washington D.C.

Best Practices in Cyber Supply Chain Risk Management
October 1-2
NIST Gaithersburg, MD.

APPENDIX C: OPPORTUNITIES TO ENGAGE WITH ITL CYBERSECURITY PROGRAM AND NIST DURING FY 2017-2018

Guest Research Internships at NIST

Opportunities are available at NIST for 6- to 24-month internships within the Computer Security Division (CSD) and the Applied Cybersecurity Division (ACD). Qualified individuals should contact CSD and/or ACD, 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, see below for contacts.

Details at NIST for Government or Military Personnel

Opportunities are available at NIST for 6- to 24-month details at NIST in CSD and/or ACD. Qualified individuals should contact CSD and/or ACD, provide a statement of qualifications, and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring agency; however, in some cases, agency salary costs may be reimbursed by NIST. For further information, see below for contacts.

Security Research

NIST occasionally undertakes security work, primarily in 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, see below for contacts:

CONTACTS:

CSD Contact:
Mr. Matthew Scholl
(301) 975-2941
matthew.scholl@nist.gov

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

ANTD Contact:
Dr. Abdella Battou
(301) 975-5247
abdella.battou@nist.gov

IAD Contact:
Dr. Shahram Orandi
(301) 975-3261
shahram.orandi@nist.gov

SSD Contact:
Dr. Ram Sriram
(301) 975-3507
ram.sriram@nist.gov

Federal Computer Security Managers' (FCSM) Forum

The FCSM Forum is covered in detail in the Outreach section of this report. Membership is free and open to federal employees. For further information, contact:

Team Email Address: sec-forum@nist.gov

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

Ms. Jody Jacobs
(301) 975-4728
jody.jacobs@nist.gov

Visit the FCSM Forum website:
http://csrc.nist.gov/groups/SMA/forum/membership.html

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. NIST also offers other grants to encourage work in specific fields: precision measurement, fire research, and materials science. Grants/awards supporting research by 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